# INFOSEC
# YEAR IN REVIEW
# 2003

## as of 2004-10-31

**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**

# 01 Introduction

*Category 01* *Introduction*

2004-06-15 **Introduction**

M. E. Kabay, PhD, CISSP

WELCOME

Welcome to the 2004 edition of the Information Security Year in Review (IYIR) project.

In 1993 and 1994, I was an adjunct professor in the Institute for Government Informatics Professionals in Ottawa, Canada under the aegis of the University of Ottawa. I taught a one-semester course introducting information security to government personnel and enjoyed the experience immensely. Many of the chapters of my 1996 textbook, _The NCSA Guide to Enterprise Security_ published by McGraw-Hill were field-tested by my students.

In 1995, I was asked if I could run a seminar for graduates of my courses to bring them up to date on developments across the entire field of information security. Our course had twenty students and I so enjoyed it that I continued to develop the material and teach the course with the NCSA (National Computer Security Association; later called ICSA and then eventually renamed TruSecure Corporation, its current name) all over the United States, Canada, Europe, Asia and the Caribbean.

After a few years of working on this project, it became obvious that saving abstracts in a WordPerfect file was not going to cut it as an orderly method for organizing the increasing mass of information that I was encountering in my research. I developed a simple database in 1997 and have continued to refine it ever since then. The database allows me to store information in an orderly way and -- most important -- to _find_ the information quickly. For that purpose, I put in as many keywords as I can think of quickly; I also classify each topic using a taxonomy that has grown in complexity and coverage over the years (more about the taxonomy in the next section).

In 2004, I was privileged to begin working with Norwich students Karthik Raman (project leader), Krenar Komoni and Irfan Sehic as my research assistants. These excellent students have provided invaluable assistance in transferring data from NewsScan, NIPC/DHS reports and other sources into the database and have also done the first cut of classification and keyword generation. They have enormously improved the coverage of the field and are continuing their work with me to expand the database to further sources in the coming year. It is difficult to estimate the hundreds of hours of time they have saved me.

The IYIR reports are posted on my Web site now; see the introductory page at < http://www2.norwich.edu/mkabay/index.htm > and click on the IYIR button for a list of PDF files you can read on screen, search, or print out at will.

# 02 Taxonomy of INFOSEC Issues

*Category 02* *Taxonomy of INFOSEC Issues*

2004-06-15 **Introduction**

TAXONOMY

The taxonomy (classification scheme) of INFOSEC issues has grown over the years since I began the IYIR project. This taxonomy in now way represents a structurally sound classification with unambiguous, non-overlapping, atomic concepts; it is simply an organic development of my wish to present information in an orderly way in my courses and to be able to find examples of specific issues when I need them for teaching or writing.

The taxonomy changes almost every time I use it; the current taxonomy is listed here and is used throughout this edition of the IYIR report as well as in the INFOSEC UPDATE course based on the IYIR.

CATA Codes & Description

0 Unclassified
10 Computer Crimes (cases, indictments, convictions, sentences)
11 Breaches of confidentiality
  11.1 Data leakage
  11.2 Unauthorized disclosure
  11.3 Data theft
  11.4 Covert channels
12 Wiretapping, interception (not jamming; not govt/law enforcement)
12.1 Wiretapping
12.2 Interception
13 Data diddling, data corruption, embezzlement
13.1 Data diddling
13.2 Data corruption & destruction
13.3 Embezzlement
13.4 Obsolescence
14 Viruses, virus-hoaxes, Trojans (assembly level or macro: not ActiveX or Java)
14.1 Viruses
14.2 Worms
14.3 Virus/worms
14.4 Trojans
14.5 Virus hoaxes
15 Fraud (not embezzlement), extortion, slamming
15.1 Fraud
15.2 Extortion
15.3 Slamming
16 INFOWAR, industrial espionage, hacktivism
16.1 Industrial espionage
16.2 Industrial information systems sabotage
16.3 Infrastructure protection
16.4 Military perspectives on INFOWAR
16.5 Hacktivism
16.6 Disinformation, PSYOPS
17 Penetration, phreaking (entering systems, stealing telephone service)
17.1 Penetration
17.2 Web vandalism
17.3 Phreaking
18 Theft & loss of equipment (laptops, ATMs, computers, cables, network components)
18.1 Theft
18.2 Loss
19 Counterfeits, forgery
19.1 Software piracy
19.2 Music
19.3 Movies / TV
19.4 Books / e-books
19.5 Games
19.6 Credit-cards, other tokens
19.7 Legal or business documents
19.8 Plagiarism

19.9 Products (hardware, clothing etc.)
1A Criminal hacker scene
1A1 Conventions and meetings
1A2 Testimony in court or committees
1A3 Biographical notes on individual criminals
1A4 Publications
1A5 Organizations
1A6 Psychology
1B Net-mediated harm / crime
1B1 Adult pornography
1B2 Child pornography
1B3 Pedophilia, kidnapping, Net-adoption fraud
1B4 Stalking
1B5 Gambling
1B6 Auctions
1B7 Hate groups
1B8 Traffic in women, slavery
1B9 Non-virus hoaxes, urban myths
1C Identity, impersonation, spoofing
1C1 Impersonation
1C2 Identity theft
1C3 Pseudonymity
1C4 Anonymity
1C5 Phishing
1D Law Enforcement & Forensics (technology, organizations, proposals, litigation, rulings, judgements)
1D1 Organizations, cooperation
1D2 Technology
1D3 Litigation, legal rulings, judgements
1D4 Government funding
1E Homeland Security
20 Emerging Vulnerabilities & Defenses
21 Quality assurance failures including design flaws
21.1 General QA failures
21.2 Security product QA failures
22 Availability problems
22.1 DoS attacks
22.2 DDoS attacks
22.3 DoS countermeasures
22.4 Accidental availability disruptions
23 Internet tools
23.1 Java
23.2 Javascript
23.3 ActiveX
23.4 HTML, XML
23.5 E-mail & instant messaging or chat
23.6 Web-site infrastructure, browsers
23.7 VoIP
23.8 SMS
24 Operating systems, network operating systems,TCP/IP problems (alerts)
24.1 Windows 9x/Me/XP
24.2 Windows NT/2K
24.3 UNIX flavors
24.4 TCP/IP & HTTP
24.5 LAN OS
24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11
24.7 SWDR (Software-defined radio)
24.8 MAC OS
24.9 Peer-to-peer networking
24.A Secure processors
25 Computer remote control & disruption
25.1 Remote control, RATs, reprogramming, auto-updates
25.2 Jamming
25.3 RFI, HERF, EMP/T
26 Health effects of electronic equipment (phones, screens, etc.)
26.1 Radiation
26.2 Toxic materials
27 Tools

27.1 Vulnerability assessment
27.2 Port scans
27.3 Intrusion detection systems
27.4 Firewalls & other perimeter defenses
27.5 Honeypots
27.6 Honeynets
27.7 Antimalware technology
28 Automated surveillance
28.1 Spyware, Web bugs & cookies
28.2 Scumware
28.3 Keystroke loggers
28.4 Cell/mobile phones / GPS (tracking)
28.5 Serial numbers
28.6 RFID tags
29 Sociology of cyberspace
29.1 Addiction
29.2 Cybersyndromes
29.3 Digital divide
29.4 Online & electronic voting
29.5 Online legal proceedings
29.6 Flash crowds, social links
30 Management & Policy
31 The state of information security
31.1 Surveys, studies, research
31.2 Estimates, guesses, predictions, forecasts
31.3 New technology with security implications
32 Censorship, indecency laws, 1st amendment (law)
32.1 USA
32.2 Non-USA
33 Acceptable-use policies, authorization, access controls, spam & anti-spam (policies, technology, civil law)
33.1 Acceptable use
33.2 Spam
33.3 Antispam
33.4 Authorization, access controls
34 Net filters, monitoring (technologies)
34.1 Net filters
34.2 Usage monitoring, audit trails
35 DNS conflicts, trademark violations (Net, Web)
35.1 Cybersquatting
35.2 Trademarks vs DNS
35.3 Politics of the DNS
36 Responses to intrusion
37 Education in security & ethics
37.1 Grade & middle school
37.2 High school
37.3 Undergraduate degrees
37.4 Master's degrees
37.5 Doctoral degrees
37.6 Industry courses
37.7 Conferences
37.8 Web sites
37.9 White papers
38 Consumer/employee privacy, profiling, trade in personal information
38.1 Consumer profiling
38.2 Trade in personal information
38.3 Industry efforts
38.4 International agreements
38.5 EU legislation & regulation
38.6 US legislation & regulation
38.7 Other legislation & regulation
38.8 Law enforcement
38.9 Surveillance
38.A Medical / HIPAA
40 Cryptography, Law & E-commerce
41 Cryptanalysis techniques & tools
42 Crypto algorithms (weakness, brute-force attacks, implementation flaws)
42.1 Weaknesses

42.2  Brute-force attacks
42.3  Implementation flaws
43  I&A products (tokens, biometrics, passwords, Kerberos)
43.1  Tokens
43.2  Biometrics
43.3  Passwords
43.4  Kerberos
43.5  Single sign-on
44  Encryption algorithms, products (including steganography)
44.1  Crypto algorithms
44.2  Crypto products
44.3  Steganography
45  E-commerce security, digital signature, products, digital cash, e-payments
45.1  PKI (Digital signatures / certificates)
45.2  Digital cash
45.3  Micropayments
45.4  E-payments / e-wallets
45.5  Watermarks / digital-rights management
45.6  Smart cards & other e-commerce security measures
45.7  Sales taxes on Internet commerce
45.8  E-commerce laws
46  Cryptography exports from US; Key escrow
47  US computer-crime laws
48  Foreign cyberlaws (not cases or sentences)
48.1  Non-US cryptography laws
48.2  Non-US computer-crime laws
49  Privacy, government surveillance, legislation, agreements
4A  Evolution of Net law
4A1  Framing
4A2  Pointing, linking, deep linking, metatext
4A3  Jurisdiction
4A4  Blocking
4A5  Archives
4A6  Libel
4A7  Spam
4A8  Liability
4B  Intellectual property: patents, copyrights (law)
4B1  Copyright
4B2  Patents
4B3  Reverse engineering
4B4  EULA (End-user license agreements)
4B5  Trademarks
4C  Security paradigms, risk management, site-security certification, professional certification
4C1  Paradigms, security standards
4C2  Risk management methodology & tools
4C3  Certification of site security, privacy protection
4C4  Professional certification in security, auditing
4C5  Academic/Industry/Vendor/Govt efforts
4D  Funny / miscellaneous

# 03 Sources of Information

*Category 03* *Sources of Information*

2004-06-15 **Introduction**

In the early days, I wrote all the abstracts myself. As the size of the database grew, this practice became a terrible and limiting burden. I was thrilled -- and still am -- to get permission to quote the superb abstracts written by John Gehl and Suzanne Douglas, original editors of EDUPAGE and now of the daily _NewsScan_ and weekly _Innovation_ e-publications. At this point, their work is a major component of the IYIR.

In addition, I have been quoting (with attribution) many of the contributors to Peter G. Neumann's RISKS Forum Digest.

Lately, the Daily Report from NIPC (National Infrastructure Protection Center) (now the DHS daily report) have proven valuable in supplementing the material at hand.

Bruce Schneier, famed cryptographer and a valued commentator on all matters of security, has kindly allowed me to include excerpts from his monthly columns in his Crypto-Gram newsletter.

I also naturally continue to write my own abstracts of interesting articles when necessary.

For a list of news sources that cover information security news, see < http://www2.norwich.edu/mkabay/overviews/infosec_ed.pdf >.

For more information about NewsScan and Innovation, see < http://www.newsscan.com >.

For more information about RISKS Forum Digest, see the archives at <http://catless.ncl.ac.uk/Risks/ > for HTML versions or at < http://the.wiretapped.net/security/textfiles/risks-digest/ > for text versions.

Dr Neumann asks that reprints from RISKS include the following note and the following should be considered as a blanket notification for all verbatim republication of RISKS materials throughout this database:

* * *
From the
FORUM ON RISKS TO THE PUBLIC IN COMPUTERS AND RELATED SYSTEMS (comp.risks)
ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator
See < http://www.csl.sri.com/users/risko/risksinfo.html > for full information.
Reused without explicit authorization under blanket permission granted for all Risks-Forum Digest materials. The author(s), the RISKS moderator, and the ACM have no connection with this reuse.
* * *

Information Security Magazine is at < http://www.infosecmag.com > and subscriptions to the Security Wire Digest are available through < http://infosecuritymag.bellevue.com >.

The NIPC Daily Report is available through < http://www.nipc.gov/ >.

For free subscriptions to Bruce Schneier's Crypto-Gram, see < http://www.counterpane.com/crypto-gram.html >.

# 04 Copyright

*Category 04* *Copyright*

2004-06-15 **Introduction**

As you can see at the bottom of every page of the IYIR report and the INFOSEC UPDATE, I assert copyright over this presentation of the information I have collected. This is called a _compilation copyright_ and in no way derogates the copyrights of all original copyright holders. My contribution is primarily the organization and presentation of this information. I do hold the copyright on my own abstracts and on the keywords.

# 05 Using IYIR

*Category 05 Using IYIR*

2004-06-15 **Introduction**

Anyone who wants to refer to these IYIR and INFOSEC UPDATE documents is completely welcome to do so freely _provided_ that no one tries to make other people pay for the materials. You are welcome to reprint the documents provided that each page you choose to print is in the original format (that's why I use Acrobat PDF files to distribute the information). Just remember, if I ever find out that someone has charged somebody for what I freely give away I am going to be really, really mad!

You may, of course, use the original documents as you and the copyright owners agree.

As for posting these files on your own Web sites, DON'T! I update the files constantly and absolutely do not want to have to hunt down old copies of the work and replace them with newer versions. So you're welcome to link to the files, but please do not copy them to any other Web sites.

# 06 The INFOSEC UPDATE Course

*Category 06* *The INFOSEC UPDATE Course*

2004-06-15 **Introduction**

The INFOSEC UPDATE course is a two-day workshop that brings participants up to date on topics across the entire field of information security. The four half-day sessions cover the following broad areas:

Day 1:
AM: Computer Crime Update
PM: Emerging Vulnerabilities

Day 2:
AM: Management , Corporate Policy
PM: Cryptography, Law, Public Policy

For full details, see section 2 on Taxonomy.

I used to prepare slides based on the abstracts so that the students would have a workbook consisting of keywords in the slide and the details at the bottom of the page. However, this approach became unmanageable by the time I reached workbook lengths of 475 pages. It was simply too much effort for relatively minor benefits. I have therefore tried a different, much simpler approach over the last few years. I mark selected topics in my database and created the workbook from a report file. The whole thing takes me a few minutes and allows me to keep the workbook absolutely up to date. I hope that course participants will find it a useful resource and an acceptable format for the course.

# 07 Acknowledgements

*Category 07* *Acknowledgements*

2004-06-15 **Introduction**

ACKNOWLEDGEMENTS

I would like to acknowledge the encouragement and support of many colleagues who have contributed to this project over the years. In particular, John Gehl and Suzanne Douglas, original editors of EDUPAGE and now of NEWSSCAN and INNOVATION, stand out for their kindness in so generously allowing me to quote them verbatim in so many hundreds of stories. Thanks guys -- I simply could not do this without your help.

My colleagues at TruSecure Corporation were always supportive and encouraging; I thank my favorite curmudgeon, David Kennedy, Director of Resarch for TruSecure, for many years of continuing friendship.

I also want to thank my colleagues Phil Susmann and COL Tom Aldrich at Norwich University for their encouragement and support and the opportunity to teach the two-day INFOSEC Update every year at the annual e-ProtectIT Conference ( http://www.e-protectIT.org ).

My sincere thanks to my research assistants, Karthik Raman, Krenar Komoni and Irfan Sehic.

And finally, as always, I thank my wife, Deborah Black, light of my life, for all her infinitely varied support over many years and in all ways.

# 08 About the Editor

*Category 08* *About the Editor*

2004-06-15 **Introduction**

Here's a little information about me. For exhaustive, not to say exhausting, details, you can visit my Web site at < http://www2.norwich.edu/mkabay > and click on my CV link.

M. Kabay ( mailto:mkabay@norwich.edu ) began programming in assembler at age 15 in 1965. In 1976, he received his PhD from Dartmouth College in applied statistics and invertebrate zoology. In 1979, he joined a compiler team for a new 4GL and RDBMS in the U.S. and then joined Hewlett-Packard Canada in 1980, winning the Systems Engineer of the Year Award in 1982. He has published over 850 technical papers in operations management and security, has published a 1996 textbook on security, and was Technical Editor of the 4th Edition of the _Computer Security Handbook_ (Wiley, 2002) and is working on the 5th edition. He has lectured on security and information warfare at the US Army War College, NATO HQ, NATO Counterintelligence, and in the UK, France, Germany, Japan and China. He returned to academia in July 2001 and is now Associate Professor of Information Assurance in the Division of Business & Management at Norwich University, Northfield, VT 05663-1035 USA where he is also the Director of the Master's Program in Information Assurance (http://www3.norwich.edu/msia ) and of the Bachelor's program in IA (http://www2.norwich.edu/mkabay/bsia).

V: 802-479-7937
E: mkabay@norwich.edu
W: http://www2.norwich.edu/mkabay

# 11.1 Data leakage

*Category 11.1* *Data leakage*

2003-01-16 **data leakage remanence**

NewsScan

JUNKED HARD DRIVES YIELD LOTS OF PERSONAL DATA
MIT graduate students Simson Garfinkel and Abhi Shelat bought 158 hard drives at second hand computer stores and eBay over a two-year period, and found that more than half of those that were functional contained recoverable files, most of which contained "significant personal information." The data included medical correspondence, love letters, pornography and 5,000 credit card numbers. The investigation calls into question PC users' assumptions when they donate or junk old computers — 51 of the 129 working drives had been reformatted, and 19 of those still contained recoverable data. The only surefire way to erase a hard drive is to "squeeze" it — writing over the old information with new data, preferably several times — but few people go to the trouble. The findings of the study will be published in the IEEE Security & Privacy journal Friday. (AP 16 Jan 2003)
http://apnews.excite.com/article/20030116/D7OJBBBG0.htm

*Category 11.1* *Data leakage*

2003-02-10 **discarded computer disk data leakage confidential information medical**

NewsScan

SURPLUS COMPUTER IN KENTUCKY HELD 'DELETED' AIDS FILES
A state auditor found that at least one computer used by staffers counseling clients with AIDS or HIV was ready to be offered for sale to the public even though it still contained files of thousands of people. Auditor Ed Hatchett said: "This is significant data. It's a lot of information lots of names and things like sexual partners of those who are diagnosed with AIDS. It's a terrible security breach." Health Services Secretary Marcia Morgan, who has ordered an internal investigation of that breach, says the files were thought to have been deleted last year. (AP/USA Today 7 Feb 2003)

*Category 11.1* *Data leakage*

2003-04-17 **CNN obituraries famous people blunder**

NewsScan

CNN GLITCH REVEALS PREMATURE OBITS
A glitch on the CNN.com Web site accidentally made available draft obituaries written in advance for Dick Cheney, Ronald Reagan, Fidel Castro, Pope John Paul II and Nelson Mandela. "The design mockups were on a development site intended for internal review only," says a CNN spokeswoman. "The development site was temporarily publicly available because of human error." The pages were yanked about 20 minutes after being exposed. (CNet News.com 17 Apr 2003)

*Category 11.1* *Data leakage*

2003-05-29 **hacker vulnerability Cingular Adrian Lamo website line LLC random finding Sacremento California dumpster customer records exploit**

NIPC/DHS

May 29, Wired — Hacker exposes vulnerability in Cingular claims site. Hacker Adrian Lamo found a security hole in a website run by lock\line LLC, which provides claim management services to Cingular customers. Lamo discovered the problem last weekend through a random finding in a Sacramento, CA dumpster, where a Cingular store had discarded records about a customer's insurance claim for a lost phone. By simply typing in a URL listed on the detritus, Lamo was taken to the customer's claim page on the lock\line website. Lamo was able to access individual claims pages containing customer's name, address and phone number, along with details on the insurance claim being made. Altering the claim ID numbers in the URL gave Lamo access to some 2.5 million Cingular customer claims dating back to 1998. Lamo said he had no intent of profiting from the exploit, just pointing out a security flaw. Cingular and lock\line closed the hole by Wednesday morning.

*Category 11.1* *Data leakage*

2003-06-16 **CERT Linux PDF flaw hacker tips confidential vulnerability hack4life Unix Jeffrey Carpenter**

NIPC/DHS

June 16, IDG News Service — Hacker tips CERT's hand on Linux/PDF flaw. Confidential vulnerability information managed by the CERT Coordination Center has again been leaked to the public. The latest report was posted to a vulnerability discussion list by an individual using the name "hack4life." The latest information concerns a flaw in Adobe Systems Inc.'s PDF (Portable Document Format) readers for Unix and could allow a remote attacker to trick users into executing malicious code on their machines, according to a copy of the leaked vulnerability report. The leaked information was taken from communication sent from CERT to software vendors affected by the PDF problem, according to Jeffrey Carpenter, manager of the CERT Coordination Center. The information appears to be from a vulnerability report submitted to CERT by a Cincinnati security researcher by the name of Martyn Gilmore. Adobe's Acrobat Reader 5.06 and the open-source reader Xpdf 1.01 are affected by the problem, according to the report.

*Category 11.1* *Data leakage*

2003-06-30 **PetCo security hole storefront 500000 credit card numbers open Jeremiah Jacks computer SQL security**

NIPC/DHS

June 30, SecurityFocus — PetCo plugs security hole. Pet supply retailer PetCo.com plugged a hole in its online storefront over the weekend that left as many as 500,000 credit card numbers open to anyone able to construct a specially-crafted URL. Twenty-year old programmer Jeremiah Jacks discovered the hole. He used Google to find active server pages on PetCo.com that accepted customer input and then tried inputting SQL database queries into them. "It took me less than a minute to find a page that was vulnerable," says Jacks. The company issued a statement Sunday saying it had hired a computer security consultant to assist in an audit of the site.

*Category 11.1* *Data leakage*

2003-09-15 **data leakage remanence used equipment confidentiality personal financial consumer customer information auction**

http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_PrintFriendly&c=Article&cid=1063577414565&call_pageid=968332188492

Two Bank of Montreal computers containing hundreds, potentially thousands, of sensitive customer files narrowly escaped being sold on eBay.com late last week, calling into question the process by which financial institutions dispose of old computer equipment.

Information in one of the computers included the names, addresses and phone numbers of several hundred bank clients, along with their bank account information, including account type and number, balances and, in some cases, balances on GICs, RRSPs, lines of credit, credit cards and insurance.

Many of the files were dated as recently as late 2002, while some went back to 2000. The computers appeared to originate from the bank's head office on St. Jacques St. in Montreal, but customers, many of them also bank employees, had addresses ranging from Victoria, B.C., to St. John's, Nfld.

# 11.4 Covert channels

*Category 11.4* *Covert channels*

2003-11-14 **meta data dodgy-dosier syndrome Workshare hidden history histories information**

NewsScan

DODGING THE 'DODGY-DOSSIER SYNDROME' PROBLEM
Ninety percent of business documents are adapted from other documents, but 68% of the people doing the adapting don't know that the revised versions often contain metadata that identify the source documents, according to a study by UK software firm Workshare. The phenomenon has been dubbed "the dodgy-dossier syndrome" after the infamous UK government report on Iraq's alleged weapons of mass destruction program, a significant portion of which was found to have been copied from a 12-year-old thesis written by a PhD candidate. "There are inherent dangers due to document metadata, which identifies the historical changes within a document, author histories and document origins," says Workshare in its report. "Awareness of the term 'metadata' is low and fewer still know of its dangers." Exacerbating the problem of document adaptation is "document anarchy" — which describes the lack of standard practice in the workplace for contributing to or giving feedback on a document. "More business users are contributing to shared documents than ever before," says Workshare European VP Andrew Pearson, "and companies are losing control of what happens inside the process. Changes in the way organizations work have made this problem more acute in recent years with restructuring and flattening of the organization (bringing) these problems to the fore." (ZDNet UK 14 Nov 2003)

# 14.1 Viruses

*Category 14.1 Viruses*

2003-02-19 **spoof e-mail virus Pentagon Defense Technology Information Center DTIC thwarted**

NIPC/DHS

February 18, Federal Computer Week — Pentagon thwarts spoofed e-mail. The Pentagon said today that an attempt to send a virus through its systems last week was thwarted before damage could be caused. On the morning of February 14, someone "spoofed" the Defense Technology Information Center (DTIC) header, camouflaging the sender's real address to make recipients think the message had come from the Defense Department. The message had a virus attached and was sent through Pentagon computers to two mailing lists. "Our computers caught the virus and stripped it out," said Terry Davis, manager of the Public Web Program in the Office of the Secretary of Defense. "So what went out was the original text message that was sent in the e-mail, but the virus and the attachment were both stripped." Davis said he and a few co-workers then went into the system to put safeguards in place to prevent someone else from spoofing a DTIC header.

*Category 14.1 Viruses*

2003-04-30 **anti virus monthly subscription AOL America Online McAfee**

NewsScan

AOL TO OFFER ANTIVIRUS PROTECTION FOR MONTHLY FEE
AOL has begun offering its subscribers a $2.95-a-month antivirus service that will automatically update a customer's computer as new viruses occur. Jupiter research analyst Michael Gartenberg explains, "It takes antivirus stuff from a more technology-aware audience to a more novice audience." The new AOL service uses McAfee antivirus software and will be seamlessly integrated into the AOL customer experience. (USA Today 30 Apr 2003)

*Category 14.1 Viruses*

2003-05-06 **mobile virus PDA smartphone backdoor Rob Bamforth Bloor Research problems exploit**

NIPC/DHS

May 06, vnunet — The danger of mobile viruses. PDAs and smartphones create backdoors into corporate infrastructures that can be exploited by viruses and malicious code to spread infections. Rob Bamforth of Bloor Research, a British IT analyst company, said that one of the principal security problems with mobile devices is that they are typically brought into organizations by individuals who have purchased them independently, rather than being issued as part of a co-ordinated IT department rollout. This makes them very difficult to control and manage when they are connected to corporate networks. Bamforth added that, while viruses currently present little danger to the actual mobile handsets themselves, the greatest problem comes from the devices being used as a transmission medium through which viruses could infect company infrastructures.

*Category 14.1 Viruses*

2003-08-02 **DHS W32*Mimail virus attachment message.zip malicious code mass mailer MS03-014 microsoft outlook express**

NIPC/DHS

August 02, U.S. Department of Homeland Security — Department of Homeland Security Advisory "W32/Mimail Virus". First reported on on Friday, August 1, the W32/Mimail virus is a malicious file attachment containing a specially crafted HTML file named 'message.html'. This file is delivered inside of a .ZIP archive file named 'message.zip'. Viewing the 'message.html' file on a vulnerable system will cause the malicious code, which is a mass-mailer, to be installed and executed. The vulnerability, which was identified in April 2003 and described in Microsoft Security Bulletin MS03-014, makes it possible for W32/Mimail to execute automatically once the .ZIP archive is opened. DHS/IAIP encourages sites to review Microsoft Security Bulletin MS03-014 and apply the Cumulative Patch for Outlook Express available on the Microsoft Website: http://www.microsoft.com/technet/treeview/default.asp?url=/t echnet/security/bulletin/MS03-014.asp.

*Category 14.1 Viruses*

2003-08-12 **Virus Maryland Motor Vehicle Administration MVA Cheron Wicker**

NIPC/DHS

August 12, — Virus forces Maryland Motor Vehicles Administration to close. A computer virus forced the Maryland Motor Vehicle Administration to shut all of its offices at noon Tuesday, August 12. The department expected to reopen its offices Wednesday, officials said. "We have closed all of our offices and facilities statewide. So there's no telephone service right now. There's no online service right now. There's no kiosk or express office service," MVA spokeswoman Cheron Wicker said. Drivers who had business with Tuesday deadlines at the MVA were told not to worry. People who needed to renew registrations were told to wait for Wednesday. Wicker said it was too early to tell what damage may have been done.

*Category 14.1 Viruses*

2003-08-19 **Navy Marine Corps Intranet down virus NMCI e-mail secure network**

NIPC/DHS

August 19, Federal Computer Week — Navy Marine Corps Intranet goes down. A virus took the Navy Marine Corps Intranet (NMCI) off-line Tuesday, August 19. A phone recording on the NMCI Strike Force hotline stated: "We are currently experiencing connectivity issues enterprise wide to include e-mail, Web and shared drive access due to a virus." NMCI is an enterprisewide network designed to connect everyone in the Navy and Marine Corps on a single, secure network. Since users started being moved to the system in 2001, almost 97,000 seats have been shifted from legacy systems.

*Category 14.1 Viruses*

2003-08-20 **Sobig virus e-mail systems MessageLabs Inc. hacker bacdoor trojan horse**

NIPC/DHS

August 20, Dow Jones Newswire — Sobig virus spread is fastest ever. The "Sobig.F" computer virus that began attacking e-mail systems globally Tuesday, August 19, has been declared the fastest-spreading e-mail virus of all time. E-mail filtering company MessageLabs Inc. said it intercepted more than one million copies of Sobig.F Tuesday, the most ever in a single day. The interception rate was one in every 17 e-mail messages the firm scanned. Sobig.F continued to spread aggressively Wednesday. Sobig.F, which is the sixth and latest strain of a virus that first emerged in January, spreads through Windows personal computers via e-mail and network file-share systems. Besides clogging e-mail systems full of messages with subjects like "Re: Details" and "Re: Wicked screensaver," the virus also deposits a Trojan horse, or hacker back door, that can be used to turn victims' PCs into spam machines. The worm is programmed to stop spreading on September 10.

*Category 14.1 Viruses*

2003-09-17 **windows flaw Blaster exploit Ken Dunham Trojan horses MSBlast worm unpatched computers root access underground source code**

NIPC/DHS

September 17, CNET News.com — Flaws set to spawn another Blaster. Tools exploiting a new Windows flaw have started to appear, prompting warnings of imminent virus attacks. Ken Dunham, an analyst at a private security firm, said on Tuesday, September 16, that it is "highly likely" that new worms or Trojan horses will emerge in the next few days. These bugs are expected to prey on computers that have not been updated with the latest security patch for Microsoft's operating system. "A new Blaster-like worm family could be created in a matter of hours or days, now that exploit source code has been posted in the underground," Dunham wrote in an email. "The new attack tool makes it trivial for any malicious actor to gain unauthorized root access to an unpatched computer." Experts advised people last week that a new virus was reasonably likely, given the fact that the recently discovered Windows vulnerabilities are similar to those that paved the way for the MSBlast worm.

# 14.2 Worms

*Category 14.2* *Worms*

2003-01-10 **virus alert Internet anti-virus undetected mass mailing F-Secure**

NIPC/DHS

January 09, eSecurity Planet — Virus Alert: W32.Lirva.A and ExploreZip. Two major viruses have struck the Internet at the same time. ExploreZip, an Internet worm first let loose in the wild back in 1999, has reemerged with just enough changes made to allow it to slip through anti-virus software undetected. And it has the added ability to override files on the infected computer, as well as on any other computer in the same network. Once ExploreZip infects a computer, it will automatically respond to any email received with a seemingly valid subject line and the user's name, along with an infected attachment. Another problematic virus is the mass-mailing worm that pays tribute to Canadian singer Avril Lavigne. The worm is going under a few different names, including Avril and Lirva (which is Avril spelled backwards). Although this virus is less destructive than ExploreZip, anti-virus software company F-Secure Corp. has rated both viruses as Level 2 Threats, the second-highest threat category. The Lirva worm got a Level 2 rating because of the speed with which it's spreading around the world. It reportedly originated, in middle Europe and has spread to Turkey, the United States and Southeast Asia in less than 48 hours. Once Lirva infects a computer, it opens the computer's Internet Explorer browser to official Avril Lavigne Web site on the 7th, 11th and 24th of the month. It then starts to display colored circles on

*Category 14.2* *Worms*

2003-01-14 **virus Internet alert SMTP engine self-propagating**

NIPC/DHS

January 13, ZDNet — Virus alert: W32/Sobig-A. Anti-virus experts are warning of a new virus, code-named W32/Sobig-A, which was discovered late last week and spread rapidly over the weekend. Sobig is a mass-mailing worm incorporating its own SMTP engine, according to antivirus companies. It arrives from the e-mail address "big@boss.com" and bears a subject line such as "Re: here is that sample", "Re: Movies", "Re: Document" or "Re: Sample". The e-mail contains an attachment called "Document003.pif", "Sample.pif", "Untitled1.pif" or "Movie_0074.pif". It affects the Windows 95, 98, Me, NT, 2000 and XP platforms. When the attachment is clicked on, it runs a program that searches for files containing e-mail addresses and uses these to send infected e-mails. It also connects to a Web site and downloads a text file containing another Web address, from which it attempts to download and run another program. MessageLabs speculated that this program was a backdoor trojan horse, which could allow a hacker to take control of the user's PC. If there is a local-area network connection, Sobig attempts to copy itself onto shared network folders. CERT/CC has received over one hundred reports of this worm. Anti-virus software companies Sophos, Symantec and McAfee have published instructions on their websites for blocking and removing the worm.

*Category 14.2* *Worms*

2003-01-27 **worm damage Internet servers patches**

NewsScan

INTERNET WORM TOOK ONLY 10 MINUTES TO CAUSE GLOBAL HAVOC
The "SQL Slammer" worm that slowed Internet traffic significantly [in late January 2003] managed to infect computer servers worldwide in about 10 minutes, making it the fastest such virus seen, according to a University of California at San Diego team. "At its peak, achieved approximately three minutes after it was released, the worm scanned 55 million Internet hosts per second. It infect ed at least 750,000 victims, and probably considerably more," says one team member. The SQL Slammer worm was only the third of its type seen on the Net, and managed to spread nearly 100 times faster than the Code Red infection 18 months ago. (The Independent 4 Feb 2003)

THE WORM TURNED BACK: SLAMMER DAMAGE CONTAINED
[By the 27th of January, it was] unlikely that there [would] be much additional destruction from the so-called Slammer computer worm that wreaked damage on the Internet over the weekend, by infecting more than a quarter of a million computer servers and clogging networks throughout the world. The worm targeted a known [vulnerability] in Microsoft's 2000 SQL server database server; the company had issued software security patches in July but many network administrators had failed to install them. But now the worst appears to be over, says an executive at the security firm Symantec. (USA Today 27 Jan 2003)

MICROSOFT, HEAL THYSELF!
Microsoft has been embarrassed by having to acknowledge that the SQL Slammer virus, which infected computer servers all over the world, also contaminated some of Microsoft's own servers, because system administrators had failed to heed the company's own advice to install a software patch months ago to fix a known system vulnerability. A Microsoft executive had to admit: "We, like the rest of the industry, struggle to get 100% compliance with our patch management. We recognize — now more than ever — that this is something we need to work on. And, like the rest of the industry, we're working to fix it." (New York Times 28 Jan 2003)

---

*Category 14.2* *Worms*

2003-02-03 **Slammer worm avoidable vulnerability detection tool available NSA NIPC FBI SANS**

NIPC/DHS

January 31, Computerworld — Free benchmark could have found Slammer vulnerability. Industry experts and users said the Slammer worm should have been a non-issue for companies because the patches and a free tool capable of detecting the vulnerability exploited by the worm were available six months ago. In particular, they point to the issuance in July of the Consensus Minimum Security Benchmarks, also known as the Gold Standard. Developed jointly by five federal agencies, including the National Security Agency (NSA) and the FBI's National Infrastructure Protection Center, as well as the SANS Institute and the Center for Internet Security (CIS), the Gold Standard benchmark can be used to test Windows 2000 Professional systems running as workstations for proper configuration. Alan Paller, director of research at SANS, said an NSA study of the benchmark concluded that by running it on a network a company could eliminate more than 90% of known vulnerabilities. Claude Bailey, an IT security analyst at one of the nation's largest financial management firms, said that while the Gold Standard is a good starting point, his security administrators say the problem isn't in detecting the vulnerability but in deploying the patches and fixes across an organization of 50,000 employees — and guaranteeing that the patch won't cause more problems. "We tested the original patch [for the SQL vulnerability], and it had problems," said Bailey. Now, with the financial firm in the middle of tax season, there's too much to lose to deploy patches that break other parts of the network.

---

*Category 14.2* *Worms*

2003-02-05 **study Slammer worm fastest ever SQL Server Microsoft vulnerability**

NIPC/DHS

February 03, IDG News Service — Study: Slammer was fastest-spreading worm yet. A just-completed study into the Slammer worm, which hit the Internet a week ago, has concluded that Slammer was the fastest-spreading worm yet seen. The study was conducted by a group of experts representing the Cooperative Association for Internet Data Analysis (CAIDA); the International Computer Science Institute; security company Silicon Defense; the University of California, Berkeley's electrical engineering and computer sciences department; and the University of California, San Diego's computer science and engineering department. Slammer's spread was fast for several reasons. At just 376 bytes in size, the worm and required headers fit inside a 404-byte Universal Datagram Protocol packet. Code Red, which hit in mid-2001, was 4KB in size. The worm also worked differently from Code Red. Slammer generated random IP addresses and dispatched itself to those addresses without scanning to find out whether the target machine was running either of the two pieces of software that were vulnerable to attack: Microsoft Corp.'s SQL Server 2000 database and MSDE 2000 (Microsoft SQL Server 2000 Data Engine). Because of its random nature, given enough time, the worm would hit all vulnerable machines. Spread of the worm eventually began to slow because bandwidth from infected machines to the Internet couldn't support the exponential growth in IP packets being generated. Its signature, attacking a specific port on vulnerable systems, was also easy to detect, and network-level blocking of the ports in question was effective in slowing the worm. In the past, worms often targeted only software for which there was a large installed base of users. But given the speed with which Slammer-like worms can spread, less popular software now also presents a viable breeding ground for worms, the report said.

*Category 14.2* *Worms*

2003-03-11 **worm network Windows passwords target F-Secure**

NIPC/DHS

March 10, IDG News Service — New worm targets weak Windows passwords. A new worm, W32/Deloder-A (Deloder), appeared on Sunday and is considered a low risk for infection, according to an alert posted by anti-virus company F-Secure. The worm, which is believed to have originated in China, attempts to connect to other computers on a network through TCP (Transmission Control Protocol) port 445, randomly generating IP addresses to locate vulnerable machines. If the worm succeeds in breaking the Administrator account password, it places copies of a backdoor (trojan) program known as "inst.exe" in several locations on the infected machine. Machines running Windows 95, 98, NT, 2000, ME and XP are vulnerable to attack by Deloder, Symantec said. No infections from Deloder have been reported and most firewalls block access to port 445. Computer users are advised to contact their anti-virus company for further details.

*Category 14.2* *Worms*

2003-03-11 **worm dictionary attack password administrator**

NewsScan

DELOADER WORM ATTACKS EASY-TO-GUESS PASSWORDS
A new software worm called W32/Deloader-A tries to guess passwords on machines running many of the Microsoft Windows operating systems: it attempts to log on to a machine's administrator account by trying likely passwords such as 'admin', 'password,' '12345', and 'administrator', and so forth. The worm is thought to have originated in China. Although Deloader is considered a low risk for infection, many home computers without firewalls may be vulnerable to its attacks.
(IDG/Computerworld 11 Mar 2003)

*Category 14.2* *Worms*

2003-03-12 **worm network Code Red II variant discover Internet Information System IIS infect**

NIPC/DHS

March 11, eWEEK — New variant of Code Red II discovered. Security experts are watching a new variant of the Code Red II worm that began appearing on some monitoring networks Tuesday. The worm is nearly identical to its ancestor, save for a modified drop-dead date that is now several thousand years in the future. Known as Code Red.F, the worm uses the same infection method as the previous versions, attacking Web servers running Microsoft Corp.'s IIS software. The worm so far has infected only a few machines, and because most administrators patched their servers after the initial Code Red outbreak in 2001, it is unlikely to spread extensively, experts say. All of the Code Red worms exploit an unchecked buffer in the Index Server in the IIS software. They then spread by infecting one machine and then scanning a list of random IP addresses and attempting to connect to port 80. The original Code Red, which struck in July 2001, infected several hundred thousand IIS servers and caused massive traffic disruptions on some portions of the Internet.

*Category 14.2* *Worms*

2003-03-19 **worm network vulnerability lax security policy**

NIPC/DHS

March 17, eWEEK — Deloder, Lovgate worms mark perils of slack security policy. Many computer users persist in using their names or children's birthdays as log-on credentials, and two recent worm outbreaks have shown why that's such a risky practice. Deloder, the latest worm to hit vulnerable Windows machines, as well as a recent version of Lovgate, both use a list of common passwords in an attempt to compromise computers. Lovgate began spreading late last month, while Deloder appeared last week. Although neither worm has spread as far or as fast as threats such as SQL Slammer or Code Red, both Deloder and Lovgate clearly illustrate the danger inherent in lax security policies. In Deloder's case, the worm tries to connect to random Windows NT, Windows 2000 and Windows XP machines on TCP port 445, normally used by Microsoft Corp.'s Active Directory. It then looks for network shares on the remote machine and, if it finds any, tries to copy itself to the shares by using easily guessed passwords to gain access. The worm also installs a Trojan horse and a utility for executing commands on remote machines. Lovgate behaves in a similar fashion. It spreads from an infected machine using the Messaging API Windows functions by answering recent mail with an infected reply. It then tries to copy itself to network shares and their subfolders. If the folders are password- protected, Lovgate tries passwords such as "admin" and "123."

*Category 14.2* *Worms*

2003-03-21 **Iraq war worm network social engineering spy satellite photos entice**

NIPC/DHS

March 18, Sophos — Swedish computer worm lures with Iraq spy satellite photos. Sophos researchers report that they have discovered a new email-aware worm that feeds on public interest in the imminent war in Iraq in an apparent attempt to lure unsuspecting users. The W32/Ganda-A worm, which appears to have been written in Sweden, uses a variety of different email subject lines and message bodies in both English and Swedish to try and encourage computer users to run its viral attachment. Possible subjects are "Spy pics," "GO USA" and "Is USA always number one?" In a bizarre twist, the author of W32/Ganda-A claims to have a grievance with the Swedish educational system. Companies should consider blocking all Windows programs at their email gateway. Computer users should keep their anti-virus software updated.

*Category 14.2* *Worms*

2003-05-19 **e-mail worm Palyh internet masking support@microsoft.com F-Secure registry windows address directories**

NIPC/DHS

May 19, IDG News Service — Palyh worm disguises itself as an email from Microsoft. A mass-mailing e-mail worm known both as W32/Palyh and W32.HLLW.Mankx@mm is spreading on the Internet, masking itself as a message from support@microsoft.com. The worm arrives as an executable attachment to e-mail messages with a variety of subjects and messages. The virus can be released only when a user clicks on the attachment file, anti-virus company F-Secure Corp. said. Once released the virus code modifies the Windows registry so that the worm program is launched whenever Windows is run. It also searches an infected computer for files containing e-mail addresses that it can send itself to and looks for computers that are accessible through shared directories on a network and copies itself to those machines. Anti-virus vendors are advising customers to update their anti-virus software.

*Category 14.2* *Worms*

2003-06-02 **e-mail virus bill gates Sobig-C forward addresses infected computers MessageLabs Please see the attached file screensaver.scr movie.pif documents.pif infect computers bill@microsoft.com**

NIPC/DHS

June 02, BBC News — E-mail virus uses Bill Gates. A Windows virus, called Sobig-C, is spreading widely across the Internet. It does not harm a computer but forwards itself to any addresses found on the infected computer, using several faked addresses such as bill@microsoft.com. Anti-virus companies have rated Sobig-C as a high risk virus. According to e-mail filtering firm MessageLabs, it was first spotted on May 31 in the U.S. Users should watch for e-mails containing subject lines such as "Re: Movie", "Re: Approved", or "Re: Your application", with the message "Please see the attached file". The worm uses a number of different attachment names including "screensaver.scr", "movie.pif" and "documents.pif". Users are advised to delete any suspect e-mails and to update their anti-virus software.

*Category 14.2* *Worms*

2003-06-05 **Bugbear virus internet logging keystrokes PCs confidential information**

NIPC/DHS

June 05, Reuters — Variant of Bugbear virus spreading on PCs. A variant of the Bugbear worm, which spread around the Internet last October, opening back doors on computers and logging keystrokes, has started to infect users around the world, putting them at risk of losing confidential information. According to Mikael Albrecht of computer security company F-Secure, the worm includes a large list of domains belonging mostly to banks. "The list...includes banks from all over the world; Europe, US, Asia and Africa. Bugbear.B changes system settings if activated in one of these banks," he said. The worm variant is better at using addresses in a user's e-mail program than the original, sending itself to those addresses using the infected user's identity, said David Emm of anti-virus company Network Associates Inc. Once activated, Bugbear.B tries to disable some security programs and starts to snoop on an infected system. Bugbear.B takes advantage of a known vulnerability in Microsoft Corp.'s Internet Explorer and can be run automatically simply by reading the e-mail and not opening the attachment. Users are advised to keep their anti-virus software updated.

*Category 14.2* *Worms*

2003-06-06 **University Stanford spam e-mail sensitive information computer system campus PCs salary bonus**

NIPC/DHS

June 06, Mercury News — Virus sends confidential Stanford information out in e-mail. People at Stanford University got spam Thursday containing sensitive information including confidential details about employee salaries and bonuses. The Bugbear.B virus that infected the university's computer system Thursday sent out files at random from campus PCs. It's unclear if outsiders read the rogue e-mails, but some of the 35,000 computer users inside Stanford did — including the man in charge of Stanford's computer systems. The university Web site said Stanford's computer crew intercepted messages containing salary and bonus information.

*Category 14.2* *Worms*

2003-06-18 **Sobig-D worm variant support@microsoft.com admin@support.com network shares e-mail randomized subject lines anti-virus**

NIPC/DHS

June 18, The Register — Fresh variant to Sobig worm. A new variant in the Sobig series appeared Wednesday. Sobig-D is a little different from its predecessors the Sobig-B (support@microsoft.com) and Sobig-C (bill@microsoft.com) worms. Infectious emails sent out by Sobig.D appear to come from admin@support.com. The worm is spreading modestly and causing only a minimal amount of damage. Most vendors rate it as low risk. Although it normally spreads via email, Sobig-D can also spread through network shares. In its more common email form, Sobig-D appears as email with randomized subject lines (such as Re: Documents and Re: Movies) and carries infectious .scr and .pif attachments. Like its predecessors, Sobig-D has a built-in expiration date—in this case July 2. Users should keep their anti-virus software updated.

*Category 14.2* *Worms*

2003-06-23 **Fortnight worm exploits Windows JavaScript worm VM ActiveX micorosft anti-virus registry keys**

NIPC/DHS

June 23, The Register — Fortnight worm exploits antique Windows vuln. Windows users are being infected by a JavaScript worm - even though protection has been available for almost three years. The Fortnight JavaScript worm exploits a vulnerability in Microsoft VM ActiveX which makes it possible for malicious code to execute simply by reading an message in an HTML aware email client. Microsoft issued protection against the vulnerability in October 2000. Despite this, users are still becoming infected to a modest extent with recently released variants of JS/Fortnight-D and JS/Fortnight-F. The worm's actions include changing registry keys and adding links to various Web sites to a victim's favourites list. Users should keep their anti-virus software updated.

*Category 14.2* *Worms*

2003-06-26 **Sobig.E worm computer networks CERT Carnegie Mellon web browser cache hard drives**

NIPC/DHS

June 26, Computerworld — Sobig.E worm spreading around globe. The latest version of the Sobig worm, Sobig.E, has been making its way through computer networks around the world since Wednesday. The worm spreads by scouring an infected computer's hard drive for e-mail addresses in address books or even Web browser cache files, then sends itself out to the addresses it finds. It can spoof its sender's address, so the recipients believe they are receiving a message from someone they know. Graham Cluley of anti-virus software vendor Sophos says the new version of Sobig, which is set to expire on July 14, is being sent as a .zip file, perhaps to allow it to spread in corporate environments where .exe and other file types are automatically blocked in incoming e-mails. Marty Lindner of the CERT Coordination Center at Carnegie Mellon University in Pittsburgh, said the rapid spread of the worm since yesterday means recipients are still opening files in messages even when they have been warned countless times that it's unsafe to do so. Users should update their anti-virus software and should not open unsolicited attachments.

*Category 14.2* *Worms*

2003-06-30 **computer virus data leakage Harvard university bugbear.b machine infection student records**

NIPC/DHS

June 30, U-Wire — Computer virus leaks files from Harvard. The Bugbear.b virus hit the Harvard University campus June 6. When Bugbear.b infects a machine, it sends messages to recipients in an individuals' address book. In addition to a virus-laden attachment, such e-mails often contain text fragments from files on that machine, which may include documents and private correspondence. Harvard students reported receiving seemingly misaddressed messages bearing harmless communications. But at least one message received by at least three Harvard undergraduates contained a confidential memo concerning a case before the Administrative Board. Educational privacy law can penalize institutions who negligently or intentionally transmit their students' records. Director of Harvard Arts and Sciences Computer Services Frank Steen said that his department reacted quickly to the Bugbear virus and that the actual number of computers infected was minimal.

*Category 14.2* *Worms*

2003-08-11 **W32/Blaster worm DCOM vulnerability RPC Remote Procedure Call msblast.exe denial of service**

NIPC/DHS

August 11, CERT/CC — CERT Advisory CA-2003-20: W32/Blaster worm. The W32/Blaster worm exploits a vulnerability in Microsoft's DCOM RPC interface as described Microsoft Security Bulletin MS03-026. Upon successful execution, the worm attempts to retrieve a copy of the file msblast.exe from the compromising host. Once this file is retrieved, the compromised system then runs it and begins scanning for other vulnerable systems to compromise in the same manner. In the course of propagation, a TCP session to port 135 is used to execute the attack. However, access to TCP ports 139 and 445 may also provide attack. The worm includes the ability to launch a TCP SYN flood denial-of-service attack against windowsupdate.com. Unusual or unexpected traffic to windowsupdate.com may indicate a network infection, so system administrators may wish to monitor network traffic. Sites that do not use windowsupdate.com to manage patches may wish to block outbound traffic to windowsupdate.com. Users are encouraged to apply the patches available on the Microsoft Website: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp.

*Category 14.2* *Worms*

2003-08-12 **MsBlast LoveSan Blaster microsoft update worms server target DHS copy cat attacks TCp UDP**

NIPC/DHS

August 12, U.S. Department of Homeland Security — Potential for Significant Impact on Internet Operations Due to Vulnerability in Microsoft Operating Systems (2nd UPDATE: Worm Spreading on the Internet). The Department of Homeland Security (DHS) has issued a second update to the July 24, 2003 advisory on Microsoft operating systems. Today's update warns that malicious code dubbed "MSBlast," "Lovesan," or "Blaster" began circulating on the Internet on August 11th. This worm takes advantage of the vulnerability discussed in the July 24th advisory and contains code that will target Microsoft's update servers on August 16th. This additional attack could cause significant Internet-wide disruptions. It is possible that other worms based on this vulnerability will be released over the next few days as "copy cat" attacks. In this 2nd update, DHS recommends that the Microsoft update (available at http://microsoft.com/technet/treeview/default.asp?url=/techn et/security/bulletin/MS03-026.asp) be applied as soon as possible to the systems affected. In addition to blocking the TCP and UDP ports listed in the July 24th advisory, DHS further recommends that Ports 69 (TFTP) and 4444 be blocked when possible. Both of these ports are used to spread the worm.

*Category 14.2* *Worms*

2003-08-13 **Blaster worm fix patch download site microsoft NT 2000 XP LoveSan Comcast Corp cable modem**

NIPC/DHS

August 13, eWEEK — Worm: long wait for fix. Computer users were scrambling Wednesday, August 13, for alternate fixes for the havoc wreaked by the Blaster worm as many people were unable to reach Microsoft Corp.'s main patch download site. The Windows Update Web site was extremely sluggish Tuesday and Wednesday, and some users reported being unable to reach the site at all. The Blaster worm, also known as LoveSan, began infecting Windows NT, 2000 and XP machines Monday and continues to spread rapidly. The worm exploits a vulnerability in the Windows RPC (Remote Procedure Call) service and uses a lot of bandwidth scanning for other vulnerable machines once it has infected a PC. Microsoft made a patch available for the flaw in mid-July. Blaster is also causing service problems on Comcast Corp.'s cable modem network. Several Comcast customers said their service had been down for extended periods during the last couple of days and that Comcast officials said Blaster was to blame.

*Category 14.2* *Worms*

2003-08-18 **MS-RPC DCOM worm infeting machines DoS Denial Service nacho welchia msblast.d ICMP**

NIPC/DHS

August 18, U.S. Department of Homeland Security — New version of the MS-RPC DCOM Worm infecting machines and creating Denial of Service Conditions. A new worm that exploits the same security weakness as the Blaster worm (also known as "lovsan" or "msblast") has been released on the Internet. This new worm, dubbed "nachi", "welchia", or "msblast.d" does not infect systems that have been updated to counter the Blaster worm but will re-infect computers that are currently infected with Blaster or one of its variants. It deletes the original worm, patches the system by downloading the update from Microsoft, and replaces the original worm with itself. The variant then begins scanning or flooding the network with high volumes of ICMP (Internet Control Message Protocol) traffic causing network congestion which can result in denial of service conditions. Users should patch the MS-RPC DCOM vulnerability immediately using the instructions available on the Microsoft Website: http://www.microsoft.com/security/incident/blast.asp.

*Category 14.2* *Worms*

2003-08-21 **virus network hacker Windows spread Sobig**

NewsScan

SOBIG IS FASTEST-SPREADING VIRUS EVER
The newest version of the Sobig virus is said to be the fastest-spreading network virus ever, and MessageLabs (a company that filters e-mail for corporate clients) intercepted more than a million copies of the "Sobig.F" virus in a single day — or one in every 17 e-mail messages the firm scanned. The virus spreads through Windows PCs via e-mail and corporate networks, and deposits a Trojan horse, or hacker back door, that can be used to turn victims' PCs into relayers of spam e-mail. Yesterday, a worm virus brought down the signaling systems of railroad company CSX Corp, causing delays and canceled trains through the Eastern states. (Dow Jones/AP/SJMN 21 Aug 2003)

*Category 14.2* *Worms*

2003-09-03 **virus worm denial of service DoS availability patch operations interruption shutdown power plant**

NewsScan;http://www.usatoday.com/tech/news/computersecurity/2003-09-03-nuclear-plants-threat_x.htm

NRC ISSUES WARNING ABOUT VIRUS AND WORM ATTACKS
The Nuclear Regulatory Commission (NRC) is issuing a general warning to nuclear plant operators about computer failures that caused by network infections that caused a several-hour shut-down last January at the Davis-Besse nuclear power plant in Ohio. (The NRC emphasized that safety of that plant was not compromised by the computer failures or the shutdown.) The Davis-Besse plant operator, FirstEnergy Nuclear, determined that a contractor had established an unprotected computer connection to its corporate network, thereby allowing the Slammer worm to spread internally, since the utility had also failed to install a corrective software patch from Microsoft. (AP/USA Today 3 Sep 2003)

*Category 14.2* *Worms*

2003-09-19 **internet explorer worm Anti-Virus companies Swen Gibe KaZaA Outlook Express shared networks e-mail Microsoft Corp. victim computer attachment patches Trojan Horse**

NIPC/DHS

September 19, Reuters — New worm targets Internet Explorer. Anti-virus companies warned on Thursday, September 18, of a new computer worm circulating through e-mail that purports to be security software from Microsoft Corp. but actually tries to disable security programs that are already running. The worm, dubbed "Swen" or "Gibe," takes advantage of a two-year-old hole in Internet Explorer and affects systems that have not installed a patch for that security hole, according to an Internet security company. The malicious program arrives as an attachment to an e-mail pretending to contain a patch for holes in Internet Explorer, Outlook and Outlook Express and then mails itself off to addresses located on the victim's computer. The worm also can spread over Internet relay chat and the Kazaa peer-to-peer network, as well as copy itself over shared networks. Microsoft has cautioned customers in the past against e-mail software updates, saying it does not distribute patches as attachments, but rather directs them to its website.

*Category 14.2* *Worms*

2003-11-04 **virus worm network Web Internet SMTP engine**

NIPC/DHS

November 03, vnunet.com — Destructive MiMail variant hits Web. Antivirus firms have warned of a destructive worm that has just emerged in the wild. The W32/Mimail.c@MM, also known as Mimail.c, is a dangerous worm that bears similarities to W32MiMail@MM. Mimail.c contains its own SMTP engine for constructing messages, and mails itself as a zip or upx attachment. After being executed, Mimail.c e-mails itself out as an attachment with the filename 'Photos.zip'. Target e-mail addresses are harvested from the victim's machine and are written to the file eml.tmp in WinDir. Users should immediately delete any email containing the following 1)
Subject: Re[2]: our private photos [plus additional spaces then random characters] 2) Attachment: 'photos.zip' (12,958 bytes) which contains 'photos.jpg.exe' (12,832 bytes). Also, in a bid to make the virus e-mails less conspicuous, the 'From' address of infected outgoing messages may be spoofed with james@(target domain.com) - for example, james@abc.com.

*Category 14.2* *Worms*

2003-11-28 **worms malware mobile phones cellular spam SMS**

NYT http://www.nytimes.com/2003/11/28/technology/28cell.html?th

In Asia, where mobile phones are more popular than in the rest of the world, users are increasingly reporting problems due to worms — the electronic kind. Already, in Japan, there have been two worm attacks (in 2000 and in 2001) which caused cell phones to call emergency numbers. Antispam filters already block 55% of all messages to phones in the largest service providers in Japan, NTT DoCoMo. Cell phone manufacturers are designing new phones with the capability for fast software downloads to help fight malicious code and spam.

*Category 14.2* *Worms*

2003-12-24 **Sober virus worm network anti-virus threat file sharing peer-to-peer mass-mailer**

NIPC/DHS

December 22, eSecurity Planet — Sober mutant starts to squirm. Anti-virus vendors on Monday, December 22, issued upgraded threat warnings for a mutant of the W32/Sober-C worm now squirming its way through e-mail in-boxes. The mass-mailer, which also spreads via file-sharing on P2P networks, has added a bilingual element and arrives with a range of attachment filenames—EXE, SCR, PIF, COM, CMD or BAT. Chris Beltoff of Sophos Inc. said the increased sightings of a mass-mailing virus at the height of the Christmas shopping season puts new PC owners at the highest risk. "The risk is high because of the new, unprotected computers that are being sold off the shelf. Depending on how long that PC has been sitting on the shelf, it's likely new PCs are unprotected against the latest viruses. Remember, the average consumer isn't going to make patching his main priority on a new computer, Beltoff said. Network Associates warned that 80 percent of the intercepted virus comes from Germany and said the characteristics of Sober-C has put Germans or users in German-speaking regions at higher risk.

# 14.4 Trojans

*Category 14.4* *Trojans*

2003-02-14 **Trojan horse social engineering pornography**

NewsScan

'REVEALING' CELEBRITIES PHOTOS USED FOR TROJAN HORSE
E-mail purporting to offer revealing photos of Catherine Zeta-Jones, Britney Spears, and other celebrities is actually offering something quite different: the secret installation of Trojan horse software that can be used by intruders to take over your computer. Users of the Kazaa file-sharing service and IRC instant messaging are at risk. (Reuters/USA Today 14 Feb 2003)

---

*Category 14.4* *Trojans*

2003-05-22 **Kaspersky labs trojan internet explorer startpage vulnerability automatic send function java script executes**

NIPC/DHS

May 22, ITWEB — New Trojan exploits known Internet Explorer vulnerability. Data security software developer Kaspersky Labs reports that a new Trojan program, StartPage, is exploiting an Internet Explorer vulnerability for which there is no patch. If a patch is not released soon, other viruses could exploit the vulnerability. StartPage is sent to victim addresses directly from the author and does not have an automatic send function. The program is a Zip-archive that contains an HTML file. Upon opening the HTML file, an embedded Java-script is launched that exploits the "Exploit.SelfExecHtml" vulnerability and clandestinely executes an embedded EXE file carrying the Trojan program.

---

*Category 14.4* *Trojans*

2003-07-14 **porn ads 2000 windows-based computers hijacked Migmaf Migrant Mafia trojan spam website Network Associate's**

NIPC/DHS

July 14, Reuters — Program hijacks PCs to send porn ads. Close to 2,000 Windows-based PCs with high-speed Internet connections have been hijacked by a stealth program and are being used to send ads for pornography, computer security experts warned. It is unknown exactly how the trojan (dubbed "Migmaf" for "migrant Mafia") is spreading to victim computers around the world, whose owners most likely have no idea what is happening, said Richard M. Smith, a security consultant in Boston. The trojan turns the victim computer into a proxy server which serves as a middle man between people clicking on porn e-mail spam or Web site links, according to Smith. The victim computer acts as a "front" to the porn Web site, enabling the porn Web servers to hide their location, Smith said. Broadband Internet users should always use firewalls to block such stealth activity, he said. Computers with updated anti-virus software will also be protected, said Lisa Smith of network security company Network Associate's.

---

# 14.5 Virus hoaxes

*Category 14.5 Virus hoaxes*

2003-01-06 **virus hoaxes continue fool users anti-virus vendor information**

NIPC/DHS

January 02, ZDNet — Virus hoaxes continue to fool computer users. Fuelled by concern over genuine threats such as Klez, Bugbear and Magistr, computer users are continuing to fall for false warnings of non-existent viruses. These hoaxes typically warn the reader not to open an e-mail with a certain subject line, or to immediately delete a particular file on their hard drive, because they contain a virus. They will also tell the reader to forward the warning to their friends and colleagues. Even though these hoaxes didn't encourage the reader to delete files from their machine, they are harmful because they waste both time and bandwidth. All the major anti-virus companies include information on such hoaxes on their Web sites.

# 15.1 Fraud

*Category 15.1* *Fraud*

2003-10-31 **4-1-9 advance-fee fraud lottery scam**

http://www.theregister.co.uk/2003/10/31/pensioner_accused_of_aus_5m/

Nick Marinellis, a 39-year-old Australian man in Sydney has been charged with operating a 4-1-9 advance-fee fraud revolving around bogus lotteries, inheritances or "business opportunities." A Saudi prince reportedly contributed A$500K in "advance fees" in one case. Total theft was estimated to be more than A$5M.

# 15.2 Extortion

*Category 15.2* *Extortion*

2003-07-29 **movie piracy Malaysia extortion impersonation**

NewsScan

THE MOVIE PIRATES
An unanticipated by-product of Malaysia's campaign against the sale of illegal video discs is the rise of extortionists who impersonate law enforcement officers on surprise checks and demand 50 ringgit (US$13) for each illegal disc they find. Illegal copying of movies and computer software is pervasive in Malaysia and cheap versions of the latest Hollywood, Indian and Hong Kong films have been widely available at street stalls and in stores. (AP/San Jose Mercury News 29 Jul 2003)

---

*Category 15.2* *Extortion*

2003-08-25 **steganography extortion anonymizer credit card forgery e-mail**

http://www.expatica.com/index.asp?pad=2,18,&item_id=33655

In June 2003, a high-tech extortionist in the Netherlands threatened to poison the products of the Campina food company in Utrecht unless he were paid €200,000. The steps for payment used an unusual degree of technical sophistication:

1. Campina had to open a bank account and get a credit card for it.
2. The victims deposited the payoff in the bank account.
3. They had to buy a credit card reader and scan the credit card to extract the data from the magnetic strip.
4. Using a steganography program and a picture of a red VW car sense by the criminal, the victims encoded the card data and its PIN into the picture using the steganographic key supplied with the software.
5. They then posted the modified picture in an advertisement on a automobile-exchange Web site.
6. The criminal used an anonymizing service called SURFOLA.COM to mask his identity and location while retrieving the steganographic picture from the Web site.

The victims worked with their local police, who in turn communicated with the FBI for help. The FBI were able to find the criminal's authentic e-mail address along with sound financial information from his PAYPAL.COM account. Dutch police began surveillance and were able to arrest the 45-year-old micro chip designer when he withdrew money from an ATM using the forged credit card.

---

# 15.3 Slamming

*Category 15.3* *Slamming*

2003-09-29 **Internet redirect explorer bug long distance telephone dial up patch porn**

NewsScan

VANDALS DIVERTING COMPUTERS TO $5-A-MINUTE PORN SITES
Network vandals have been exploiting a security gap in Microsoft's Internet Explorer software and using it to connect their computers to $5-a-minute porn lines by sending computer users to sites that change a computer's dial-up settings, connecting it to expensive long distance telephone numbers instead of the user's ISP. The original hole in Internet Explorer was discovered last month, and Microsoft issued a software patch to fix it, there but new variations of the malicious code seem to be evading the existing patch. (Internet News 29 Sep 2003)

# 16.1 Industrial espionage

*Category 16.1* *Industrial espionage*

2003-05-08 **ericsson investigation sweden espionage spy Mansour Rokkgireh Alireza Rafiei Bejarkenari russia**

NIPC/DHS

May 08, Associated Press — Three charged in Ericsson spy investigation in Sweden. Three Swedish employees of wireless equipment maker LM Ericsson face espionage charges, Swedish prosecutors said Thursday. Afshin Bavand is accused of handing over secret company information to a Russian intelligence agent, while Mansour Rokkgireh and Alireza Rafiei Bejarkenari are accused of helping him gather the information. "If these company secrets have been given away, it is my opinion that it may cause harm to the overall defense or to the security of the country," chief prosecutor Thomas Lindstrand told The Associated Press. But Ericsson spokesman Henry Stenson said the espionage involved the company's commercial telecommunications systems, and not its military-related work. Stockholm-based Ericsson also makes radar systems for defense programs worldwide, including for the JAS-39 Gripen fighter planes made by Sweden's Saab and Britain's BAE Systems.

# 16.3 Infrastructure protection

*Category 16.3* *Infrastructure protection*

2003-01-08 **Department Homeland Security cyber terrorism combat secure cyberspace**

NIPC/DHS

January 07, Associated Press — Revised White House security initiative focuses on agencies. An internal draft of the Bush administration's revised plan to improve cybersecurity, the National Strategy to Secure Cyberspace, is circulating among government offices and industry executives this week. In the new plan, the number of initiatives to tighten security for vital computer networks was reduced from 86 to 49. The plan no longer includes a number of voluntary proposals for America's corporations to improve security, focusing instead on suggestions for U.S. government agencies, such as a broad new study assessing risks. Among the draft's changes was the removal of an explicit recommendation for the White House to consult regularly with privacy advocates and other experts about how civil liberties might be affected by proposals to improve Internet security. The draft notes that the new Department of Homeland Security (DHS) will include a privacy officer to ensure that monitoring the Internet for attacks would balance privacy and civil liberties concerns. The draft proposes to use the DHS to launch some test attacks against civilian U.S. agencies and to improve the safety of automated systems that operate the nation's water, chemical and electrical networks. The new version also says the Defense Department can wage "cyber warfare" if the nation is attacked. It warns that although it can be difficult or even impossible to trace an attack's source, the government's response "need not be limited to criminal prosecution." The new version also puts new responsibilities on the CIA and FBI to disrupt other countries' use of computer tactics to collect intelligence on government agencies, companies and universities.

---

*Category 16.3* *Infrastructure protection*

2003-01-14 **war Iraq technology security battlefield PKI training biometric**

NIPC/DHS

January 13, Government Computer News — Possible war, terrorist threats shape Defense IT agenda. The prospect of war with Iraq is defining the Defense Department's 2003 technology initiatives. U.S. soldiers on the front lines are preparing to use the latest technologies-including wireless communications and high-end cryptography tools-being tested and deployed by DOD, senior department officials said. In the coming months, DOD's technical focus will be squarely on security, boosting projects to develop antiterrorism tools, creating a DOD-wide public-key infrastructure (PKI), expanding IT training, and beginning biometric pilots.

---

*Category 16.3* *Infrastructure protection*

2003-02-03 **US infrastructure protection cyber terrorism threat security**

NIPC/DHS

February 02, New York Times — Departing security official highlights cyber threat. Richard A. Clarke, the blunt, sometimes abrasive White House adviser who raised the alarm about unconventional national security threats ranging from failed states to biological and computer terrorism for more than a decade, quietly resigned as President Bush's special adviser for cyberspace security on Friday. In an interview after his last day in office, Clarke warned that although the government had made considerable progress in defending its electronic infrastructure from computer attacks, the United States faced ever greater peril, given its growing dependence on the Internet. "A sophisticated cyberattack may not result in massive deaths," he said. "But it could really hurt our economy and diminish our ability to respond to a crisis, especially if it is combined with a war, or a terrorist attack." Clarke said the attack last weekend by a computer bug known as the Sapphire worm showed the vulnerability of the United States' increasingly Internet-based economy. Though it was a relatively simple bug, he said, Sapphire, which has also been called Slammer, ravaged systems throughout the United States and overseas in just a few hours, shutting down some of the Bank of America's automated teller machines and Continental Airlines' online ticketing system, and denying access to the Internet to millions of personal computer owners. "Don't assume that the damage done by hackers in the past is predictive of the future," Clarke said. "As Sept. 11 showed, as long as our vulnerabilities are large, some enemy will exploit them in a new and hugely damaging way." Clarke said the nation is safer today than before Sept. 11 because al Qaeda's sanctuary in Afghanistan is gone and because Americans had rounded up hundreds of al Qaeda operatives abroad and tightened aviation security overseas and domestically. Clarke said he was leaving his post now because "11 years in the White House and a total of 30 in government is more than enough," and because President Bush would soon unveil a new national strategy to protect the nation's information infrastructure, which Clarke and his team had drafted.

---

*Category 16.3* *Infrastructure protection*

2003-02-18 **cyberattack homeland defense infowar information warfare government policy**

NewsScan

WHITE HOUSE OUTLINES NEW INTERNET SECURITY STRATEGY
The White House has released a new Internet security strategy focused largely on voluntary efforts by institutions in the private sector and by individual Americans. The plan suggests, without mandating, numerous steps that government agencies should take to set the example for good security procedures, and specifies that the five major priorities for action are: setting up a security response system; identifying threats and vulnerabilities; increasing awareness and training; securing critical government sites; and fostering cooperation nationwide and abroad. Acting chief White House security czar Howard Schmidt says, "This is a good start. It's a very practical and pragmatic plan and it gives us the capability to move forward in the confines of the current budget situation. There's never enough money in security, but this gives us the ability to have a dialogue with industry and set goals." (San Jose Mercury News 15 Feb 2003)

*Category 16.3* *Infrastructure protection*

2003-02-18 **industry government plan secure cyber space anti-terrorism infrastructure**

NIPC/DHS

February 14, Government Computer News — Industry will work with government on cyberspace plan . The White House unveiled its National Strategy to Secure Cyberspace on Friday. The plan's five priorities are: 1) A national cyberspace security response system; 2) A threat and vulnerability reduction program; 3) A security awareness and training program; 4) A plan to secure governments' cyberspace; 5) An approach to intelligence agency and international cybersecurity. The plan called for exercises to evaluate the impact of cyberattacks and pinpoint weaknesses for correction. The plan put the Justice Department and other agencies in charge of improving information sharing, investigative tools and cybercrime research. It said the General Services Administration and Department of Homeland Security will continue to cooperate on a federal software patch clearinghouse and work with the private sector on a similar clearinghouse. Federal agencies were told to tighten security measures, expand their use of security assessment tools and install applications to check continuously for unauthorized network connections. The plan said the government will also review the National Information Assurance Partnership to assess whether it is properly dealing with security flaws in commercial software. It further said the government will consider licensing or certifying private security service providers for minimum capabilities, "including the extent to which they are adequately independent." In the international arena, the plan noted that the U.S. government will not necessarily limit its response to cyberattacks to criminal prosecution and it "reserves the right to respond in an appropriate manner." That mirrors the government's pursuit of al-Quaida, which has been carried out partly by legal prosecution and partly by warfare. It called for building North America into a "cyber safe zone" with the cooperation of Canadian and Mexican public and private sectors.

*Category 16.3* *Infrastructure protection*

2003-02-20 **cyber terrorism threat steps action States critical infrastructure protection**

NIPC/DHS

February 19, Government Computer News — States take first step toward cyberthreat sharing. Last weekend thirteen states conducted a communications exercise that could lead to a new, multistate information sharing and analysis center (ISAC). The ISAC, which would pool cyberthreat data gathered by states, is led by William Pelgrin, director of the New York City Office of Cyber Security and Critical Infrastructure. No formal center exists yet, however. During the dry run, participating states reported to a central location any suspicious activities they monitored on the Internet over the Presidents Day weekend. "There was no malicious activity," said Mike Russo, chief information security officer in Florida's state technology office. "The exercise was about the communications and working relationships with the other states." Because sharing information about security threats and vulnerabilities is seen as essential to protect the nation's critical infrastructures, the federal government has encouraged the creation of ISACs to share information in commercial sectors such as banking, public utilities and IT. It also encourages information sharing with federal agencies. The ISACs serve as central collection points where data can be gathered and evaluated. Most such information is sanitized before distribution because of participating organizations' liability concerns.

*Category 16.3* *Infrastructure protection*

2003-02-25 **National Infrastructure Protection Center NIPC Indiana University cooperate cyber infrastructure protection security**

NIPC/DHS

February 25, National Infrastructure Protection Center — NIPC and Indiana University agree on cooperative cyber infrastructure security efforts. In an effort to support and enhance the security and readiness of the cyber infrastructure, the National Infrastructure Protection Center (NIPC) has signed an agreement with Indiana University, operator of the Research and Education Network Information Sharing and Analysis Center (REN-ISAC). Indiana University, via the REN-ISAC, will ensure that research and education network operators receive the most current counter-terrorist threat alerts, warnings and analysis. In turn, the network operators and participating universities and research centers will be encouraged to work through the NIPC to voluntarily pass incident information. Incident information will include not only specific incidents immediately threatening participating networks, but trend information that may indicate an organized attack is in preparation or underway. "The Nation's research and education networks carry not only information critical to research but critical commercial and financial information as well. That is why information sharing between the federal government and network operators is vital in the war against terrorism," said Admiral James Plehal, Acting Director of the NIPC. "Advance knowledge of the type and nature of attacks can make a vital difference in their readiness to prevent, and mitigate the consequences of an attack," he said. Indiana University is home to a Global Network Operations Center (Global NOC) which manages several national and international high-speed networks and network links. The NIPC will transition into the Department of Homeland Security on March 1st.

*Category 16.3* *Infrastructure protection*

2003-03-06 **Congress cyber security threat terrorism panel infrastructure civilian protection**

NIPC/DHS

March 04, News.com — Congress sets up cybersecurity panel. The U.S. Congress on Tuesday established its first panel devoted to cybersecurity. In its first meeting, the new House Homeland Security Committee voted to create a subcommittee that will oversee the federal government's "cybersecurity, science, and research and development" efforts relating to homeland security. The office of chairman Chris Cox (R-CA) said the cybersecurity subcommittee will be in charge of the "protection of government and private networks and computer systems from domestic and foreign attack (and) prevention of injury to civilian populations and physical infrastructure caused by cyberattack." The Senate does not have a parallel effort, though its subcommittee on technology, terrorism and government information shares similar duties.

*Category 16.3* *Infrastructure protection*

2003-03-12 **US federal government secure Internet net DHS**

NIPC/DHS

March 10, eWEEK — Federal government moves to secure net. The White House and the new Department of Homeland Security have begun in earnest the process of implementing the plan to secure the nation's critical networks. The most significant move is the development of a private, compartmentalized network that will be used by federal agencies and private-sector experts to share information during large-scale security events, government officials said at the National Information Assurance Leadership conference in Washington D.C. last week. The system is part of the newly created Cyber Warning Information Network (CWIN), a group of organizations including the National Infrastructure Protection Center, the Critical Infrastructure Assurance Office and others that have some responsibility for the security of federal systems. The private-sector Information Sharing and Analysis Centers will also be included. The CWIN, a key part of the Bush administration's National Strategy to Secure Cyberspace, will use a secure, private IP network separate from the public Internet, according to officials. As part of the plan to improve security, the CIO of each federal agency is, by statute, now accountable for the security of that agency's network.

*Category 16.3* *Infrastructure protection*

2003-03-24 **security built up telecom companies East coast US anti-terrorism FCC**

NIPC/DHS

March 24, Washington Post — Telecom firms rebuild, beef up security. Since the terrorist attacks in New York and at the Pentagon crippled communications networks along the East Coast, telecommunications companies have invested heavily to fortify their facilities. All over the country, telecommunications companies have added fiber-optic lines, increased their ability to reroute traffic and beefed up their security in response to lessons learned in the September 2001 attacks. Jeffrey M. Goldthorp, chief of network technology at the Federal Communications Commission, has been working with the nation's leading telecommunications companies for the past year. He was reluctant to discuss specifics but did point to one unnamed company that he said recently moved a huge database to a hardened underground shelter. The database will be a key resource in case the network, or any section of it, needs to be rebuilt. The FCC also recently orchestrated a series of "mutual aid" contracts between companies that allow them to work together immediately after a disaster without having to negotiate costs or other legal issues.

*Category 16.3* *Infrastructure protection*

2003-04-04 **Department Homeland Security DHS Internet infrastructure design critical system**

NIPC/DHS

April 01, National Journal — DHS may oversee Internet infrastructure. The Bush administration's acting cybersecurity adviser Howard Schmidt said Tuesday that homeland security and government agencies officials are working to formalize a security apparatus for the global Internet root servers, a series of computer systems that underpin the Internet's address system. After an attack on those servers and the Internet domain-name system last October, Schmidt, several agencies officials, computer-security experts and root-server operators discussed in January how they could better respond to such incidents. Their talks identified the need to develop a framework for determining when individuals and companies that operate the Internet's mission-critical domain system should report an attack or disturbance to government officials.

*Category 16.3* *Infrastructure protection*

2003-04-04 **NIST national infrastructure protection IAIP Homeland Security DHS secure cyberpsace**

NIPC/DHS

April 02, Federal Computer Week — NIST security division expands role. The National Institute of Standards and Technology's (NIST) Computer Security Division will be playing a significant role in the Bush administration's cybersecurity strategy, according to Howard Schmidt, acting chairman of the President's Cybersecurity Board. The NIST division did not move to the new Information Analysis and Infrastructure Protection (IAIP) Directorate at the Department of Homeland Security (DHS), as originally set out in the White House's plan. Discussions are under way to determine how the organization can and will contribute to the implementation of the National Strategy to Secure Cyberspace, Schmidt said. Schmidt also is working with the recently appointed IAIP directorate leaders to make sure that all of the work being done by the President's Critical Infrastructure Protection Board — dissolved in a February executive order — is carried over into DHS.

*Category 16.3* *Infrastructure protection*

2003-04-17 **cyber attack terrorism cyberspace action war Iraq**

NIPC/DHS

April 15, Reuters — More talk, little action in war on cyber terrorism. At a time when war in Iraq has heightened fears of terrorism, the technology industry is not moving quickly enough to guard against intrusions from hackers, identity thieves and more concerted attacks by rogue governments, computer experts said Tuesday at the RSA conference in San Francisco. Howard Schmidt, the White House cyber security adviser who is working with the technology industry to improve security, said that work to date had been strong on new ideas to improve security, but slow to execute. Despite repeated warnings of rogue nations preparing for cyber-attacks that could cripple vital computer-run U.S. infrastructure, no such attacks are known to have occurred to date. If computer systems have so far been spared a massive terrorist attack, smaller security breaches from hackers and pranksters with no political agenda occur on a daily basis. The Computer Emergency Response Team (CERT) tracked some 52,658 online security "incidents" in 2001, more than double the 21,756 reported in 2000, and way up from 9,859 in 1999. Members of the high-tech advocacy group TechNet said that while the threat of a political-based cyber terrorist attack may have been overstated, random pranksters had the ability to do much damage.

*Category 16.3* *Infrastructure protection*

2003-04-21 **US President IT security adviser resign critical infrastructure protection**

NIPC/DHS

April 18, Washington Post — President's top IT security adviser to resign. White House cybersecurity adviser Howard Schmidt will resign from his post at the end of the month. The former chief of security at Microsoft Corp., Schmidt became chair of the President's Critical Infrastructure Protection Board in February following the departure of his predecessor, Richard Clarke. Schmidt played a key role in drafting the administration's recently released cybersecurity strategy, and has spent the last two years building ties with the private sector in a joint effort to protect the nation's most important information systems from cyber-attack. Schmidt's imminent departure would leave the administration without a high-ranking official solely in charge of cybersecurity. In January, the administration consolidated the work of five federal cybersecurity offices into the Department of Homeland Security (DHS). Full responsibility for cybersecurity matters currently rests with Robert Liscouski, a former Coca-Cola executive who was recently named assistant secretary of infrastructure protection at the DHS.

*Category 16.3* *Infrastructure protection*

2003-04-24 **Department Homeland Security cyberwar game simulation anti-terrorism**

NIPC/DHS

April 23, Government Computer News — DHS gets into the cyberwar game. The Department of Homeland Security (DHS) is simulating cyberattacks and biological assaults to help prepare for the possibility of the real thing, deputy secretary Gordon England said. "A week ago, I participated in a war game with the Business Roundtable," England told attendees at the U.S. Chamber of Commerce's Conference on Critical Infrastructure and Homeland Security today. The Business Roundtable is an association of corporate chief executive officers that makes policy recommendations for economic growth. Part of the war game involved a cyberattack on financial institutions "that sucked money out of the financial system," England said. England endorsed the Business Roundtable's approach of periodically reviewing its members' plans for recovery from attacks and urged the Chamber of Commerce to adopt similar plans. In response to a question about the department's approach to regulation, England said, "I would like the DHS to have as few regulations as possible-our job is to coordinate the work of other federal agencies."

*Category 16.3* *Infrastructure protection*

2003-04-25 **cyber space cyberterrorism anti-terrorism threat networkks**

NIPC/DHS

April 24, New York Times — Defending the cyber realm. Security experts have warned that cyberterrorism presents a great potential threat to the U.S., with its increasing dependence on computer networks for everything from weapons systems to hydroelectric dams to commerce. However, security technology developer Symantec says it has yet to record a single cyberterrorist attack — by its definition, one originating in a country on the State Department's terror watch list. That could be because those inclined to commit terrorist acts do not yet have the know-how to do significant damage, or perhaps because hackers and adept virus writers are not motivated to disrupt networks for a cause. But should the two groups find common ground, the result could be devastating, said Michael A. Vatis, head of the Institute for Security Technology Studies at Dartmouth College.

*Category 16.3* *Infrastructure protection*

2003-04-29 **threat cyber terrorism Internet infrastructure protection**

NIPC/DHS

April 25, London Free Press — Cyber attacks a concern? The FBI calls cyber-terrorism a "premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by subnational groups or clandestine agents." Some fear cyber-terrorists could shut down the Internet or substantially interfere with the use of oil, gas, power grids, telecommunications and emergency services. Others, however, say these fears are overstated as many critical systems are based on secured networks not accessible through the Internet. Terrorists and computer hackers can be a dangerous combination. There are reports that after investigations regarding several hijackings, authorities were led to believe terrorists had gained access to the architectural schematics of the planes through cyber-crime.

*Category 16.3* *Infrastructure protection*

2003-04-30 **Korea Information Communication Ministry Internet attack SQL slammer**

NIPC/DHS

April 28, The Korea Herald — Korea's MIC takes measures to prevent online attacks. The massive Internet shutdown caused by the SQL Slammer computer virus on January 25 caused chaos for Korea's 10 million high-speed Internet users. Now, Korea's Ministry of Information and Communication (MIC) has announced that it will take an active role in promoting security countermeasures aimed at creating fast and accurate communication routes where fixing and preventing network attacks will take only a matter of minutes. The MIC plans to create an information security base, develop information security related technology and standardization, and train manpower in the sector. It will build a support center dealing with attacks and security breaches on the Internet that will run 24 hours per day. MIC is also working on introducing rights to request information and investigate the scene of the crime. Other preventative measures involve working and communicating with multiple online businesses and service providers to make sure that each complies with standards in prevention.

*Category 16.3* *Infrastructure protection*

2003-05-09 **PITAC cybersecurity Bush President's Information Technology Advisory Committee IT homeland security**

NIPC/DHS

May 09, Federal Computer Week — PITAC nominees strong in cybersecurity. President Bush announced May 8 that he plans to appoint 25 new members to the President's Information Technology Advisory Committee (PITAC), which offers advice on maintaining America's dominance in advanced information technologies. The panel provides information to the president, Congress and federal agencies involved in IT research and development, and helps guide the Bush administration's efforts to accelerate the development and adoption of IT policies for the nation. Its members are leading IT experts from industry and academia, many of whom have worked in or with the government. "These appointments come at a critical time for our economic security and our homeland security, particularly in the area of cybersecurity," said House Science Committee Chairman Sherwood Boehlert (R-NY).

*Category 16.3* *Infrastructure protection*

2003-05-12 **IT security Bush administration information technology OMB white house**

NIPC/DHS

May 12, National Journal — Report to recognize agencies' progress toward IT security. President Bush's administration is readying a report that will recognize several government agencies for making tangible progress in their efforts to meet security goals for information technology, according to administration officials. The White House Office of Management and Budget (OMB) is preparing to send Congress an annual report highlighting the status of those IT initiatives, OMB analysts told members of a National Institute of Standards and Technology advisory board last Wednesday. The report will be the last IT security review by OMB before it updates its guidelines and agency reporting requirements under new IT rules created under a recent e-government law.

*Category 16.3* *Infrastructure protection*

2003-05-14 **cyber attack critical computer systems terrorism critical infrastructure**

NIPC/DHS

May 14, Silicon Valley — U.S. still vulnerable to cyber attack. The United States remains ill-prepared to defend against a strike on the nation's critical computer systems because of slow-moving federal research efforts, members of Congress said Wednesday. "The nation quite simply has been under-investing woefully in cyber security R&D," said Rep. Sherwood Boehlert (R-NY), chair of the House Science Committee, which brought the heads of the four agencies to Capitol Hill to testify about their efforts. The heads of the four lead agencies for cyber-security research — the directors of the science foundation, DARPA, and the National Institute of Standards and Technology, and the undersecretary for science and technology at the Department of Homeland Security — said they were making progress and beginning to work collaboratively on projects. Terrorism experts fear attacks on computer systems that operate electricity grids, phone systems or other critical infrastructure as part of a terrorist strike.

*Category 16.3* *Infrastructure protection*

2003-05-26 **critical infrastructure lawmakers cyber terror vulnerability government agencies Richard Clarke regulations police**

NIPC/DHS

May 26, The Hill — Lawmakers see cyberterror vulnerability. Lawmakers are charging that government agencies and industry are not doing enough to protect the country's power plants, industries and financial institutions from the threat of cyberterrorism attacks. Science committee staffers have noted that 80 to 90 percent of the country's infrastructure is under private control. Staffers for the House Government Reform Technology Subcommittee are making site visits to private sector companies to assess its state of preparedness. At a subcommittee hearing in April, former White House advisor on cyber security Richard Clarke said, "I think we want to avoid regulation" and a "cyber security police." But a few weeks later, members of the National Infrastructure Advisory Committee, a White House advisory group. concluded that regulation might be the best way to get some industries to implement better cyber security, as well as physical infrastructure security. An alternative to government regulation is self-regulation through regional Information Sharing and Analysis Centers. But the threat of having competitors aware of a company's vulnerabilities has made this problematic for many organizations.

*Category 16.3* *Infrastructure protection*

2003-07-15 **terrorism awareness infrastructure protection Senate education funding withheld**

NewsScan

SENATE PUTS THE SQUEEZE ON TIA FUNDING
U.S. senators deliberating over next year's defense budget have proposed eliminating all funding the Defense Department's Terrorism Information Awareness project. The TIA project, under the supervision of retired Adm. John Poindexter, seeks to develop computer software capable of scanning vast public and private databases of commercial transactions and personal data around the world to ferret out possible terrorist activities. The committee's proposal "reflects deep, deep skepticism in Congress of the Pentagon's assurances about this system," says a spokesman for the Center for Democracy and Technology. "There appears to be some spillover skepticism from Iraq where they voted to go to war and now are questioning whether that was based on clever use of words or selective use of intelligence." (AP 15 Jul 2003)

*Category 16.3* *Infrastructure protection*

2003-07-23 **cyberthreat warning Homeland Security council WMD information security protections John Gordon critical infrastructure**

NIPC/DHS

July 23, Federal Computer Week — Security adviser warns of cyberthreats. Officials must still figure out how to fully secure the nation's critical infrastructure against cyber attacks, said General John Gordon, retired lieutenant general from the U.S. Air Force, presidential assistant and adviser to the Homeland Security Council Tuesday, July 22. Attacks over electronic networks might become a threat as great as weapons of mass destruction, he told a meeting of the National Infrastructure Advisory Council in Washington, DC. The council, which consists of a gathering of industry and government officials, is expected to issue recommendations for tougher information security protections in October. One of the council's toughest challenges is determining what should be disclosed to private industry and the public and when it should do so, officials told the council.

*Category 16.3* *Infrastructure protection*

2003-07-23 **digital control systems traditional computer networls physical infrastructure LAN WAN remote administration vulnerability risk assesment**

NIPC/DHS

July 23, Government Computer News — NDU prof: digital control systems can weaken security. The growing integration of digital control systems with traditional computer networks is opening a new avenue of attack against the nation's physical infrastructure, John H. Saunders, a professor at the National Defense University, said Wednesday, July 23, at the GOVSEC security conference in Washington. Controls for operating utilities, buildings and campuses are being turned over to cost-effective digital systems with remote access capabilities. Proprietary protocols and single-purpose firmware have offered a degree of security for these systems. But standardizing on a few protocols is increasing the risk. Digital control systems also are being connected to LANs, WANs and the Internet for remote administration. Government administrators can do little about the level of security at utilities, but they can increase security within their own buildings, Saunders said. Building engineers need to focus on security the way systems administrators do, by performing systems inventories and vulnerability and risk assessments, and by implementing policy, he said.

*Category 16.3* *Infrastructure protection*

2003-07-26 **terrorism Ciso funding grants Treasury Department**

NewsScan

THE SECOND-ORDER COSTS OF TERRORISM
Cisco and other high-tech companies are faced now with the problem of monitoring charitable contributions made on behalf of their employees, to make sure the money isn't being sent to terrorist organizations. Taylor Griffin of the U.S. Treasury Department says: "It's the reality of a post-Sept. 11th world. Glossy brochures say they are funding orphans and people in need. But money is actually going to fund suicide bombings that kill innocents." But Janne Gallagher of the Council on Foundations complains that "adding a lot of other questions to due diligence increases the cost of making each grant," and Brian Lehnen of the Village Enerprise Fund, which has provided more than 100,000 small grants and loans to East African business startups, asks hypothetically: "Let's say one of them decides to be a terrorist... Suddenly, we support terrorism. It's on the minds of foundations and other deep-pocket organizations that fund groups overseas and don't know what they are liable for." (San Jose Mercury News 26 Jul 2003)

*Category 16.3* *Infrastructure protection*

2003-07-31 **Homeland Security Windows PC buffer overflow exploit vulnerability tool**

NewsScan

GOVERNMENT SOUNDS THE ALARM ON HACK ATTACKS
The U.S. Department of Homeland Security warns that in recent days computer hackers have successfully tested new tools that exploit a vulnerability known as "buffer overflows" in order to gain control of Windows PCs via the Internet. The vulnerability was discovered by Polish researchers who call themselves the "Last State of Delirium Research Group" and Microsoft has posted a patch on its Web site that individual PC owners can install to safeguard their machines. Experts warn that the attack tools, once perfected, could be used to disrupt Internet traffic by clogging data networks, or could allow crackers to delete or steal sensitive files. However, a senior security manager at Symantec says hackers haven't yet worked out all the glitches in these tools. "It is a little early. The exploit needs to be perfected. The effort applied to the exploit is certainly increased, but we're not sure if that's indicative of when we might see a widespread threat. People certainly need to be aware of this." Meanwhile, Internet Security Systems, which operates an early warning network for the technology industry, has raised its alert level to the second notch, indicating "increased vigilance" is warranted. "Everybody is predicting a widespread event, going from zero to 60 very quickly," says Internet Security Systems engineering director Dan Ingevaldson, who rates the probability of a major attack as "closer to imminent than probable." (AP/CNN.com 31 Jul 2003)

*Category 16.3* *Infrastructure protection*

2003-08-25 **virus network Sobig organized crime fraud**

NewsScan

ORGANIZED CRIME BEHIND SOBIG MESS?
Antivirus specialist Peter Simpson warns that the Sobig.F virus is the latest in a series of attempts on the part of organized crime to shift some of their illicit activities online. "Sobig smashed all the records in terms of pure numbers, but that's not nearly the whole story. This is the sixth in a series of controlled experiments. This isn't about some kiddy writing viruses in his bedroom — this is really a very sophisticated example of organized crime," says Simpson, a manager at Clearswift's ThreatLab. Simpson explained that the purpose of a virus such as Sobig isn't to cause damage, but to gain control of the machine in order to access information such as financial details for the purpose of fraud. It also comes in handy for disguising the source of spam by hijacking the victim's machine and identity. "The real question here has to be about the motives of the virus writer. This isn't just about writing a virus that will spread rapidly and break records; the motives here are very different and are clearly criminal. It's all about the hidden agenda." (ZDNet/Silicon.com 25 Aug 2003)

*Category 16.3* *Infrastructure protection*

2003-09-15 **homeland security cybersecurity incident response awareness federal agency strategy**

http://www.fcw.com/fcw/articles/2003/0915/web-cyber-09-15-03.asp

YORAN TO LEAD U.S. CYBER SECURITY
The Department of Homeland Security has announced that Amit Yoran will head the recently created National Cyber Security Division. Yoran currently serves as vice president of managed security services at Symantec Corp. The National Cyber Security Division comprises the Federal Computer Incident Response Center, the National Infrastructure Protection Center, and the Critical Infrastructure Assurance Office. It is responsible for awareness of and preparation for cybersecurity, including coordinating warnings and responses to cyber threats. The division, which was created in June, has been working on such issues since its inception. A spokesperson from the division said that having someone in charge will allow the division to pursue projects included in the National Strategy to Secure Cyberspace. [Federal Computer Week, 15 September 2003]

*Category 16.3* *Infrastructure protection*

2003-09-23 **MTA security systems computer hackers New York Metropolitan Transportation Authority firewalls website Intrusion Detection System IDS computer employees encryption software**

NIPC/DHS

September 23, Associated Press — MTA upgrading its security system against computer hackers. The New York Metropolitan Transportation Authority said it would strengthen its defenses against computer viruses and theft now that officials have said its computer system could be attacked. The agency has already installed "Critical Tier I" computer firewalls at its headquarters. Documents say the firewalls will protect access to the MTA's network and its website. An "Intrusion Detection System" has also been placed in MTA computers and employees have been offered encryption software. An additional firewall and other virus protectors will be installed later. The agency is also expected to approve $5.25 million in upgrades for the security of regional bridges and tunnel facilities.

*Category 16.3* *Infrastructure protection*

2003-11-03 **infrastructure protection recommendation US FCC**

NIPC/DHS

October 30, FCC — Media Security and Reliability Council to review infrastructure security recommendations. Recommendations to ensure the continued operation and security of media infrastructure will be presented to leaders from the broadcast, cable and satellite industries at the biannual Media Security and Reliability Council (MSRC) meeting Thursday, November 6. MSRC is a Federal Advisory Committee that reports to FCC Chairman Michael K. Powell. Chairman Powell formed MSRC following the events of September 11, 2001, in order to study, develop and report on best practices designed to assure the optimal reliability, robustness and security of the broadcast and multichannel video programming distribution industries. The Communications Infrastructure Security, Access and Restoration Working Group will present detailed best practices recommendations relating to physical security, including prevention and restoration matters. The council members have until November 26 to vote on the recommendations.

*Category 16.3* *Infrastructure protection*

2003-11-06 **cyber security cyberspace plan halt Congress FBI report incident**

NIPC/DHS

November 04, Washington Post — Congressman puts cybersecurity plan on hold. A congressional plan to require publicly traded companies to get computer security audits will be put on hold while technology businesses try to come up with a proposal of their own. Rep. Adam Putnam, R-FL, chairman of a House technology subcommittee, said he will postpone plans to introduce his bill and wait about 90 days to see what kind of alternative the business community proposes. There are no similar bills in the Senate. Businesses often keep cybercrime incidents under wraps and are generally unwilling to publicize any computer security measures, even with law enforcement. According to an April study by the Computer Security Institute and the FBI, just 30 percent of companies that experienced cyberattacks last year reported such incidents to authorities. The business community is also generally opposed to government-sponsored requirements on cybersecurity, whether from Congress or the White House.

*Category 16.3* *Infrastructure protection*

2003-11-26 **terrorism evaluation US government simulation ISTS Dartmouth DHS**

NIPC/DHS

November 24, Associated Press — Government evaluates simulated terrorist attacks. Experts inside government and the Institute for Security Technology Studies at Dartmouth College are still formally evaluating results of a simulated terrorist attack carried out by the Department of Homeland Security (DHS) over five days in October. The "Livewire" exercise simulated physical and computer attacks on banks, power companies and the oil and gas industry, among others. "There were some gaps," said Amit Yoran, the chief of the agency's National Cyber-Security Division. "The information flow between various sectors was not as smooth as we would perhaps have liked." Yoran said the mock attacks during the exercise tried to broadly disrupt services and communications across major industrial sectors, enough to make consumers to lose economic confidence. It modeled bombings at communications facilities outside Washington and cyberattacks aimed at companies and other networks. Yoran said the exercise affirmed that troublesome interdependencies exist throughout the nation's most important systems. A broad power outage could also bring down key telephone or computer networks, disrupting repair efforts.

*Category 16.3* *Infrastructure protection*

2003-12-05 **technology companies secure cyberspace Department Homeland Security DHS urge infrastructure protection**

NIPC/DHS

December 05, Mercury News (CA) — Tech firms urged: secure cyberspace. Department of Homeland Security (DHS) Secretary Tom Ridge warned Wednesday, December 4, that terrorists who "know a few lines of code can wreak as much havoc as a handful of bombs." It is important that "we share information, work together and close any gaps and weaknesses that terrorists would otherwise seek to exploit," Ridge told an audience of about 350 business leaders and technology experts attending the National Cyber Security Summit in Santa Clara, CA. "It only takes one vulnerable system to start a chain reaction that can lead to a devastating result," Ridge added. Robert Liscouski, the DHS's assistant secretary for infrastructure protection, made clear there would be consequences if the corporations that control 85 percent of the nation's critical infrastructure chose not to cooperate. The DHS wants businesses to provide information about cyber attacks so it can identify major threats to computer networks that control everything from water supplies and power lines to banking and emergency medical services. DHS officials say they need such data to create an early warning system. The full text of Secretary Ridge's remarks are available on the DHS Website:
http://www.dhs.gov/dhspublic/interapp/speech/speech_0151.xml

*Category 16.3* *Infrastructure protection*

2003-12-05 **information security cyber chief security officer council**

NIPC/DHS

December 04, Federal Computer Week — Fed cybersecurity chiefs get a council. Information security has become important enough to warrant a federal Chief Security Officers Council to work with similar groups of government executives, the man in charge of national cybersecurity said this week. There is already a CIO Council, a CFO Council and a Chief Human Capital Officers Council, but security is so complicated now that Amit Yoran, director of the Department of Homeland Security's National Cyber Security Division, decided to initiate a council focused specifically on that one issue. "The CIOs have a lot on their plate and under [the Federal Information Security Act] every agency must have a security official...and this allows them to collaborate and discuss issues," Yoran said. The new CSO Council will work closely with the CIO Council, but having a separate forum where chief security officers can get together and discuss problems, tactics and best practices should make improvement easier, Yoran said.

*Category 16.3* *Infrastructure protection*

2003-12-11 **US government agencies cybersecurity secure critical information systems fail test**

NIPC/DHS

December 09, Government Executive — Agencies get failing grades on cybersecurity. Federal efforts to secure critical computer systems and sensitive information are improving, but more than half of all agencies are still doing very poorly at the task, lawmakers said Tuesday, December 9. Overall, the federal government received a grade of D for cybersecurity, up from a grade of F a year earlier, according to the 2003 Federal Computer Security Scorecard released Tuesday. The scorecard, which is compiled by the House Government Reform subcommittee, is based on information reported by each agency and federal inspectors general to Congress and the Office of Management and Budget. Senator Susan Collins (R-ME), who chairs the Senate Governmental Affairs Committee, urged agencies to take immediate action to improve cybersecurity. "The administration has reason to believe that cyberattacks could be part of terrorists' game plans," she said. "We cannot afford to be caught off guard."

# 16.4 Military & government perspectives on INFOWAR

*Category 16.4 Military & government perspectives on INFOWAR*

2003-01-22 **battlespace battlefield videophones communications wireless**

NewsScan

PENTAGON TO SUPPLY COMBAT VIDEOPHONES
In an effort to counter hostile propaganda, the Pentagon plans to equip public-affairs officers with two-way videophones, enabling them to set up on-the-spot video interviews with frontline military commanders. The $27,000 Austrian-made Scotty Tele-Transport videophones come in a rugged briefcase that cradles a laptop computer with video-editing and recording capability and includes a built-in camera, a keyboard and a pair of collapsible satellite dish antennas. Television networks have begun using such equipment extensively in the past year, and the Department of Defense and U.S. intelligence agencies already own similar devices. "They have these systems, but they hadn't thought about using it in this kind of way," says Lt. Col. David Lamp, a spokesman for the U.S. Joint Forces Command. "We're finally getting a realization in the world that information is power." Instead of sitting quietly while enemy forces broadcast claims that U.S. forces have bombed a hospital or distributed poisoned emergency food rations to refugees, as happened in Afghanistan, "the best thing to do is to try to manage it, to use it. Commanders who don't do that, or leaders who don't do that, they usually end up learning the hard way." (AP 22 Jan 2003)

*Category 16.4 Military & government perspectives on INFOWAR*

2003-02-07 **cyberattacks retaliation response infowar information warfare homeland defense deterrence policy government**

NewsScan

BUSH SIGNS ORDER AUTHORIZING CYBER-ATTACKS
President Bush has signed a secret order allowing the government to proceed with developing guidelines on circumstances under which the U.S. could launch cyber-attacks against foreign computer systems. The directive signals Bush's desire to pursue new forms of potential warfare — already the Pentagon has moved ahead with development of cyber-weapons that could by used by the military to invade foreign networks and shut down radar, disable electrical facilities and disrupt phone service. (AP 7 Feb 2003)
http://apnews.excite.com/article/20030207/D7P1UJDO0.htm

*Category 16.4 Military & government perspectives on INFOWAR*

2003-02-10 **Department of Defense DOD US computer network attack CNS task force**

NIPC/DHS

February 07, Federal Computer Week — DOD plans network attack task force. The Defense Department is planning to form a joint task force focused solely on computer network attack (CNA) as part of the ongoing reorganization of U.S. Strategic Command (Stratcom). Stratcom recently acquired oversight of DOD's information operations and global command, control, communications, computer, intelligence, surveillance and reconnaissance (C4ISR) capabilities. Currently, Stratcom's Joint Task Force-Computer Network Operations is charged with defending all DOD networks from attack, as well as initiating cyberattacks when instructed by the president or Defense secretary. However, Stratcom's reorganization also will result in splitting the JTF-CNO into two separate task forces - one focused on computer network defense, and the other on CNA, according to DOD officials. A DOD spokesman said that CNA is "bound by largely the same rules that apply to any war strategy or tactic - very clear rules of engagement (ROE) will prove necessary. "All pieces of the enemy's system of systems that are valid military targets have been - and will be - on the table as we go about war planning," the spokesman said. "It is unimportant whether we take out a computer center with a bomb or a denial-of-service program. If it's critical to the enemy and we go to war, it will be in our sights."

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

2003-03-12 **infowar information warfare traffic analysis interception e-mail**

NewsScan

E-MAIL GOES TO WAR
E-mail is a great morale-booster for military personnel, but military historian Keith Eiler worries that "the volume of message traffic can be very dangerous. It's a potentially serious problem and not one that is easily solved." There are fears that enemy forces could obtain a soldier's message home and find ways of misusing it. But though some military advisors have discussed ways of clamping down on personal e-mail from the front lines, Army chief information officer Lt. Gen. Peter M. Cuviello says: "We have not had a problem in Bosnia, Kosovo, Sinai, East Timor, or Korea in recent times, so I don't expect there is going to be a problem," and an Army spokesman in Qatar says, "There are no restrictions on e-mails, it's kind of up to the judgment of the individual person." The father of Army soldier, Gary K. Richardson probably speaks for most families of service men and women, saying that the Internet is "more wonderful than you can imagine. When you get a message, you know that her hands were just on the keyboard and that she was alive and well just a few minutes ago." (New York Times 12 Mar 2003)

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

2003-03-14 **Iraq war satellite communication jam subvert GPS US**

NIPC/DHS

March 12, Associated Press — Iraqis could try to jam satellite signals. Iraq could try to jam U.S. military satellite signals during a possible invasion, but the United States has defenses against such attempts, Pentagon officials said Wednesday. Iraq also reportedly is seeking ways to jam the Global Positioning Satellite (GPS) signals that help guide U.S. bombs. At the Pentagon, Brig. General Franklin Blaisdell and Army Col. Steven Fox promoted what they said was America's dominance of space as a key strength in any future military operations. Satellites allow U.S. commanders to see what is going on in hostile countries, communicate with soldiers and pilots, and guide precision weapons. The Army has more than 1,000 transmitters that help it keep track of soldiers and units while a battle is going on, Fox said. As it did during the 1991 Persian Gulf War, the Defense Department is buying access to commercial communications satellites to help serve the massive bandwidth needed to connect all the high-tech gear, Blaisdell said. The military also successfully launched a broadband communications satellite on Monday, he said.

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

2003-03-28 **US Army Defense Message System DMS faster secure e-mail**

NIPC/DHS

March 27, Federal Computer Week — Army taps DMS for wartime comm. The Army recently implemented the Defense Message System (DMS) to provide users with better-protected and faster communications than e-mail over the Defense Department's Secret Internet Protocol Router Network (SIPRNET). DMS messages travel over the Defense Information Systems Network, which distributes voice, video and data messages. The system - a $1.6 billion effort to secure DOD communications worldwide - is designed to provide writer-to-reader service for classified and top-secret information, delivering messages to DOD users at their desktops and to other agencies and contractors, if necessary. Retired Air Force Master Sgt. Arthur Edgeson, senior systems engineer at the Fort Detrick, MD, office of Data Systems Analysts Inc., said DMS became active at Camp Doha (Kuwait) at the end of last month and has experienced a noticeable increase in traffic since Operation Iraqi Freedom began March 20. "Yes, SIPR e-mail is classified, but it could be hacked into. Or if we're overrun by the enemy, they would have access to the computers and could send messages...to mislead or misdirect [coalition] forces," said Edgeson. Edgeson acknowledged that DMS still has bugs to work out and that many DOD users remain faithful to Autodin, another system. But Autodin does not allow users to include attachments. It requires users to pick up messages at a central message center twice daily and is run on antiquated equipment. DMS may not be perfect, but it can send and receive all messages for both systems and deliver them to the user's desktop quickly and securely, Edgeson said. The other military services also are using DMS, but each has its own time lines, personnel and priorities, he said.

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

2003-04-02 **Iraq war communication network Internet computer hardware software intelligence support**

NIPC/DHS

March 29, Washington Post — Computer support staff at home is crucial to war effort. To a greater extent than any war before it, Operation Iraqi Freedom depends on an elite group of technicians, engineers and other specialists in the United States who are standing by 24 hours a day, seven days a week to assist the troops. Pentagon officials have called this conflict a "network centric" one, with computers and wireless technology linking intelligence from the 250,000 U.S. troops and the drones, tanks, planes and other vehicles in a way that has compressed decision-making from what in the past might have been days into minutes. A single mix-up, glitch or crash in the technology could cost lives. So far, the technology has held up well, and there have been few major problems, according to about a dozen of the contractors who provide technical support services to the military. Working in classified "safe rooms" or reachable via pagers and cell phones around the country, they have been working behind the scenes to make sure the multitude of software and hardware systems is working properly.

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

2003-04-02 **Iraq war computer cyber warfare information virus scanning Army**

NIPC/DHS

March 31, Federal Computer Week — Cyberwarriors guard virtual front. As coalition forces continue to engage the enemy throughout Iraq, the number of battles being fought in cyberspace also has risen, according to one Army information assurance officer. Col. Mark Spillers, information assurance program manager in the Coalition Forces Land Component Command communications office at Camp Doha, Kuwait, said "if a device is thought to be compromised, it is immediately isolated, taken off the network and scanned for viruses." Spillers said he could not go into any details about how the Army is protecting its systems or if any have been compromised." On the physical battlefield, if troops are in danger of being defeated, procedures are in place to safeguard or even destroy endangered equipment and systems to keep sensitive data from falling into enemy hands.

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

2003-04-11 **physical infrastructure attack Iraq war bomb communication Corporate America disaster recovery**

NIPC/DHS

April 08, Security Net — Physical attack still the biggest threat. Baghdad's telecommunications infrastructure fell silent during the first week of April under a rain of precision-guided bombs. U.S. and British planes targeted phone facilities and other critical pieces of the Iraqi communications infrastructure to isolate the leadership from the levers of power. The U.S. military chose to use bombs — not hackers — to drop Iraqi networks for a reason. Nothing brings a network to a halt more easily and quickly than physical damage. Yet as data transmission becomes the lifeblood of Corporate America, most big companies haven't performed due diligence to determine how damage-proof their data lifelines really are. Only 20% of midsize and large companies have seriously sussed out what happens to their data connections after they go beyond the company firewall, says Peter Salus of MatrixNetSystems, a network-optimization company based in Austin, TX. The collapse of the World Trade Center left most of Lower Manhattan, the epicenter of the global financial system, without data connections for a week or more. Many of the affected companies thought they were covered for any eventuality, having contracted for not one but two high-capacity data connections from their offices. Redundancy doesn't help much, however, if your connections pass through the same geographical location. Unfortunately, massing huge chunks of connectivity in so-called "telecom hotels" is the norm.

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

2003-04-22 **government Infosec White House security advisor resigns**

NewsScan

WHITE HOUSE SECURITY ADVISER RESIGNS
Howard Schmidt, the former Microsoft security chief who became White House cybersecurity adviser in February following Richard Clarke's departure from that office, has tendered his resignation, saying: "While significant progress has been made, there still is much to do. The nation as a whole is much better at responding to cyberattacks then at any time in the past, but cybersecurity cannot now be reduced to a `second tier' issue. It is not sufficient to just respond to attacks, but rather proactive measures must also be implemented to reduce vulnerabilities and prevent future attacks." (AP/San Jose Mercury News 22 Apr 2003)

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

2003-05-14 **cyber R&D DHS center Charles McQueary cybersecurity cyberterrorism**

NIPC/DHS

May 14, Federal Computer Week — DHS creating cyber R & D center. Charles McQueary, the under secretary for Department of Homeland Security 's (DHS) Science and Technology Directorate, told the House Science Committee Wednesday that the DHS is creating a research and development center to coordinate cybersecurity efforts across civilian and defense agencies, universities, and the private sector. In an effort to help develop state-of-the-art and low-cost technology to prevent cyberterrorism, the DHS center will partner with the National Science Foundation and the National Institute of Standards and Technology, two federal agencies that deal with R & D, as well as with academic institutions and private corporations. "The center will foster national and international cooperation in creating a robust and defensible cyber infrastructure," McQueary said. DHS spokesman David Wray said there is no date yet for the start-up of the cybersecurity center.

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

2003-07-03 **Illinois supercomputer cybersecurity thwart hackers NCSA battlefield communications**

NIPC/DHS

July 03, Associated Press — Illinois supercomputer center to head military cybersecurity effort. Hoping to thwart hackers, the military is launching a new research effort at the University of Illinois to improve the security of battlefield computers and communications systems. Officials at the school's National Center for Supercomputing Applications (NCSA) on Thursday announced an initial $5.7 million grant from the Office of Naval Research to establish a new research center to develop technology against enemy hackers, NCSA director Dan Reed said. Other research projects will include developing remotely programmed radios and refining ways for monitoring battlefield environments. The NCSA is a high-performance computing center that develops and deploys computing, networking and information technology for government and industry. Software developers will try to determine the best way to share information among military forces without fear of interception. The government also is seeking a framework for determining quickly when and how a computer network is under attack, Reed said.

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

2003-07-29 **new jersey army intrusion detection systems IDS cyberterrorism**

NIPC/DHS

July 29, InformationWeek — New Jersey teams with the Army on intrusion detection. The Army will help New Jersey analyze the state's network as a step in developing an intrusion-detection system. The agreement with the U.S. Army Communications-Electronics Command Research, Development, and Engineering Center based at Fort Monmouth, NJ, is the first such collaboration between the center and a state. Charles Dawson, New Jersey's chief technology officer, says a comprehensive intrusion-detection program is a key component in the state's homeland security plans to protect its IT infrastructure from cyberterrorism. The technical components of the program include host-based intrusion-detection systems, network-based intrusion-detection systems, and security information-management systems. The state also will receive guidance in developing policies and procedures to effectively manage the program.

# 16.5 Hacktivism

*Category 16.5* *Hacktivism*

2003-03-18 **hacktivism Iraq war Web defacement propaganda**

NIPC/DHS

March 17, Computer Weekly — U.S. diplomatic site hacked by anti-war protestors. The website of the American Academy of Diplomacy (www.academyofdiplomacy.org ) was hacked into Sunday while U.S., U.K. and Spanish leaders met at the Azores summit to discuss the crisis over Iraq. A message of "No War" was plastered over the site by hacking group "Rooting Sabotage Forced". Other messages on the site included protests over the Israeli-Palestinian situation. With a war on Iraq thought to be as little as days away digital attacks on American and British business and government targets remain at an all-time high, according to the British-based digital risk specialist mi2G. For 12 months, the number of independently verifiable digital attacks on the US stand at 48,155 and for the UK they stand at 7,607 according to the mi2g SIPS database. In comparison, the number of attacks recorded over the same period for France was 3,082.

*Category 16.5* *Hacktivism*

2003-03-21 **Iraq war hacktivism Web defacement warn cyber attack**

NIPC/DHS

March 20, Washington Post — Antiwar digital graffiti prompts security experts to warn of further cyberattacks. A hacker group marred hundreds of Web sites with digital graffiti Wednesday night in an apparent response to the onset of the U.S.-led war against Iraq, prompting security experts to warn of further cyberattacks in the days to come. Unix Security Guards, a pro-Islamic hacking group which includes hackers from Egypt, Morocco, Kuwait and Indonesia, defaced nearly 400 Web sites Wednesday evening with antiwar slogans written in Arabic and English, according to iDefense, a U.S. Internet security firm. Text posted on sites by the hacker group said the defacements were the beginning of "the new era of cyber war we promised! More is coming, just like the US do [sic] what it wants to the world, we will do what we want to the Internet. Stop the US terroristes [sic] and we will stop! Viva Iraq!" The attacks were typical of the sort of "hacktivism" that has accompanied international conflicts in the past, said Jim Melnick, director of threat intelligence for iDefense.

*Category 16.5* *Hacktivism*

2003-03-25 **Denial of Service DoS hacking hackivism Al-Jazeera Iraq**

NIPC/DHS

AL-JAZEERA SITE ATTACKED
The Web site of Al-Jazeera, the Arab satellite TV network, was subjected to denial-of-service attacks yesterday, making it intermittently unavailable. The servers that host the Al-Jazeera site are in both France and the U.S., but only the U.S. servers were affected. The site's English-language page, which was launched one day before the attacks began, had been showing images of U.S. soldiers killed in Iraq. (AP/Washington Post 25 Mar 2003)

*Category 16.5* *Hacktivism*

2003-03-26 **anti-war Web defacement vandalism hacker hacking Iraq war**

NIPC/DHS

March 25, Associated Press — Anti-war hackers alter South Carolina Secretary of State's Web site. Hackers apparently took over the South Carolina Secretary of State's Web site this weekend, posting anti-war slogans and obscenities. Officials were notified of the altered page Sunday afternoon and took it down. The regular site was restored later the same day. The pirated site was up for about 12 hours, officials said. "This country has a history of civil disobedience, but this has crossed the line and is a criminal matter," Secretary of State Mark Hammond said Monday. The State Law Enforcement Division is investigating, spokesman Kathryn Richardson said.

*Category 16.5* *Hacktivism*

2003-04-02 **Utah Internet Service Provider hacking attack Al-Jazeera anti-war Iraq war Web vandalism**

NIPC/DHS

March 28, Associated Press — Utah ISP is victim of retaliation following hackers' attack on al-Jazeera. The Salt Lake City-based Internet service provider Networld Connections became the unwitting tool of hackers attacking Arab television network al-Jazeera, and then was itself struck by a retaliatory attack, possibly from anti-war hackers. The original hackers, impersonating an al-Jazeera employee, tricked the Web addressing company Network Solutions into making technical changes that effectively turned over temporary control of the network's Arabic and English Web sites. "We have no idea who the hacker is, but now there is a 'denial-of-service' attack going on against us because of what happened," Ken Bowman, Networld's president and chief executive, said late Thursday. Bowman said the attacks were from all over the world, but seemed concentrated most from nations such as Russia, China and France that have among the most vocal opponents of the U.S.-British coalition's attack.

*Category 16.5* *Hacktivism*

2003-04-03 **Al-Qaeda terrorism information warfare Web vandalism hacktivism**

NIPC/DHS

April 01, The Oregonian — Al Qaeda supporters hack into student's Web site. The Web site of a Portland State University graduate student was targeted in a wave of Internet hackings supporting al Qaeda. Files planted in Conrado Salas Cano's personal Web site housed threats against the United States, tributes to the September 11 attacks and purported messages from Osama bin Laden. The FBI reportedly launched an investigation, and some cyberterrorism followers said it resembled attacks by al Neda, the online propaganda unit of al Qaeda. Josh Devon, an analyst at the Search for International Terrorist Entities Institute, said some of the pages contain pictures of guns and bomb-making manuals in Arabic. Specific plans of future attacks aren't on the site, although Devon said it's possible they use code words to communicate attacks. Since losing their domain name last summer, Devon said al Neda has been hacking into various sites around the globe to spread its message. Once the sites are discovered and shut down, a new al Neda site pops up within 48 hours. News of the Web sites, he said, spreads by word of mouth and in Arabic newspapers.

*Category 16.5* *Hacktivism*

2003-04-18 **Iraq war protest Internet hacktivism Web defacement vandalism security attack**

NIPC/DHS

April 16, Mena Report — High profile digital targets hit by hackers protesting Iraq war. Over 3,000 successful digital attacks took place last weekend primarily against U.S. and U.K. online targets with hackers protesting a further escalation in the war with Iraq. The main concern being expressed by hackers is over the conflict spreading to Syria or Iran. High profile targets hit include Coca-Cola's web site in Singapore, which was attacked on Saturday, April 12. It was unreachable throughout Sunday and is now back up again. There are other examples of NASDAQ and NYSE listed companies, such as one with over 1,650 employees and a market capitalization in excess of $275 million that were hit over the weekend. Also, Fuji Film online sites in the U.S. and Switzerland were targeted by Hackweiser—a pro-war U.S. patriotic group — and in the U.K., the London Fire Brigade and Scottish Police online sites were successfully targeted by Unix Security Guards (an anti-U.S./U.K./Israel group).

# 16.6 Disinformation, PSYOPS

*Category 16.6* *Disinformation, PSYOPS*

2003-01-14 **information warfare Iraq war e-mail campaign convince leaders defect United Nations UN**

NIPC/DHS

January 12, CNN — U.S. e-mail attack targets key Iraqis. U.S. military and other U.S. government agencies have begun a surreptitious e-mail campaign inside Iraq in an effort to get some Iraqis to defy President Saddam Hussein. Thousands of e-mail messages have been sent out since Thursday. The disguised e-mails, being sent to key Iraqi leaders, include instructions to the e-mail recipients to contact the United Nations in Iraq if they want to defect. If they do not, the messages warn, the United States will go to war against them. Senior military sources told CNN this was the first time the military had engaged in this type of "information warfare campaign." The U.S. military and intelligence officials were apparently hoping that the Iraqis do not realize where the e-mails are coming from. One official tells CNN the Pentagon wanted "to preserve this capability as long as possible," but once the e-mail campaign was discovered it would be acknowledged publicly. The official also says the United States acknowledges that Iraq may have already shut off some Internet gateways to prevent the e-mails from getting through. He said these same types of messages will now be sent by radio broadcast in the days ahead from U.S. airborne and ground platforms.

---

*Category 16.6* *Disinformation, PSYOPS*

2003-03-26 **disinformation malicious imposters news corporate Web sites Iraq war**

NIPC/DHS

March 25, The Register — Malicious impostors sow seeds of disinformation. Security testing outfit NTA Monitor has warned of the increased likelihood of attacks against news sites and corporate Web sites during the current war in Iraq. News sites are especially at risk, because attackers could use weaknesses in sites or domain registration tricks to 'rewrite' breaking news to try to create confusion and panic, according to NTA. The most obvious risk is denial of service attacks, in which sites are deliberately brought down by extreme traffic volumes. However the subtler attacks are of much greater concern. By registering similar domain names or 'typo squatting' - booking domains with common typo errors (e.g., wwwcompany.com) - traffic intended for official news sites could be re-directed. Attackers can impersonate Internet news sites and make major changes to the news, with potentially disastrous impact.

---

*Category 16.6* *Disinformation, PSYOPS*

2003-04-03 **Iraq Information Ministry war disinformation propaganda US attack**

NIPC/DHS

March 31, salon.com — Iraq goes offline. U.S. Tomahawk cruise missiles aimed at destroying Saddam Hussein's propaganda machine reportedly destroyed several satellite dishes and an Internet server housed at Iraq's Ministry of Information building Saturday. Local phone service in the city was also reportedly disrupted by separate missile strikes on two telecommunications switching centers. Yet Babil Online, the home page of an Iraqi newspaper run by Saddam Hussein's son Uday, was still reachable following the bombing. Babil Online may have escaped the attacks because of its physical location — the site appears to be hosted on a server not in Baghdad but in Beirut, Lebanon. Some observers have speculated that the United States left Iraq's Internet infrastructure untouched for the first week of the war in order to maintain communications with potential defectors in the high ranks of Iraq's government and military personnel. But Peter W. Singer, a fellow at the Brookings Institute, said he doubted that preserving Iraq's Internet capabilities was high on the priority lists of U.S. military planners. "Internet access is still limited mostly to elites in the country. The U.S. is mostly concerned about protecting things like water and electricity and bridges," said Singer. He said the mission of Iraq's Information Ministry has been not only to fire up nationalism but also to manipulate world opinion and to raise international protests against the war.

---

*Category 16.6* *Disinformation, PSYOPS*

2003-04-03 **biological virus hoax Website misinformation disintermedation Hong Kong**

NIPC/DHS

April 01, Reuters — Website hoax fans virus panic. A teenager's website hoax about a killer virus that is sweeping Hong Kong sparked panicked food buying and hit financial markets on Tuesday, forcing the government to deny it would isolate the entire territory. "We have no plan to declare Hong Kong an infected area," Director of Health Margaret Chan told reporters. "We have adequate supplies to provide (for) the needs of Hong Kong citizens, and there is no need for any panic run on food." In Hong Kong, 685 people are infected by severe acute respiratory syndrome, also known as SARS, and 16 have died from the virus. The fake website scare fueled dismay in the territory adjoining China's Guangdong province, where the virus is believed to have originated four months ago. The hoaxer copied the format of the public Internet portal of the Mingpao, one of Hong Kong's leading newspapers, and posted a message saying the government would declare the city of seven million "an infected place."

*Category 16.6* *Disinformation, PSYOPS*

2003-04-04 **biological virus hoax SARS Website misinformation disintermedation Hong Kong SMS text message**

NIPC/DHS

April 03, Associated Press — Six million mass text messages avert SARS panic. When a false Internet story about Asia's mystery illness sent fears through Hong Hong, authorities used a fast and simple way to shoot down the rumor: they sent a blanket text message to about 6 million mobile phones that denied the territory had been declared an "infected city." Severe Acute Respiratory Syndrome, or SARS, has killed at least 78 people and sickened more than 2,200 worldwide. The government used the text message on Tuesday after the "infected city" hoax report appeared online, prompting panic among some residents who thought the territory would be shut down. The government's text response said: "Director of Health announced at 3pm today there is no plan to declare Hong Kong as an infected area." The hoax story was allegedly posted by a 14-year-old boy who was quoted as saying he did it for fun, and didn't think anybody would believe the story. A telecommunications professor said mass text messaging - or SMS messaging - was justified in emergencies, but could potentially be abused. "It's very important for phone operators to identify where the information comes from," said KL Ho, who teaches at the Department of Electrical and Electronic Engineering at the University of Hong Kong. "It's also very important to remind users not to believe just one single source," Ho said.

*Category 16.6* *Disinformation, PSYOPS*

2003-04-16 **CNN information filtering operation propaganda Iraq**

NewsScan

CNN DEFENDS ITSELF AGAINST NEWS-FILTERING CHARGES
In a memo to his staff, CNN top news executive Eason Jordan has denied that his motive for failing over a 12-year period to report horrors of the Saddam Hussein regime was to keep the CNN Baghdad bureau open. "A number of people have told me CNN should have closed its Baghdad bureau, helped everyone who told me the horror stories flee Iraq, with me thereafter telling those stories publicly long before now. While that is a noble thought, doing so was not a viable option." He says that such victims would not have left their country simply to be able to share their stories with the world. "So we reported on Iraq's human rights record from outside Iraq and featured many interviews with Iraqi defectors who described the regime's brutality in graphic detail. When an Iraqi official, Abbas al-Janabi, defected after his teeth were yanked out with pliers by Uday Hussein's henchmen, I worked to ensure the defector gave his first TV interview to CNN. He did." (Atlanta Journal-Constitution 16 Apr 2003)

*Category 16.6* *Disinformation, PSYOPS*

2003-07-29 **Disinformation HIV Internet**

NewsScan

IS HIV AN INTERNET PROBLEM?
A presentation made at the 2003 National HIV Prevention Conference suggests that online chat rooms and Web sites are partly responsible for the fact that a growing number of U.S. gay and bisexual men are engaging in risky activities with partners they met on the Internet. New HIV diagnoses among those groups have jumped more than 17% since 1999, and 850,000 to 950,000 Americans have the AIDS virus. Dr. Ron Valdiserri of the Centers for Disease Control in Atlanta says: "It's clear we need to reach gay and bisexual men with appropriate messages, not only in traditional high-risk settings but also online. (Washington Post 29 Jul 2003)

*Category 16.6* *Disinformation, PSYOPS*

2003-12-05 **psychological operations disinformation false news propaganda military**

NYT
http://www.nytimes.com/2003/12/05/politics/05STRA.html?th=&pagewanted=p
rint&position=

In December 2003, analysts raised the alarm upon discovering a modest $300K contract from DoD to SAIC for a study of how to "design an 'effective strategic influence' campaign combat global terror….[Eric Schmitt, NY Times] Schmitt continued his report with an explanation that Pentagon spokespersons assured questioners that although establishing a "road map for creating an effective D.O.D. capability to design and conduct effective strategic influence and operational and tactical perception-management campaigns" might be a poor choice of words, it was not a call for a propaganda machine. "We're asking for a menu of thoughts on how to approach this," one official explained. "This is not a secret document on how we're going to change the Arab world's perception of the U.S."

*Category 16.6* *Disinformation, PSYOPS*

2003-12-07 **Google bomb linking search engine information warfare psyops**

BBC http://news.bbc.co.uk/2/hi/americas/3298443.stm

Pranksters deliberately agreed to link the words "miserable failure" on their Web pages to the biography of George W. Bush, resulting in "Google Bombing" as his site climbed to the number one position on the search engine's listing for — wait for it — "miserable failure." Responding to the attack, conservatives used the same technique to link the insulting words to sites about Jimmy Carter, Michael Moore and Hillary Rodham Clinton. The phenomenon is yet another wrinkle in the evolution of psychological operations and information warfare, although a minor and amusing one. Google declined to interfere.

# 17.1 Penetration

*Category 17.1* *Penetration*

2003-02-19 **penetration data theft fraud credit card**

NewsScan

VANDALS BREAK INTO SYSTEM HOLDING MILLIONS OF CREDIT CARD NUMBERS
A third-party processor of Visa and MasterCard credit card accounts was invaded by network vandals, but Visa and MasterCard executives say that none of the credit information was used for fraudulent purposes. In any event, no customer will be liable for any charges that might fraudulently be made to their accounts. A statement from Visa says that its fraud team "immediately notified all affected card-issuing financial institutions and is working with the third-party payment card processor to protect against the threat of a future intrusion. This is not something regional, it was throughout the nation and could be any bank." (Reuters/CNet News 18 Feb 2003)
http://news.com.com/2102-1017-984842.html

---

*Category 17.1* *Penetration*

2003-02-24 **criminal hackers hacking America Online AOL customer database private personal sensitive information disclosed**

NIPC/DHS

February 21, Wired — Hackers compromise security at AOL. Hackers have compromised security at America Online, potentially exposing the personal information of AOL's 35 million users. The most recent exploit, launched last week, gave a hacker full access to Merlin, AOL's latest customer database application. Merlin, which runs only on AOL's internal network, requires a user ID, two passwords and a SecurID code; hackers obtained all of these by spamming the AOL employee database with phony security updates, through online password trades, or by "social engineering" attacks over AOL's Instant Messenger (AIM) or the telephone. Another hole has allowed hackers to steal AIM screen names, even those of AOL staff members and executives. Most at risk are screen names that hackers covet, like Graffiti, or single-word names like Steve. While many of these hacks utilize programming bugs, most hackers are finding it far easier and quicker to get access or information simply by calling the company on the phone. These social engineering tactics involve calling AOL customer support centers and simply asking to have a given user's password reset. Logging in with the new password gives the intruder full access to the account.

---

*Category 17.1* *Penetration*

2003-03-07 **criminal hacker hacking penetration theft sensitive private data university students Austin**

NIPC/DHS

March 06, American Statesman — Hackers steal vital data about university students and staff. Computer hackers have obtained the names, Social Security numbers, and e-mail addresses of about 59,000 current and former students, faculty members and staff at the University of Texas at Austin in one of the largest cases of potential identity theft ever reported. Authorities do not know whether the information has been put to illegal uses such as obtaining credit cards or withdrawing money from financial accounts. Law enforcement officials were expected to obtain and execute search warrants late Wednesday in Austin and Houston at homes where computers are thought to have been used in the cyberspace break-in. UT officials said the computer breach could easily have been prevented with basic precautions, adding that the incident will prompt them to redouble security measures and to accelerate a plan to phase out most uses of Social Security numbers on campus. The university has set up a Web site - www.utexas.edu/datatheft - where it plans to post information. A telephone hot line will also be established, possibly staffed round the clock seven days a week, said Don Hale, vice president for public affairs. The university has reported the theft to the FBI, the Austin Police Department, the Travis County district attorney's office and other authorities.

---

*Category 17.1* *Penetration*

2003-03-18 **hacking penetration theft conviction University Texas Austin sensitive private information**

NIPC/DHS

March 15, Washington Post — Student charged with hacking at U-Texas. Federal prosecutors charged a University of Texas student Friday with breaking into a school database and stealing more than 55,000 student, faculty and staff names and Social Security numbers in one of the nation's biggest cases of data theft involving a university. Christopher Andrew Phillips, 20, a junior who studies natural sciences, turned himself in at the U.S. Secret Service office in Austin. He was charged with unauthorized access to a protected computer and using false identification with intent to commit a federal offense. Authorities had announced the cyber-theft last week. There is no evidence that Phillips disseminated or used the information, officials said. Phillips was released without bail and will have "limited access to computers," Johnny Sutton, U.S. attorney for western Texas, said at a news conference. If convicted, Phillips faces as many as five years in prison and a $500,000 fine, Sutton said.

*Category 17.1* *Penetration*

2003-03-19 **hacking compromise Army Web server Windows 2000 vulnerability exploit Microsoft CERT CC**

NIPC/DHS

March 18, Federal Computer Week — Army Web server hacked. A hacker last week exploited a previously unknown vulnerability in Microsoft Corp.'s Windows 2000 operating system to gain control of an Army Web server. Russ Cooper of security services company TruSecure Corp. said that on March 10 the hacker used an attack code to operate the Army system as if he or she had the highest security clearance and therefore was able to gain complete control of the system. The Army identified the problem after performing a network scan and finding data output from a port on one of its internal servers to an "unspecified region," he said. Both Microsoft and Carnegie Mellon University's CERT Coordination Center issued security warnings about the "buffer overflow" vulnerability and Microsoft has developed a patch, available on the Microsoft Web site, to fix it. The vulnerability affects systems running Microsoft Windows 2000 with Internet Information Server (IIS) 5.0 enabled and the code exploits an unchecked buffer in the WebDAV protocol. Exactly which Army computer was attacked, the sensitivity of the data contained on the system, and the attacker's intentions are still unknown. Compounding the surprising nature of an attack on a Defense Department system is the fact that this was a previously unknown vulnerability, or "zero-day exploit," which are extremely rare in the computer security arena. Vendors often issue patches before hackers have infiltrated a system.

*Category 17.1* *Penetration*

2003-03-24 **criminal hackers hacking penetration National Security Agency NSA US**

NIPC/DHS

March 20, SecurityFocus — Hackers claim NSA breach. Hackers claim to have compromised a computer at the National Security Agency (NSA). However, instead of obtaining a cache of highly-classified documents about the NSA's global surveillance work, the purported hackers mostly found biographies of agency personnel, and a handful of routine, correspondences between NSA spokespersons and media outlets. Journalist and NSA expert James Bamford says the apparent breach probably isn't a threat to national security. "I certainly don't think that it's acceptable that even unclassified computers can be hacked into there, but it doesn't sound like they've gotten beyond the non-classified computers in public affairs," said Bamford. An e-mail message sent to the hackers' address in Switzerland was not immediately answered Thursday. The group signed their message "Nescafé Open Up", the slogan of an ad campaign for flavored instant-coffee. The hackers' motives are unknown at this time.

*Category 17.1* *Penetration*

2003-04-02 **hacking criminal hacker penetration theft sensitive private information credit card social security**

NIPC/DHS

March 28, The Atlanta Journal-Constitution — Hackers strike Georgia Tech computer, gain credit card data. Computer hackers invaded a computer at Georgia Tech and copied names, addresses and — in some cases — credit card information for 57,000 patrons of the Ferst Center for the Arts in Atlanta. Tech said the database held credit card records for about two-thirds of the 57,000 people. The hackers had access to the computer between February 4 and March 14, when the attack was discovered. There's no evidence any credit card numbers have been used by hackers. Tech sent letters to patrons this week warning of "a potentially serious security breach." Tech's computer security experts discovered the attack through internal monitoring, said Bob Harty, a Tech spokesman.

*Category 17.1* *Penetration*

2003-04-09 **criminal hacking Russia hacker hospital systems Al-Jazeera Trojan access**

NIPC/DHS

April 07, Associated Press — Ely hospital hacker traced to former Soviet Union. A hacker who invaded the computer system at William Bee Ririe Hospital in Ely, Nevada, has been traced to the former Soviet Union, authorities said. The FBI said the hacker used the Web site of Al-Jazeera, the Arab news network, as a conduit to the hospital. Officials at the hospital said patient records are safe, but added that the cyber intruder may have accessed employee Social Security and bank information. Jim Crosley, information technology manager for the Ely hospital, detected the Ely break-in on March 20. He said the system seemed to be protected from attacks, but the FBI lab's analysis of the hospital's hard drives showed a game program, "Blaster Ball," contained a Trojan horse, a hidden code that acted as a beacon and let hackers into the hospital's system. "Two employees admitted downloading the game from the Internet and installing it at a work station," Crosley said. "The Trojan horse reported back to the hackers, and the system was compromised."

*Category 17.1* *Penetration*

2003-05-28 **student break-in systems high school santa cruz California internet service parents credit card information grades e-mail**

NIPC/DHS

May 28, Santa Cruz Sentinel — Hackers threaten confidential student records. Some Santa Cruz County, CA schools and many nationwide use online systems that allow parents to monitor their children's assignments, attendance and marks over the Internet. However, the expulsion of two students who allegedly hacked into the computer system of the county's San Lorenzo Valley High School exposes the the vulnerability of online record systems. Sheriff's investigators allege that in November 2000 and January 2001, the students broke into the school's computer system using stolen passwords. They allegedly changed grades, read staff e-mail and stole credit card information. Students also allegedly carried out "denial of service" attacks on the school's computer system in August and September 2002.

*Category 17.1* *Penetration*

2003-07-30 **Kentucky government computers french hackers user password files computer security Ed Hatchett**

NIPC/DHS

July 30, Associated Press — French hackers break into Kentucky government computers. State investigators in Kentucky believe French hackers have been using the Transportation Cabinet's computers to store pirated computer files including newly released movies and video games. State auditor Ed Hatchett said he believed the hackers entered the system on April 2, and have been using it since. Because they also gained access to the system's administrator and user password files, they could be able to manipulate any state file on the infected network, Hatchett said. Based on the Internet addresses investigators were able to trace, they suspect the hackers were from France, said B.J. Bellamy, chief information for the auditor's office. Other Internet addresses they found were based in Canada and Croatia, he said. Transportation Cabinet inspector General Bobby Russell said the department had already been working to tighten its computer security system before the auditor's findings.

*Category 17.1* *Penetration*

2003-08-04 **Telecast Fiber Systems hacker worker computer deleting valuable files John Corrado remote location modem**

NIPC/DHS

August 04, Boston Business Journal — Former Telecast Fiber worker pleads guilty to hacking. A former employee of Telecast Fiber Systems Inc. in Worcester, MA, pleaded guilty Friday, August 1, in federal court to breaking into the company's computer system and deleting valuable files, according to the U.S. Attorney's office. John Corrado, 35, agreed to pay $10,360, the estimated financial loss suffered by the company. His formal sentencing is scheduled for October 7 where he faces a maximum penalty of one year imprisonment and a fine of $100,000. The U.S. Attorney's office says that in July 1999, about one month after Corrado had stopped working for the company, he accessed the company's network server using a modem from a remote location. The files he deleted included those used for research and development as well as those used by sales reps to demonstrate company products.

*Category 17.1* *Penetration*

2003-08-07 **e-vote hacker break security web server largest electronic voting sensitive information**

NIPC/DHS

August 07, Wired — New security woes for e-vote firm. A hacker has come forward with evidence that he broke the security of a private Web server operated by Diebold Election Systems and made off last spring with the company's internal discussion-list archives, a software bug database and software. The company is one of the largest electronic voting systems vendors, with more than 33,000 machines in service around the country. Director of Communications John Kristoff said the stolen files contained "sensitive" information, but he said Diebold is confident that the company's electronic voting system software has not been tampered with.

[MK asks, "Why? Why is is confident?]

*Category 17.1* *Penetration*

2003-08-07 **hacking hacker attack 2000 computers Stanford University Cedric Bennett infected machines campus**

NIPC/DHS

August 07, The Mercury News — Hacker attack damages 2,000 computers at Stanford. Officials at Stanford University scrambled Thursday, August 7, to repair the damage from a hacking attack that has infected thousands of campus computers. Cedric Bennett, Stanford's director of information security services, said unknown hackers had exploited a newly discovered vulnerability in Microsoft's Windows operating system. About 10 percent of Stanford's 20,000 desktop computers that run Windows were affected. The attack placed a mysterious bit of computer coding on each of the infected machines, which Bennett said the hackers could later activate. University technicians have disconnected the infected machines, used by students, faculty and staff, from the campus network.

*Category 17.1* *Penetration*

2003-08-07 **Acxiom customer information hacker private files clients credit card companies identity theft computer**

NIPC/DHS

August 07, Associated Press — Hacker gets Acxiom customer information. A computer hacker gained access to private files at Acxiom Corp., one of the world's largest consumer database companies, and was able to download sensitive information about some customers of the company's clients, the company said Thursday, August 7. Jennifer Barrett, the company's chief privacy officer, said about 10 percent of the company's customers were affected and that, "it would include some of our larger customers." Acxiom's Website says the company serves 14 of the top 15 credit card companies, seven of the top 10 auto manufacturers and five of the top six retail banks. The individual in police custody is a former employee of one of Acxiom's clients and gained access by hacking encrypted passwords from clients who access the server. Barrett said much of the information taken from the server was encrypted and that the risk of identity theft is slim.

*Category 17.1* *Penetration*

2003-08-21 **Navy purchase cards hackers Department Defense DoD cancelled accounts Citibank gained access Criminal Investigate**

NIPC/DHS

August 21, Government Computer News — Hackers compromise Navy purchase cards. Hackers recently broke into a Navy system and gained access to 13,000 Navy purchase cards, according to Department of Defense (DoD) officials who are investigating the incident. The DoD Purchase Card Program Management Office has issued a release stating that the Navy has cancelled all of its purchase card accounts-about 22,000-to minimize the number of unauthorized purchases, and is working closely with the issuing company, Citibank. "Emergency purchases are being handled on a case-by-case basis to fully support Navy requirements," according to the statement. A DoD team is working to determine how hackers gained access to the system and what needs to be done to fix the breach. A Defense Criminal Investigative team is also pursuing the investigation.

*Category 17.1* *Penetration*

2003-11-12 **criminal hacker hacking penetration Australian Defense top-secret data information file**

NIPC/DHS

November 10, Australian Associated Press — Hackers reach Australian Defense files. Hackers have reportedly accessed top-secret files inside the Australian Department of Defense. "There have been three incidents in which an external security breach has led to unauthorized access to computer systems," Senator Hill had told an inquiry into computer security in the public service. According to the minister, the Defense Department also reported 13 cases since 2000 of its own staff trying to hack into computer systems without authorization. A review of electronic security inside commonwealth agencies has reportedly uncovered a culture of theft and lax security inside the public service. The inquiry comes amid a series of thefts of computers containing classified information from a customs office at Sydney Airport and the Transport Department in Canberra. Submissions by the major departments to the Joint Committee of Public Accounts and Audit has found that more than 1600 computers have vanished since 1998. Senator Hill said three computers stolen in the past two years contained information classified as "secret", but they had been recovered and the risk to national security had been assessed as low, he told the inquiry in a memo.

*Category 17.1* *Penetration*

2003-12-29 **election break-in computers intruder indentified VoteHere Inc. Bellevue**

NewsScan

BREAKING-IN: NOT AN ACCEPTABLE DEBATING TACTIC
VoteHere Inc., a Bellevue, Washington company that markets a security technology for electronic voting, says that U.S. authorities are investigating a break-in of its computers months ago, when someone roamed its internal computer network. VoteHere chief executive Jim Adler says: "We caught the intruder, identified him by name. We know where he lives. We think this is political. There have been break-ins around election companies over the last several months, and we think this is related. I have no problem debating the merits of electronic voting with anyone, but breaking and entering is not an appropriate forum for technology debate." (AP/Washington Post 29 Dec 2003)

# 17.2 Web vandalism

*Category 17.2* *Web vandalism*

2003-05-02 **internet radio station site hacker damage Denver Colorado Larry Nelson w3w3 FBI e-mail**

NIPC/DHS

May 02, Rocky Mountain News — Hackers damage Internet radio site. Hackers broke into the Web site of an Internet radio station in Denver, CO that's sponsoring a Denver conference next week aimed at thwarting computer break-ins. The attack is believed to have caused more than $50,000 in damage. Larry Nelson of the w3w3 network, the target of the attack and sponsor of the conference dubbed "Cyber Security Super Bowl," said the hackers got away with up to 1,000 names and e-mail addresses for people attending the conference. The conference will bring together industry and government experts from around the nation to discuss homeland defense and cybersecurity - a growing field that aims to protect computer systems from hackers. Nelson said the FBI and two cybersecurity firms probing the attack plan to use the case as a model to underscore the threat of Internet-based break-ins.

*Category 17.2* *Web vandalism*

2003-06-26 **cyber thief web addresses los angeles county pornographic e-mail junk Atriva bogus company hijacker**

NIPC/DHS

June 26, Pasadena Star News — Cyber-thief nets 65,000 county Web addresses. An Internet hijacker stole 65,000 Web site addresses belonging to Los Angeles County between April 3 and May 1. The addresses were then sold and used to send pornographic material and junk e-mail, and to try to hack into other computers. No harm was done to the county during the scam. It apparently only took a phone call and follow-up e-mail to the American Registry of Internet Numbers for the hijacker to change ownership of the county's Web addresses into another name, according to the county's Chief Information Officer Jon Fullinwider. The registry, according to county officials, put the addresses into the name of Atriva, which turned out to be a bogus company. An investigation is continuing to find the hijacker.

*Category 17.2* *Web vandalism*

2003-07-02 **warning message 6000 websites hackers challenge.com Critical Infrastructure necessary measures security server**

NIPC/DHS

July 02, Associated Press — Warning of massive hacker attacks. Hackers plan to attack thousands of Web sites Sunday in a loosely coordinated "contest" that could disrupt Internet traffic. Organizers established a Web site, defacers-challenge.com, listing in broken English the rules for hackers who might participate. The Chief Information Officers Council cautioned U.S. agencies and instructed experts to tighten security at federal Web sites. The New York Office of Cyber-Security and Critical Infrastructure Coordination warned Internet providers and other organizations that the goal of the hackers was to vandalize 6,000 Web sites in six hours, and urged companies to change default computer passwords, begin monitoring Web site activities more aggressively, remove unnecessary functions from server computers and apply the latest software repairs. The purported "prize" for participating hackers was 500-megabytes of online storage space, which made little sense to computer experts who said hackers capable of breaking into thousands of computers could easily steal that amount of storage on corporate networks.

*Category 17.2* *Web vandalism*

2003-07-07 **hackers web vigilante-style attacks break-ins online vandalism small internet sites disrupted**

NIPC/DHS

July 07, Associated Press — Hackers limit disruption to small Internet sites. A battle among hackers erupted on the Internet yesterday as some factions disrupted a loosely coordinated effort among other groups trying to vandalize Web sites around the world. Unknown attackers for hours knocked offline an independent security Web site that was verifying reports of online vandalism and being used by hackers to tally points for the competition. U.S. government and private technology experts warned last week that such vandalism was likely. After three such vigilante-style attacks, the hacker organizer extend the contest until 6 p.m. yesterday. With continued attacks disrupting the ability of vandals to claim credit for their break-ins, some experts said it could be later this week before damage from the weekend's hacking would be known. There were no reports of vandalism involving larger, more well-known Internet sites, which may be a testament to improved online security at large companies, government agencies and organizations.

*Category 17.2* *Web vandalism*

2003-07-14 **ten internet sites hacker destroy Sudanese major corporations Airlines Al-Sahafa Khartoum University Aptec Computers revenge**

NIPC/DHS

July 14, Arab Times — Hacker destroys ten Internet sites. A Sudanese hacker claimed to have destroyed the Internet websites of 10 major corporations, one of which is the Sudanese Airlines, Al-Sahafa newspaper said Sunday. The hacker sent an e-mail to Sudanese Airlines saying that by hacking the company webpage he is taking revenge for the families of victims of the plane crash that took place last Tuesday killing 115 passengers. The hacker claimed to have destroyed the websites of Khartoum University, Aptec Computers and the Sudanese Internet Company. He said he is working on the destruction of more websites.

*Category 17.2* *Web vandalism*

2003-12-02 **domain name Website registry .name hacked Global Name Registry GNR**

NIPC/DHS

December 01, The Register — Website .name registry hacked. The Website of the .name registry was hacked over the weekend through an Apache exploit. London-based Global Name Registry (GNR) was updating its Apache and PHP system when hackers broke into the system and replaced the frontpage index file. The hackers didn't manage to access the system and no data was lost, GNR's president Hakon Haugnes said. The site was taken offline and was back up by Sunday, November 30 with added security. "We were adding patches but in spite of that someone managed to get to the index file," said Haugnes. The .name domain—one of seven approved by ICANN in 2001—now has around 100,000 registrants.

*Category 17.2* *Web vandalism*

2003-12-19 **NASA Websites hacked Brazilian defacement vandalism Netcraft PHP**

NIPC/DHS

December 18, ComputerWorld — NASA sites hacked. Thirteen NASA Websites were defaced Wednesday by a Brazilian crew dubbed drwxr, according to a statement from Zone-H, an organization that monitors hacking. Zone-H said the defacer apparently modified the index pages on the sites to express his opinion about the Iraq war. The main NASA Web site did not appear to be among those hit by the attack. Zone-H, citing Netcraft Ltd., a British Internet consultancy, said the sites were running the Apache 1.3.27 Web server with PHP (an open-source scripting language often used to create dynamic Web pages) and several Apache modules on a Linux system. "We can suppose that the server was remotely compromised using a vulnerability in a PHP script, then the defacer probably gained root privileges using the local root exploit for the Linux kernel 2.4.22 published by iSEC Security Research last week." NASA spokesman Brian Dunbar confirmed that the sites had been hacked and defaced and said the agency had taken them offline. The hacked NASA Web sites include its Computing, Information and Communications Technology Program site; the NASA Advanced Supercomputing Division; the NASA Information Power Grid; and the NASA Research & Education Network.

# 17.3 Phreaking

*Category 17.3* *Phreaking*

2003-02-18 **telephone PBX phone fraud hacking Taiwan credit card information stolen scam**

NIPC/DHS

February 14, SC Infosecurity News — Taiwanese telco virtual operator system hacked. Chungwa Telecom of Taiwan has issued warnings about its virtual telephone operator service, which allows the company's staff to act as PBX operators for those Taiwanese companies without their own operator staff. Hackers have been taking advantage of companies that had not changed their control PIN from the default settings of 0000, 9999 or 1234. The result has been that hackers have been able to intercept calls originally destined to be handled by Chungwa's operators, routing to their prepaid (and anonymous) mobile phones. The hackers are said to have taken card details from callers and used the information to swindle them. Taiwan's Morning Post newspaper says that Chungwa Telecom has not revealed the scale of the problem, or the names of the companies affected, although the paper says the firms are known to be in the courier and allied business markets. The paper adds that affected customers' claims have been settled, while police are investigating the scam. The firms affected by the scam are said to have suspended their use of the virtual operator facility, switching back to using their own staff to answer calls.

---

*Category 17.3* *Phreaking*

2003-05-16 **New Jersey company illegal advertising pornographic internet charging telephone connection dial-up**

NewsScan

13 STATES SUE OVER POP-UP ADS
Thirteen states have sued a New Jersey company that allegedly billed Internet users who tried to close pop-up windows advertising p*rnographic Web sites. The lawsuit maintains that Alyon Technologies automatically connected users to its toll telephone number when they tried to close the ads, and then charged them $5 a minute, resulting in bills ranging from $14 to more than $1,000. "The way this organization has allegedly been doing business is illegal, irresponsible and an outrageous misuse of Internet technology," said Wisconsin Attorney General Peg Lautenschlager. Joining Wisconsin in the suit are California, Connecticut, Florida, Illinois, Kentucky, Missouri, New Jersey, Ohio, North Carolina, Nebraska, Texas and West Virginia. (AP 16 May 2003)

---

*Category 17.3* *Phreaking*

2003-06-10 **compromising PBX Private Brach Exchange systems voice mail internet service providers overseas Bill Murray FBI 911 center**

NIPC/DHS

June 10, Washington Post — Phone networks open doors for hackers. Federal law-enforcement officials said last week that they are tracking numerous reports of hackers who gain access to corporate voice mail and telephone systems to launch Internet attacks. The hackers, according to the Department of Homeland Security (DHS), tap into corporate phone systems, or private branch exchange (PBX) systems, using them to make long-distance calls to Internet service providers in other cities or overseas. Hackers compromising PBX systems can use them as entryways into computer systems, said Lisa Pierce, a research fellow for the Giga Information Group. From there they can steal corporate information, eavesdrop on conversations and create havoc on the system because no one knows where the attacks are coming from, she said. FBI cyber division spokesman Bill Murray said poorly secured PBX systems also present a serious national security threat. A hacker could use a compromised PBX system to route dozens of calls simultaneously to an emergency 9-1-1 center, overloading the emergency call center and preventing real emergency calls from getting through. A tutorial on locking down PBX and voicemail systems is available from the National Institute of Standards & Technology at:
http://www.csrc.nist.gov/publications/nistpubs/800-24/sp800- 24pbx.pdf

---

*Category 17.3* *Phreaking*

2003-06-20 **Indian cellular fraud Hutchison Essar telecommunications company New Delhi**

NIPC/DHS

June 20, SC Infosecurity News — Four men charged in major Indian cellular fraud. A U.S.-based IT professional and three Indian citizens have been arrested, charged with defrauding Hutchison Essar, an Indian telecommunications company, of around $200,000. Delhi Police arrested two of the men in the city of New Delhi, while the other two, including the U.S. citizen originally from India, were arrested in the city of Kochi at the start of June. The losses were incurred after the men conspired to activate and use 19 GSM SIM cards in the U.S., making significant volumes of calls back to India and other countries. The case highlights the delays that some cellular carriers experience before forwarding roaming call data on to other networks in other countries. While all GSM networks authenticate roaming SIM card accounts with their home network before each roamed call is connected, information on the actual value of the call is not shared in real time.

*Category 17.3* *Phreaking*

2003-06-25 **phone phreaking victims pay AT&T**

NIPC/DHS

April 21, New York Times — AT&T trying to collect bills from the victims of hackers. The city of East Palo Alto, CA, is battling with AT&T over who is responsible for a $30,000 long-distance phone bill that resulted from voice mail hacking. Last summer, hackers in the Philippines and Belgium penetrated the agency's voice mail system, operated by SBC Communications, the local phone service provider, by figuring out system pass codes. AT&T wants the city to pay the bill for the fraud, which it says was the customer's responsibility to prevent. It offered a settlement in which it would pay 30 percent of the charges, but the city says the company should pay the whole thing. Voice mail hackers have discovered that if voice mail customers do not change their default pass code when the system is set up, they can sometimes break in by figuring out assigned pass codes. Hackers breaking into the system then change the outgoing message to one that automatically accepts collect calls. Once connected, the hackers can leave the line open for hours, charging up enormous bills. AT&T now requires that individuals accepting collect calls, besides having to respond "yes" when prompted, also enter a three-digit number.

June 25, SecurityFocus — AT&T lets phone fraud victims off the hook. AT&T said Wednesday that it would forgive all of the outstanding long distance charges that the company had been trying to collect from victims of the so-called "Yes-Yes" voicemail subversion fraud. Last year fraudsters began cracking weak and default PINs on individual and small business voice mail boxes provided by local phone companies, then changing the outgoing messages to say "yes, yes, yes" over and over again. The newly-agreeable voice mail could then be used for third-party billings. The scam left scores of victims holding liable for thousands of dollars of long distance calls they never made-typically between $8,000 and $12,000. AT&T insisted that the victims pay up, arguing that it was the consumer's poor voice mail security that was at fault. When pressed, the company sometimes offered to absorb 35% of a fraudulent billing. The company announced Wednesday that it's will abandon those collection, but the amnesty offer only applies to past victims of this particular type of fraud.

*Category 17.3* *Phreaking*

2003-09-11 **Voice mail hijacked passwords small businesses outgoing messages protection accept collect calls Yes positive**

NIPC/DHS

September 11, KIRO TV (Seattle, WA) — Voice mail hijacked to accept collect calls from crooks. The words "Yes, Yes, Yes" usually mean something positive, but not in this case. A new con uses these three words to rip off voice mail users. Maureen Claridge says she got stuck with a large phone bill because someone hijacked her voice mail. Maureen's voice mail usually sounded like this: "This is Maureen; I'm in the office, but on the other line, leave a number and I'll get back to you as soon as I can." But a crook hacked into it and recorded the words "yes, yes, yes." The crooks target people who have simple voice mail passwords. They use the password to hack into the system and change the message to accept collect calls. Then they ask you a series of questions, usually three, and the answer is "yes, yes, yes." The voice mail telephone company says small business people are often targeted, because they don't answer their phones on the weekend. To protect yourself, check your outgoing message from time to time and change your password to something only you would know.

# 18.1 Theft

*Category 18.1* *Theft*

2003-01-10 **computer data theft military member information health care records**

NIPC/DHS

January 09, Government Computer News — DOD says system pilot not affected by TriWest thefts. The December 14 theft of computer equipment containing information on more than 500,000 military members poses no threat to the Composite Health Care System II, the Defense Department's pilot computerized medical system still in development, a Defense health official said yesterday. The computers were stolen from a TriWest Healthcare Alliance office in Phoenix. TriWest provides managed health care to 1.1 million military personnel and their families in 16 states for DOD's health care service, known as the Tricare Management Activity. But Tricare is not part of CHCS II, the official said. "There is no relationship between those two (systems)," said Dr. William Winkenwerder, Jr., assistant secretary of Defense for health affairs. Furthermore, Winkenwerder said, CHCS II information is stored at "very secure sites" and that DOD had implemented steps to increase CHCS II security. CHCS II eventually will store the records of more than 8.5 million military personnel and their families, allowing doctors to retrieve medical histories on their patients. Defense has approved use of CHCS II at seven military hospitals across the country. The thefts at TriWest are still unsolved.

*Category 18.1* *Theft*

2003-04-03 **computer data theft sensitive critical information radioactive waste details**

NIPC/DHS

April 02, Associated Press — Thieves take computers containing details on radioactive material. Eight state-owned computers containing details on all of the New Mexico companies that use radioactive material have been stolen, officials said Tuesday. The names, addresses and phone numbers of more than 210 businesses are contained in the stolen computers, along with what radioactive materials each is licensed to have, said Bill Floyd, manager of the state Environment Department's Radiation Control Bureau. Thieves took the eight computer towers from the bureau's office in Santa Fe either Thursday night or early Friday. While the files are legally accessible to the public, anyone seeking them would need to do so under the Freedom of Information Act, Floyd said. He said he believed the culprits were seeking the machines themselves — not the data in them.

# 18.2 Loss

*Category 18.2* *Loss*

2003-10-16 **top data loss disasters**

NewsScan

TOP 10 DATA DISASTERS
Although machine failure is at fault for the majority of lost data disasters, humans are increasingly culpable as well, according to recovery experts at Kroll Ontrack. "Despite being the easiest problem to prevent, we are seeing more cases where human error is to blame. Interestingly, we see a 15 to 20% increase in calls to recover lost data on Mondays. This could be a result of the rush to complete work and leave early for the weekend on Friday afternoons, as well as a lack of staff concentration on Monday mornings," says a Kroll spokesman. The Top 10 list of unusual data loss stories includes laptops being shot or thrown against the wall in a fit of e-rage; laptops suffering spills of red wine or latte because users were "drinking on the job," laptops falling off mopeds or car roofs, then being crushed by oncoming traffic; and PCs being thrown out a window or into a river to destroy evidence of theft or fraud. Our favorite? The laptop that slipped into the bathtub with its owner while he was working on accounts. Amazingly, Kroll Ontrack says in all these cases, it was able to rescue and restore computer files. (BBC News 16 Oct 2003)

# 19.1 Software piracy

*Category 19.1* *Software piracy*

2003-06-24 **Microsoft worker $17m racket office exchange SQL server XP Richard Gregg internal store program coordinator**

NIPC/DHS

June 24, The Register — MS worker 'ran' $17m software racket. A Microsoft worker has been charged with stealing $17 million of software from Microsoft's internal store. Richard Gregg, a Windows program coordinator, has pleaded not guilty to 62 counts of mail and computer fraud. From January to October 2002, Gregg allegedly ordered 5,436 copies of software such as Windows XP, SQL Server, Exchange and Office which he subsequently resold.

*Category 19.1* *Software piracy*

2003-12-01 **asian pirate longhorn microsoft operating system secure fewer annoying reboots**

NewsScan

ASIAN PIRATES HAWKING 'LONGHORN' OPERATING SYSTEM
Microsoft's next-generation operating system, code-named "Longhorn," won't be released before 2005, but an early version is already on sale in southern Malaysia for $1.58 (6 ringgit). The software was demonstrated and distributed at a conference for Microsoft programmers in October, but the company's corporate attorney says, "It's not a ready product. Even if it works for awhile, I think it's very risky" to install it on a home or office computer. Longhorn purportedly promises new methods of storing files, tighter links to the Internet, greater security and fewer annoying reboots. (Reuters 1 Dec 2003)

# 19.2 Music piracy

*Category 19.2* *Music piracy*

2003-01-31 **copyright intellectual property music piracy prosecution investigation legal proceeding injunction subpoena identity ISP Internet service provider**

NewsScan

MUSIC INDUSTRY PRESSURES VERIZON ON FILE-SWAPPER'S IDENTITY
The Recording Industry Association of America is pressuring a federal judge to force Verizon to reveal the identity of an Internet service subscriber accused of illegally trading copyrighted songs. Verizon general counsel Sarah Deutsch says if the judge capitulates, it would set a precedent that would harm the privacy rights of Verizon's ISP customers and could force other ISPs to give up the names of subscribers without judicial review. Verizon has already agreed to hand over the information if the RIAA files a separate "John Doe" suit against the alleged file-swapper, but the RIAA refused, saying that anti-piracy laws don't require a separate lawsuit. The Verizon subscriber who's the focus of the controversy is accused of sharing thousands of songs on the Kazaa network, and is located in the Pittsburgh area. Deutsch pointed out that the person in question may be totally unaware of the dispute. "Our general policy is to inform a user when we receive a subpoena. Since in our view this isn't valid, we haven't gotten the customer involved in the debate." (AP 4 Oct 2002)
http://apnews.excite.com/article/20021004/D7MENVS00.htm

COURT ORDERS INTERNET PROVIDER TO IDENTIFY A SUBSCRIBER
To facilitate the enforcement of the 1998 Digital Millennium Copyright Act, a federal district court judge in Washington has ordered Verizon Communications to identify a subscriber whom the Recording Industry Association of America (RIAA) suspects of using to Internet to make available unauthorized copies of several hundred copyrighted songs. The ruling is significant for at least two reasons. First, it shows that the recording industry is now targeting not only big companies accused of large-scale copyright violations but also individual violators. Second, it indicates that a willingness by the court to compel Internet service providers to yield subscriber information without requiring a copyright holder to file a lawsuit. (New York Times 22 Jan 2003)

VERIZON GOES TO COURT TO DEFEND CUSTOMER PRIVACY
Verizon Communications is asking a federal appeals court to declare unconstitutional a lower-court decision that ordered it to reveal the identity of a customer suspected of downloading copyrighted music files over the Internet. Verizon deputy general counsel John Thorne says, "I see a great jeopardy of privacy for people who are not doing anything wrong," and notes the lower court's ruling would make it possible for "strangers, stalkers, telemarketers, pollsters, creditor and anybody else" to obtain the identity of almost any Internet user. "No matter where you go, your identity can be compelled to be revealed under this process." (Reuters/USA Today 30 Jan 2003)

---

*Category 19.2* *Music piracy*

2003-04-03 **agreement recording industry Internet webcasters**

NewsScan

RECORDING INDUSTRY, WEBCASTERS REACH ROYALTY PACT
In a move to head off a potentially difficult arbitration process, the recording industry and Internet radio operators have agreed on terms for paying royalties to labels and artists for songs played on the Web. The rate set for 2003-2004 is nearly identical to that set by the Librarian of Congress for 2002 — webcasters can either pay a rate of 0.0762 cents per song per listener, or 0.0117 cents per listener hour. Webcasters that sell subscriptions to listeners can also choose to pay 10.9% of their subscription revenue. Both groups appeared to be satisfied with the agreement, which will save them millions of dollars in legal fees by avoiding arbitration. (Wall Street Journal 3 Apr 2003)

---

*Category 19.2* *Music piracy*

2003-04-04 **music piracy lawsuit RIAA**

NewsScan

MUSIC PIRACY VIOLATIONS: $150K A SONG
The Recording Industry Association of America (RIAA) has filed lawsuits against four students it says it misappropriated academic computing resources to "illegally distribute millions of copyrighted works over the Internet." Two of the accused students are enrolled at Rensselaer Polytechnic Institute, one student is enrolled at Princeton, and the fourth is at Michigan Technological University. If they are convicted, they could be fined as much as $150,000 for each song they illegally traded. Digital media analyst Phil Leigh says of the RIAA's action: "This is just another step in the direction of demonstrating to the public that there will be penalties for what they consider to be copyright violations. I think they're attempting to take a carrot-and-stick approach here. They're whacking a few people with a stick now. And the carrot is the more liberal rules relating to label-backed subscription online services." (San Jose Mercury News 4 Apr 2003)

*Category 19.2* *Music piracy*

2003-04-14 **Apple legal music download iTunes server**

NewsScan

APPLE TO LAUNCH ITS OWN MUSIC SERVICE
Apple Computer is launching its own music service in the next few weeks, offering users songs from all five major record labels. The new music service will be integrated with Apple's iTunes music software, which is used to organize and play MP3 files on Macs. Rather than following the subscription-based model adopted by the record-label-backed pressplay and MusicNet services and others, Apple plans to sell its songs individually for about 99 cents a track. And while the service is rumored to be more consumer-friendly than many of the other legitimate online music services, it's available only to Mac users — a group that comprises about 5% of the global market. (Wall Street Journal 14 Apr 2003)

*Category 19.2* *Music piracy*

2003-04-25 **music industry lawsuit RIAA DMCA Verizon intellectual property rights**

NewsScan

JUSTICE DEPT. SUPPORTS MUSIC INDUSTRY IN VERIZON CASE
The U.S. Justice Department filed a brief Friday supporting the effort by the Recording Industry Association of America to force Verizon Internet Services to identify a subscriber suspected of violating copyrights by offering more than 600 songs online. Verizon had asked a federal judge to block the subpoena, arguing that it violated the First Amendment's "protection of the expressive and associational interests of Internet users." However, the Justice Dept. filing said the subpoena, which was sought under the Digital Millennium Copyright Act, was legal. The judge will now have to decide the constitutional issue, which is viewed as an important test of the DMCA's applicability in Internet copyright cases. The filing comes as the recording industry is becoming increasingly aggressive in its quest to identify and punish music "pirates." (AP 19 Apr 2003)

JUDGE SAYS IT AGAIN: VERIZON MUST REVEAL CUSTOMERS' IDENTITIES
U.S. District Court Judge John Bates has reaffirmed his previous ruling requiring Verizon to reveal to the Recording Industry Association of America (RIAA) the names of two Verizon customers accused by RIAA of illegally downloading hundreds of copyrighted songs from the Internet. The ruling will probably be appealed to the U.S. Supreme Court, with Verizon asserting that the subpoena is invalid, since it relies on the Digital Millennium Copyright Act (DMCA), yet falls outside the scope of DMCA, which does not cover material that is merely transmitted over a network, and not stored on it. Verizon is asserting that the protection of its customers' privacy takes precedence over the subpoena that was issued. (Internet.com 25 Apr 2003)

*Category 19.2* *Music piracy*

2003-04-26 **music services not responsible piracy intellectual property rights copyright peer-to-peer P2P**

NewsScan

GROKSTER AND STREAMCAST: WE DIDN'T DO IT
A federal judge has ruled that two Internet music services that offer peer-to-peer software used by millions of people to share copyrighted music illegally are not themselves guilty of copyright infringement. The judge's reasoning was that, since the technology is also used for many perfectly legal purposes, the two services should not be held responsible in those cases when it happens to be used for illegal purposes. The ruling will be appealed. The music industry insists that the two services, Grokster and StreamCast, are overwhelmingly used by people to exchange copyrighted material, and that legal uses are insignificant. Many industry analysts predict that the industry will soon have to change fundamentally and begin providing inexpensive, easy-to-access music over the Internet. (New York Times 26 Apr 2003)

RULING FORCES ENTERTAINMENT INDUSTRY TO RETHINK STRATEGY
Friday's ruling exonerating Grokster and StreamCast of charges of violating copyright laws will force the entertainment industry to broaden its battle against Internet piracy on three fronts: the courts, in Congress and in the marketplace. In addition to appealing the most recent ruling, the movie studios and record labels may start suing individuals who trade copyrighted files. One music label president, who spoke on condition of anonymity, says the ruling leaves industry no choice: "It makes them [consumers] angrier, but we have no other path right now. It's ridiculous what we're doing, but we have so few options." The industry is also lobbying Congress for stricter anti-piracy laws, and at the same time must find a way to give consumers a compelling alternative to piracy: "The most effective way to combat unlicensed sites is to offer licensed services with reasonable consumer rules at attractive prices," says a digital media analyst at Raymond James. "This attempt to enforce prohibition is a failure." The fact that many of the illegitimate sites are polluted with viruses, pop-up ads and low-quality files creates an opportunity for industry to offer a high-quality, hassle-free online service, he adds. (Los Angeles Times 26 Apr 2003)

*Category 19.2* *Music piracy*

2003-04-28 **music piracy countermeasure fails artist Madonna profanity**

NewsScan

MADONNA FIGHTS PIRACY WITH PROFANITY
Madonna and Warner Music Group decided to play a trick on music pirates and hackers responded by defacing her Web site and offering yet-unreleased songs for downloading. It all started when Madonna lent her voice to a popular antipiracy technique. "Decoy" files purportedly carrying her new songs were uploaded onto peer-to-peer file-sharing services, but when unsuspecting fans downloaded them, they heard Madonna saying "What the f*** do you think you're doing??" While some music fans got angry, others saw a creative opportunity and the now-infamous phrase is turning up in dozens of remixes and the computer-aided musical collages called mashups. "Madonna was trying to put one over on the kids… and they in turn wanted to let her know that she's not in as much control as she thinks she is," says TechTV's Morgan Webb. (CNN.com/Reuters/Hollywood Reporter 28 Apr 2003)

---

*Category 19.2* *Music piracy*

2003-04-29 **music downloading legal iTunes Apple Steve Jobs**

NewsScan

JOBS: 'WE BELIEVE IN THE FUTURE OF MUSIC'
Apple Computer launched its iTunes Music Store on Monday in a move that CEO Steve Jobs called "a major milestone in the evolution of the real digital music age. We believe in the future of music." iTunes offers 200,000 downloadable songs for 99 cents apiece and is the first industry-endorsed online music service to forgo subscription fees in favor of a "pay-per-download" business model. Jobs said the real draw for music fans will be the easy-to-use interface and high-quality files available at the iTunes Music Store. "Using current piracy services is very frustrating. It takes you 15 minutes to find and download a song of reasonable quality that doesn't have the last four seconds cut off or a break in the middle. We offer super-fast, high-quality downloads with pristine encoding. You certainly can't get that on any other service — pirate or legal." (Los Angeles Times 29 Apr 2003)

---

*Category 19.2* *Music piracy*

2003-05-03 **music wars piracy freeze lock computers halt downloads intenret connections attack Stanford Law School**

NewsScan

CYCLES OF VIOLENCE IN THE MUSIC WARS
The record industry's options for fighting illegal music downloads from the Internet include some that may be illegal, such as attacking personal Internet connections to slow or halt the downloads, or the use of software called "freeze" that locks up a computer system for a certain minutes or hours and risks the loss of data, as well as software called "silence" that would scan a computer's hard drive for pirated music files and attempt to delete them, at the risk of deleting legitimate music files as well. Stanford Law School professor Lawrence Lessig, who specializes in Internet copyright issues, says: "Some of this stuff is going to be illegal. It depends on if they are doing a sufficient amount of damage. The law has ways to deal with copyright infringement. Freezing people's computers is not within the scope of the copyright laws." (New York Times 3 May 2003)

---

*Category 19.2* *Music piracy*

2003-06-05 **Verizon identity personal information music RIAA illegal download pirated**

NewsScan

VERIZON AGREES TO REVEAL IDENTITIES OF SUBPOENAED CUSTOMERS
Following a federal appellate court's rejection of its efforts to resist a subpoena, Verizon has relented and is releasing the names of four individuals alleged to have illegally downloaded copyrighted music. The music-downloading lawsuit was filed by the Recording Industry Association of America (RIAA), whose president, Cary Sherman, says: "The Court of Appeals decision confirms our long-held position that music pirates must be held accountable for their actions and not be allowed to hide behind the company that provides their Internet service." Privacy advocates and Internet service providers are unhappy with the decision, and some are urging new legislation to prevent the release of the identities of previously anonymous Internet subscribers; however, entrepreneur Jorge A. Gonzales of Zeropaid.com thinks that new laws will be unnecessary: "The technology will move faster than the court systems. The new programs being developed are going to mask users. By the time Verizon has to start turning over a lot of names, the identities of users will be unknown." (New York Times 5 Jun 2003)

---

*Category 19.2* *Music piracy*

2003-06-26 **recording industry RIAA KaZaA Grokster file sharing peer-to-peer**

NewsScan

RECORDING INDUSTRY TO MUSIC SWAPPERS: WE'RE GONNA GET YOU
Cary Sherman, president of the Recording Industry Association of America (RIAA), says his organization plans to file at least several hundred lawsuits within the next 10 weeks against individual computer users who share substantial amounts of copyrighted music online. The RIAA, which represents the five major music labels, will start gathering evidence against file-swappers by using software to scan the public directories of peer-to-peer networks such as KaZaA and Grokster. Sherman says, "A lot of people think they can get away with what they are doing because peer-to-peer file sharing allows them to hide behind made-up screen names. They are not anonymous. The law is very clear. What they are doing is stealing." (New York Times 26 Jun 2003)

---

*Category 19.2* *Music piracy*

2003-07-14 **intellectual property copyright P2P peer-to-peer file-sharing RIAA lawsuits**

NewsScan

DECLINE IN FILE-SWAPPING ATTRIBUTED TO RIAA THREATS
The recording industry's threats to sue individuals who involved in illegal music file-swapping are generating results, according to Nielsen/NetRatings, which reports use of popular file-trading sites such as Kazaa and Morpheus have dropped by 15% since the end of June. "I would definitely say it's not a coincidence that the numbers fell that far," says a Nielsen/NetRatings senior analyst. "A drop this significant probably has some kind of external cause." The Recording Industry Association of America issued its threat on June 25 and says it plans to start filing copyright infringement lawsuits next month. Officials at StreamCast Networks, which distributes Morpheus software, disputed the Nielsen/NetRatings findings, maintaining that there had been no perceptible decline in the number of visitors to its site, and the company plans to release a new version of Morpheus that will enable users to upload and download files through proxy servers in an effort to shield their identities online. (CNet News.com 14 Jul 2003)

---

*Category 19.2* *Music piracy*

2003-07-16 **music download service Buy.com legal**

NewsScan

BUY.COM'S NEW MUSIC DOWNLOAD SERVICE
Buy.com, a mainstream Internet shopping site, will soon be offering a new music download service that (like the Apple iTunes Music Store) will sell individual music tracks without collecting an up-front monthly subscription fee. Since Apple has not yet developed a Windows version of its service, the PC music market offers a broad target for a company such as Buy.com, which will try to surpass its much larger rival, Amazon.com, which has 34.5 million monthly visitors compared to Buy.com's 3.1 million, according to Nielsen/NetRatings. (San Jose Mercury News 16 Jul 2003)

---

*Category 19.2* *Music piracy*

2003-07-16 **P2P peer-to-peer file-sharing corporations traffic slowdown**

NewsScan

P2P PERVADES THE CORPORATE SUITE
Peer-to-peer file-swapping software is deeply entrenched in corporate networks, according to a study of 560 companies by Canadian firm AssetMetrix, which found that 77% of the companies reported P2P applications such as Kazaa and Morpheus installed. Among companies with more than 500 employees, 100% had at least one P2P program installed. "Corporations are frantic about how to rein in some control over this," says AssetMetrix president Paul Bodnoff. "Like with software licenses, most companies want to be on the right side of the law. The challenge is how they do that." In addition to worries over legal liability for employee's file-swapping activities, corporate IT managers say they're also concerned about the drain of resources caused by such activities. Transfers of large media files can bog down legitimate data traffic, and P2P software can also allow viruses to worm their way onto the systems, compromising network security. (CNet News.com 16 Jul 2003)

---

*Category 19.2* *Music piracy*

2003-07-18 **intellectual property peer-to-peer P2P copyright RIAA lawsuits ISP caching**

NewsScan

P2P CACHING PUTS ISPs AT RISK FOR COPYRIGHT VIOLATION
Swedish firm Joltid is marketing its PeerCache technology, which is designed to ease network traffic gridlock by caching frequently traded digital files within file-swapping systems. The software, which has been licensed by three major European ISPs, is built to work with FastTrack, one of the most popular P2P protocols which forms the basis for applications such as Kazaa and iMesh. PeerCache plugs into the ISP network and temporarily caches FastTrack P2P traffic, easing the bandwidth crunch. However, the technology is raising the hackles of the recording industry, which warns that even temporarily storing copyright files could make ISPs accomplices in illegal file trading. "Just using the word 'caching' doesn't mean that the service is automatically exempt from copyright liability," says the IFPI, the international counterpart to the U.S.'s RIAA. Meanwhile, Joltid founder Niklas Zennstrom, who co-founded Kazaa, maintains that European Union laws allow ISPs to temporarily cache traffic on their servers regardless of the file's legal status. "One should bear in mind that [whether] an ISP is caching a file or not does not make the file more or less available for end users. It only impacts the load on the ISP's network. Thus, by caching P2P traffic, ISPs are not encouraging or [discouraging] users to download files. It is just a way for the ISP to organize their network." Zennstrom says PeerCache is being tested by a number of European ISPs. (CNet News.com 18 Jul 2003)

---

*Category 19.2* *Music piracy*

2003-07-21 **intellectual property RIAA lawsuits peer-to-peer file-sharing**

NewsScan

OPPOSING ARMIES LINE UP IN INTELLECTUAL PROPERTY WAR
In an effort to battle Internet theft of copyrighted music, the Recording Industry Association of America (RIAA) has subpoenaed 871 individuals, and demanded that the Internet service providers used by those individuals reveal personal data about them. Verizon's Sarah Deutsch complains, "We've received 150 subpoenas in two weeks. This type of activity is unprecedented." Fred von Lohmann of the Electronic Frontier Foundation says, "The privacy questions are huge. They treat everyone as a copyright infringer, and you're assumed guilty until proven innocent." (USA Today 21 Jul 2003)

---

*Category 19.2* *Music piracy*

2003-07-23 **intellectual propery copyright RIAA file-sharing peer-to-peer P2P universities subpoenas**

NewsScan

SCHOOLS RELUCTANT TO ENFORCE RIAA FILE-SWAP SUBPOENAS
Citing procedural concerns, MIT and Boston College have asked a court to quash subpoenas requesting that they provide the Recording Industry Association of American the identification of certain students accused of illegally downloading copyrighted music. The two institutions merely said that the subpoenas didn't allow for adequate time to notify the students, and a Boston College official explained: "We're not trying to protect our students from the consequences of cspyright infringement. Once the subpoenas are properly filed, we will comply with the subpoenas." The RIAA is trying to discourage illegal file-sharing by pursuing not only large-scale downloaders but small-time ones as well. Some schools (for example, Northeastern University) are complying with the subpoenas without protest. (AP/San Jose Mercury News 23 Jul 2003)

---

*Category 19.2* *Music piracy*

2003-07-24 **copyright intellectual property RIAA lawsuits MP3 P2P peer-to-peer**

NewsScan

RIAA UNLEASHES LAWYERS ON PARENTS, GRANDPARENTS
The Recording Industry Association of America is targeting parents and, in some cases, grandparents of youthful music file-swappers, threatening them with legal action over their offspring's music-sharing activities. The subpoenas have come as a shock to both parents and their children, who assumed that using cryptic nicknames such as "hottdude0587" guaranteed them anonymity. The RIAA says it has cited the numeric Internet addresses of high-volume music downloaders on its subpoenas and can track users only by comparing those addresses against subscriber records held by ISPs, but the Associated Press had no trouble using those addresses and some details culled from the subpoenas to identify and locate some of the targets. Outside legal experts warned that the music industry should move carefully in selecting targets for prosecution. "If they end up picking on individuals who are perceived to be grandmothers or junior high students who have only downloaded in isolated incidents, they run the risk of a backlash," says one Hollywood attorney. (AP 24 Jul 2003)

---

*Category 19.2* *Music piracy*

2003-07-28 **EFF RIAA subpoena database copyright intellectual property P2P peer-to-peer lawsuits**

NewsScan

EFF SETS UP DATABASE OF RIAA SUBPOENA TARGETS
The Electronic Frontier Foundation has stepped right into the middle of the file-swapping fray, offering potential targets of the subpoenas recently issued by the Recording Industry Association of America (RIAA) a way to check and see if they're on the list.
We hope that the EFF's subpoena database will give people some peace of mind and the information they need to challenge these subpoenas and protect their privacy," says EFF senior counsel Fred Von Lohmann. The database allows people to check their file-sharing "handle" (e.g., hottdude123) against a list of subpoenas issued. If they see their name, they can access an electronic copy of the subpoena, which includes the name of their ISP, a list of songs pirated and the Internet address of the user. By the end of last week, nearly 900 subpoenas had been issued, with 75 additional being added every day. The subpoenas are intended to force the ISPs to divulge the identity of the alleged file-swappers and the RIAA is threatening lawsuits, claiming damages ranging from $750 to $150,000. "The recording industry continues its futile crusade to sue thousands of the more than 60 million people who use file-sharing software in the U.S.," says Von Lohmann. The EFF has teamed with the U.S. Internet Industry Association to set up a Web site called subpoenadefense.org, which provides information on lawyers and other resources for those facing legal action. (BBC News 28 Jul 2003)

*Category 19.2* *Music piracy*

2003-07-28 **file-sharing P2P intellectual property peer-to-peer tips avoid lawsuit RIAA music piracy**

NewsScan

EXPERTS SHARE TIPS ON AVOIDING FILE-SHARING LAWSUITS
In the wake of the recording industry's unprecedented moves against individual consumers to enforce copyright laws, legal experts are warning people who engage in music file-swapping to immediately stop sharing potentially infringing files or to disable file-sharing software. "…(T)he first thing you should do if you want to be off (the RIAA's) radar is to stop uploading," says Electronic Frontier Foundation senior intellectual property attorney Fre von Lohmann. But whether that strategy will prove successful is uncertain, because the RIAA has been collecting snapshots of individuals' shared file folders since June 26 to use as evidence lawsuits. Even if a file-swapper has since deleted those files, "that snapshot establishes enough evidence to establish infringement," says copyright expert Evan Cox. An RIAA spokeswoman says her group might be "willing to talk settlement" if a file-sharer has erased the evidence, but that will be considered on a case-by-case basis. The RIAA is using a provision included in the 1998 Digital Millennium Copyright Act to issue subpoenas requiring ISPs to disclose the names of suspected infringers, raising the stakes in its battle against unauthorized use of its copyrighted music. "What I think they're going to do is start suing moms and dads and families across America," says California attorney Ira Rothken. "They could lose their house or lose their ability to send their kids to college. That is not the intent of copyright statutes, to bankrupt a middle-class family." (San Francisco Chronicle 28 Jul 2003

*Category 19.2* *Music piracy*

2003-08-21 **music download RIAA subpoena lawsuit**

NewsScan

LISTENING IN THE DARK: 'JANE DOE' WANTS TO REMAIN ANONYMOUS
Lawyers for an anonymous Verizon Communications customer known as "Jane Doe," who's accused of illegal music downloading from the Internet, have filed a motion in federal court in Washington, D.C., to assert her privacy and other constitutional rights. So far, the Recording Industry Association of America (RIAA) has issued more than 1,000 subpoenas to Internet service providers demanding the names and addresses of people it intends to sue for illegal use of copyrighted music found online. An RIAA official said the woman's arguments "have already been addressed by a federal judge — and they have been rejected. Courts have already ruled that you are not anonymous when you publicly distribute music online." (Reuters/USA Today 21 Aug 2003)

*Category 19.2* *Music piracy*

2003-08-21 **file-sharing peer-to-peer P2P copyright infringement RIAA lawsuit**

NewsScan

ONLINE MUSIC SWAPPERS IN FEAR OF LAWSUITS
A new report from NPD Group, a market research firm, suggests that threats of copyright infringement suits by the Recording Industry Association of America (RIAA) seem to be having a chilling effect on individuals who swap online music. The report indicates that the number of households acquiring music files dropped from 14.5 million in April 2003 to 12.7 million households in May and to only 10.4 million households in June. NPD VP Russ Crupnick says, "Today, file sharing is the most popular method of digital music acquisition. While we can't say categorically that the RIAA's legal efforts are the sole cause for the reduction in file acquisition, it appears to be more than just a natural seasonal decline." (AtNewYork.com 21 Aug 2003)

*Category 19.2* *Music piracy*

2003-08-27 **music RIAA lawsuit file-sharing MP3 copyright infringement**

NewsScan

THE RIAA HASHES IT OUT
How is the RIAA tracking down music file-swappers? (RIAA is the Recording Industry Association of America, a music-industry trade association.) It uses a library of digital fingerprints (or "hashes") that uniquely identify MP3 music files traded as far back as May 2000, and compares the hashes of music files on a person's computer against those in the library. Finding MP3 music files that precisely match copies that have been traded online provides evidence that a person may have participated in file-sharing services. One lawyer for a person already charged with illegal file-swapping protests: "You cannot bypass people's constitutional rights to privacy, due process and anonymous association to identify an alleged infringer." (AP/San Jose Mercury News 27 Aug 2003)

*Category 19.2* *Music piracy*

2003-09-16 **indentity personal information SBC music downloaders piracy ISP RIAA**

NewsScan

SBC RESISTS SUBPOENAS TO IDENTIFY MUSIC DOWNLOADERS
In another challenge to the recording industry, No. 2 regional phone company and Internet service provider SBC is refusing to comply with subpoenas requiring it and other ISPs to turn over to the Recording Industry Association of America (RIAA) the identities of subscribers suspected of music copyright infringers. SBC's general counsel James D. Ellis sees it as a privacy issue: "Clearly, there are serious legal issues here, but there are also these public policy privacy issues. We have unlisted numbers in this industry, and we've got a long heritage in which we have always taken a harsh and hard rule on protecting the privacy of our customers' information." Matthew J. Oppenheim, a top RIAA executive, says: "SBC believes that free music drives its business. That's the only explanation for why they would relitigate issues that have been resolved." (New York Times 16 Sep 2003)

*Category 19.2* *Music piracy*

2003-09-24 **RIAA mistaken indentity DHCP internet EFF attorney Kazaa ISPs**

NewsScan

RIAA WITHDRAWS IN A CASE OF MISTAKEN IDENTITY
The Recording Industry Association of America (RIAA) has withdrawn a lawsuit that accused a 66-year-old woman of illegally downloading and sharing more than 2,000 songs online. An attorney for the Electronic Frontier Foundation says the woman and her husband simply use the Internet to send e-mail to their children and grandchildren. Also, they use a Macintosh, which cannot run the software needed for the Kazaa file-sharing service they are accused of using illegally. The RIAA accusation seems to have been a case of mistaken identity, and the EFF attorney says more mistaken-identity cases are expected because many Internet service providers do not assign IP addresses to any one user but shuffle them around. (San Francisco Chronicle 24 Sep 2003)

*Category 19.2* *Music piracy*

2003-10-01 **RIAA peer-to-peer P2P networking crackdown Kazaa**

NewsScan

RIAA CALLS ON P2P TO POLICE NETWORKS
Recording Industry Association of America (RIAA) chairman and CEO Mitch Bainwol suggested at a Senate hearing on Tuesday that Kazaa and other peer-to-peer file-sharing software vendors could institute three reforms that would discourage users from illegal activities: change the default settings so users aren't unwittingly sharing private documents; incorporate "meaningful" warnings about trading copyrighted content; and filter unauthorized copyrighted works off the P2P networks. "The file-sharing business must become responsible corporate citizens… moving beyond excuses. If the Kazaas of the world can institute three common-sense reforms, lawsuits can be avoided, the record industry will be healthier, there will be more jobs, consumers will get the music they want." Kazaa responded that it's already instituted the first two recommendations but that the third would be technically impossible. "If you're going to block the titles of every song, every word in every copyright song, every copyright movie, and every copyright book, you might as well input the whole dictionary," said Philip Corwin, attorney for Kazaa parent Sharman Networks. Meanwhile, rapper LL Cool J said though royalties generated through legitimate online music downloads were small, they were better than nothing. "Some of the artists may only get a nickel out of the 99 cents [charged per song]. Can we at least get that? Is it alright for us to make a living as Americans?" (IDG News Service/InfoWorld 1 Oct 2003)

*Category 19.2* *Music piracy*

2003-10-03 **Napster file-sharing peer-to-peer legitimate Roxio**

NewsScan

NAPSTER TO MAKE A COMEBACK
Napster, the digital file-swapping service that had 60 million active users at the time court rulings caused it to go out of business, is planning to relaunch next week as a legitimate music subscription service. The relaunch will be made in a "star-studded gala in New York City" by Roxio, the company that acquired Napster's software last year for $19 million. (Beta News 3 Oct 2003)

*Category 19.2* *Music piracy*

2003-10-06 **music download encrypted RIAA crackdown Kazaa**

NewsScan

MUSIC INDUSTRY CRACKDOWN SPAWNS 'CYBER-SPEAKEASIES'
Music download enthusiasts are flocking to 21st century versions of "speakeasies" —high-tech clubs that offer encrypted software designed to shield users from identification and prosecution by a zealous recording industry. Coincidentally, the software now being served up may have broader appeal in the business world as well. "The software that users are moving toward, it has characteristics that businesses need — which is a high degree of privacy, a high degree of security and the ability to handle large files," says New York University telecommunications professor Clay Shirky. "Thanks to the RIAA, ease of use surrounding encryption technologies, which was never a big deal before, is a big deal now." In addition to old favorites such as Kazaa and Morpheus, file-swappers are now turning to newer iterations, such as Blubster, which features both stronger privacy protection as well as easy-to-use encryption and decryption. Another program, called Waste, can be used to set up an encrypted instant-messaging and content-sharing network of 50 users, without the potential liability of a central server. And an offshoot of Freenet, dubbed Locutus, is targeting corporate users with its ability to search corporate networks for information distributed across a wide range of computers. "It's kind of like Google for people's hard disks, but with added security. You can define who has permission to find what kind of files," says Ian Clarke, who heads up Freenet and Locutus parent Cematics. (AP/CNN.com 6 Oct 2003)

*Category 19.2* *Music piracy*

2003-10-10 **Napster peer-to-peer RIAA return Roxio file-sharing file-swapping legitiamate legal**

NewsScan

NAPSTER BACK, WITH BLESSING OF RECORDING INDUSTRY
The rapper Ludacris is hailing the return of Napster, which had been forced out of business by lawsuits brought against the once-free music file-swapping service by the recording industry: "To see them come back and do it right, it means the world to the music business. It's a legitimate, cool, fair service that can and will bring artists and fans back together." The new service is being formally released Oct. 29th by Roxio, whose chief executive, Chris Gorog, says: "We have been deeply focused on the liberation of online music from the PC." Napster 2.0 allows subscribers to tune in to the songs that other users are listening to, look at what others have downloaded, and send songs and playlists to other subscribers. (Los Angeles Times 10 Oct 2003)

*Category 19.2* *Music piracy*

2003-10-16 **Apple iTunes Windows download music legal**

NewsScan

APPLE iTUNES DOES WINDOWS
Apple is expanding its popular iTunes music download service into Windows territory, promising a wider selection of songs and some new features to maintain its lead in an increasingly competitive market. The launch was accompanied by the usual Apple glitz — CEO Steve Jobs chatted via remote link-up with U2 lead man Bono and the Rolling Stones' Mick Jagger in a prelude to a live performance by singer-songwriter Sarah McLachlan. "It's like the pope of software meeting up with the Dali Lama of integration," gushed Bono — referring to the iTunes software and Apple's integrated online music store. Analysts say that iTunes faces stiff competition in the Windows space, but that its flexibility to download tunes onto multiple devices gives it an edge. "There's going to be a lot of jockeying for position in the next 12 months," says a Forrester Research analyst. "But I think iTunes is a real winner because it has the portable player, the jukebox and the store all together." (Reuters 16 Oct 2003)

*Category 19.2* *Music piracy*

2003-10-27 **Napster music download pre-paid card Roxio**

NewsScan

PRE-PAID MUSIC CARDS FROM NAPSTER
The reincarnation of Napster is allowing customers to use prepaid cards to pay for music from the Napster online store. The cards will soon will be on sale at 14,000 electronics retailers and other stores around the U.S. Mike Bebel, head of Roxio's Napster division, says: "We're positive that the effect here is to substantially increase the opportunity for people to engage in online music legitimately. To reach all of the consumers that have in some cases not been reachable through typical channels, we felt that this made sense." Will it be necessary to educate customers in how to use the cards? No, says Bebel: "I'd say the average consumer has a pretty good understanding of what these cards are and what they represent. They wouldn't mistake it for an air freshener." (Los Angeles Times 27 Oct 2003)

*Category 19.2* *Music piracy*

2003-11-06 **RIAA delete key households U.S. digital music deleted NDP hardball tactics**

NewsScan

U.S. HOUSEHOLDS HIT THE DELETE KEY
The aggressive campaign waged by the Recording Industry Association of America against illegal music downloads is showing results: 1.4 million U.S. households deleted all the digital music files residing on their computers in August, according to a report by the NPD Group. NPD said recent publicity over the RIAA's hardball tactics prompted the massive cleanup, but added that consumers' overall opinion of the recording industry is suffering because of it. (Reuters/CNN.com 6 Nov 2003)

*Category 19.2* *Music piracy*

2003-11-26 **iTunes protection apple software digital rights management Jon Johansen QTFairUse DRM**

NewsScan

NEW SOFTWARE DERAILS APPLE ITUNES PROTECTION
Norwegian computer whiz Jon Johansen is at it again — the teenager best known for writing the DeCSS code that bypasses the copyright protection on DVDs has come up with a new program that does the same thing on Apple's iTunes songs. Johansen's QTFairUse software does not unlock the actual digital rights management (DRM) encryption, but rather intercepts the file while it is streaming, before the DRM gets locked on. The program, categorized as a "memory dumper," works only on Windows-based PCs and requires significant technical expertise to use. For the curious, it can be found on Johansen's Web page at www.nanocrew.net. (Hollywood Reporter/Reuters 26 Nov 2003)

*Category 19.2* *Music piracy*

2003-12-23 **internet service providers music intellectual property EFF downloaders**

NewsScan

SUING DOWNLOADERS JUST GOT MORE EXPENSIVE
Friday's court ruling absolving Internet service providers of the duty to reveal subscribers' names when music companies serve them with a subpoena means that the costs for going after people who download music illegally just got a lot higher. Legal experts say the music industry can still bring civil lawsuits against individuals without knowing their names — so-called "John Doe" suits — and then ask a judge for permission to issue subpoenas, but "That's a time-consuming and fairly expensive process," says one intellectual property attorney. Previously, recording industry lawyers had been issuing subpoenas before filing any lawsuits. The new procedure will also allow targeted individuals to contest the subpoenas in court. "It's not going to stop (the recording industry) from filing legitimate claims. It's going to give the targets of those claims procedural protection if they're incorrectly named," says a lawyer for the Electronic Frontier Foundation. "This is certainly a setback for the industry if they're looking to threaten without suing. It raises the stakes all around," says Jonathan Zittrain, co-director of the Berkman Center for Internet and Society at Harvard Law School. (AP/Washington Post 23 Dec 2003)

# 19.3 Movies / TV piracy

*Category 19.3* *Movies / TV piracy*

2003-10-09 **digital piracy Disney scare entertainment privacy**

NewsScan

DISNEY WANTS TO 'SCARE THE HECK OUT OF' DIGITAL PIRATES
Disney executives think that Hollywood need to find digital locks on entertainment content to bar people who don't pay. Chief Operating Officer Bob Iger says: "I realize that there are a lot of concerns regarding privacy in this regard, invading people's homes and their home PCs, but at some point we've got to somehow ... scare the heck out of these people that they could get caught." (USA Today 9 Oct 2003)

*Category 19.3* *Movies / TV piracy*

2003-10-24 **movie piracy prevent Oscars screeners VHS coded**

NewsScan

SCREENERS CODED TO PREVENT MOVIE PIRACY
A compromise has been reached that will make possible a carefully controlled distribution of free cassettes to Oscar voters for private screening during the upcoming awards season. The movies will be numbered VHS cassettes rather than easily copied DVDs, and they will be coded for tracing if they are sold or pirated. Academy members will sign contracts taking responsibility for any "screeners" they accept, and making them subject to possible banishment from the Academy if the screeners are later found on the black market. (Washington Post 24 Oct 2003)

*Category 19.3* *Movies / TV piracy*

2003-10-29 **MPAA digital piracy Dick Valenti copyright infringement**

NewsScan

VALENTI ON DIGITAL PIRACY
Dick Valenti, president of the Motion Picture Association of America, sees the fight against digital piracy as vital to America's economic future: "Piracy is a fact plain and real, with the unwanted prospect of its rapid spread in the future. Antipiracy must take precedence over everything. Current conservative estimates indicate that the film industry loses $3.5 billion each year to hard-goods piracy (counterfeit DVDs, VHS tapes and optical discs). That figure does not take into account the damage done by online piracy. The digital world with its zeroes and ones and perfect copies of originals has changed the movie landscape forever, which is why the movie world's priorities have been permanently altered. The industry wants to use the Internet to dispatch films to consumers. But as we do, we must also challenge piracy and defeat it with every weapon we can summon — and we will succeed, I am convinced — or one day we will sit upon the ground and tell sad stories of the decline and fall of America's greatest artistic triumph and an awesome engine of job and economic growth." (Wall Street Journal 29 Oct 2003)

*Category 19.3* *Movies / TV piracy*

2003-12-23 **DVD copying anti-copying Jon Johansen MPAA Motion Picture Association of America film television industry**

NewsScan

OSLO COURT EXONERATES 'DVD JON'
An Oslo appeals court has upheld a lower court ruling clearing 20-year-old Jon Johansen (dubbed "DVD Jon" by fans) of piracy charges, saying he had broken no Norwegian law by developing and distributing software that disables digital locks that prevent unauthorized copying of DVDs. The court noted that such software prevents DVD owners from making personal copies that could be used as backup if the original sustains damage. The ruling applies only in Norway, but the case has been closely watched by advocates on both sides who see it as a test for cyberspace copyright rules around the globe. The U.S. Motion Picture Association of America expressed its disappointment in the verdict in a statement: "The actions of serial hackers such as Mr. Johansen are damaging to honest consumers everywhere. While the ruling does not affect the laws outside of Norway, we believe this decision encourages circumvention of copyright that threatens consumer choice and employment in the film and television industries." (Reuters/Los Angeles Times 23 Dec 2003)

# 19.5 Games piracy

*Category 19.5* *Games piracy*

2003-10-07 **gaming piracy steal popular Half-Life code online**

NewsScan

VANDALS STEAL SOURCE CODE OF POPULAR COMPUTER GAME
Network vandals have stolen the source code of the new computer game "Half-Life 2" and are circulating it on the Internet. The company that owns the game spent five years developing it, a fact that prompted Dave Kosak, executive editor of GameSpy.com, an online gaming service provider, to see the silver lining in this criminal act, which is that it "points out that game developers have really valuable property. They spend years coding this engine, and the bigger you are, the bigger target you are." (AP/San Jose Mercury News 7 Oct 2003)

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

*Category 19.6* *Counterfeit currency, credit-cards, other negotiable tokens*

2003-07-14 **hacking fraud vandalism universities vending machines**

NewsScan

STUDENTS ADMIT TO OVERSTATING THEIR FEATS OF VANDALISM
Two student hackers have finally admitted that they never finished a device that was intended to cheat university campus debit card systems out of food, laundry machine use or sports tickets. In view of the admission, the manufacturer of the vending machine system used on more than 200 colleges nationwide has agreed to drop its lawsuit against the two students, one from Georgia Tech and the other from the University of Alabama. The device was intended to manipulate the amount of money on a debit card used in the system, but a spokesman for Blackboard, the vending machine company, says: "They actually didn't do a lot of the things they were claiming to do. They knew full well the claims they were making were silly. They're obviously bright young guys, but a little misguided in where they were focusing their attention." (AP/Washington Post 14 Jul 2003)

# 1A1 Criminal hacker conventions and meetings

*Category 1A1* *Criminal hacker conventions and meetings*

2003-04-14 **student hacking demonstration intellectual property systems disallowed Georgia**

NewsScan

COURT BLOCKS PRESENTATION ON HACKING UNIVERSITY SYSTEMS
A Georgia state court has issued a restraining order prohibiting two students from making a conference presentation on how to break into and modify a university electronic transactions system. Blackboard, an education software company, argued that the information in the presentation was gained illegally and would have harmed the company's commercial interests and those of its clients, but Interz0ne conference organizers argued that the students' free speech rights were abridged. "The temporary restraining order pointed out that the irreparable injury to Blackboard, our intellectual property rights and clients far outweighed the commercial speech rights of the individuals in question," said a Blackboard spokesman. The information was gleaned after one of the students had physically broken into a network and switching device on his campus and subsequently figured out how to emulate Blackboard's technology. Because that alleged act was illegal, publication of the resulting information should be blocked, said the court. The court's decision was grounded largely in federal and Georgia state antihacking laws and a state trade secrets act, rather than the Digital Millennium Copyright Law, which has been invoked in several similar cases. (CNet News.com 14 Apr 2003)

*Category 1A1* *Criminal hacker conventions and meetings*

2003-07-31 **manifesto superworm Cide Red Brandon Wiley Curious Yellow bandwidth sapphire worm cybersecurity**

NIPC/DHS

July 31, Government Computer News — Superworm Manifesto unveiled at cybersecurity briefings. Typical worms, such as Code Red, use random scanning to propagate, wasting bandwidth and competing with themselves once released. The Sapphire worm, an example of a theoretical worm concept called Warhol, succeeded in infecting 90 percent of vulnerable machines within about 10 minutes, but continued trying to spread randomly, drawing attention to itself and quickly running out of bandwidth. Brandon Wiley of the Foundation for Decentralised Research unveiled a guide for creating a new generation of worms this week at the Black Hat Briefings security conference in Las Vegas, NV. He also offered a way for systems to be inoculated. Wiley's superworm concept, called Curious Yellow, would combine the fast-spreading characteristics of a Warhol worm with an algorithm that would let the worms coordinate their activities to avoid overlap, multiple infections and competition. The result is a large, robust network of exploited machines that can be continually updated to carry out tasks, benign or malicious.

# 1A2 Criminal hacker testimony in court or committees

*Category 1A2* *Criminal hacker testimony in court or committees*

2003-02-21 **criminal hackers sentencing study analysis**

NewsScan

LAWYERS SAY HACKERS ARE GETTING BUM RAP
The National Association of Criminal Defense Lawyers has joined with the Electronic Frontier Foundation and the Sentencing Project in publishing a position paper that argues people convicted of computer-related crimes tend to receive harsher sentences than perpetrators of comparable non-computer-related offenses. "The serious nature of the offenses is overplayed," says Jennifer Granick, author of the paper and clinical director at Stanford University's Center for Internet and Society. "The (majority) of the offenses are generally disgruntled employees getting back at the employer or trying to make money." In a review of 55 cases prosecuted under the most-often used computer crime statute, only 15 involved harm to the public and only one resulted in a threat to safety. Those convicted "are receiving sentences based on the fear of the worst-case scenario rather than what the case may really be about," says Granick. The paper was submitted in response a request for public comment by the U.S. Sentencing Commission as required by the Homeland Security Act of 2002. Cybercrime legal expert Scott Frewing says he agrees with many points raised in the paper, but recommends a two-tiered sentencing threshold: "I would be comfortable in a situation where the code addresses the discrepancy between those who cause bodily injury and those that don't. If that results in the law being unfair to a virus writer, maybe that's enough to put them on notice." (CNet News.com 20 Feb 2003)
http://news.com.com/2100-1001-985407.html

---

*Category 1A2* *Criminal hacker testimony in court or committees*

2003-09-10 **hacker arrested Adrian Lamo FBI new York Times Yahoo Google WorldCom ExciteAtHome**

NewsScan

HACKER ARRESTED
Twenty-two-old hacker Adrian Lamo turned himself in to federal marshals — with the surrender filmed by an independent camera crew that had been following him for days for a documentary film. He has publicly acknowledged involvement in some dramatic computer break-ins at large corporations during the past several years, including The New York Times, Yahoo!, WorldCom and ExciteAtHome, and captured the Social Security numbers of celebrities and government officials who contributed to the op-ed pages of the Times. In the past, Lamo has offered to work for free with his hacking victims after each break-in to improve the security of their networks. (AP/San Jose Mercury News 10 Sep 2003)

---

*Category 1A2* *Criminal hacker testimony in court or committees*

2003-09-17 **blaster teen innocent case court Jeffrey Parson**

NewsScan

TEEN PLEADS INNOCENT IN BLASTER CASE
In an appearance yesterday before a federal court in Seattle, high school senior Jeffrey Parson entered a plea of innocence to a charge that he had unleashed the Blaster.B worm that infected more than 7,000 computers. If convicted, the young man faces a maximum sentence of 10 years in prison. Parson's contention is that the government overstated its case to try to make an example of him. (AP/San Jose Mercury News 17 Sep 2003)

---

*Category 1A2* *Criminal hacker testimony in court or committees*

2003-09-18 **FBI bust hackers David Smith Melissa Virus creator helps AP Associated Press 1999 arrest track viruses senders DeWit Netherlands**

NIPC/DHS

September 18, Associated Press — Virus sender helped FBI bust hackers. Federal prosecutors credited the man responsible for transmitting the Melissa virus — a computer bug that did more than $80 million in damage in 1999 — with helping the FBI bring down several major international hackers. Court documents unsealed Wednesday, September 17, at the request of The Associated Press show that David Smith began working with the FBI within weeks of his 1999 arrest, primarily using a fake identity to communicate with and track hackers from around the world. According to the court document, Smith helped the FBI bust virus senders abroad and stop viruses in the U.S. The letter says that two months after his arrest, Smith gave the FBI the name, home address, e-mail accounts and other Internet data for Jan DeWit, the author of the so-called Anna Kournikova virus in the Netherlands. The FBI passed the information on to authorities in the Netherlands. DeWit was arrested and later sentenced to probation. The federal prosecutor also said that Smith was working with the FBI to develop an investigative tool that theoretically could help identify an e-mail sender who was trying to mask his or her identity.

# 1A3 Biographical notes on individual criminals (including arrests, trials)

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-01-06 **Xbox hacking mastermind Microsoft Linux Lindows rivalry**

NIPC/DHS

January 03, CNN — Mystery man named in Xbox hack contest. A longtime Microsoft opponent has emerged as the mystery backer and mastermind behind a contest that offers $200,000 to anyone who successfully hacks into the software giant's Xbox video game console, a top technology news site reported. Michael Robertson, a former dot-com entrepreneur and now chief executive of U.S. software company Lindows.com, revealed himself as the anonymous donor and contest's creator in an interview on Thursday with CNET News.com. Last July, Robertson anonymously dangled the prize money to any programmers who could successfully hack into the Xbox and adapt it so that it would run on the Linux operating system, an emerging competitor to Microsoft's Windows operating system. Robertson recently extended the deadline as no group has fully mastered the challenge. The hack contest goes beyond a sporty challenge. Linux proponents have long charged that its freely distributed operating system, designed and modified by mainly unaffiliated groups of programming enthusiasts, is an important step for the future development of computing devices. They argue that the market dominance of Windows, which is the operating system on more than 90 percent of all PCs, gives Microsoft and a small number of its business partners unfair and anti-competitive control in the design of the growing number of devices that come equipped with computing capabilities. Robertson's firm Lindows.com is a start-up that aims to promote the use of the Linux open-source operating language in computer systems, a move that would challenge Microsoft's dominant Windows operating system.

---

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-01-06 **criminal hacker sentencing Web defacement vandalism government Websites**

NIPC/DHS

January 03, Government Computer News — Hacker of federal Websites could spend a decade in jail. NASA's inspector general has announced that William Douglas Word of Pelham, Alabama faces up to ten years in prison after pleading guilty to defacing sites of NASA, Defense Department agencies, Interior Department and the International Trade Commission, among others, according to a grand jury indictment handed down in the U.S. District Court for the Northern District of Alabama. Much of the criminal activity occurred in late 1999, the inspector general said. The NASA Office of Inspector General (OIG) investigated the crime together with the Defense Criminal Investigative Service, the Naval Criminal Investigative Service and the FBI. James E. Phillips, U.S. attorney for the Northern District of Alabama, prosecuted the case. Word "was rolled up in a group of hackers that decided to turn themselves in after we got close to confronting them," a NASA official said. "This was the typical hacker case where they were demonstrating their skills." Word is to be sentenced April 24.

---

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-01-21 **punishment criminal hacker sentence law**

NewsScan

BANNED FOR LIFE ON THE NET?
Kevin Mitnick, once tagged by the government as "the most-wanted computer criminal in U.S. history," is now ending his probation and will once again be free to start using the Internet. (He intends to set up shop as a computer security consultant.) Legal experts disagree about whether computer criminals can be banned from Internet activity even after they have served sentences and finished their probationary periods. Jennifer S. Granick of the Stanford Center for Internet and Society says no: "Computers are everywhere. The A.T.M. is a computer; the car has a computer; the Palm Pilot is a computer. Without a computer in this day and age, you can't work, you can't communicate, you can't function as people normally do in modern society." Ross Nadel of the U.S. Attorney's office in Northern California says yes, arguing that banning someone from the Internet may be necessary if in a particular case Internet use was integrated and inseparable from the crime that was committed. The courts are similarly divided on the issue, and legal observers don't expect the question to be fully resolved for many years. (New York Times 21 Jan 2003)

---

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-01-24 **virus writer criminal prosecution trial judgement sentence prison**

NewsScan

COMPUTER VIRUS WRITER GETS TWO YEARS IN PRISON
Simon Vallor, from Llandudno, Wales, was sentenced two years in prison by a London magistrate who said that Vallor's actions "cried out for the imposition of a deterrent sentence." The judge brushed aside Vallor's request for leniency, saying: "These offenses were planned and very deliberate. Frankly, when you go to this trouble to make a sophisticated virus, programmed to leave damage this week, next week and the week after, it is absurd to claim you do not intend to do harm. These were by no means isolated offenses and they were committed over a period of time." Vallor wrote the viruses called Admirer, Redesi B, and Gokar, and was judged to be responsible wreaking damage in at least 46 countries. (The Western Mail, Wales, 22 Jan 2003)

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-02-07 **criminal hacker indictment impersonation fraud theft college university student penetration**

NewsScan

BOSTON COLLEGE STUDENT INDICTED FOR ONLINE VANDALISM
Boston College computer science major Douglas Boudreau has been indicted for hacking into dozens of campus computers and using stolen identities to charge food, books, and services to the accounts of other students. An assistant attorney general said that the scheme "required technical aptitude and an enormous amount of time." Boudreau, who has been suspended from school, is being charged with wiretap violations, hacking and larceny. (Boston Globe 7 Feb 2003)

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-02-07 **computer virus writers held England hacking organization**

NIPC/DHS

February 07, silicon — Two held in computer virus raid. Two men from northeast England are being interviewed today by the National Hi-Tech Crime Unit (NHTCU). The move follows the execution of search warrants this morning in County Durham, United Kingdom (UK). Two addresses were searched and evidence retrieved relating to computer and drugs offences. The operation was jointly conducted with officers from Durham Constabulary and the United States multi-agency CATCH team (Computer and Technology Crime Hi-Tech Response Team), which is based in Southern California. A simultaneous search warrant was executed at an address in the state of Illinois where additional evidence in the case was seized. The two UK-based men have been identified as members of an international hacking group known as "THr34t-Krew". The NHTCU claims this group is behind a worm called the TK which has infected approximately 18,000 computers worldwide.

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-02-28 **DVD DeCSS decryption copyright infringement intellectual property piracy lawsuit trial indictment DMCA international jurisdiction**

NewsScan

TEENAGER "DVD-JON" CHARGED AS CRIMINAL FOR BREAKING DVD CODE [11 Jan 2002]
Norwegian prosecutors have lodged a criminal indictment against Jon Lech Johansen, who three years ago when he was 15 years old, wrote and distributed on the Internet software that could break the code protecting DVDs from being copied by individuals who did not pay for them. Johansen says he wrote the software to be able to use his computer to play movies he had purchased. A lawyer for the Electronic Frontier Foundation, which is defending the young man, says the law under which he's being prosecuted was intended to protection financial institutions, rather than to prevent an individual from accessing his own property. The prosecution is charging that in the three months after the young man (now widely known as "DVD-Jon" posted the software on the Internet, it was downloaded by more than 5,000 individuals. (AP/San Jose Mercury News 11 Jan 2002)
http://www.siliconvalley.com/docs/news/svfront/034227.htm

'DVD JON' ACQUITTED BY NORWEGIAN COURT
Jon Lech Johansen (also known as DVD Jon), who was accused of illegally developing and distributing the DeCSS program for breaking the digital copy-protection mechanism on DVDs, has been acquitted in a Norwegian court. The rationale for the judge's decision was that the software could be used for legal purposes as well as illegal ones. "If a person's motive is to solely encourage or solicit illegal actions, then it would be illegal to distribute it" — but the court made the judgment that Johansen was not motivated in that way. (PC World 7 Jan 2003)
http://www.pcworld.com/news/article/0,aid,108462,00.asp

NORWEGIAN DVD-PIRACY CASE TO BE RETRIED
What's going on, property theft or the exercise of intellectual freedom? Norwegian teenage programmer Jon Johansen was acquitted last month of using software he developed to steal DVD movies, but an appellate court in Oslo has ruled that the case needs to be reexamined. The software involved is known as DeCSS. What it does is unscramble manufacturers' security locks on DVDs, much to the distress of the Hollywood movie studios. (Reuters/USA Today 28 Feb 2003)

---

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-03-17 **computer criminal hacking Web defacement prosecution conviction Pakistani**

NIPC/DHS

March 14, Associated Press — Pakistani pleads guilty to hacking U.S. Web sites. A hacker who breached the computer network at Sandia National Laboratories and posted an anti-Israeli message on the Eglin Air Force Base Web site pleaded guilty to computer and credit card fraud charges, the U.S. attorney's office said Thursday. There were no known political or terrorist overtones to the breaches of four computer networks by 18-year-old Adil Yahya Zakaria Shakour of Los Angeles, said Patty Pontello, a spokeswoman for federal prosecutors. Shakour penetrated the Florida air base's computer server repeatedly in April and May 2002, altering the Web page to denounce the Israeli advancement into Palestine and crediting the defacement to the "Anti India Crew." Shakour is a Pakistani who could face deportation after he completes a prison term of up to 15 years, to be set at his June 12 sentencing. He agreed to make restitution of approximately $100,000 for damage to the computer networks. More than $2,700 in damage was done to the Sandia Labs unclassified Web site in Livermore.

---

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-04-29 **U.K. Fluffi Bunni hacker Lynn Htun FBI 9/11 cyberprotest war terrorism SAND institute**

NIPC/DHS

April 29, Associated Press — U.K. arrests 'Fluffi Bunni' hacker. Lynn Htun, the man thought to be the leader of a group of hackers known as "Fluffi Bunni," was arrested Tuesday by British authorities. Fluffi Bunni captured the attention of the FBI just days after the September 11 terror attacks, when thousands of commercial Web sites were vandalized with a single break-in that included the message, "Fluffi Bunni Goes Jihad." The FBI characterized the act in a November 2001 report as an anti-American cyberprotest against the war on terrorism. Victims have included the Washington-based SANS Institute, Security Focus, and Attrition.org, a site run by experts who formerly tracked computer break-ins.

---

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-05-22 **KINGPIN Ukranian cracker arrested thailand Maksym Vysochansky microsoft adobe back door buyers financial reports credit cards**

NewsScan

'KINGPIN' CRACKER ARRESTED IN THAILAND
Thai officials arrested a Ukrainian man described by a U.S. embassy spokesman as a "kingpin" of international computer crime. Maksym Vysochansky, 25, is accused of selling counterfeit versions of flagship software products by major companies such as Microsoft and Adobe. Vysochansky, who used a number of aliases, is thought to have been involved in fraudulent schemes worth up to $1 billion. "This guy was on the U.S. Secret Service's 10 most wanted list. He's definitely a big shot," said the embassy official. Authorities allege that Vysochansky also built a "back door" into the software he sold that allowed him to hack into buyers' financial and credit card information. "It was a very complicated and sophisticated fraudulent scheme," said the embassy official. Vysochansky likely will be extradited to the U.S. where he'll face charges of copyright violations, trafficking in counterfeit goods and money-laundering. (News24.com 22 May 2003)

---

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-05-22 **incorrect stocks fraud UCLA false identities**

NewsScan

EX-STUDENT FINED MORE THAN $500,000 FOR STOCK FRAUD ON NET
Former UCLA student Refael Shaoulian has been ordered by a federal judge to pay $534,000 in fines for using university computers and false identities to post intentionally incorrect about stocks so that he could profit from the buying and selling sprees he caused. The civil suit was brought by the Securities and Exchange Commission. (APOnline/USA Today 22 May 2003)

---

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-06-12 **Al-Jazeera hacker John William Racine DNS Servers Let Freedom Ring court password Network Solutions**

NIPC/DHS

June 12, The Register — Al-Jazeera hacker charged. Web designer John William Racine, of Norco, CA, has been charged with breaking into DNS servers and rerouting surfers visiting the Web site of Al-Jazeera to a "Let Freedom Ring" patriotic Web site he created. Racine is also accused of intercepting 300 emails sent to the Arab satellite TV network between March 25 and 27. The 24 year-old is out on bail pending a Monday court appearance when he will face charges of unlawful interception of an electronic communication and wire fraud. Prosecutors allege that Racine obtained a password for Al-Jazeera's Web site by posing as a representative of the station in forged requests faxed to Network Solutions, who handed over the vital information without verifying his identity.

---

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-06-13 **Sandia Laboratories hacker sentenced Adil Yahya Zakaria Shakour pakistan israeli palestine web page debounce air base eglin AFB**

NIPC/DHS

June 13, The Mercury News (CA) — Hacker sentenced for breaching Eglin AFB, Sandia lab. An 18-year-old hacker who breached computers at Sandia National Laboratories and posted an anti-Israeli message on the Eglin Air Force Base Web site was sentenced Thursday to a year and a day in federal prison. Adil Yahya Zakaria Shakour also was ordered to pay $88,253 in restitution, and his computer use was restricted during the three years he will spend under supervised release after his prison term. Shakour, a Pakistani national who lives in Los Angeles, pleaded guilty in March to computer and credit card fraud charges. Shakour penetrated the Florida air base's computer server repeatedly in April and May 2002, altering the Web page to denounce the Israeli advance into Palestine. Damage to the air base computer system was estimated at $75,000, while more than $2,700 in damage was done to the Sandia Laboratories Web site.

---

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-07-10 **DOE Department Energy cracker 1-year Londoner UK police unauthorized access computers**

NIPC/DHS

July 10, The Register — London police quiz suspected DOE cracker. An 18 year-old Londoner suspected of commandeering U.S. Department of Energy (DOE) computers to store illicitly obtained music and video files was arrested and questioned by UK police Wednesday. Officers from the Metropolitan Police's Computer Crimes Unit were asked to investigate unauthorized access to 17 unclassified computers at a U.S. Department of Energy research laboratory in Batavia, IL, during June 2002 after the trail of the attacker led back to the UK. The teenager was released on police bail until mid-August pending further enquiries, including a forensic examination of a PC seized from his home. Police are working on the belief that no sensitive information was seized during the June 2002 attack on the U.S. DOE's network. Officers from the Metropolitan Police's Computer Crimes Unit are been assisted in their enquiries by representatives from the Office of the Inspector General of the U.S. Department of Energy.

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-07-10 **teenage hacker violate 2000 sites french student DKD web technical skill prison**

NIPC/DHS

July 10, Associated Press — Teenage hacker suspected of violating 2,000 sites. A French high school student is being investigated on suspicion of breaking into and defacing some 2,000 Web sites police said Thursday. The 17-year-old boy, who went by the pseudonym "DKD," hacked into sites and often replaced their welcome pages with political slogans, said Eric Voulleminot of the Regional Service of Judicial Police in Lille, France. The teenager is accused of attacking sites in France, Britain, Australia and the United States, Voulleminot said. The boy allegedly concentrated on government office and military sites, including that of the U.S. Navy. Suspected of attacks over 14 months, he was arrested June 24 at his parents' home outside of Paris and released under surveillance. Investigators think his goal was showing off technical skill rather than spreading a political message. The suspect faces a maximum sentence of three years in prison and a fine $50,850.

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-08-29 **MsBlaster creator copycat teenager hacker worm house detention monitored electronically Blaster.B FBI Symantec**

NIPC/DHS

August 29, TechWeb — Accused MSBlaster creator placed under house detention. A teenager has admitted creating a copycat of the MSBlaster worm, Seattle-based U.S. Attorney John McKay said Friday, August 29. Jeffrey Lee Parson, 18, of Hopkins, MN, was arrested early Friday morning on one count of intentionally causing or attempting to cause damage to a computer. Parson was placed under house detention and is being monitored electronically, said McKay. All computers in his home were seized by the FBI, and he has been denied access to the Internet. Parson is accused of modifying the original MSBlaster worm, and a variant, Blaster.B. The variant shared the same destructive characteristics as its parent, attacking PCs which had not been patched against a vulnerability in the Windows operating system. The worm, which according to security firm Symantec infected more than 500,000 systems worldwide, caused some computers to constantly reboot, snarled enterprise network and Internet traffic, and forced Microsoft to take the unusual step of disabling one of the addresses used to connect with its WindowsUpdate service. Estimates by analysts as to the damage done by MSBlaster and its follow-ups range as high as $1.3 billion.

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-08-29 **worm Blaster network spread FBI teenager vandal**

NewsScan

TEENAGER IDENTIFIED AS 'BLASTER' VANDAL
An 18-year-old man has been identified as one author of the Blaster and LovSan computer worms that have slowed corporate networks throughout the world. The FBI says he will be arrested today. Another individual apparently alerted authorities after seeing the man testing the code. All the Blaster virus variants took advantage of a flaw in that part of Windows software that's used to share data files across computer networks. Infected computers were programmed to automatically launch an attack on a Web site operated by Microsoft, windowsupdate.com, where Microsoft customers will find software patches to ward off attacks by computer vandals. (AP/San Jose Mercury News 29 Aug 2003)

Jeffrey Lee Parson, 18, of Hopkins, MN was arrested iand charged with creating a particularly nasty version of the Blaster virus, Blaster.B, by modifying the code of the original virus.
[NYT http://www.nytimes.com/2003/08/30/technology/30VIRU.html]

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-09-15 **Adrian Lamo hacker NY Times Sacramento employee records phone numbers SSN Social Security Excite Home Corp Yahoo Inc WorldCom**

NIPC/DHS

September 09, Reuters — New York Times hacker surrendered, booked. Hacker Adrian Lamo, 22, turned himself in to federal authorities in Sacramento, CA, on Tuesday, September 9, to face charges related to breaking into the internal network of The New York Times newspaper. Lamo could face fines and prison time under the Computer Fraud and Abuse Act of 1986, which outlaws unauthorized access to computer networks. Lamo hacked into the New York Times network in February 2002 and accessed employee records, phone numbers, and Social Security numbers of editorial page contributors. In the past Lamo has also discovered holes in corporate networks of Excite@Home Corp., Yahoo Inc., and WorldCom, among others, often through laser printers and other unlikely entry points. Lamo's defense is likely to be the "white-hat hacker" defense, said Mark Rasch, former head of the computer crime unit at the U.S. Department of Justice. White-hat hacker is a term used for people who work to protect computers from attack while "black-hat hackers" are those who attempt to break into them. However, the law focuses on the intent to break into the computer, not the motive, said Rasch.

September 15, CNET News.com — Restrictions lifted on NY Times hacker. A federal judge on Friday, September 12, said Adrian Lamo, the so-called "homeless hacker," could go free on bail with only limited restrictions on his computer use until his next court date in October. U.S. Magistrate Judge Debra Freeman kept Lamo's bail at the earlier amount of $250,000 but lifted the restrictions that barred him from using a computer at all. Instead, Freeman said, the 22-year-old California resident can use a computer for email and to apply for a job or a college program. Lamo is facing two criminal charges. One claims he illegally entered the network of The New York Times, viewed confidential employee records and created a false administrator account; the other says he ran up about $300,000 on the paper's Lexis-Nexis account.

---

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-10-17 **evidence trial exculpation defense criminal hacker compromise Trojan horse**

NewsScan; http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/3202116.stm

In England, 19-year-old Aaron Caffrey was charged with crashing computers and networks at the port of Houston, TX after breaking into its systems in September 2001. In October 2003, a jury acquitted the young man because they accepted his defense that criminal hackers had taken control of his computer and used it to attack the port even though he admitted being a member of the criminal hacker organization, admitted breaking into other computer systems, and was unable to provide a shred of evidence that his computer contained any remote-control software or other indications that his computer had been taken over by others.

NEW DEFENSE: THE COMPUTER DID IT
Prosecutors in computer hacking cases are facing a new defense strategy that likely will become more prevalent in the age of hijacked PCs: the computer did it. Defense lawyers in three cases recently tried in the U.K. successfully argued that the crimes committed by their clients were, in fact, the results of "Trojan" programs placed on their computers without their knowledge. While it is relatively easy to trace a hack back to a particular computer, it's much more difficult to prove that the owner of that computer committed the crime. "On the one hand, this is 100% correct that you can not make that jump from computer to keyboard to person," says Bruce Schneier, chief technology officer for Counterpane Internet Security. "On the other hand, this defense could be used to acquit everybody. It makes prosecuting the guilty harder, but that's a good thing." But computer security consultant Dave Morrell says the defense also gives the green light to hackers. "It sets a precedent now in the judicial system where a hacker can just claim somebody took over his computer, the program vanished and he's free and clear." The Trojan defense has not yet been put to the test in the U.S. (Reuters/CNN.com 28 Oct 2003)

---

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-10-21 **airport security test amateur box cutters jets charges criminal trial**

NYT http://www.nytimes.com/2003/10/20/national/20PLAN.html?th

Nathanial T Heatwole, North Carolina college student who turned himself in after placing box cutters and other banned items aboard two Southwest Airlines jets to demonstrate gaps in airport security, was charged with breaching airport security in one count of carrying a dangerous weapon onto an aircraft.

---

*Category 1A3* *Biographical notes on individual criminals (including arrests, trials)*

2003-11-25 **hacking criminal hacker indictment prosecution Aventis unauthorized access**

NIPC/DHS

November 20, Associated Press — Kansas City man indicted for computer hacking. A man from Kansas City, MO, was indicted by a federal grand jury for allegedly hacking into Aventis Pharmaceuticals computers. Thomas S. Millot was charged in a single-count indictment of unauthorized computer intrusion. Millot was employed as an information technology security officer at Aventis' office in Kansas City until October 2000. The federal indictment alleges that Millot gained unauthorized access to the Aventis computer network on nine separate occasions between December 16, 2000, and August 26, 2002, including five times after Millot left the company. The indictment also accuses Millot of deleting an Aventis associate's account from the computer network.

# 1A5 Criminal hacker organizations

*Category 1A5* *Criminal hacker organizations*

2003-09-02 **spammers internet e-mailers Bilk Club message board Damon Decrescenzo junk**

NewsScan

CALLING ALL SPAMMERS
Who would ever have thought? It turns out that spammers need online community, too, and they can find it at The Bulk Club — a support group for junk e-mailers. The overnight success of The Bulk Club (159 members signed up since its launch six months ago) belies the stereotype of the spammer as lone sociopath, lurking in the Internet's shadows. In fact, the club's rapidly swelling membership signals a move on the part of spammers to circle the wagons in an effort to protect and legitimize the embattled bulk e-mail industry. And what do members get for their $20 per month fee? Access to a variety of how-to articles (such as "How to Spoof"), spamming software, a members' message board and "300,000 FRESH e-mails/week." Also, thanks to a Web site security flaw uncovered last week, they received a bit of unwanted publicity — the entire Bulk Club membership roster was revealed, including some of the biggest names in bulk e-mailing: Damon Decrescenzo, a Florida junk e-mail who's been sued by both Microsoft and Amazon; Internet porn king Seth Warshavsky; and John Milton — an alias used by former neo-Nazi Davis Wolfgang Hawke — and Jon Thau, both of whom are responsible for many of those penis enlargement ads you might have received. (Wired.com 2 Sep 2003)

# 1A6 Criminal hacker psychology

*Category 1A6* *Criminal hacker psychology*

2003-03-18 **virus writer psychological profile study**

NewsScan

PROFILE OF A VIRUS WRITER
According to the UK's Sophos, one of the world's largest antivirus companies, about 1,000 viruses are created every month, and in almost all cases the perpetrators are computer-obsessed males between the ages of 14 and 34. "They have a chronic lack of girlfriends, are usually socially inadequate and are drawn compulsively to write self-replicating codes. It's a form of original graffiti to them," says Sophos CEO Jan Hruska. Virus writers tend to explore known bugs in existing software or look for vulnerabilities in new versions in order to create and spread their infections, and Hruska notes that the next target for the virus writing community could be Microsoft's .Net platform for Web services. To boost the impact of their creations, virus writers also tend to share information to create variants of the same infection, such as the infamous Klez worm, which has been among the world's most prolific viruses in the last year. (Reuters/CNet News.com 18 Mar 2003)
http://news.com.com/2100-1002-993023.html

---

*Category 1A6* *Criminal hacker psychology*

2003-04-28 **hackers e-commerce white hats exploit software systems IBM Global Services Ontario Canada global security**

NIPC/DHS

April 28, National Post (Canada) — Ethical hackers uncover system problems. With the proliferation of e-commerce activity, a new breed of hacker has come along: "white hats," or ethical hackers, who dedicate themselves to identifying and exploiting flaws in supposedly impregnable software systems. Interest in hiring white-hat security investigations is on the rise. Some people point to the realities of the world after September 11, 2001, as the reason. "9/11 told us that virtually anything is possible now," says Trevor Townsend, national principal, critical infrastructure protection systems, IBM Global Services, in Ontario, Canada. "There's a new global security posture because terrorists will stop at nothing to achieve their ends...It has changed things for technology as a whole."

---

*Category 1A6* *Criminal hacker psychology*

2003-08-26 **virus Sobig network vandal motivation attacker**

NewsScan

MORE THEORIES ABOUT SOBIG VANDAL'S MOTIVATION
Is money the real motivation for the spread of the Sobig virus? Sobig is transmitted as an e-mail attachment and is the sixth variant of the malicious code by an unknown attacker. Mikko H. Hypponen, director of antivirus research at F-Secure corporation in Finland says: "I think the motivation is clear: it's money. Behind Sobig we have a group of hackers who have a budget and money." Computer security expert Russ Cooper suggests that the vandal is acting out comic book fantasies: "You can liken this guy to Lex Luthor and we're all Supermen. Luckily, we've been able to get the kryptonite from around our necks each time so far." One popular theory is that Sobig is the work of an e-mail spammer who is aggressively trying to build a clandestine infrastructure for blitzing the Internet with junk e-mail. Antivirus software researcher Joe Hartman of TrendMicro says, "If machines remain infected they could be used in any kind of attack. The question we ask ourselves is, What is he trying to achieve? We don't think it's planned for a specific threat, rather its more likely a money-making spam scheme." And Bruce Hughes of Trusecure points out: "There is some evidence that he's been tied in with spammers." Sobig spreads further only when a computer user selects the attached program that then secretly mails itself to e-mail addresses stored in the user's computer. The Computer Emergency Response Team at Carnegie Mellon University says, "Our current advice is: Don't open an attachment unless you are expecting one." (New York Times 26 Aug 2003)

---

*Category 1A6* *Criminal hacker psychology*

2003-09-28 **Torvalds kids dates script kiddies geeks teenagers**

NewsScan

TORVALDS: GEEKY KIDS NEED DATES
Asked how to end virus and worm attacks, Linux creator Linus Torvalds told an interviewer: "When you have people who hook up these machines that weren't designed for the Internet, and they don't even want to know about all the intricacies of network security, what can you expect? We get what we have now: a system that can be brought down by a teenager with too much time on his hands. Should we blame the teenager? Sure, we can point the finger at him and say, 'Bad boy!' and slap him for it. Will that actually fix anything? No. The next geeky kid frustrated about not getting a date on Saturday night will come along and do the same thing without really understanding the consequences. So either we should make it a law that all geeks have dates — I'd have supported such a law when I was a teenager — or the blame is really on the companies who sell and install the systems that are quite that fragile." (New York Times Magazine 28 Sep 2003)

# 1B1 Adult pornography

*Category 1B1* *Adult pornography*

2003-04-30 **P2P peer-to-peer file swapping music piracy**

NewsScan

FILE-SWAPPERS' DIRTY LITTLE SECRET
Despite the best efforts of the music industry, file-swapping services like Kazaa and Morpheus just keep getting bigger. But that doesn't mean music piracy is burgeoning out of control; instead, file-swappers increasingly are trading in smut. A February survey showed that 42% of all Gnutella users were seeking blue images and movies, a phenomenon that Greg Bildson, COO of LimeWire, a leading maker of Gnutella software, refers to delicately: "We're about all different kinds of content sharing." Wayne Rosso, president of Grokster, is a little more blunt: "P*rn — there's a ton of it being traded around." The surge in p*rn-trading has some smut-peddlers considering RIAA-type retaliations against the Gnutellas and Kazaas of the world. Like the movie executives, they blame the free services for their falling revenues. "The explosion of free p*rnography, fueled by file sharing, has diminished interest in pay sites," warns one veteran p*rn industry observer. Meanwhile, some businesses have taken a more collaborative approach. "We love file trading. Why? It's called greed. We've found a way to monetize that sharing," says the sales director for Triple X Cash. His company embeds hidden links in video clips and sends them out on file-sharing networks. When a file-swapper downloads a clip and clicks somewhere in the video's frame, he's taken to one of Triple X's sites. The company gets 25 to 40 "joins" — $30 monthly subscriptions — per day from this technique. "The record industry should have taken a cue from the p*ornographers," says Grokster's Rosso. (Wired.com 30 Apr 2003)

---

*Category 1B1* *Adult pornography*

2003-05-29 **broadband internet pornography music consumer demand**

NewsScan

EUROPEAN BROADBAND GROWTH FUELED BY P*RN, MUSIC
High-speed Internet access growth is booming in Europe, boosted by consumer demand for music and p*rnography downloads, according to a new study by Nielsen/NetRatings. "The adult entertainment sector has increased its reach year-on-year in all European markets except Italy, where, not coincidentally, broadband access is the relative lowest in Europe," says the report. The biggest gains were in the UK, where broadband penetration has more than tripled to 3.7 million users. With only one in five Internet users opting for a broadband connection, however, the UK still remains second from the bottom in terms of percentages. France, Spain and the Netherlands head the top of the list, with 39%, 37% and 36% broadband penetration rates. In comparison, 35% of U.S. users connect via broadband, but the total number — 38 million — makes it No. 1 in the world in terms of sheer volume. (Reuters 29 May 2003)

---

*Category 1B1* *Adult pornography*

2003-07-11 **pornography PC hijacking spread**

NewsScan

HAS YOUR PC BEEN HIJACKED TO SPREAD PORNOGRAPHY?
Computer security expert Richard M. Smith says that in the last month network vandals (possibly linked to Russian organized crime) have found ways to take over PCs with high-speed connections to the Internet and use them, without their owners' knowledge, to send Web pages advertising pornographic sites. Smith says that "people are sort of involved in the porno business and don't even know it." Most PC owners don't know when their computers have been hijacked and the hijacking apparently doesn't damage the computer or disrupt its operation. Because so many different machines are hijacked to perpetrate this scheme, there's no single computer that be shut down to end the problem. Smith adds: "We're dealing with somebody here who is very clever." (New York Times 11 Jul 2003)

---

*Category 1B1* *Adult pornography*

2003-09-24 **MSN Microsoft misuse internet forums chat room pornography sexual predator activities**

NewsScan

MSN MUZZLES CHAT ROOMS
Microsoft MSN is closing down Internet chat services in most of its 34 markets in Europe, Latin America and Asia, and is limiting service in the U.S., citing concerns over use of the online forums for pornography scams and pedophile and sexual predator activities. "We recognize that it's a common industry-wide problem," says an MSN spokeswoman. "We've taken a look at our service and how can we make efforts to step up our efforts to provide a safe environment." In the U.S., MSN will now require chat room users to subscribe to at least one other paid MSN service, so that it will have credit card numbers that it can use to track down those who violate MSN's terms of use. In Canada, Brazil, New Zealand and Japan, MSN will offer some moderated chat rooms and discussions. The move to restrict chat use will probably turn out to be a good thing for the company, says one Microsoft watcher, by allowing it to shed a number of freeloaders. "I think this change will have welcome side effects, like keeping spammers out of the chat rooms. But fundamentally I believe this is a move to make MSN more profitable. It will allow the company to get rid of some infrastructure that was supporting chat, and to make money on what it leaves in place." (AP 24 Sep 2003)

*Category 1B1* *Adult pornography*

2003-12-30 **net nudity pornography naked Nebraska Melissa J. Harrington public**

NewsScan

STOPPING NET NUDITY AT ITS SOURCE — IN LINCOLN, NEBRASKA
Since it's unlawful to be naked in public in Lincoln, Nebraska, that city's police chief ticketed 21-year-old Melissa J. Harrington for posting on her Web site photos "showing her naked at one of our downtown bars and in several other locations around the city." Harrington works as a Web designer at a local Bank and says that she likes "being naked in public... even more when there's a lot of people there to watch." The objectionable photos of the lady were taken inside the Marz Intergalactic Shrimp and Martini Bar, and the owner of the bar is the one who called the police to complain about the nude pictures. If convicted, Harrington faces a maximum penalty of six months in jail and a $500 fine. (AP/Los Angeles Times 30 Dec 2003)

# 1B2 Child pornography

*Category 1B2* *Child pornography*

2003-03-14 **child pornography arrests international**

NewsScan

INTERNET CHILD PORN ARRESTS CONTINUE IN BRITAIN
British law enforcement officials have arrested 43 more men on suspicion of having downloaded child pornography from U.S. porn sites. The officials are working their way through a list (obtained some months ago from U.S. postal investigators) of 7000 British subjects who used their credit cards to enter the sites. Out of the 1,600 individuals arrested in London, 46 have allegedly been directly involved in the abuse of children. A British police official says: "We are sending out a strong warning to those who think they can remain anonymous and escape the law by using the Internet to access abusive images of children." (The Inquirer (UK) 13 Mar 2003
http://www.theinquirer.net/?article=8299

---

*Category 1B2* *Child pornography*

2003-06-13 **spammers target users' pc hijacking microsoft vulnerability MessageLabs windows**

NewsScan

SPAMMERS TARGET USERS' PCs
Security experts at UK firm MessageLabs say that a "trojan virus" mailed to up to 1 million computer users last week was designed to exploit a vulnerability on Windows PCs that would enable the perpetrator to use the recipients' PCs to distribute ads for Web sites carrying incest pornography. Internet security experts have suspected for some time that spammers would use viruses to access third-party computers, but MessageLabs says their investigation offers the first conclusive proof. "This is a massive discovery. It completely undermines the spammers' claim that they are legitimate marketers and shows that they are nasty insidious hijackers who drive me and the vast majority of computer users nuts," says MessageLabs senior technologist Matt Sergeant. The virus targeted a feature known as open proxy, which is often installed by software companies as the default setting on home PCs. Proxy servers are designed to allow the machine to link to the Internet through a local network, but if left open, they provide a back door for computer crackers to hijack the machine. The incident last week targeted customers of Outblaze, a Hong Kong-based webmail company that has about 30 million customers worldwide and owns domain names such as usa.com. "Open proxies are becoming the spammers' lifeline so they are always looking for more. Now we know how they are going about it," says Sergeant. (The Guardian 13 Jun 2003)

---

*Category 1B2* *Child pornography*

2003-09-03 **mousetrapping website disney children porn sites thousand inernet addresses**

NewsScan

MAN ARRESTED FOR 'MOUSETRAPPING' CHILDREN
Federal agents have arrested a Florida man they say runs Web sites that exploit misspellings by computer users to redirect children looking for Disneyland or the Teletubbies to explicit porn sites instead. The government say it is the first prosecution under a provision of the new Amber Alert legislation that makes it a crime to use a misleading Web address to draw children to pornography. The man registered thousands of Internet addresses and was earning up to $1 million per year off them — much of it from sites that paid him when he sent Web users their way. The redirection technique is called "mousetrapping." U.S. Attorney James Comey said: "Few of us could imagine there was someone out there in cyberspace, essentially reaching out by hand to take children to the seediest corners of the Internet." (San Jose Mercury News 3 Sep 2003)

---

*Category 1B2* *Child pornography*

2003-09-04 **ICANN lawmakers pornography scammers stolen credit cards registering**

NewsScan

ICANN TAKES HITS FROM LAWMAKERS
Rep. Howard Berman (D-Calif.) is critical of ICANN (the Internet Corporation for Assigned Names and Numbers) for not doing enough to stop scammers and child pornographers from registering under false names with stolen credit cards: "I'm disappointed with the failure of the marketplace and regulators to deal with this problem. A legislative solution seems necessary." And Rep. Lamar Smith (R-Texas) agrees: "There's not a real seriousness of intent either by ICANN or the Department of Commerce to have an accurate whois database." Commerce Department General Counsel Theodore Kassinger says that ICANN is busy working on solving the problem. (Reuters/USA Today 4 Sep 2003)

---

# 1B3 Pedophilia, kidnapping, Net-adoption fraud

*Category 1B3* *Pedophilia, kidnapping, Net-adoption fraud*

2003-01-07 **pedophiles Internet chat rooms children victims confidence tricksters warning education advertising**

NewsScan

U.K. EFFORT TO CONTROL CHAT-ROOM PEDOPHILES
The British Home Security Office has launched a major advertising campaign to alert children and parents to the dangers of pedophiles who use the Internet to "groom" a young victim by spending many months gaining the child's confidence in chat rooms and e-mail. Home Office minister Hilary Benn said: "Parents can play a role in making their children aware that strangers on the Internet may not always be who they say they are. The messages to children are clear: do not give out personal contact details online and never meet up with someone you have met online unless accompanied by an adult." (The Enquirer, UK, 6 Jan 2003)
http://www.theinquirer.net/?article=7048

# 1B4 Stalking & harassment

*Category 1B4* *Stalking & harassment*

2003-04-18 **cyberstalking Internet rising privacy personal safety**

NewsScan

CYBERSTALKING ON THE RISE
Cyberstalking — stalking people over the Net — is increasing across the U.S., according to a new study by Wired Safety. And while women remain the most likely targets, they're getting into the act as perpetrators, too. In addition, growing numbers of children are cyberstalking children. "We didn't find much good news," said Wired Safety executive director Parry Aftab. "Identity theft is increasing. And because more people are cyber dating they become victims of cyberstalking when things don't work out." Aftab expressed concern over a recent court ruling that compelled Verizon to turn over the name of an ISP subscriber under the subpoena power of the Digital Millennium Copyright Act. "This is an outrageous and dangerous ruling. It was supposedly about music piracy, but the result of the case is that anyone can obtain personal information about any Internet user by simply filling out a one-page form and submitting it to a court clerk. There is absolutely nothing you can do to protect yourself, even if you are a police officer doing undercover work against s*xual predators. The future safety and privacy of all Americans engaged in online communications now rests with Verizon winning this case on appeal." [Asterisk inserted so that NewsScan Daily doesn't get caught in the software filters meant to ward off pornography.] (Internet News 18 Apr 2003)

# 1B5 Gambling

*Category 1B5* *Gambling*

2003-03-31 **eBay illegal gambling Paypal**

NewsScan

EBAY REACTS TO CHARGES AGAINST ITS PAYPAL OPERATION
Federal prosecutors in Maryland have accused PayPal, the Internet payments company acquired by eBay, of violating the [U.S.A.P.A.T.R.I.O.T.] Act by facilitating illegal gambling. The company disclosed the accusation in its annual report filed with the Securities and Exchange Commission; it says that prosecutors have offered a complete settlement of all possible claims and notes that the amount of its earnings from online gambling was less than what prosecutors asserted. (AP / San Jose Mercury News 31 Mar 2003)

*Category 1B5* *Gambling*

2003-05-06 **internet gambling restricted house committee prohibit credit card checks electronic transfer funds**

NewsScan

HOUSE COMMITTEE APPROVES RESTRICTIONS ON INTERNET GAMBLING
The House Judiciary subcommittee approved legislation that would prohibit the use of credit cards, checks and electronic fund transfers as means to pay for online wagering. The bill, which is sponsored by Rep. Jim Leach (R-Iowa), has already been approved by the House Financial Services Committee. The House approved a similar bill last year in Congress, but it died in the Senate. Meanwhile, Rep. Jim Conyers (D-Mich.) and a small group of bipartisan lawmakers are taking a different approach to the issue: they have proposed creating a commission to explore legalizing Internet gambling in states interested in licensing, overseeing and collecting taxes on Internet gambling transactions. A report by the General Accounting Office last year called Internet gambling "a fast-growing industry" with estimated 2003 revenues of more than $4 billion. (AP 6 May 2003)

*Category 1B5* *Gambling*

2003-09-02 **gaming gambling cheap players gaming for money profit by playing**

NewsScan

GAMING FOR MONEY
The game Ultimate Arena allows players to wager small sums to play a match against a single challenger or group of opponents at a similar skill level. At the end of a 10-minute match, the winner of a $2 bet would take home $1.70 home (with Ultimate Arena keeping 30 cents). The maximum bet for a single game is $20 and the most someone can lose in a month is $100, while there is no upper limit on how much players can win. (San Jose Mercury News 2 Sep 2003)

# 1B6 Auctions

*Category 1B6* *Auctions*

2003-02-03 **online auction illegal materials drugs arrest**

NewsScan

MAN ARRESTED FOR SELLING OPIUM POPPY ON E-BAY
The federal Drug Enforcement Administration (DEA) has arrested a Sacramento CA man for selling opium poppy pods on Internet auction site eBay, where he advertised them as "decorations"; each pod is the size of a golf ball and is at the end of a two-foot high stalk. An eBay executive said, "We check the site frequently for any illegal or illicit items and we remove them as fast as we find them," and he said that trying to use eBay to sell illicit drugs online "might be one of the dumbest things you can do." (AP/San Francisco Chronicle 31 Jan 2003)

*Category 1B6* *Auctions*

2003-05-01 **internet auction fraud Federal Trade Commission FTC criminal failure deliver**

NewsScan

INTERNET AUCTION FRAUD
The Federal Trade Commission, together with 33 state and local law enforcement agencies, has announced the filing of 51 criminal and civil cases charging Internet auction fraud, most of them involving failure of the seller to deliver an item (usually items such as computers, plasma TVs, or diamond jewelry). Online auctions accounted for 46% of all complaints lodged with the Internet Fraud Complaint Center last year. (New York Times 1 May 2003)

# 1B9 Non-virus hoaxes, urban myths

*Category 1B9* *Non-virus hoaxes, urban myths*

2003-06-25 **British Airway free tickets e-mail hoax plane valuable bandwidth SARS virus war Iraq encouraging people fly**

NIPC/DHS

June 25, eSecurity Planet — 'Free flight' e-mail hoax serves as security warning. An e-mail chain letter is tricking people into wasting their own time, cluttering corporate inboxes around the country and hogging up valuable bandwidth. Anti-virus software company Sophos, Inc. is reporting the Free Flight chain e-mail is convincing people that British Airways is giving away free plane tickets to anywhere in the world to anyone who forwards the email to 10 or more people. The e-mail claims that it is encouraging more people to fly, following a downturn in the airlines industry because of concerns about the SARS virus and the war in Iraq. It also contends that the airline is working in conjunction with Microsoft, monitoring the distribution of the message. "There's no malicious content. It won't cause damage to the system," says Chris Belthoff, a senior security analyst with Sophos.

*Category 1B9* *Non-virus hoaxes, urban myths*

2003-09-16 **health hazardous internet breast cancer yahoo accuracy information**

NewsScan

INTERNET COULD BE HAZARDOUS TO YOUR HEALTH
A survey conducted by Holly Cardamone, a Melbourne, Australia nurse and communications consultant, indicates that most Web sites that dispense health-related information fail to meet basic standards of impartiality and accuracy. Cardamone evaluated the top 100 Web sites returned in Yahoo searches on breast cancer, diabetes and depression, using the international Health On The Net Foundation's code of conduct. The code's guidelines address issues relating to the authority of the information given, user confidentiality, openness about corporate sponsorship, and emphasis on treating the information as complementary to medical treatment, rather than replacing it. Forty-two of the sites presented useful information: "Such sites contained quality, appropriate information with potentially lifesaving content such as explanations of the symptoms of depression, and healthy recipes for diabetics," says Cardamone. But the other 58 were a disappointment, containing unverified information. Meanwhile, other researchers have cited the growing phenomenon of "cyberchondria" — hypochondriacs who feed their health obsession with information from the Web. Such people are especially drawn to multiple choice quizzes that provide diagnoses based on a list of symptoms. (Sidney Morning Herald 16 Sep 2003)

# 1C1 Impersonation

*Category 1C1* *Impersonation*

2003-02-07 **impersonation fraud misrepresentation lies journalist worm**

NewsScan

REPORTER PERPETRATES WEB HOAX ON FELLOW JOURNALIST
Although it violates journalistic ethics for a reporter to misrepresent his identity, freelance journalist Brian McWilliams (whose work has appeared Salon and Wired News) used a fake Web site and phony to deceive Computerworld's Dan Verton into believing that he was a Pakistan-based terrorist who unleashed the recent Slammer network worm on the world. Computerworld published, then quickly retracted, Verton's story. McWilliams says he wanted to teach reporters "to be more skeptical of people who claim they're involved in cyber-terrorism." Computerworld editor-in-chief Maryfran Johnson says, "I couldn't believe a journalist could do this to another journalist," and Verton says, "I feel like I've been had, and that's never an easy thing to swallow. So, I'm left here scratching fleas as the price you sometimes pay for sleeping with dogs." (AP/San Jose Mercury News 7 Feb2003)

# 1C2 Identity theft

*Category 1C2* *Identity theft*

2003-02-28 **fraud misrepresentation impersonation spoofing privacy confidentiality**

NewsScan; NIPC/DHS

MONSTER.COM WARNS JOB-SEEKERS ABOUT POTENTIAL ID THEFT
Monster.com, a job-seeker's Web service whose database holds a quarter of a million resumes, has issued an e-mail message to its customers warning that "regrettably, from time to time, false job postings are listed online and used to illegally collect personal information from unsuspecting job-seekers." What should job-seekers do to protect themselves? Monster.com advises them not to give out their social security, credit card or bank account numbers, not to disclose marital status or other information not relevant to their job qualifications, and to be especially careful when responding to job-postings from prospective employers outside the country. (AP/San Jose Mercury News 28 Feb 2003)

February 28, Associated Press — Monster.com warns job seekers of ID theft. An e-mail labeled a "critical service message" is being sent from Internet job board Monster.com to all active users of Monster's main site. It cautions that "from time to time, false job postings are listed online and used to illegally collect personal information from unsuspecting job seekers." Pam Dixon, a research fellow with the Denver-based Privacy Foundation, said the e-mail confirms a growing hazard for online job seekers. "It's not just on Monster. I've heard of this on all the major sites." Dixon said most of the cases she's familiar with involve job seekers who have provided credit card numbers, social security numbers or agreed to ship overseas materials that are prohibited from being sold outside U.S. borders. Company spokesman Kevin Mullins said he did not know exactly how many people would receive the e-mail, but that it is "definitely well into the millions." Monster, the nation's largest Internet job board, says it has 24.5 million resumes posted on its main site. Mullins said the warning was not precipitated by any specific incident. Instead, the company is merely trying to protect its users, he said.

---

*Category 1C2* *Identity theft*

2003-09-02 **identity theft microsoft e-commerce coalition ITAA fighting online financial institutions**

NewsScan

COALITION FORMED TO BATTLE IDENTITY THEFT
The Information Technology Association of America has organized a new coalition aimed at fighting identity theft. The Coalition on Online Identity Theft, which includes e-commerce giants Amazon, eBay and Microsoft among its members, plans to launch a public education program and will encourage its members to work more closely with law enforcement officials to fight online crime. According to the Federal Trade Commission, the number of U.S. consumers who complained about some sort of identity theft nearly doubled last year to 162,000, but the Gartner Group says that statistic only scratches the surface of the problem. It estimates that 3.4% of U.S. consumers — some 7 million adults — suffered some form of identity theft in the past year. A report issued by Gartner in July says that while a consumer education campaign may make online users more savvy, there's still a major problem in the way ID theft cases are handled by financial institutions, who tend to treat such fraud as the cost of doing business rather than a crime against their customers: "There is a serious disconnect between the magnitude of identity theft that innocent consumers experience and the industry's proper recognition of the crime. Without external pressure from legislators and industry associations, financial services providers may not have sufficient incentive to stem the flow of identity theft crimes." (CNet News.com 2 Sep 2003)

---

# 1C5 Phishing

*Category 1C5* *Phishing*

2003-02-27 **Canada Internet Service Provider ISP e-mail scam fraud**

NIPC/DHS

February 25, Reuters — Canada's Sympatico targeted in Internet scam. Company officials at Sympatico, one of Canada's biggest Internet service providers (ISP), said Tuesday that organizers of a scam had sent out fraudulent e-mails to some 1,900 of Sympatico's 1.4 million customers last week. The e-mails told customers to fill out an online form to correct an error in their billing information and directed them to a fake site which asked for details, including driver's license, credit card and bank numbers and security codes. The fake site has since been shut down. "We did take immediate action to minimize the impact. E-mails that were going out to our customers were stopped and we contacted the ISP that was hosting this particular site," said Andrew Cole, a spokesman for Bell Canada. Cole said those who filled out the online forms should contact the police, their banks and credit card issuers. The company does not know who was behind the scam. "What we do know is the site was hosted in the United States. However, the e-mail itself was relayed through Japan...law enforcement and Bell security are certainly looking into the source," he said. He said the company did not think it was necessary to e-mail all of its customers, but that it had included several warnings about it on its sites. Sympatico.ca is owned by BCE Inc.'s Bell Canada unit, Canada's largest phone company.

---

*Category 1C5* *Phishing*

2003-03-19 **pornography swindle extortion organized crime**

NewsScan

PORN SWINDLE
Federal prosecutors in Brooklyn, NY, have arrested three men for using pornography Web sites to obtain credit information from visitors and then charging them as much as $90 a month, which was funneled into the coffers of the Gambino crime family. The scam worked like this: visitors to a porn site were offered a "free tour" of explicit material on the site, and asked to provide credit information as proof they were "adults." (New York Times 19 Mar 2003)

---

*Category 1C5* *Phishing*

2003-07-16 **virus Sophos antivirus ActiveX marketing trick**

NewsScan

'VIRAL MARKETING' STOOPS TO NEW LOW
Internet security company Sophos is warning of a new marketing scheme reported by its Australian tech support team, which tricks users into visiting a Web site featuring free comic video clips and then installs software that sends out e-mails from their computers to people listed in their address book. The Web site, run by Curacao-based Avenue Media, uses ActiveX to display a humorous video clip and at the same time downloads an additional software component called "Internet Optimizer" onto the PC, which then sends the e-mails. Peter Ducklin, head of technology at Sophos' Asia Pacific division, says: "What tricks a lot of people is that the ActiveX control which kicks the process off is digitally signed. Many users assume that a program which has been signed in this way is automatically both trustworthy and desirable. Ironically, even though Internet Explorer presents a 'security warning,' many people treat this as some kind of a 'security approval' and are more inclined to go ahead." (ZDNet Australia 16 Jul 2003)

---

*Category 1C5* *Phishing*

2003-09-03 **Web pornography DNS domain name service spoofing mousetrapping diversion phishing**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/6683165.htm

MAN ARRESTED FOR 'MOUSETRAPPING' CHILDREN
Federal agents have arrested a Florida man they say runs Web sites that exploit misspellings by computer users to redirect children looking for Disneyland or the Teletubbies to explicit porn sites instead. The government say it is the first prosecution under a provision of the new Amber Alert legislation that makes it a crime to use a misleading Web address to draw children to pornography. The man registered thousands of Internet addresses and was earning up to $1 million per year off them — much of it from sites that paid him when he sent Web users their way. The redirection technique is called "mousetrapping." U.S. Attorney James Comey said: "Few of us could imagine there was someone out there in cyberspace, essentially reaching out by hand to take children to the seediest corners of the Internet." (San Jose Mercury News 3 Sep 2003)

---

*Category 1C5* *Phishing*

2003-12-10 **PORN PURVEYOR GUILTY John Zuccarini deceptive domain names direct minors nudity adult content**

NewsScan

PORN PURVEYOR PLEADS GUILTY
John Zuccarini, of Hollywood, Florida, has pled guilty to 49 counts of using deceptive domain names to direct minors to nudity or other adult content, and to one count of child pornography possession. Prosecutors have recommended a three-year prison sentence with fines still to be determined. Zuccarini owned at least 3,000 domain names, most of which were misspelled versions of popular brands, such as www.dinseyland.com. (Wall Street Journal 10 Dec 2003)

# 1D1 Organizations, cooperation for law enforcement

*Category 1D1 Organizations, cooperation for law enforcement*

2003-01-31 **database sharing collaboration law enforcement State Department**

NewsScan

VISA APPLICATIONS TO BE SHARED WITH LAW ENFORCEMENT
The U.S. State Department will soon give law enforcement officials access to a database containing 50 million overseas applications for U.S. visas. The information will be accessible by intelligence agencies, the FBI, and police departments throughout the country. Although the database will not be making any new information available (but simply making existing information more accessible to law enforcement agencies), a Justice Department official says: "There is a potential source of information that isn't available elsewhere. It's not just useful for terrorism. It's drug trafficking, money laundering, a variety of frauds, not to mention domestic crimes." But some civil liberties advocates say they are worried that the system will be abused by over-use: "The availability of this information will change police conduct. You are more likely to stop someone if you have the ability to query a database. The data chases applications." (New York Times 31 Jan 2003)

---

*Category 1D1 Organizations, cooperation for law enforcement*

2003-02-12 **Europe coordination network information security agency infowar defense**

NewsScan

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY
The European Commission is planning the creation of a European Network & Information Security Agency intended to coordinate computer security activities of the 15 EC member states. Erkki Likanen, the EC's commissioner for the information society, said that the European Union "will benefit from increased coordination between member states to achieve a sufficiently high level of security in all member states. The Internet is a wonderful tool, but to be able to benefit from it, you have to guarantee security." (Computerworld 10 Feb 2003)

---

*Category 1D1 Organizations, cooperation for law enforcement*

2003-03-17 **Pakistan cyber crime wing security intelligence**

NIPC/DHS

March 13, Wired — Pakistan creates cyber crime wing. A Pakistani security agency has launched a special wing to combat cyber crimes in part because the country had to rely on U.S. investigators to trace e-mails sent by the kidnappers of American journalist Daniel Pearl a year ago. "The purpose of establishing the National Response Center for Cyber Crimes is to stop misuse of the Internet and trace those involved in cyber-related crimes," Iftikhar Ahmad, spokesman for Pakistan's Interior Ministry, told the Associated Press on Wednesday. "The importance of this special wing was felt when Daniel Pearl was kidnapped, and his captors started sending e-mails to newspapers," he said. The Wall Street Journal correspondent disappeared on January 23, 2002, from Pakistan's southern city of Karachi. "The National Response Center for Cyber Crimes will play a key role in the days to come in tracing those terrorists who often use the Internet or prepaid telephone cards to communicate messages to their associates for carrying out acts of terrorism and other purposes," Ahmad said. The special wing has been established at the headquarters of an intelligence agency in Islamabad, Pakistan's capital.

---

*Category 1D1 Organizations, cooperation for law enforcement*

2003-03-18 **anti-hacking anti-virus hotline Korea network emergency report**

NIPC/DHS

March 11, SC Infosecurity News — Korean government opens anti-hacking and virus hotline. The Korea Information Security Agency (KISA) has teamed up with 13 major ISPs and other internet bodies in Korea to create a national anti-hacking and virus hotline and information service. Their aim is to take rapid action in the event of a cyberattack. KISA, which is affiliated with the Korean government's Ministry of Information and Communication, defines a network emergency as where the volume of Korean internet traffic varies by 20 per cent internationally and 50 per cent nationally, within the space of five minutes. All Korean ISPs and internet data centers (IDCs) in Korea are expected to report their operational status twice a day to the hotline, as well as keeping the hotline staff informed of their status and countermeasures taken in the event of a network emergency.

---

*Category 1D1* *Organizations, cooperation for law enforcement*

2003-04-14 **Pakistan Network Security Working Group ISP IT intelligence defense virus Trojan**

NIPC/DHS

April 09, The International News — Pakistan sets up Working Group for Network Security. The ministry of information technology in Karachi, Pakistan, has set up a Working Group for Network Security to outline measures for cyber safety in the country. "The Working Group would comprise around 25 persons belonging to ministry of IT, intelligence agencies, representatives from internet service providers (ISPs) and the country's renowned software houses," said an official at the ministry who wished not to be named. "You can call it a professionals' forum with objectives to oversee and drive the development of network security, threat assessment, defensive and offensive mechanisms, viruses and Trojans. The Group will bring together various public and private sector entities to create synergies and establish direct contact among the specialists," the official informed. Initially, the Group would discuss growing threat of insecure networks, intrusions, web page defacements and cyber terrorism. It will then discuss formulation of policies and guidelines and encourage ideas related to strong authentication mechanism such as smart cards, PKI, biometrics, Kerberos, tokens, digital certificates.

*Category 1D1* *Organizations, cooperation for law enforcement*

2003-04-24 **hacker hacking Pakistan information telecommunication Working Group Network Security**

NIPC/DHS

April 22, The International News (Pakistan) — Pakistan to use hackers against hackers. The ministry of information technology and telecommunications in Karachi, Pakistan, has decided to hire hackers to confront cyber attacks on government websites and silicon networking. The decision came at a meeting held last week to set up a Working Group for Network Security — one of the steps to counter hackers' moves. The group is composed of ministry officials, intelligence agencies sleuths and representatives from private sector internet service providers (ISPs) and software houses in Pakistan.

*Category 1D1* *Organizations, cooperation for law enforcement*

2003-05-09 **New South Wales counter-terrorist police hackers fight terrorism mobile phones cars chips organizations court**

NIPC/DHS

May 09, Sydney Morning Herald (Australia) — Australian police enlist hackers to fight terrorism. Australian police are offering 20 computer IT specialists the opportunity to become highly paid operatives working for the New South Wales (NSW) counter-terrorist unit. The successful applicants will join a newly created unit within the police Special Service Group that will be called the State Electronic Evidence Branch. The computer specialists will examine computer drives and even microchips from cars and mobile phones of people suspected of having links with terrorist organizations. Superintendent Tony Jeffries said the cyber sleuths would examine computer pathways for hidden information and undergo training in forensic analysis so that any potential data relating to terrorist activities in NSW could be used in court in prosecutions of suspects.

*Category 1D1* *Organizations, cooperation for law enforcement*

2003-05-16 **south korea security hackers cyber-warfare north Seoul Defense Security Command Song Young business**

NIPC/DHS

May 16, Reuters — South Korea fortifying computer security. North Korea is training around 100 computer hackers each year to boost its cyber-warfare capabilities, pushing the South to fortify its own computer security, a South Korean military official said Friday. South Korea is one of the world's most wired countries, making it vulnerable to cyber attacks, Song Young-keun, commanding general of Seoul's Defense Security Command, was quoted as saying. 70 percent of households in South Korea have Internet access. Song said the military would also need the combined efforts of research institutions and private sector businesses to strengthen cyber security, the report added.

*Category 1D1* *Organizations, cooperation for law enforcement*

2003-05-16 **intrenet fraud scams identity theft goods purchase online pharmaceutical drugs**

NewsScan

U.S. CRACKS DOWN ON INTERNET FRAUD
The Justice Department has charged more than 130 people with perpetrating a variety of Internet scams, as well as identity theft and failure to deliver goods purchased online. The crackdown, dubbed Operation E-Con, involved more than 90 investigations involving 89,000 victims whose losses totaled at least $176 million. In one case, the suspects used a Web site to sell more than $2 million worth of pharmaceutical drugs without any prescriptions or physician involvement with the purchasers. In another scam, about 400 men lost about $3,000 each when they sent money off in the hope of winning the hand a Russian bride. Other scams promoted fraudulent investment opportunities, Ponzi-type pyramid schemes and the illegal sale of copyright-protected software, games and movies. Officials say they've managed to recover about $17 million from alleged perpetrators. (AP/Siliconvalley.com 16 May 2003)

---

*Category 1D1* *Organizations, cooperation for law enforcement*

2003-05-27 **UK police cyber crime victims National High Tech Crime Unit NHTCU Lyons leaks confidentialty charter report computer**

NIPC/DHS

May 27, vnunet.com — UK police provide PR help to cyber crime victims. The UK's National High Tech Crime Unit (NHTCU) is to help handle PR for firms that have been the victims of computer crime, in an attempt to encourage more prosecutions. In December the unit launched a confidentiality charter, which allows companies to report computer crime without fear of public disclosure, but some firms are pulling out of prosecutions just before they go to court, according to John Lyons of the NHTCU. Lyons said one problem is companies fear bad publicity from prosecutions. In the event of a prosecution the unit's PR staff will work to avoid leaks and promote a positive image of companies helping the police, he said.

---

*Category 1D1* *Organizations, cooperation for law enforcement*

2003-06-04 **hawaii cybercrime FBI office explosive growth computer crimes raud Honolulu**

NIPC/DHS

June 04, Honolulu Advertiser — Hawaii fights rising cybercrime. The Federal Bureau of Investigation's (FBI) Hawaii office established its first cybercrime squad this year, responding to what investigators are calling "explosive growth" in computer-related crimes. Larry Futa, supervisory special agent of the Cybercrimes Squad at the FBI's Hawaii field office, said protecting the United States against cyber-based attacks and high-technology crimes is only behind fighting terrorism and espionage on the agency's list of priorities. With about 400 computer fraud complaints reported to the fraud center in 2002, Hawaii was the second highest per capita in the United States for Internet fraud complaints, second only to the District of Columbia. Futa's cyberagents work closely with the Honolulu Police Department, the attorney general's office, the Bureau of Immigrations and Customs Enforcement, the Secret Service and other federal, state and local agencies.

---

*Category 1D1* *Organizations, cooperation for law enforcement*

2003-06-06 **cyber security government homeland cyberspace national**

NewsScan

HOMELAND SECURITY DEPARTMENT TARGETS CYBERSPACE
The Department of Homeland Security has created a National Cyber Security Division — a 60-person unit that will operate under the Department's Information Analysis and Infrastructure Protection Directorate. The new division will build on existing expertise developed at the former Critical Infrastructure Assurance Office, the National Infrastructure Protection Center, the Federal Computer Incident Response Center and the National Communications System. "Most businesses in this country are unable to segregate the cyberoperations from the physical aspects of their business because they operate interdependently. This new division will be focused on the vitally important task of protecting the nation's cyberassets so that we may best protect the nation's critical infrastructure assets," said Homeland Security Secretary Tom Ridge in a statement. (CNet News.com 6 Jun 2003)

---

*Category 1D1* *Organizations, cooperation for law enforcement*

2003-06-06 **cybersecurity offile Tom Ridge DHS Department of Homeland Security 60 employees Critical Infrastructure Assurance Office NIPC Protection**

NIPC/DHS

June 06, Washington Post — Government creates new cybersecurity office. The Department of Homeland Security said Friday it will establish an office to focus on U.S. cybersecurity. The National Cyber Security Division will "conduct cyberspace analysis" and issue warnings and alerts about online attacks, the department said. The division also will respond to major Internet attacks and assist in "national-level recovery efforts." Homeland Security Secretary Tom Ridge said the division will have 60 employees. Part of the new division's mission will be to coordinate the efforts of several cybersecurity offices that were folded into the Homeland Security Department this year. Among the former offices that will be put into the division are the Critical Infrastructure Assurance Office, the National Infrastructure Protection Center, the Federal Computer Incident Response Center and the National Communications System. The office will be part of the department's Information Analysis and Infrastructure Protection division.

*Category 1D1* *Organizations, cooperation for law enforcement*

2003-06-14 **India fight hackers internet security centre business government establishment Carnegie Mellon IIT Information Technology**

NIPC/DHS

June 14, BBC News — India gears up to fight hackers. India's first internet security centre is due to become operational in July. The centre will aim to prevent cyber attacks on key defense, business and government establishments. The project is being handled by the central information technology ministry with the help of the U.S.-based security group, CERT, a research and development centre run by the Carnegie Mellon University. The date for the launch of the net security centre was announced by India's Information Technology Secretary Rajiv Ratan Shah in the southern Indian city of Bangalore. Based in the capital, Delhi, the centre is expected to cost up to $20 million. A second centre will be set up in Bangalore at India's leading research organization, the Indian Institute of Science.

*Category 1D1* *Organizations, cooperation for law enforcement*

2003-09-16 **global war hackers U.S. cyver-attacks DHS CERT watchdog Cyber Security national international**

NIPC/DHS

September 16, vnunet.com — U.S. declares global war on hackers. The increasing sophistication and speed of cyber-attacks has prompted the launch of a U.S.-led global internet monitoring service. The Department of Homeland Security will join with Carnegie Mellon University's Computer Emergency Response Team Coordination Center (Cert/CC). Dubbed US-Cert, the watchdog aims to act as a "coordination point for the prevention, protection and response to cyber-attacks across the internet." It will coordinate national and international efforts to prevent cyber-attacks, protect systems and respond to the effects of attacks across the internet. "Our nation's growing use of the internet for safety-critical applications as well as business transactions, coupled with the increased sophistication and speed of cyber-attacks, increases the risk [of] significant damage in short periods of time," said Richard Pethia, director of Cert/CC. US-Cert will begin as a partnership between Cert/CC and the National Cyber Security Division of the Department of Homeland Security.

*Category 1D1* *Organizations, cooperation for law enforcement*

2003-10-18 **Internet drug sales law enforcement task force**

http://www.nytimes.com/2003/10/18/technology/18DRUG.html?th

Two federal agencies have formed a task force, Operation Gray Lord, to crack down on the growing tide of illicit sales of prescription narcotics on the Internet. FDA and DEA officers will be working with the DoJ and the RCMP in Canada to stop the illegal trade.

*Category 1D1* *Organizations, cooperation for law enforcement*

2003-10-27 **Brazil cybercrime lab identity data theft attack internet violent crime police officials Sao Paulo hacker commission vandalism**

NIPC/DHS

October 27, New York Times — Brazil becomes a cybercrime lab. Brazil is becoming a laboratory for cybercrime, with hackers specializing in identity and data theft, credit card fraud and piracy, as well as online vandalism. So far this year, nearly 96,000 overt Internet attacks—ones that are reported, validated or witnessed—have been traced to Brazil. Already overburdened in their fight to contain violent crime, police officials are finding it difficult to keep pace with hacker syndicates. The 20 officers working for the electronic crime division of the São Paulo police catch about 40 cybercrooks a month. But those criminals account for but a fraction of the "notorious and ever increasing" number of cybercrimes in São Paulo, Brazil's economic capital, said Ronaldo Tossunian, the department's deputy commissioner. The São Paulo department's effort is not helped by vague legislation dating back to 1988. Under that law, police officers cannot arrest a hacker merely for breaking into a site, or even distributing a software virus, unless they can prove the action resulted in the commission of a crime.

*Category 1D1* *Organizations, cooperation for law enforcement*

2003-11-13 **security chiefs think tank prevent hackers crackers secure coding software programs better internet**

NewsScan

TOP TECH SECURITY CHIEFS FORM THINK TANK
A group of top technology luminaries is forming a new think tank that will focus on ways to elevate the status of chief security officers in the private sector — a move that they say will help significantly in the escalating battle against hackers and crackers. In addition, the Global Council of Chief Security Officers will consult with technology vendors and industry groups to help design more secure products for the next-generation Internet, and will work to encourage increased compatibility between different and competing technologies. Among the Council members are top security officials from Microsoft, Sun Microsystems, Oracle, Motorola, MCI, Washington Mutual, Bank of America, Citigroup and the New York State Office of Cyberspace Security. "Many of us have a long-term connection with the Internet and an interest in seeing it survive well into the 21st century, and there is a great deal going on that could potentially threaten its stability," says MCI's Vint Cerf, often referred to as "the father of the Internet" for his early work with Darpanet. The Council is the brainchild of former White House cybersecurity adviser Howard Schmidt, who's now the chief security officer for eBay. (Washington Post 13 Nov 2003)

*Category 1D1* *Organizations, cooperation for law enforcement*

2003-11-24 **Europe EU Internet security agency crime online prevention**

NIPC/DHS

November 22, Associated Press — EU sets up Internet security agency. The European Union (EU) governments agreed Thursday, November 20, to launch an agency to protect the Internet by alerting the public about computer viruses, identity theft and other crimes committed online. The European Network and Information Security Agency is to be operational in early 2004. It is to help governments, businesses and consumers protect their computer systems and data and inject some order in the varying approaches EU nations have taken so far to combat Internet crimes. "Trust and security are crucial components in the information society," Erkki Liikanen, the EU's information society commissioner, said in a statement.

*Category 1D1* *Organizations, cooperation for law enforcement*

2003-12-17 **cyber crimes task force Ohio federal violation network attack critical infrastructure**

NIPC/DHS

December 16, Cyber Crimes Task Force of Central Ohio — Cyber task force opens in Ohio. The Central Ohio Cyber Task Force (CCTF) officially opened on on Monday, December 15. The CCTF is a joint federal task force which investigates federal violations of cyber crime in central Ohio, and is the first of its kind in Ohio. The primary crime areas the CCTF investigates and is also willing to serve as a resource for local and state law enforcement agencies are those where a computer is the primary target or tool of a criminal subject to commit any of the following: computer network attacks and intrusions, particularly for all critical infrastructure, government and the Department of Defense servers/networks and for severe commercial losses; sexual exploitation of children; Internet fraud; and intellectual property rights. The CCTF is a cooperative effort of the FBI, U.S. Department of Defense, Defense Criminal Investigative Service, the Ohio State University Police Department, City Columbus Police Department, City of Grandview Police Department, and Ohio Attorney General's Office. It is also supported by the United States Attorney's Office and Southern District of Ohio Franklin County Prosecutor's Office.

# 1D2 Technology for law enforcement

*Category 1D2* *Technology for law enforcement*

2003-01-06 **surveillance cameras analysis**

NewsScan

SMARTCAMS
Surveillance technology has gone from a technology that (if the power didn't fail) produced grainy black-and-white tapes to one using solar-powered digital cameras that can send color images over digital networks to databases, which can be examined by software to identify potential problems and immediately alert security guards. Bruce Finchbaugh, a Texas Instruments researcher, describes this development as "adding new intelligence to redefine security," and Hoover Institute research fellow Nick Imearato predicts that the new technology will get cheap enough for it to "migrate to millions of businesses and even homes." But Lee Tren, an attorney at the civil liberties-focused Electronic Frontier Foundation, urges caution because "this kind of continuous recording can be very dangerous, especially if coupled with technology to recognize faces. You have to always ask what is the compelling justification for such surveillance." (San Jose Mercury News 6 Jan 2003)

---

*Category 1D2* *Technology for law enforcement*

2003-01-13 **law enforcement databases name matching foreign spellings**

NewsScan

WHAT'S IN A NAME?
Everyone from the FBI to financial firms is struggling to keep track of an increasing number of individuals with foreign (non-European) names that may be spelled in several different ways in different databases. The issue of name-matching has become particularly acute now that the U.S. government is attempting to track visitors with a Middle Eastern background — as an example, a visit to Google produces some 50 different spellings of Mohmmar Qadaffi (or is it Muammar Gaddifi?). In response software firms are racing provide effective tools for foreign-name searches. "Last year was our best ever," says the CEO of Language Analysis Systems, which provides foreign-name searching and recognition products. While 75% of the company's business comes from the U.S. government, it's also seen increased interest from banks, airline reservation systems and data-mining companies. Language Analysis recently paired up with Basis Technology to offer the government a product called Cartouche — a name-matching system for searching and retrieving names across multiple languages. Basis CEO Carl Hoffman has urged the government to adopt Unicode-compliant systems, which would make it possible to display and process foreign names, not only as they appear in the English alphabet, but also as they appear in their native scripts. (Wired.com 13 Jan 2003)
http://www.wired.com/news/conflict/0,2100,57167,00.html

---

*Category 1D2* *Technology for law enforcement*

2003-02-12 **security camera airport scanner privacy modesty**

NewsScan

REVOLUTION SEE-THROUGH PHOTOGRAPHY
A new astronomy technique sometimes referred to as "quasi-optics" has been used to produce a so-called "T-ray image" of a human hand taken through a 15-millimeter pad of paper. The new technology —- which allows a terahertz camera to effectively see through smoke, fog, walls, a person's clothing, etc. — is likely to revolutionize imaging in astronomy, medicine, and airport security. A future version of the terahertz camera might one day be used in space to examine the early universe. (Space.com 11 Feb 2003)

---

*Category 1D2* *Technology for law enforcement*

2003-03-05 **Web hijacking redirection law enforcement domain seizure**

NewsScan

FEDS SEIZE DOMAIN NAMES OF ALLEGED OFFENDERS
Attorney General John Ashcroft says federal agents have taken control of several Web sites allegedly selling illegal "drug paraphernalia" and have redirected them to servers at the Drug Enforcement Administration. A federal judge in Pittsburgh ruled that the takeover was permitted until a trial can take place. Meanwhile, the DOJ also reported it has seized the iSoNews.com domain, whose owner pled guilty to using his site to sell "mod" chips that enable Xbox and PlayStation owners to modify their game consoles so they can play illegally copied games. Visitors to the iSoNews.com site yesterday were greeted with a notice stating: "The domain and Web site were surrendered to U.S. law enforcement pursuant to a federal prosecution and felony plea agreement for conspiracy to violate criminal copyright laws." The seizing of Internet domain names represents a new tactic in the DoJ's arsenal against crime, with a spokesman for the Electronic Privacy Information Center observing that the practice becomes a kind of "electronic flypaper" that raises novel legal questions. (CNet News.com 26 Feb 2003)
http://news.com.com/2100-1023-986225.html

CRIMINALS LOSING THEIR DOMAIN NAMES TO THE FEDS
In recent weeks the Justice Department has been seizing the Internet domain names they allege were used in commission of a crime, and have been continuing the operation of seized Web sites to greet visitors with stern warnings from government agencies. Civil libertarians are concerned that such seizures are depriving site owners not just of their property but of their livelihoods. They're also worried that by continuing operation of confiscated sites the government would be in a position (in the words of David Sobel of the Electronic Privacy Information Center "to monitor the Web-surfing activities of unwitting individuals who believe they are going to a Web site... but possibly implicating themselves in some law enforcement investigation." (AP/San Jose Mercury News)

---

*Category 1D2* *Technology for law enforcement*

2003-05-01 **internet wiretaps Cisco phone calls detection products surveillance**

NewsScan

INTERNET WIRETAPS FROM CISCO
In response to concerns by law enforcement officials that criminals can use Internet telephony to avoid court-approved wiretaps, Cisco Systems has developed a way for police to monitor Internet-based phone calls without detection. The company says it is building the capabilities into a limited number of its new products, though none have been sold as yet. The monitoring service includes an auditing mechanism by a third-party provider, in order to ensure that the surveillance complies with all laws governing interception of communication. (AP/USA Today 1 May 2003)

---

*Category 1D2* *Technology for law enforcement*

2003-05-30 **log file virtual operating system replay attack digital forensics recovery computer crime**

NewsFactor Network
http://science.newsfactor.com/story.xhtml?story_title=Virtual_Time_Machine_May_Foil_Hackers&story_id=21642#story-start

Prof. Peter Chen of the University of Michigan has proposed using a virtual machine called ReVirt to log all significant events to disk, permitting not only reversion to any given point in time, but also replay of the events in a computer attack. Chen estimates that a 100GB hard disk could easily store several months worth of log files with minimal overhead. Chen and his colleagues published an article with the following abstract < http://portal.acm.org/citation.cfm?id=844148&jmp=citings&coll=GUIDE&dl=ACM > :

Current system loggers have two problems: they depend on the integrity of the operating system being logged, and they do not save sufficient information to replay and analyze attacks that include any non-deterministic events. ReVirt removes the dependency on the target operating system by moving it into a virtual machine and logging below the virtual machine. This allows ReVirt to replay the system's execution before, during, and after an intruder compromises the system, even if the intruder replaces the target operating system. ReVirt logs enough information to replay a long-term execution of the virtual machine instruction-by-instruction. This enables it to provide arbitrarily detailed observations about what transpired on the system, even in the presence of non-deterministic attacks and executions. ReVirt adds reasonable time and space overhead. Overheads due to virtualization are imperceptible for interactive use and CPU-bound workloads, and 13—58% for kernel-intensive workloads. Logging adds 0—8% overhead, and logging traffic for our workloads can be stored on a single disk for several months.

For another summary of the system, see Kim Roth's article, "Virtual Replay" in the _Michigan Engineer_ [Fall/Winter 2003] at < http://www.engin.umich.edu/alumni/engineer/03FW/feature/ >.

---

*Category 1D2* *Technology for law enforcement*

2003-06-04 **research NSA National Security Agency supercomputing problems computational analyze intelligence data Perntagon aircraft ships nuclear**

NIPC/DHS

June 04, National Journal — Security officials urge more research into supercomputing. The nation's investment in supercomputing research and development has played a crucial role in national security, but more investment is needed to resolve numerous computational problems, a key National Security Agency (NSA) official said on Wednesday. George Cotter, chief of NSA's Office of Corporate Assessments, told attendees of an Army High-Performance Computing Research Center luncheon that the conclusion of a congressionally mandated study on high-end computing R&D determined a need for faster computing to enable the military to create better weapons, aircraft and ships, as well as to improve the nation's ability to monitor its nuclear-weapons stockpile. Faster computers also are needed to analyze intelligence data and build better mapping capabilities for the military, he said. The center has received $4 million in research funding annually over the past two years from the Army as the Pentagon decided to increase its focus on using supercomputing for military purposes. The program was initiated in 1990.

*Category 1D2* *Technology for law enforcement*

2003-08-22 **crime fight computer database check fraud**

NewsScan

DATABASE TO FIGHT FINANCIAL CRIME
Banks throughout the Midwest U.S. can make use of a computer database called FinCrime that allows financial institutions and law enforcement to share information about crimes and provide warnings. Once check fraud or some other financial crime is committed, bankers and law enforcement personnel can enter information about the crime and the suspect into the database. FinCrime looks for matching information. "Obviously the more participants we have, the more data we can gather in this electronic database, the more valuable it's going to be for participants," said John Sorensen, president and chief executive of the Iowa Bankers Association. "We're trying to expand it widely and keep the cost of participation at either nothing or very small costs... One of the unique things about our network is that it's going to be owned by state banking associations and that it will be provided really as a service as members of these state banking associations," Sorensen said. (AP/USA Today 22 Aug 2003)

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

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

2003-03-07 **probable cause judicial ruling fourth amendment**

NewsScan

TWO JUDGES REJECT FBI TESTIMONY IN INTERNET PORN CASES
Federal district judges Denny Chin in New York and Catherine D. Perry in St. Louis have rejected evidence obtained by FBI agents who claimed falsely that anyone signing up with the child porn site "Candyman" would automatically receive child porn images from other site members. Later, the agents admitted that people signing up for the group had the ability to opt out of the member mailing list and therefore did not necessarily receive pornography through that list. Judge Chin wrote: "If the government is correct in its position that membership in the Candyman group alone was sufficient to support a finding of probable cause, then probable cause existed to intrude into the homes" of thousands of people who had merely logged onto that Web site. "Here, the intrusion is potentially enormous. Thousands of individuals would be subject to search, their homes invaded and their property seized, in one fell swoop, even though their only activity consisted of entering an e-mail address into a Web site from a computer located in the confines of their homes." (New York Times 7 Mar 2003)

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

2003-04-03 **wiretapping issues VoIP voice over IP**

NewsScan

ONLINE WIRETAPPING POSES LEGAL, TECHNICAL OBSTACLES
As the Internet telephony market expands, law enforcement officials are facing both legal and technical hurdles as they seek to block the emerging services from becoming a haven for criminals and terrorists. The FBI wants regulators to affirm that tapping into Voice over Internet Protocol (VoIP) networks is covered under the 1994 Communications Assistance for Law Enforcement Act, and is also pushing the industry to create technical standards that would make such wiretaps easier and cheaper. Because VoIP is so new, standards don't yet exist for setting up networks, but several groups, including the Telecommunications Industry Association, are working on them. "We're seeing major changes in the network, and we are trying to be ahead of the curve," says the FBI's unit chief for electronic surveillance. Privacy advocates, on the other hand, fear that because of the nature of the technology, tapping into the data stream for voice would also possibly retrieve more than what the court ordered, including people's e-mail and other digital communications. (AP 3 Apr 2003)

# 1D4 Government funding for law enforcement

*Category 1D4* *Government funding for law enforcement*

2003-04-30 **Tom Ridge DHS Northern Virginia Technology Y2K 9/11 terrorist attacks ideas security**

NIPC/DHS

April 30, IDG News Service — DHS asks for tech help. Tom Ridge, secretary of the Department of Homeland Security (DHS), highlighted his department's need for technological innovations during a speech for members of the Northern Virginia Technology Council in Virginia, Tuesday. Ridge also called for the technology industry to do more to protect the U.S. technology infrastructure, noting that private companies control 85 percent of the nation's cyber resources. "We think that the lessons learned from Y2K and 9/11 should be applied and not forgotten. Ridge said he fears that some U.S. residents may be "lapsing into complacency" about the possibility of terrorist attacks. "You need to be just as worried, maybe even more worried, about somebody hacking into your system as somebody pulling up with explosives," Ridge said. Ridge asked the crowd for "good ideas and cost-effective solutions" for domestic security that can be copied across the U.S.

*Category 1D4* *Government funding for law enforcement*

2003-08-08 **NSA National Security Agency backdoor detection center information assurance director Daniel Wolf Software logic bombs**

NIPC/DHS

August 08, SecurityFocus — NSA proposes backdoor detection center. The information assurance director for the National Security Agency's (NSA) is calling on Congress to fund a new National Software Assurance Center dedicated to developing advanced techniques for detecting backdoors and logic bombs in large software applications. In testimony before the House Select Committee on Homeland Security's cybersecurity subcommittee last month, Daniel Wolf bemoaned an absence of tools capable of scouring program source code and executables for evidence of tampering. The proposed solution: a federally funded think-tank that would include representatives from academia, industry, government, national laboratories and "the national security community," said Wolf, "all working together and sharing techniques."

*Category 1D4* *Government funding for law enforcement*

2003-10-23 **internet Security Ads Government TV radio firewall virus alerts national cyber security Alliance worms FTC**

NIPC/DHS

October 23, Washington Post — U.S. government plans Internet security ads. An advertising campaign designed to educate home and small business computer users about the importance of using firewalls and anti-virus software, as well as defending against online fraud, is expected to debut next year. The $1.8 million program is the brainchild of officials at the Department of Homeland Security (DHS) and the National Cyber Security Alliance, a group of more than 50 technology companies. The campaign will air on television and radio spots and in magazines, newspapers and movie theaters throughout the country. The alliance in a June study found that roughly 67 percent of high-speed Internet users do not use firewalls. More than 60 percent of those surveyed said they did not keep their anti-virus software updated against the most current viruses and worms. Orson Swindle, a commissioner on the Federal Trade Commission, said the large number of people affected by online fraud and the recent spate of viruses and worms show just how much education needs to be done.

# 1E Homeland Security

*Category 1E* *Homeland Security*

2003-01-06 **Department Homeland Security IT key success federal agencies US government anti-terrorism**

NIPC/DHS

January 02, National Journal's Technology Daily — IT systems key to success of Department of Homeland Security. Strong information technology systems will be crucial to the success of the new Department of Homeland Security, according to the General Accounting Office (GAO). The GAO report (03-260), released December 24, found that federal agencies have made progress in addressing their homeland security missions since the September 11, 2001, terrorist attacks, and that information sharing between federal agencies has increased. But GAO said federal agencies still face many challenges, such as improving their collaboration with state and local officials and with the private sector. Twenty-two existing federal agencies and offices will move into the new DHS, which also will include an Office of State and Local Coordination and a liaison official for the private sector. GAO estimated that the full transition to the new department could take five to 10 years, and recommended that the Office of Management and Budget (OMB) work with the department to implement the appropriate management systems. "Strong financial and information technology systems will also be critical to the success of [the DHS] and other organizations with homeland security missions."

---

*Category 1E* *Homeland Security*

2003-01-07 **Department Homeland Security IT implementation worries security**

NIPC/DHS

January 06, Washington Post — Setting up IT infrastructure will help the Department of Homeland Security. One of the challenges in creating a department from a hodgepodge of 22 federal agencies and 170,000 employees is the information technology headache. "It is not enough to shuffle redundant or overlapping programs under the new bureaucracy," Michael Scardaville, a policy analyst at the Heritage Foundation, wrote in a recent report. The department "should develop and deploy an information technology infrastructure that links and fuses intelligence and law enforcement terrorism databases." Representative of the agency's challenge will be monitoring the thousands of freighters that enter U.S. ports daily. The department wants a "smart border" program in which cargo ships heading for U.S. ports would electronically file information detailing the contents of cargo containers, crew members' names and nationalities, and what stops the ships are scheduled to make before reaching the United States. Steven I. Cooper, special assistant to the president on information technology's place in homeland security, admitted, it may be a lengthy process. "I think parts of it could probably be done fairly quickly, meaning within months instead of years," he said. "To fully put together something like that across the world is obviously going to take a longer period of time." In the meantime, short term priorities for the new department will include border and transportation security technology, such as equipment that identifies radioactivity and software that identifies non-obvious trends in databases or protects computer infrastructure from hackers.

---

*Category 1E* *Homeland Security*

2003-02-28 **Department Homeland Security DHS technology barrier divide education**

NIPC/DHS

February 26, Federal Computer Week — Info sharing hobbled by lack of technology. Agencies merging into the Homeland Security Department as well as others sharing information in the government's antiterrorism efforts are working to overcome technological barriers, but the work is going to take time, according to a panel of agency officials who spoke February 26 at an AFCEA International Inc. conference in Washington, D.C. One challenge is ensuring that information stays out of the hands of those not authorized to see it. To that end, the National Security Agency (NSA) is developing "trusted control interfaces," which the CIA is implementing, said William Dawson, chief information officer of the CIA's Department of Intelligence Communications. The interfaces' intent is to strip classified information from messages before passing them to someone of a lower security class. An early stage of the system is running at the CIA, but most of the capabilities won't be ready until September, Dawson said.

---

*Category 1E* *Homeland Security*

2003-03-11 **Internet violence Islamic fundamentalism connection**

NIPC/DHS

March 02, Time Magazine — Investigators examine the links between Islamic fundamentalists and the Internet. On February 26, Sami Omar al-Hussayen, a Ph.D. Candidate in computer security at the University of Idaho, was charged with violating conditions of his student visa by registering and maintaining a dozen militant websites promoting violence against U.S. interests. U.S. officials want to know more about al-Hussayen's work for the sponsor of most of these sites, the radical Islamic Assembly of North America (IANA), a Michigan-based group known as one of the most strident voices of Islam on the Web. IANA hosted the websites of two radical Saudi sheiks - Salman al-Awdah and Safar al-Hawali - both of whom are closely associated with Osama bin Laden and who provided religious justification for the September 11 attacks, according to the SITE Institute, a Washington-based terrorist-research group that monitors the Internet. Al-Hussayen's case also may provide fresh evidence that at least some of these anti-American websites are being supported by funds coming from Saudi Arabia. Al-Hussayen is accused of covertly receiving $300,000 from abroad and disbursing much of it to IANA. A Saudi-embassy spokesman in Washington said no government money has gone to IANA.

---

*Category 1E* *Homeland Security*

2003-03-17 **DHS infrastructure protection evaluation anti-terrorism**

NIPC/DHS

March 13, Federal Computer Week — Homeland CIO outlines priorities. Steve Cooper, the CIO of the new Department of Homeland Security (DHS), told an industry gathering that it is essential to move quickly to build DHS' infrastructure because "state-sponsored terrorists and al Qaeda are not going to wait until we have our act together." He said he and his information technology team will complete an inventory of IT assets brought together by the merger of 22 federal agencies. It will be evaluated for "reuse, renewal, retirement or enhancement," and he expects to decide what systems to keep and what to retire by August. In the next six weeks, DHS will issue a series of requests for information about wireless and geospatial technology to help officials decide how to create the best systems.

---

*Category 1E* *Homeland Security*

2003-03-24 **Department Homeland Security DHS security focus infrastructure protection**

NIPC/DHS

March 20, National Journal's Technology Daily — Ridge: Cybersecurity at 'heart' of department's work. Department of Homeland Security (DHS) Secretary Tom Ridge said on Thursday that his department will work as hard to address threats to the Internet as it does to address physical threats. "We will not distinguish between physical and cyber in this new unit," Ridge told the House Homeland Security Appropriations Subcommittee in a hearing on the fiscal 2004 budget. Ridge said that he understands a cyber attack could affect every aspect of the U.S. economy and government and that preventing such an attack is "at the very heart" of his department's duties. He also said that since last month, the department has been "actively engaged" in talks about the nation's cyber infrastructure with the private sector and other groups "because they have their own list of what the vulnerabilities are." Much rests on the vulnerability assessments being done on critical infrastructures, he said. Ridge said the department's chief information officer is developing plans for a technology framework that would enable Homeland Security to share information both within and outside the department. A strategic plan to let the department's various agencies access terrorist watch lists also is being prepared, he said.

---

*Category 1E* *Homeland Security*

2003-03-25 **cyber security anti-terrorism infrastructure protection**

NIPC/DHS

March 21, Government Computer News — Leadership selected for new cybersecurity panel. Leaders have been named for the new House Homeland Security subcommittee on Cybersecurity, Science and Research and Development. Rep. Mac Thornberry (R-TX) will chair the subcommittee and the ranking minority member is Rep. Zoe Lofgren (D-CA). The Homeland Security Committee was formed to coordinate all House oversight of the Department of Homeland Security and has legislative jurisdiction over the 2002 act creating the department. The subcommittee will oversee "security of computer, telecommunications, information technology, industrial control, electric infrastructure and data systems, including science, research and development; protection of government and private networks and computer systems from domestic and foreign attack; prevention of injury and civilian populations and physical infrastructure caused by cyberattack, and relevant oversight," according to Cox's office.

---

*Category 1E* *Homeland Security*

2003-05-01 **Lucent Technologies U.S. Security Bush National Security Telecommunications Advisory Committee NSTAC Russo**

NIPC/DHS

May 01, CNET News.com — Lucent CEO tapped for U.S. security. President Bush has enlisted Lucent Technologies' chief executive Patricia Russo as a member of the National Security Telecommunications Advisory Committee (NSTAC). The NSTAC, created in 1982 by President Reagan, provides analysis and recommendations to the president regarding policy that affects national security and emergency preparedness tied to telecommunications. The terrorist attacks on New York City and Washington D.C. on September 11, 2001, exposed the susceptibility of the nation's telecommunications networks, which suffered widespread outages. In the aftermath, the NSTAC's importance swelled in its role to make the telecommunications infrastructure more secure. Russo will be involved with a wide range of policy and technical issues related to telecommunications, infrastructure protection and homeland security.

*Category 1E* *Homeland Security*

2003-05-05 **DHS Topoff2 warfare computer terrorist Ted Macklin emergency operations Dartmouth College Institute Security**

NIPC/DHS

May 05, Government Computer News — Terror attack mock-up has a cyber angle. The Department of Homeland Security (DHS) and dozens of federal, state and local agencies will launch a simulated five-day terrorist attack on May 12 designed to include a small role for cyberwarfare, officials said Monday. The attack game, called Topoff 2, will include a small element of computer warfare, said Ted Macklin, assistant director of the Office of Domestic Preparedness (ODP). It will not focus on an emergency operations center takedown but on the ability of state and local authorities to recognize a cyberattack, he said. Seattle Mayor Greg Nickles said that participants will begin with the assumption that their computers will work, but "that could be an area they surprise us with." An ODP official who is working on Topoff 2 said DHS has contracted with Dartmouth College's Institute of Security and Technology studies to prepare a "sand table" analysis of a cyberattack, in coordination with Seattle.

*Category 1E* *Homeland Security*

2003-05-15 **cybersecurity DHS Department Homeland Security cyberspace certification research**

NIPC/DHS

May 15, Federal Computer Week — DHS setting cybersecurity priorities. Now that responsibility for the National Strategy to Secure Cyberspace has shifted to the Department of Homeland Security (DHS), officials are developing a list of priorities for implementation within the next 180 days. Among the areas being examined are education and certification, metrics and benchmarks for the private sector, and research and development, said Andy Purdy, cybersecurity adviser for the Information Analysis and Infrastructure Protection (IAIP) Directorate at DHS. Purdy was speaking May 14 at a symposium sponsored by the Computing Technology Industry Association in Washington, D.C. DHS officials also are looking at a more comprehensive method to share security vulnerability and incident information between government and the private sector, Purdy said.

*Category 1E* *Homeland Security*

2003-05-16 **Netanyahu Woolsey terror technology CIA IDPartners conference U.S.**

NIPC/DHS

May 16, Computerworld — Netanyahu and Woolsey speak out on terror and technology. This week former Israeli Prime Minister Benjamin Netanyahu and former CIA director R. James Woolsey warned of the dangers of inaction and lack of preparedness when it comes to cyberterrorism and homeland security. "The power of the few to terrorize the many has grown by leaps and bounds...because of technology," Netanyahu said during an interview broadcast Tuesday as part of the Terror and Technology Online conference, sponsored by IDPartners LLC. He was referring to the ability of international terrorist organizations to physically destroy key cyber-based infrastructures or attack those infrastructures using the Internet. When asked what can be done to meet the threat, Netanyahu said, "through security systems and security norms that are enforced by governments." Woolsey said the networks and systems that power the U.S. economy "were put together by businesspeople...with an eye toward openness and ease of access, and were not put together with a single thought in most cases...to terrorism."

*Category 1E* *Homeland Security*

2003-05-27 **homeland security webcam ordinary american monitoring from home 10$ hour**

NewsScan

HOMELAND SECURITY VIA WEBCAM
Jay Walker, who made his fortune by inventing Priceline.com, is working on a new brainstorm that addresses the timely issue of homeland security. The premise behind USHomeGuard is simple: use webcams at the 47,000 "critical infrastructure facilities" that are at risk, enabling ordinary, online Americans to help monitor the sites from their homes. If a person spots a potential terrorist — a hooded man trying to scale a power plant fence, for instance, or a panel truck parked next to a reservoir — on-site security could be alerted with the click of a mouse. Walker suggests that work-at-home monitors could be reimbursed at up to $10 an hour, paid by the government agencies and companies that need the service. "We like to think of USHomeGuard as a digital victory garden," says Walker. "It lets people be part of the solution." A spokesman for the Department of Homeland Security says federal officials have not done any "serious evaluation" of the proposal, adding that the agency isn't currently contemplating any strategies that rely on Internet surveillance. Meanwhile, law enforcement officials worry that such a system would generate too many false alarms. "People get suspicious easily, and this could quadruple our call volume," says Capt. Joe Carrillo of the San Jose Fire Department. "The idea is really good. But the timing is really bad," he added, alluding to California's current budget crisis. (AP/CNN.com 27 May 2003)

*Category 1E* *Homeland Security*

2003-06-20 **democracy USAPATRIOT Act constitutional rights executive privilege homeland security counterterrorism**

NewsScan

WORTH THINKING ABOUT: HOW TO FORM A DEMOCRACY
Historian Bernard Bailyn comments on the creativity of America's Founding Fathers as shapers of the new democracy:
"The Founders of the American nation were one of the most creative groups in modern history. Some among them, especially in recent years, have been condemned for their failures and weaknesses — for their racism, sexism, compromises, and violations of principle. And indeed moral judgments are as necessary in assessing the lives of these people as of any others. But we are privileged to know and to benefit from the outcome of their efforts, which they could only hopefully imagine, and ignore their main concern: which was the possibility, indeed the probability, that their creative enterprise — not to recast the social order but to transform the political system — would fail: would collapse into chaos or autocracy. Again and again they were warned of the folly of defying the received traditions, the sheer unlikelihood that they, obscure people on the outer borderlands of European civilization, knew better than the established authorities that ruled them; that they could successfully create something freer, ultimately more enduring than what was then known in the centers of metropolitan life.

"Since we inherit and build on their achievements, we now know what the established world of the eighteenth century flatly denied but which they broke through convention to propose — that absolute power need not be indivisible but can be shared among states within a state and among branches of government, and that the sharing of power and the balancing of forces can create not anarchy but freedom.

"We know for certain what they could only experimentally and prayerfully propose — that formal, written constitutions, upheld by judicial bodies, can effectively constrain the tyrannies of both executive force and populist majorities.

"We know, because they had the imagination to perceive it, that there is a sense, mysterious as it may be, in which human rights can be seen to exist independent of privileges, gifts, and donations of the powerful, and that these rights can somehow be defined and protected by the force of law.

"We casually assume, because they were somehow able to imagine, that the exercise of power is no natural birthright but must be a gift of those who are subject to it."

*Category 1E* *Homeland Security*

2003-10-02 **foreign worker hi-tech Homeland Security track H-1B**

NewsScan

HOMELAND SECURITY SEEKS BETTER TRACKING SYSTEM FOR H1-B WORKERS
A report by the General Accounting Office (GAO), the investigative arm of Congress, says that the Homeland Security Department needs to keep track of when foreign high-tech workers with H-1B visas enter and leave the country, and to develop rules limiting the length of time workers who lose their jobs are allowed to remain in the country. According to the GAO, "much of the information needed to effectively oversee the H-1B visa program is not available." The Homeland Security Department agreed with the recommendations and is in the process of changing the systems used to track the foreign workers. (AP/San Jose Mercury News 2 Oct 2003)

*Category 1E* *Homeland Security*

2003-12-04 **national security policy review homeland security**

http://www.news.gc.ca/cfmx/CCP/view/en/index.cfm?articleid=73469&%20

SOLICITOR GENERAL DISCUSSES CANADA'S NATIONAL SECURITY POLICY
The Solicitor General of Canada, Wayne Easter, stated that it was time for a substantive review of Canada's national security policy. Easter noted that such a review would need to examine how the Canadian national security system interacts with the U.S. Department of Homeland Security. Additionally, Easter said that it was time to consider the creation of a centralized Canadian national security agency which could also assist in co-coordinating the work of the provinces and territories in times of crisis. He emphasized that keeping the border open for commerce and closed to criminals and terrorists was a priority.

*Category 1E* *Homeland Security*

2003-12-30 **new year security metal detectors New York's Times Square**

NewsScan

HIGH-TECH SECURITY FOR NEW YEAR'S EVE
On New Year's Eve, about 240 metal detectors will be used to screen the crowds of people who come to watch the ball drop in New York's Times Square, and radar-equipped Black Hawk helicopters and Citation jets will patrol the skies over the city. New York Mayor Bloomberg says: "You're going to see a lot of cops there and there will be a lot more cops that you don't see." In addition to Homeland Security air patrols, the Police Department's eight helicopters will be in the air, including one with a powerful video camera. (New York Times 30 Dec 2003)

# 21.1 General QA failures

*Category 21.1* *General QA failures*

2003-02-21 **Oracle server new vulnerabilities exploit software CERT CC advisory**

NIPC/DHS

February 19, CERT/CC — CERT Advisory CA-2003-05 Multiple Vulnerabilities in Oracle Servers. Multiple vulnerabilities exist in Oracle software. Depending on the vulnerability being exploited, an attacker may be able to execute arbitrary code; read, modify, or delete information stored in underlying Oracle databases; or cause a denial of service. Systems running the following software are affected: Oracle9i Database (Release 1 and 2); Oracle8i Database v 8.1.7; Oracle8 Database v 8.0.6; and Oracle9i Application Server (Release 9.0.2 and 9.0.3). Solutions for specific vulnerabilities can be found in Oracle Security Alerts published here:
http://otn.oracle.com/deploy/security/alerts.htm. Systems administrators should review the Oracle Security Alerts and apply patches as appropriate. Until a patch can be applied, the CERT/CC recommends that vulnerable sites disable unnecessary Oracle services, run Oracle services with the least privilege, and restrict network access to Oracle services.

---

*Category 21.1* *General QA failures*

2003-02-28 **QA quality assurance blooper**

NewsScan

WELCOME TO CORNELL. (NO, WAIT — NOT SO FAST THERE!)
Because of a "systems coding error," Cornell University sent welcoming e-mail letters to hundreds of high school students who'd already been rejected. A few hours after the university congratulated the students on their acceptance, it had to send them letters confessing its mistake and apologizing. One high school counselor said, "I know mistakes can happen, but this kind is devastating to the student and family. The apologies of the university don't quite cover the disappointment of my senior." (New York Times 28 Feb 2003)

---

*Category 21.1* *General QA failures*

2003-03-12 **new vulnerability PeopleSoft business software flaw exploit Web server compromise**

NIPC/DHS

March 10, CNET News — Security alert posted for PeopleSoft. A serious security flaw has been found in business management software from PeopleSoft. The flaw, known as a remote command execution vulnerability, gives outsiders the ability to install malicious computer code on PeopleSoft customers' Web servers, potentially leading to a "complete compromise" of their PeopleSoft business systems, according to Internet Security Systems (ISS), the Atlanta-based computer security company that issued the warning on Monday. PeopleSoft supplies software designed to streamline accounting, human resources, sales and manufacturing activities to more than 5,000 companies around the world. The flaw affects only certain releases of PeopleSoft version 8, which the company began shipping in 2000. Nearly 2,000 companies have installed version 8, according to PeopleSoft spokesman Steve Swasey. The patches and details about the vulnerability are available on the company's private Web site for PeopleSoft customers: www.peoplesoft.com. PeopleSoft has yet to hear of any problems related to the security flaw, Swasey added.

---

*Category 21.1* *General QA failures*

2003-03-20 **new advisory CERT CC integer overflow Sun RPC XDR**

NIPC/DHS

March 19, CERT/CC — CERT Advisory CA-2003-10: Integer overflow in Sun RPC XDR library routines. XDR (external data representation) libraries are used to provide platform-independent methods for sending data from one system process to another, typically over a network connection. The xdrmem_getbytes() function in the XDR library provided by Sun Microsystems contains an integer overflow that can lead to improperly sized dynamic memory allocation. Depending on how and where the vulnerable xdrmem_getbytes() function is used, subsequent problems like buffer overflows may result. Exploiting this vulnerability will lead to denial of service, execution of arbitrary code, or the disclosure of sensitive information. Specific impacts reported include the ability to crash the rpcbind service and possibly execute arbitrary code with root privileges. In addition, intruders may be able to crash the MIT KRB5 kadmind or cause it to leak sensitive information, such as secret keys. CERT recommends the application of a vendor specified patch or upgrade as specified by vendor.

---

*Category 21.1* *General QA failures*

2003-03-24 **Yahoo security obscurity obfuscation Website open access**

NIPC/DHS

March 19, SecurityFocus — Point, click, get root on Yahoo. A simple scan for unpublished websites within Yahoo's Internet address space gave an unemployed IT worker access to several of the portal company's internal systems, including root access inside the company firewall, the worker says. Yahoo URLs provided by the man routed to what appeared to be two unprotected Web-based remote administration consoles for company disk and file storage systems. In a written statement, Yahoo spokesperson Mary Osako acknowledged that the servers shouldn't have been exposed to the Internet, and said the company closed off access on Wednesday. "No user data was compromised," Osako wrote. The IT worker, who asked to remain anonymous, confirmed Yahoo's statement.

*Category 21.1* *General QA failures*

2003-03-26 **CERT CC advisory vulnerabilities Lotus Notes Domino software servers**

NIPC/DHS

March 26, CERT/CC — CERT Advisory CA-2003-11: Multiple Vulnerabilities in Lotus Notes and Domino. In February 2003, NGS Software released several advisories detailing vulnerabilities affecting Lotus Notes clients and Domino servers. Multiple reporters, the close timing, and some ambiguity caused confusion about what releases are vulnerable. The impact of these vulnerabilities range from denial of service to data corruption and the potential to execute arbitrary code. The CERT/CC has issued an advisory to help clarify the details of the vulnerabilities, the versions affected, and the patches that resolve these issues. Please refer to the CERT website for additional information.

*Category 21.1* *General QA failures*

2003-04-17 **quality assurance failure flaw bug Microsoft MS Office 200 register software**

NIPC/DHS

April 17, CNET News.com — Flaw bugs Office 2000 customers. A software slipup in Microsoft's latest update to Office 2000 results in the application repeatedly asking some customers to register the program. The glitch apparently affects only Office 2000 users who don't have administrative rights on their computer, a Microsoft representative said Thursday. "They are experiencing unexpected registration prompts, but it doesn't interfere with product functionality," he said. Administrative rights allow a PC user to exercise total control over the computer's data. Giving such rights to nontechnical employees is considered by many security experts to be an unacceptable risk for companies. Microsoft's representative didn't know if the cause of the problem had been determined but said that the software company is working on fixing the issue.

*Category 21.1* *General QA failures*

2003-04-22 **bug patch flaw fix Microsoft MS Office 2000 quality assurance failure**

NIPC/DHS

April 22, The Register — Microsoft issues Office 2000 registration bug patch. Microsoft has posted a patch to remedy the registration bug that has plagued Office 2000 users in some of the world's biggest organizations since April 15. The bug invokes Office's Registration Wizard, even if the user has already registered the product, typically through the purchase of a Select Customer volume license. In many cases, the bug is merely annoying, forcing the user to get rid of an unwanted window. In some cases, dismiss the window too often and Office ceases to function, or enters what Microsoft calls "Reduced Functionality Mode". The only way to get it back is to register the software with Microsoft. The patch may be found on the Microsoft Website:
http://support.microsoft.com/?id=818798

*Category 21.1* *General QA failures*

2003-04-27 **quality assurance failure bug software flaw expenses software engineering SEI**

NIPC/DHS

April 27, The Associated Press — Spread of buggy software raises questions. Last year, a study commissioned by the National Institute of Standards and Technology found that software errors cost the U.S. economy about $59.5 billion annually. Developers say defects stem from several sources: software complexity, commercial pressure to bring products out quickly, the industry's lack of liability for defects, and poor work methods. Programmers typically spend half their time writing code and the other half looking for errors and fixing them. That approach may have worked in the infancy of computers, when programs were small, says Watts Humphrey, of Carnegie Mellon University's Software Engineering Institute. Now, most programs in testing have five to 10 defects per 1,000 lines of code, or up to 10,000 bugs in a million-line program. It would take 50 people a year to find all those bugs, Humphrey says.

*Category 21.1* *General QA failures*

2003-04-29 **Oracle9i vulnerability operating system compromise buffer overflow patch databases link**

NIPC/DHS

April 29, eWEEK — Vulnerability puts Oracle9i at risk. A new vulnerability in Oracle Corp.'s database software puts not only the information in the database at risk, but in some cases, also can lead to a compromise of the operating system. The vulnerability is in the service that enables users to create links between two Oracle databases. In order to exploit the flaw, an attacker would need to send an overly long parameter with the connect string with a query to create a database link. This would trigger the stack buffer overflow, which would in turn overwrite the saved return address on the stack. This would give the attacker the ability to run any code he chose on the vulnerable server. The vulnerability affects Oracle 9i Release 1 and 2; all releases of 8i; all releases of 8; and 7.3.x. A patch is available at the Oracle website: http://otn.oracle.com/deploy/security/pdf/2003alert54.pdf.

*Category 21.1* *General QA failures*

2003-05-02 **Outlook 2003 microsoft beta version bug 21 steps offline folder Government Computer News**

NIPC/DHS

May 02, Government Computer News — Bug delays Outlook 2003's release. A bug lives on in the latest beta version of Microsoft Outlook 2003 despite two widely publicized fixes. The Inbox bug systematically deletes e-mail messages throughout networked systems that still have Outlook 2002 installed. One workaround proposed by Microsoft involves 21 steps to redirect the location of the cache and change the location of the default profile's Offline Folder File. That didn't work in tests conducted by Government Computer News. Another workaround, which also didn't fix the Outlook bug, is to back up all user data on the server running Microsoft Exchange Server and then delete and recreate the Outlook Profiles. Backup is necessary because this procedure deletes calendar data, e-mails and so on. Microsoft has delayed final product release from early summer to late summer or early fall.

*Category 21.1* *General QA failures*

2003-05-05 **Connectiva vulnerabilities Linux arbitrary code DoS denial of service Apache Web Server GNU C**

NIPC/DHS

May 05, Information Security — Multiple vulnerabilities in Conectiva implementations. Conectiva, a vendor of Portuguese, Spanish and English versions of Linux, has released updates to correct several vulnerabilities in its implementations. These could allow an attacker to run arbitrary code, cause denial of service or crash applications. A vulnerability in glibc, a GNU C Library could be used by an attacker to create an overflow problem in the xdrmem family of functions to run arbitrary code or crash applications. Another pair of vulnerabilities involves the Apache Web server. A memory leak could allow an attacker to deplete memory and cause a denial of service. There are also file descriptor leaks that could give privileges to untrusted CGI scripts. Updated versions are available from the Conectiva website: http://distro.conectiva.com.br/atualizacoes

*Category 21.1* *General QA failures*

2003-06-25 **MS03-021 windows media player library access 9 ActiveX control script flaw**

NIPC/DHS

June 25, Microsoft — Microsoft Security Bulletin MS03-021: Flaw In Windows Media Player May Allow Media Library Access. A flaw exists in the way in which the ActiveX control included with Windows Media Player 9 Series provides access to information on the user's computer. An attacker could invoke the ActiveX control from script code, which would allow the attacker to view and manipulate metadata contained in the media library on the user's computer. An attacker could also embed a link to a malicious site in an HTML e-mail and send it to the user. After opening the e-mail, the site could be visited automatically without further user interaction. The attacker might also be able to determine the user name of the logged-on user by examining the directory paths to media files. Microsoft has assigned a risk rating of "Moderate" to this issue and recommends that system administrators install the patch on a schedule consistent with their practices.

*Category 21.1* *General QA failures*

2003-08-21 **Orcale9iM XDB flaw open door hackers XML Database denial service DoS vulnerability insider FTP HTTP server buffer overflow**

NIPC/DHS

August 21, eWEEK — Oracle XDB flaws open door for hackers. The XDB (XML Database) in Oracle Corp.'s Oracle9i Database Release 2 has a set of potential buffer overflows that a smart attacker could exploit to cause a denial-of-service (DoS) attack or to capture an active user session on Oracle9iM. To exploit the weaknesses, an authenticated database user is required, or the FTP and HTTP servers must be enabled in the XML database. The vulnerabilities are "highly susceptible" to an insider attack that originates on a corporate intranet if users ignore best practices for secure database configuration. To minimize risk, Oracle recommends disabling the FTP and HTTP servers in the XML database. Those are both installed and enabled by default and can't be turned on or off individually. A patch is available on the Oracle Website: http://metalink.oracle.com/

*Category 21.1* *General QA failures*

2003-09-03 **MS03-035 Microsoft Word Macros Automatically Run malicious document e-mail attachment**

NIPC/DHS

September 03, Microsoft — Microsoft Security Bulletin MS03-035: Flaw in Microsoft Word Could Enable Macros to Run Automatically. A vulnerability exists because it is possible for an attacker to craft a malicious document that will bypass the macro security model. If the document was opened, this flaw could allow a malicious macro embedded in the document to be executed automatically, regardless of the level at which macro security is set. The malicious macro could take the same actions that the user had permissions to carry out, such as adding, changing or deleting data or files, communicating with a web site or formatting the hard drive. The vulnerability could only be exploited by an attacker who persuaded a user to open a malicious document -there is no way for an attacker to force a malicious document to be opened. The vulnerability cannot be exploited automatically through e-mail. A user must open an attachment sent in e-mail for an e-mail borne attack to be successful. The vulnerability only affects Microsoft Word—other members of the Office product family are not affected. Microsoft has assigned a risk rating of "Important" to this vulnerability and recommends that system administrators install the patch immediately.

*Category 21.1* *General QA failures*

2003-09-03 **MS03-036 code execution execute wordperfect converter corel malicious code buffer overrun**

NIPC/DHS

September 03, Microsoft — Microsoft Security Bulletin MS03-036: Buffer Overrun in WordPerfect Converter Could Allow Code Execution. There is a flaw in the way that the Microsoft WordPerfect converter handles Corel WordPerfect documents. A security vulnerability results because the converter does not correctly validate certain parameters when it opens a WordPerfect document, which results in an unchecked buffer. As a result, an attacker could craft a malicious WordPerfect document that could allow code of their choice to be executed if an application that used the WordPerfect converter opened the document. Microsoft Word and Microsoft PowerPoint, FrontPage, Publisher, and Microsoft Works Suite can all use the Microsoft Office WordPerfect converter. The vulnerability could only be exploited by an attacker who persuaded a user to open a malicious WordPerfect document-there is no way for an attacker to force a malicious document to be opened or to trigger an attack automatically by sending an e-mail message. Microsoft has assigned a risk rating of "Important" to this vulnerability and recommends that system administrators install the patch at their earliest opportunity.

*Category 21.1* *General QA failures*

2003-09-03 **MS03-037 flaw Visual Basic Applications Arbitrary Code Execution VBA documents e-mail attachemnt forward**

NIPC/DHS

September 03, Microsoft — Microsoft Security Bulletin MS03-037: Flaw in Visual Basic for Applications Could Allow Arbitrary Code Execution. A flaw exists in the way Microsoft VBA checks document properties passed to it when a document is opened by the host application. A buffer overrun exists which if exploited successfully could allow an attacker to execute code of their choice in the context of the logged on user. In order for an attack to be successful, a user would have to open a specially crafted document sent to them by an attacker. This document could be any type of document that supports VBA, such as a Word document, Excel spreadsheet, PowerPoint presentation. In the case where Microsoft Word is being used as the HTML e-mail editor for Microsoft Outlook, this document could be an e-mail, however the user would need to reply to, or forward the mail message in order for the vulnerability to be exploited. Microsoft has assigned a rating of "Critical" to this vulnerability and recommends that system administrators install the patch at the earliest available opportunity.

*Category 21.1* *General QA failures*

2003-09-03 **MS03-038 Microsoft Access Snapshot Viewer Code Execution Execute malicious website visit Office**

NIPC/DHS

September 03, Microsoft — Microsoft Security Bulletin MS03-038: Unchecked buffer in Microsoft Access Snapshot Viewer Could Allow Code Execution. A vulnerability exists because of a flaw in the way that Microsoft Access Snapshot Viewer validates parameters. Because the parameters are not correctly checked, a buffer overrun can occur, which could allow an attacker to execute the code of their choice in the security context of the logged-on user. For an attack to be successful, an attacker would have to persuade a user to visit a malicious Web site that is under the attacker's control. The Microsoft Access Snapshot Viewer is not installed with Microsoft Office by default. Microsoft has assigned a rating of "Moderate" to this vulnerability and recommends that system administrators install the patch at the earliest available opportunity.

*Category 21.1* *General QA failures*

2003-11-06 **critical fix patch update Microsoft MS Office 2003**

NIPC/DHS

November 05, eSecurity Planet — 'Critical' Office 2003 patch released. Microsoft has issued a 'critical' update to fix problems in the Powerpoint, Word and Excel products in Microsoft Office 2003, which was released on October 21. Microsoft said the errors occur when a user tries to open or save files that includes an OfficeArt shape that was previously modified or saved in an earlier version of Microsoft Office. The errors mean that documents may not open completely or may be corrupted. In some cases, the documents may open but with missing content. There is no word on whether the 'critical' patch will be shipped with all new sales of the Office 2003 suite going forward. The update is available on the Microsoft Website: http://support.microsoft.com/?kbid=828041

*Category 21.1* *General QA failures*

2003-11-13 **new critical vulnerability Microsoft security bulletin buffer overflow overrun patch fix exploit**

NIPC/DHS

November 13, Microsoft — Microsoft Security Bulletin MS03-051: Buffer Overrun in Microsoft FrontPage Server Extensions Could Allow Code Execution. There are two vulnerabilities in Microsoft FrontPage Server Extensions. The first vulnerability exists because of a buffer overrun in the remote debug functionality of FrontPage Server Extensions. This functionality enables users to remotely connect to a server running FrontPage Server Extensions and remotely debug content using, for example, Visual Interdev. An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system, or could cause FrontPage Server Extensions to fail. The attacker could then take any action on the system. The second vulnerability is a Denial of Service vulnerability that exists in the SmartHTML interpreter. This functionality is made up of a variety of dynamic link library files, and exists to support certain types of dynamic web content. An attacker who successfully exploited this vulnerability could cause a server running Front Page Server Extensions to temporarily stop responding to requests. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that system administrators install the patch immediately.

*Category 21.1* *General QA failures*

2003-11-13 **new critical vulnerability Microsoft security bulletin Word Excel arbitrary code execution patch fix exploit**

NIPC/DHS

November 11, Microsoft — Microsoft Security Bulletin MS03-050: Vulnerability in Microsoft Word and Microsoft Excel Could Allow Arbitrary Code to Run. A vulnerability exists in Microsoft Excel that could allow malicious code execution. If successfully exploited, an attacker could craft a malicious file that could bypass the macro security model. If an affected spreadsheet was opened, this vulnerability could allow a malicious macro embedded in the file to be executed automatically, regardless of the level at which the macro security is set. The malicious macro could then take the same actions that the user had permissions to carry out. A vulnerability exists in Microsoft Word that could allow malicious code execution. If a specially crafted document were to be opened it could overflow a data value in Word and allow arbitrary code to be executed. If successfully exploited, an attacker could then take the same actions as the user had permissions to carry out. Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators install this patch immediately.

*Category 21.1* *General QA failures*

2003-11-14 **BEA Tuxedo Administration vulnerability fix patch Fortune 500 software denial-of-service**

NIPC/DHS

November 10, Information Security — BEA Tuxedo Administration vulnerability requires fix. Thousands of customers in Fortune 500 enterprises are urged to patch or upgrade to remedy a security issue in BEA Tuxedo Administration Console. A problem with processing input arguments can allow denial of service, disclosure of file system information or cross-site scripting. BEA Tuxedo provides middleware for building scalable enterprise applications in heterogeneous, distributed environments. The BEA Tuxedo administration console is a CGI application for remote administration of Tuxedo functions. Vulnerable versions include BEA Tuxedo 8.1 and prior. A patch is available for Tuxedo 8.1, and previous versions should be upgraded to 8.1:
http://edocs.bea.com/tuxedo/tux81/install/insadm.htm

*Category 21.1* *General QA failures*

2003-12-09 **Oracle new critical vulnerability warning OpenSSL denial-of-service**

NIPC/DHS

December 05, eWEEK — Oracle issues high-severity vulnerability warning. Oracle issued a high severity security alert warning Thursday, December 4, confirming that a variety of its server products could be tampered with through vulnerabilities via the OpenSSL protocol. The flaws could potentially open the door for a remote hacker to cause a denial-of-service (DoS) attack, execute arbitrary code, and gain access privileges. The notification addresses SSL vulnerabilities detailed in CERT Advisory CA-2003-26 and SSL vulnerabilities detailed in several older Common Vulnerabilities and Exposures (CVE) Candidates. Products concerned with the vulnerability include certain releases of Oracle9i Database Server, Oracle8i Database Server, Oracle9i Application Server, and Oracle HTTP Server. Additional information is available on Oracle's Website:
http://otn.oracle.com/deploy/security/pdf/2003alert62.pdf

*Category 21.1* *General QA failures*

2003-12-24 **MySQL release bug fix patch open-source database software**

NIPC/DHS

December 22, eWEEK — MySQL Quashes Defects in Database Release. MySQL AB on Monday, December 22, released Version 4.0.17 of its MySQL open-source database software. The update features a number of cleaned up code defects. Available in source code and binary form, the MySQL 4.0.17 maintenance release for the current MySQL production version corrects all valid bugs discovered during an October poll conducted within the development community via an independent study. According to the study, 21 software defects in 235,667 lines of MySQL source code were found. The report's Defect Summary noted 15 defect instances of NULL Pointer Deference, three defect instances of an allocated memory leak, and three defect instances of an uninitialized variable prior to usage. Additional information is available on the MySQL Website:
http://www.mysql.com/downloads/mysql-4.0.html

# 21.2 Security product QA failures

*Category 21.2* *Security product QA failures*

2003-02-07 **Microsoft problematic patch pulled Windows NT XP uninstall**

NIPC/DHS

February 05, eSecurity Planet — Problematic Windows NT patch pulled. Microsoft has pulled the security patch for Microsoft Security Bulletin MS02-071: Flaw in Windows WM_TIMER Message Handling Could Enable Privilege Elevation. The patch, which was first issued on December 11, actually introduces an error that may cause systems to fail. While the Slammer worm inflicted its damage on copies of Microsoft SQL Server 2000, the latest problem revolves around a security patch for Windows NT 4.0 systems. But it comes at a time when sysadmins are being scolded for not updating systems with the necessary patches in the first place. (The patch for Slammer has been around since July.) The security vulnerability was found in the WM_TIMER Message Handling in NT 4.0 and could enable privilege elevation. Patches for Windows 2000 and Windows XP were unaffected by the latest withdrawal, Microsoft said. In the updated advisory, Microsoft said it was investigating the cause of the problematic patch and promised to release an updated fix soon. The company urged Windows NT 4.0 administrators to uninstall the patch until a new fix is issued. This vulnerability has a severity rating of "Important". The updated advisory may be found on the Microsoft website:
http://www.microsoft.com/technet/treeview/default.asp?url=/t echnet/security/bulletin/MS02-071.asp

---

*Category 21.2* *Security product QA failures*

2003-03-04 **new vulnerablility snort buffer overflow NIPC advisory execute arbitrary code**

NIPC/DHS

March 03, Department of Homeland Security, National Infrastructure Protection Center — NIPC Advisory 03-003: "Snort buffer overflow Vulnerability". There is a buffer overflow in the Snort Remote Procedure Call normalization routines which can cause Snort to execute arbitrary code embedded within sniffed network packets. Depending upon the particular implementation of Snort this may give local and remote users almost complete control of a vulnerable machine. The vulnerability is enabled by default. Snort is a widely used Intrusion Detection System from Sourcefire. The affected Snort versions include all version of Snort from version 1.8 through current. Snort 1.9.1 has been released to resolve this issue. More information can be found on the Sourcefire website:
http://www.sourcefire.com/services/advisories/sa022503.html.

---

*Category 21.2* *Security product QA failures*

2003-03-20 **new vulnerability Microsoft security bulletin ISA DNS Intruction Detection Filter denial-of-service**

NIPC/DHS

March 19, Microsoft — Microsoft Security Bulletin MS03-009: Flaw In ISA Server DNS Intrusion Detection Filter Can Cause Denial Of Service. Microsoft Internet Security and Acceleration (ISA) Server 2000 contains the ability to apply application filters to incoming traffic. A flaw exists in the ISA Server DNS intrusion detection application filter, and results because the filter does not properly handle a specific type of request when scanning incoming DNS requests. An attacker could exploit the vulnerability by sending a specially formed request to an ISA Server computer that is publishing a DNS server, which could then result in a denial of service to the published DNS server. DNS requests arriving at the ISA Server would be stopped at the firewall, and not passed through to the internal DNS server. All other ISA Server functionality would be unaffected. By default, no DNS servers are published. DNS server publishing must be manually enabled. The vulnerability would not enable an attacker to gain any privileges on an affected ISA Server or the published DNS server or to compromise any cached content on the server. It is strictly a denial of service vulnerability. Microsoft has assigned a risk rating of "Moderate" to this vulnerability. A patch is available at the Microsoft website.

---

*Category 21.2* *Security product QA failures*

2003-04-10 **new vulnerability Microsoft security bulletin Winsock ISA firewall flaw patch exploit fix**

NIPC/DHS

April 09, Microsoft — Microsoft Security Bulletin MS03-012: Flaw In Winsock Proxy Service And ISA Firewall. There is a flaw in the Winsock Proxy service in Microsoft Proxy Server 2.0, and the Microsoft Firewall service in ISA Server 2000, that would allow an attacker on the internal network to send a specially crafted packet that would cause the server to stop responding to internal and external requests. Receipt of such a packet would cause CPU utilization on the server to reach 100%, and thus make the server unresponsive. The Winsock Proxy service and Microsoft Firewall service work with FTP, telnet, mail, news, Internet Relay Chat (IRC), or other client applications that are compatible with Windows Sockets (Winsock). These services allow these applications to perform as if they were directly connected to the Internet. They redirect the necessary communications functions to a Proxy Server 2.0 or ISA Server computer, thus establishing a communication path from the internal application to the Internet through it. Microsoft has assigned a risk rating of "Important" to this vulnerability. A patch is available at the Microsoft website.

*Category 21.2* *Security product QA failures*

2003-04-18 **CERT CC advisory Snort IDS intrusion detection system new vulnerability exploit patch fix**

NIPC/DHS

April 17, CERT/CC — CERT Advisory CA-2003-13: Multiple Vulnerabilities in Snort Preprocessors. The Snort intrusion detection system ships with a variety of preprocessor modules that allow the user to selectively include additional functionality. There are vulnerabilities in two of these modules. CORE Security Technologies has discovered a remotely exploitable heap overflow in the Snort "stream4" preprocessor module. To exploit this vulnerability, an attacker must disrupt the state tracking mechanism of the preprocessor module by sending a series of packets with crafted sequence numbers. This causes the module to bypass a check for buffer overflow attempts and allows the attacker to insert arbitrary code into the heap. This vulnerability affects Snort versions 1.8.x, 1.9.x, and 2.0 prior to RC1. Internet Security Systems has discovered a remotely exploitable buffer overflow in the Snort RPC preprocessor module. When the RPC decoder normalizes fragmented RPC records, it incorrectly checks the lengths of what is being normalized against the current packet size, leading to an overflow condition. The RPC preprocessor is enabled by default. This vulnerability affects Snort versions 1.8.x through 1.9.1 and version 2.0 Beta. Both issues are addressed in Snort version 2.0, which is available at the Snort website:
http://www.snort.org/.

*Category 21.2* *Security product QA failures*

2003-04-24 **patch fix slow Microsoft Windows XP security bulletin**

NIPC/DHS

April 24, IDG News Service — Microsoft fixing patch that can slow Windows XP. Microsoft is revising a security patch for Windows XP systems with Service Pack 1 installed after customers complained that installing the patch slowed their systems down to a crawl. Removing the patch brings system speed back to normal. Originally released on April 16, Security Bulletin MS03-013 addressed a buffer overrun vulnerability in the Windows kernel, which manages core services for the operating system such as allocating processor time and memory, as well as error handling. Microsoft is working on a revised patch which will be re-issued when it has been completed and fully tested. Microsoft said that customers running Windows XP Service Pack 1 should still consider applying the flawed patch as protection until a new version is released. The revised bulletin is available at the Microsoft Website:
http://www.microsoft.com/technet/treeview/default.asp?url=/t echnet/security/bulletin/MS03-013.asp.

*Category 21.2* *Security product QA failures*

2003-05-08 **VPN vulnerabilities Cisco 3002 hardware client DoS Attack ICMP packets performance degradation**

NIPC/DHS

May 08, IDG News Service — Cisco reports VPN vulnerabilities. Cisco on Wednesday warned customers of three vulnerabilities in its Cisco 3005, 3015, 3030, 3060 and 3080 VPN (virtual private network) Concentrators and the Cisco VPN 3002 Hardware Client. In one of the vulnerabilities, an interloper could access systems on a private network from a workstation on the public network without any form of authentication. Another vulnerability can be exploited to carry out a DOS attack on the VPN concentrator. In the third vulnerability a flood of malformed ICMP (Internet Control Message Protocol) packets could cause a performance degradation on the concentrator or cause it to restart. Workarounds and an upgrade are available on the Cisco Website:
http://www.cisco.com/warp/public/707/cisco-sa-20030507-vpn3k.shtml

*Category 21.2 Security product QA failures*

2003-05-08 **microsoft security flaw intenret passport hackers consumer accounts vulnerability**

NewsScan; NIPC/DHS

MICROSOFT SCRAMBLES TO FIX SECURITY FLAW
Microsoft says it has fixed a security glitch in its Internet Passport service that left 200 million consumer accounts vulnerable to hackers. Product manager Adam Sohn said the flaw apparently had existed since at least September 2002, but investigators found no evidence that anyone had tried to exploit it before last month. The flaw was discovered by Pakistani researcher Muhammed Faisal Rauf Danka after hackers repeatedly hijacked Passport accounts belonging to him and a friend. Danka says it took him only about four minutes to find the problem. The embarrassing security lapse could leave Microsoft open to sanctions by the Federal Trade Commission, as well as a possible hefty fine. Under a settlement last summer, the government had accused Microsoft of deceptive claims about Passport's security, and in response the company had pledged to beef up its safeguards and submit to audits every two years for the next 20 years, or risk fines of up to $11,000 per violation. "If we were to find that they didn't take reasonable safeguards to protect the information, that could be an order violation," says an FTC official. Meanwhile, Microsoft is currently touting its "trustworthy computing initiative," which is intended to improve security for all its software products and services. (AP 8 May 2003)

May 08, Associated Press — Microsoft admits Passport was vulnerable. Computer researcher Muhammad Faisal Rauf Danka of Pakistan discovered how to breach Microsoft Corp.'s security procedures for its Internet Passport service. The service is designed to protect customers visiting some retail Web sites, sending e-mails and in some cases making credit-card purchases. Microsoft acknowledged the flaw affected all its 200 million Passport accounts but said it fixed the problem early Thursday, after details were published on the Internet Wednesday night. Under a settlement with the Federal Trade Commission (FTC) last year over lapsed Passport security, Microsoft pledged to take reasonable safeguards to protect personal consumer information during the next two decades or risk fines up to $11,000 per violation. The FTC's Jessica Rich said Thursday that each vulnerable account could constitute a separate violation - raising the maximum fine that could be assessed against Microsoft to $2.2 trillion.

---

*Category 21.2 Security product QA failures*

2003-05-13 **security flaws virtual machines random bit change cosmic rays IEEE physical access**

NewsScan

May 13, CNET News — Security flaws exposed in virtual machines. Princeton University student Sudhakar Govindavajhala has found security flaws in Java and .Net virtual machines. The technique relies on the ability of energy to "flip bits" in memory. While cosmic rays can very occasionally cause a random bit in memory to change value, from 0 to 1 or from 1 to 0, Govindavajhala decided not to wait. He used a lamp to heat up the chips inside a computer and cause one or more bits of memory to change. By doing so, the researcher broke the security model that virtual machine's rely on—that the computer faithfully executes its instruction set. An attack requires physical access to the computer, so the technique poses little threat to virtual machines running on PCs and servers. But it could be used to steal data from smart cards, Govindavajhala said Tuesday at the Institute of Electrical and Electronic Engineers (IEEE) Symposium on Security and Privacy in Berkeley, CA. He also pointed out that as processors and memory get faster, the energy needed to induce bit flips becomes smaller, suggesting that his technique will only become more effective.

---

*Category 21.2 Security product QA failures*

2003-06-25 **Symantec Security Check activeX control holes buggy code attack operating system**

NIPC/DHS

June 25, IDG News Service — Serious security holes, buggy code found in Symantec products. On Monday, anti-virus software company Symantec acknowledged a report about a serious security flaw in Symantec Security Check, an online service that enables users to scan their computer's vulnerability to a number of security threats. An ActiveX control installed by the Security Check service contains a buffer overflow vulnerability that could enable a remote attacker to crash or run malicious code on systems that had the control installed. Symantec updated the ActiveX control in the Security Check service, but security researchers monitoring the issue noted attackers who have a copy of the flawed ActiveX code with a valid Symantec digital signature could trick a Microsoft Windows system into accepting the control, opening that system to attack. Also on Monday customers using Symantec AntiVirus Corporate Edition reported that an automated anti-virus definition update from the company caused the anti-virus software to fail. Symantec subsequently provided instructions on how to repair systems that had downloaded the faulty update.

---

*Category 21.2* *Security product QA failures*

2003-10-20 **Windows security problems fix Microsoft operating systems vulnerabilities**

NIPC/DHS

MICROSOFT VOWS TO FIX WINDOWS SECURITY PROBLEMS
Microsoft CEO Steve Ballmer has admitted the inadequacy the company's current collection of security software patches for the Windows operating system and says the company will modify them in the coming year. Customers have complained that the company's system of frequently issuing new patches is too time-consuming and difficult, so Microsoft is now designing technology to shield Windows from malicious e-mail messages, viruses and worms. The changes will include shipping Windows with an Internet firewall turned on by default, which would have blocked the recent "Blaster" virus, and will prevent attachments from executing commands — a common method network vandals use to hijack computers. (San Jose Mercury News 10 Oct 2003)

*Category 21.2* *Security product QA failures*

2003-10-23 **revisions Microsoft Security Bulletin MS03-047 045 Outlook Web Access OWA language versions patches exchange third-party software**

NIPC/DHS

October 23, Computerworld — Microsoft posts 'revisions' to security bulletins. Microsoft issued "major revisions" to two patches last week, MS03-045 and MS03-047, after they caused problems on foreign language versions of the Windows operating system and Exchange e-mail server. Security bulletin MS03-045, rated "Important," concerns a buffer overrun vulnerability in a component of most supported versions of Windows. Microsoft discovered compatibility problems between the patch and third-party software on systems running foreign language editions of Windows 2000 with Service Pack 4. Russian, Spanish and Italian versions of Windows 2000 were affected, in addition to versions in a number of other languages, including Czech, Finnish and Turkish. Security bulletin MS03-047, rated "Moderate," described a cross-site scripting vulnerability in Exchange Server 5.5, Service Pack 4. The patch did not work for some customers who installed foreign language versions of Outlook Web Access (OWA), an Exchange service that enables e-mail users to access their Exchange mailboxes using a Web browser instead of the Outlook mail client. While customers running English, German, French and Japanese versions of OWA were covered by the original patch, those running OWA in other languages need to apply the rereleased version, Microsoft said. The patches are available on the Microsoft Website:
http://www.microsoft.com/technet/treeview/default.asp?url=/t echnet/security/current.asp

*Category 21.2* *Security product QA failures*

2003-11-03 **security patch fix exploit vulnerability Microsoft buffer overflow Messenger Service**

NIPC/DHS

October 30, eSecurity Planet — Microsoft revises critical patches. Microsoft has issued major revisions to several 'critical' security patches because of problems associated with Debug Programs. The "major revisions" issued on October 30 have been released to correct problems in the MS03-042, MS03-043, and MS03-045 patches. The MS03-042 patch, which plugs a 'critical' buffer overflow issue in the Windows Troubleshooter ActiveX Control, has been re-issued because of problems related to CPU resource usage. The Debug Problems afflict all three faulty patches—MS03-043, which is a buffer overrun in Messenger Service that could lead to code execution and MS03-044, which could allow PC takeover because of buffer overflows in the ListBox and ComboBox Control. Additional information is available on the Microsoft Website:
http://www.microsoft.com/technet/treeview/default.asp?url=/t echnet/security/bulletin/winoct03.asp

*Category 21.2* *Security product QA failures*

2003-12-23 **fix patch vulnerability flaw buffer overflow Internet Explorer browser software third-party Microsoft**

NIPC/DHS

December 22, CNET News.com — New open-source patch released for IE. A Website that published a third-party patch to fix a security hole in Microsoft's Internet Explorer (IE) has had to re-issue the patch Saturday, December 20, after the original was found to contain a buffer overflow exploit. This exploit, which allowed an attacker to take control of the patched PC, might have been far more damaging than the flaw that the patch was trying to fix. According to Openwares, only about 6,500 people downloaded the original patch. Security experts warned people against installing it last week, saying that aside from trust issues, the patch author would not have had access to IE source code and so the patch could interfere with future updates from Microsoft. The IE vulnerability, which was first reported in late November, allows a browser to display one URL in the address bar while the page being viewed is actually hosted elsewhere, making the user more susceptible to ruses like "phishing." However, Openwares' first fix, which worked by filtering out any URLs containing suspicious characters, would work only with addresses that had less than 256 bytes. Larger addresses produced a buffer overflow. Microsoft has still not released a fix for the IE problem or given any indication as to when one might be available.

# 22.1 DoS attacks

*Category 22.1* *DoS attacks*

2003-01-15 **denial-of-service attack DoS saturation e-mail fraud**

NewsScan

UNIVERSITY BOMBARDED WITH FAKE MESSAGES
Campus police at Ohio State University are evaluating charges against an individual they think is responsible for bombarding the university's computer network last month with 11 million phony e-mail messages over a several-day period, crippling Internet access and delaying e-mail distribution for days. The police have not disclosed the content of the messages, nor identified the suspect, who may be facing charges of illegal tampering with records, theft, unauthorized use of a computer system, and vandalism. (AP/USA Today 15 Jan 2003)

---

*Category 22.1* *DoS attacks*

2003-03-26 **news Iraq war Al-Jazeera denial-of-service hack attack**

NIPC/DHS

March 25, Associated Press — Al-Jazeera site experiences hack attack. Hackers attacked the Web site of Arab satellite television network Al-Jazeera on Tuesday, rendering it intermittently unavailable, the site's host said. The newly launched English-language page, which went live Monday, was hardest hit in a bombardment of data packets known as a denial-of-service attack. Ayman Arrashid, Internet system administrator at the Horizons Media and Information Services, the site's Web host, said the attack began Tuesday morning local time. The Web host is based in the Persian Gulf state of Qatar. The servers that host the Al-Jazeera site are in France and the United States. Only the U.S. servers were under attack, said Arrashid, so the attackers were likely in the United States. He said technicians were working to thwart the attack, but could not estimate when the site would be fully available again.

---

*Category 22.1* *DoS attacks*

2003-05-15 **denial service attack hole kernel Linux DoS Secunia Red Hat hash collisions spoofed source address 400 packets per sencond**

NIPC/DHS

May 15, internetnews.com — DOS hole found in Linux Kernel. Security experts Thursday warned of a vulnerability in the Linux Kernel 2.4 branch, which can be exploited to cause denial-of-service (DOS) attacks. "By flooding a Linux system with packets with spoofed source addresses, the handling of the cache will consume large amounts of CPU power. This could potentially bring a Linux system offline with a rate of only 400 packets per second by using carefully chosen source addresses that causes hash collisions in the table," according to a security advisory from computer security firm Secunia. Secunia rated the flaw as "moderately critical" and cautioned that it could be exploited to bring a Linux system offline with a rate of only 400 packets per second by using carefully chosen source addresses that causes hash collisions in the table. Red Hat has issued updated kernel packages to patch Red Hat Linux versions 7.1 through 9:
http://rhn.redhat.com/errata/RHSA-2003-172.html.

---

*Category 22.1* *DoS attacks*

2003-06-02 **net attack computers Dan Wallach Scott Crosby internet hash functions offline packets process power Rice University Houston Texas**

NIPC/DHS

June 02, New Scientist — Net attack overwhelms computers with complexity. Dan Wallach and Scott Crosby, researchers at Rice University in Houston, TX, have found an Internet attack that can knock a web-connected computer offline using specially crafted packets of data. Many programs perform small calculations - called hash functions - on substantial amounts of data to make it easier to sort through. Tables of hashed information can then be referred to, to check that information has not been corrupted or lost en route. Wallach and Crosby calculated that some data would force a program to perform the most intensive hash calculations possible. They tested a number of commercial computer programs and found that sending these types of packets could use up nearly all of a computer's processing power, preventing it from carrying out normal tasks. Wallach and Crosby were able to disrupt target computer program using just a dial-up modem connection. The only way to defend against the attack is to use more efficient, better designed hashing algorithms. A paper outlining the attack will be presented in August at the Usenix Security Symposium in Washington D.C.

---

*Category 22.1* *DoS attacks*

2003-12-11 **SCO Group denial-of-service hacker attack Linux Unix**

NIPC/DHS

December 10, Dow Jones Business News — SCO Group Website disabled by another hacker attack. The Website of SCO Group Inc. has been temporarily disabled by a hacker attack that began early Wednesday, December 10, the company said. It marks the third time this year the Lindon, UT, software firm's site has been the target of a "denial of service" attack. In such assaults, hackers bombard an Internet site with traffic in an attempt to overwhelm its server computers and shut it down. The latest attack began at 6:20 a.m. EST, and it isn't clear when it will cease, said SCO spokesman Blake Stowell. Past attacks against the company's site have lasted for several days. Stowell said the company has notified law-enforcement authorities. The attack is preventing SCO customers from downloading updates or security fixes to their software.

# 22.2 DDoS attacks

*Category 22.2 DDoS attacks*

2003-11-03 **spam DDoS distributed denial of service vigilante information warfare**

WP http://www.washingtonpost.com/ac2/wp-dyn/A56072-2003Nov3?language=printer

Spammers retaliated against antispammers by launching DDoS attacks on them that wiped them off the 'Net. Ron Guilmette, an antispam activist, had his DSL Internet access saturated when 4,000 zombies on compromised computers flooded him with unwanted traffic.

# 22.3 DoS countermeasures

*Category 22.3* *DoS countermeasures*

2003-08-16 **Blaster worm Sean Sundwall Microsoft spokesman msblaster exploit windows server software redirection disabling**

NIPC/DHS

August 16, Associated Press — Microsoft says no major problems from 'Blaster' worm. Microsoft spokesman Sean Sundwall said the company had not noticed any extraordinary network congestion Saturday, August 16, from attempts by the "blaster" worm to force thousands of infected computers to target the software company's Website and network. The virus-like infection exploits a flaw in most current versions of Microsoft's Windows operating system for personal computers, laptops and server computers. Although Microsoft posted a software patch on July 16, many users failed to download it, leaving them vulnerable. The exploiters of the Microsoft flaw made a mistake. The worm instructed computers to call up an incorrect address for reaching the actual Microsoft Website that houses the software patch. Although Microsoft has long redirected those who visited that incorrect address to the real site, the company disabled the automatic redirection Thursday. That has helped Microsoft's real Web site stay accessible to users, Sundwall said.

# 22.4 Accidental availability disruptions

*Category 22.4 Accidental availability disruptions*

2003-01-08 **MSN Messenger instant messaging denial-of-service DoS outage**

NIPC/DHS

January 07, InfoWorld — MSN Messenger outage affects millions. Microsoft Corporation's MSN Messenger service went down yesterday. According to a Microsoft spokesman, the service went down at approximately 9 a.m. EST, and the root cause of the outage is still unknown. The outage affected all 75 million worldwide users of Microsoft's .Net Messenger Service, including Windows Messenger and MSN Messenger subscribers, according to a statement from Larry Grothaus, lead product manager for MSN. The .Net Messenger Service is the back-end service that powers both the Windows Messenger and the MSN Messenger clients. MSN Hotmail e-mail service and other MSN services weren't affected, he said. Although service was restored for some users by about 2 p.m. EST, some users were still unable to log onto the messaging software later in the afternoon. Microsoft didn't have any more difficulties with the service late yesterday, but some users may still be shut out as the service scales back up, according to Grothaus.

*Category 22.4 Accidental availability disruptions*

2003-03-24 **Iraq war information online newspapers slow down**

NIPC/DHS

March 20, InternetWeek — War information demand slows U.S. military, Arab, alternative news sites. The Arab news site Al Jazeera, U.S. military sites, and a U.S. alternative press site were among those suffering massive slowdowns and outages in the first day of the war in Iraq, according to Web performance measurement firm Keynote Systems. The slowdowns and outages were presumed to be due to overwhelming demand for access to information, rather than hacker attacks, said Eric Siegel, principle Internet consultant for Keynote. Likewise, British government sites are seeing significant slowdowns and outages. Siegel speculated that the entire online Arab world is turning to Al Jazeera for news, whereas the West has a diversity of sources online.

*Category 22.4 Accidental availability disruptions*

2003-04-22 **Global Positioning System GPS satellite failure denial-of-service risk**

NIPC/DHS

May 01, Wired — What if GPS fails? Eighteen of the 28 satellites in the GPS constellation are operating past their intended lifespan or suffering from equipment failure. There have been three launch incidents in the past five years, and the Air Force, which maintains the 20-year-old network, is overburdened with competing space priorities. According to John Petersen, director of the Arlington Institute, a scenario-planning outfit in Virginia, "If GPS were to fail completely...civil aviation, trucking, shipping, and telecommunications would be worst hit." Internet activity would slow to a crawl, because many backbone operators rely on precise GPS time stamps to route data. The $12 billion market for GPS devices would be sent reeling, and the arrival of location-based wireless services would be set back years. However, Owen Wormser of the Office of the Assistant Secretary of Defense says GPS can withstand the loss of several satellites before becoming completely dysfunctional. "The system would degrade slightly, rather than seize up," he says.

*Category 22.4 Accidental availability disruptions*

2003-07-28 **e-mail essential downtime traumatic IT lose jobs**

NewsScan

E-MAIL DOWNTIME MORE STRESSFUL THAN DIVORCE?
A study sponsored by data-storage firm Veritas Software found that for 34% of chief information officers and IT managers, a weeklong failure of the corporate e-mail system would be more traumatic than a minor car accident, moving to a new home, or getting married or divorced. Smooth-running e-mail systems are essential to the enterprise, and 68% of the companies polled reported workers becoming irate within as little as 30 minutes after an e-mail system goes down. In the case of a failure lasting as long as 24 hours, one fifth of IT managers said their jobs would be on the line at that point. "E-mail has become far more than a communication tool, placing a huge responsibility on organizations to ensure that e-mail is always available," says Mark Bregman, Veritas' executive VP for product operations. "When IT managers fail to keep the systems running, they inhibit the ability of the entire organization to conduct business." (CNet News.com 28 Jul 2003)

*Category 22.4 Accidental availability disruptions*

2003-11-28 **cable failure UK Internet traffic affect denial-of-service**

NIPC/DHS

November 26, CNET News.com — Cable failure hits UK Net traffic. A major failure in one of the key communications links between the United States and Europe appears to have caused widespread disruption to Internet services in the UK. The fault occurred Tuesday, November 25, in the TAT-14 fiber-optic cable system that connects the United States, Denmark, Germany, the Netherlands, France and the UK, and is understood to have left the system unusable for traffic. TAT-14 is a dual, bidirectional ring of cable, so a single serious fault should not be enough to break it, since traffic would still be able to flow between the countries on the ring. But a part of the cable near the U.S. coast had already suffered a technical fault earlier this month, which meant there was no built-in redundancy to cope with Tuesday's failure. According to BT, a member of the consortium of telephone companies that owns TAT-14, the U.S.-side fault should be fixed by the end of this week, which will bring the cable network online again. Tuesday's failure affected BT's voice calls, rather than its data services, but it is understood that a number of Internet service providers experienced faults.

# 23.1 Java

*Category 23.1* *Java*

2003-01-15 **information warfare interoperability intellectual property**

NewsScan

SUN SUES MICROSOFT FOR DAMAGES OVER JAVA
Sun Microsystems has filed a new lawsuit against Microsoft, alleging that Microsoft's business practices damaged the market for Sun's Java programming language. It also alleges that Microsoft kept more than 20 technologies secret, preventing Sun and other server makers from incorporating the features needed to maker their servers work with Microsoft's software. Sun's suit follows an earlier filing in 1997, which focused on a contractual dispute over Microsoft's licensing of Java. The two companies eventually settled out of court. This time around, however, Sun is seeking, potentially, billions of dollars in damages in addition to an injunction that would require Microsoft to distribute the latest version of Java, to disclose technical information so that other companies can write compatible software, and to cease bundling some Microsoft products. The Sun suit follows similar suits recently filed by AOL Time Warner and Be Inc. (Wall Street Journal 11 Mar 2002)
http://online.wsj.com/article/0,,SB1015608994249257320.djm,00.html (sub req'd)

SUN'S CHRISTMAS COMES EARLY IN VICTORY OVER MICROSOFT
A U.S. district court judge ruled Monday that Microsoft had violated Sun Microsystems' copyright for its Java software and ordered the software giant to include Sun's version of Java with its Windows operating system, handing Sun a double-barreled victory over its high-tech rival. The case stems from Sun's claims that Microsoft dropped Sun's Java software in favor of its own variation, which Sun alleges is incompatible with its technology. "Unless Sun is given a fair opportunity to compete in a market untainted by the effects of Microsoft's past antitrust violations, there is a serious risk that in the near future the market will tip in favor of .Net, that it is impossible to ascertain when such tipping might occur in time to prevent it from happening, and that if the market does tip in favor of .Net, Sun could not be adequately compensated in damages," wrote Judge J. Frederick Motz in his decision. Microsoft says it plans to appeal the decision. (CNet News.com 23 Dec 2002)
http://news.com.com/2100-1001-978786.html

SUN AND MICROSOFT GET SET FOR JAVA LEGAL BATTLE
Sun and Microsoft are appearing in federal court to argue their positions before U.S. District Judge J. Frederick Motz, who will be ruling on Sun's request for an injunction requiring Windows to include Sun's latest Java software immediately, pending resolution of the larger Sun lawsuit against Microsoft. Sun claims Microsoft has gained an unfair advantage by shipping Windows with a version of Java that is both outdated and strongly biased toward Windows, even though Java is meant to make it possible for programs to run on all computers, regardless of the operating system. (AP/San Jose Mercury News 15 Jan 2003)

---

*Category 23.1* *Java*

2003-06-10 **sun java everywhere growing market**

NewsScan

SUN PROCLAIMS 'JAVA EVERYWHERE'
Sun Microsystems hopes its new "Java Everywhere" branding effort will be as successful as Intel's "Intel Inside" campaign was, and claims that Java "means a new way of interacting with consumers, giving them new experiences," providing Sun with "a new electrified brand, more market opportunities, more fun, more money." Sun executive vice president Jonathan Schwartz continues: "The opportunity for Java growing the market is everywhere, to create the best sites, devices, games, stores, Web games, smart cards, and security." (EWeek 10 Jun 2003)

---

*Category 23.1* *Java*

2003-06-12 **hp dell java sun microsoft richard green**

NewsScan

HP AND DELL PCs TO INCLUDE JAVA
Hewlett-Packard and Dell will be including Java as a standard component on their personal computers. (Java, a creation of Sun Microsystems, makes it easy to run a program on many different kinds of computers.) Sun, of course, is happy that, as a result of the 1998 Microsoft antitrust trial, computer manufacturers can no longer be pressured by Microsoft to run only that company's products. Sun executive Richard Green says, "The back and forth with Microsoft has limited the success of Java on the personal computer desktop. It is remarkable that the two largest computer makers have committed to Java for their customers." (New York Times 12 Jun 2003)

---

*Category 23.1* *Java*

2003-06-27 **microsoft sun java court windows programming**

NewsScan

COURT OVERTURNS ORDER THAT WINDOWS INCLUDE JAVA
A federal appeals court has overturned a lower-court injunction that would have required Microsoft to incorporate Sun's Java programming language in Microsoft's Windows operating system. On the other hand,, the court also upheld the lower court's ruling that Microsoft had broken a 2001 legal settlement between the two companies and had infringed on Sun's copyrights. The case has been sent back to the district court for further proceedings. (Reuters/USA Today 27 Jun 2003)

# 23.4 HTML, XML

*Category 23.4* *HTML, XML*

2003-07-09 **MS03-023 Buffer Overrun HTML converter allow code execution vulnearbility microsoft security bulletin Internet Explorer Enhanced Security Configuration**

NIPC/DHS

July 09, Microsoft — Microsoft Security Bulletin MS03-023: Buffer Overrun In HTML Converter Could Allow Code Execution. There is a flaw in the way the HTML converter for Microsoft Windows handles a conversion request during a cut-and-paste operation which results in a vulnerability. A specially crafted request to the HTML converter could cause the converter to fail in such a way that it could execute code. An attacker could craft a specially formed Web page or HTML e-mail that would cause the HTML converter to run arbitrary code on a user's system. If Internet Explorer Enhanced Security Configuration has been disabled, the protections put in place that prevent this vulnerability from being automatically exploited would be removed. Exploiting the vulnerability would allow the attacker only the same privileges as the user. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that system administrators install the patch immediately.

*Category 23.4* *HTML, XML*

2003-12-16 **denial-of-service SOAD document type definition DTD parameter vulnerability XML parser error**

NIPC/DHS

December 15, eSecurity Planet — DoS Flaw in SOAP DTD Parameter. IBM and Microsoft have released fixes for a potentially serious vulnerability that could be exploited to trigger denial-of-service attacks. The companies said the vulnerability was caused by an error in the XML parser when parsing the DTD (Document Type Definition) part of XML documents. Affected software include the IBM WebSphere 5.0.0 and Microsoft ASP.NET Web Services (.NET framework 1.0, .NET framework 1.1). According to IBM, the security patch fixes a flaw that could be exploited by sending a specially crafted SOAP request. "This can cause the WebSphere XML Parser to consume an excessive amount of CPU resources," the company warned. IBM's security patch is available here: http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQ TP&q=PQ709%2021&uid=swg24005582. Microsoft confirmed the DTD error parsing vulnerability. In some cases, Microsoft recommended the rejection of XML messages that contain DTS, because of its limitations. The company said the SOAP 1.1 specification states that a SOAP message must not contain a DTD. Microsoft's security patch is available here: http://support.microsoft.com/default.aspx?kbid=826231.

# 23.5 E-mail & instant messaging or chat

*Category 23.5 E-mail & instant messaging or chat*

2003-03-04 **new vulnerablility Sendmail NIPC advisory server root access CERT CC**

NIPC/DHS

March 03, Department of Homeland Security, National Infrastructure Protection Center — NIPC Advisory 03-004: "Remote Sendmail Header Processing Vulnerability". The Remote Sendmail Header Processing Vulnerability allows local and remote users to gain almost complete control of a vulnerable Sendmail server. Attackers gain the ability to execute privileged commands using super-user (root) access/control. This vulnerability can be exploited through a simple e-mail message containing malicious code. Sendmail is the most commonly used Mail Transfer Agent and processes an estimated 50 to 75 percent of all Internet e-mail traffic. System administrators should be aware that many Sendmail servers are not typically shielded by perimeter defense applications. A successful attacker could install malicious code, run destructive programs and modify or delete files. Additionally, attackers may gain access to other systems thru a compromised Sendmail server, depending on local configurations. Sendmail versions 5.2 up to 8.12.8 are known to be vulnerable at this time. Due to the seriousness of this vulnerability, the NIPC is strongly recommending that system administrators who employ Sendmail take this opportunity to review the security of their Sendmail software and to either upgrade to Sendmail 8.12.8 or apply the appropriate patch for older versions as soon as possible. Patches for the vulnerability are available from Sendmail at http://www.sendmail.org. Additional information is available from CERT/CC at http://www.kb.cert.org/vuls/id/398025.

---

*Category 23.5 E-mail & instant messaging or chat*

2003-04-24 **new vulnerability Microsoft security bulletin Outlook Express e-mail client patch exploit fix**

NIPC/DHS

April 23, Microsoft — Microsoft Security Bulletin MS03-014: Cumulative Patch for Outlook Express . A vulnerability exists in the MHTML URL Handler that allows any file that can be rendered as text to be opened and rendered as part of a page in Internet Explorer. As a result, it would be possible to construct a URL that referred to a text file that was stored on the local computer and have that file render as HTML. If the text file contained script, that script would execute when the file was accessed. Since the file would reside on the local computer, it would be rendered in the Local Computer Security Zone. Using this method, an attacker could attempt to construct a URL and either host it on a website or send it via email. If the cumulative patch for Internet Explorer MS03-004 has been installed, known means by which an attacker may place a file onto a user's computer will be blocked. Microsoft has assigned a risk rating of "Critical" to this vulnerability and a patch is available at the Microsoft website.

---

*Category 23.5 E-mail & instant messaging or chat*

2003-05-06 **AOL ICQ America Online Core Security e-mail execute arbitrary code updating hostile flaw**

NIPC/DHS

May 06, CNET News.com — Security group: AOL's ICQ is flawed. There are six flaws, two of them critical, in America Online's (AOL) ICQ software, security firm Core Security Technologies warned in an advisory Monday. Three of the vulnerabilities, including one of the critical flaws, occurred in the software's e-mail feature. A bug in the component could allow an attacker to use the way the software handles e-mail to cause it to execute code, if the attacker can impersonate the user's e-mail server. The other critical vulnerability appeared in a feature of ICQ that allows automated updating. Because that component doesn't have adequate security, an attacker could pretend to be sending a legitimate update when in reality the upgrade is hostile code. No one from AOL's ICQ subsidiary was available Monday to comment on the alleged flaws. The advisory is available on the Core Security Technologies website: http://www.coresecurity.com/common/showdoc.php?idx=315ccion=10.

---

*Category 23.5* *E-mail & instant messaging or chat*

2003-05-09 **instant messaging software ICQ America Online Inc. Mirabilis IM client holes firewalls elnterprise**

NIPC/DHS

May 09, Computerworld — Security problems persist with instant messaging. Security problems relating to the unfettered use of consumer chat software on corporate networks are fueling the adoption of tougher security measures and more commercial-grade products, users and analysts said. Ongoing concerns about instant messaging (IM) security were heightened this week by the disclosure of six vulnerabilities in America Online Inc.'s Mirabilis ICQ IM client software. Security analysts for some time have been warning that unchecked use of such software could cause dangerous holes in enterprise firewalls, leading to sensitive corporate data being exposed on public networks and files being transferred in an unprotected fashion.

*Category 23.5* *E-mail & instant messaging or chat*

2003-05-30 **Yahoo IM buffer overflow delete files executable code malicious programmer chat updates**

NIPC/DHS

May 30, CNET News.com — Yahoo issues IM, chat security patches. Yahoo issued on Friday security patches for its Yahoo Instant Messenger and Yahoo Chat clients in an effort to fix a buffer overflow vulnerability discovered in the software. When users of the software log on to the IM network or enter a chat room, Yahoo is prompting them to install the patches. In addition, the company posted the patches on its Web site. Buffer overflow attacks in Yahoo IM and Yahoo Chat could lead to a number of problems. Users could be involuntarily logged out of an application, or it could allow the introduction of executable code, allowing a malicious programmer to take control of a user's machine, delete files and otherwise wreak havoc with a victim's computer system.

*Category 23.5* *E-mail & instant messaging or chat*

2003-08-25 **e-mail attachments scanning virus worm policy**

NewsScan

ISPs TO START SCANNING ATTACHMENTS
Several large U.S. Internet service providers, including Cox Communications, EarthLink and BellSouth, say they are preparing to scan all e-mail attachments for computer viruses before they forward them on to subscribers' accounts. The policy change comes on the heels of a month of e-mail problems caused by the Sobig and Blaster worms, resulting in consumer demand for better security measures on ISP servers. "Virus filtering is quickly becoming one of the check marks for the big ISPs," says Todd Dean, director of data operations and support for Cox. However, the cost of filtering e-mail can be daunting, says Forrester Research analyst Michael Rasmussen. "With ISPs of those sizes, you're easily looking at ongoing costs of several million dollars — not just the cost of purchasing the technology, but making it work with your existing systems, administrative costs and increased support costs associated with customers who are confused about what to do when their ISP tells them they have an e-mail with a virus inside." Several leading ISPs already scan mail, including AOL, Microsoft Network, Comcast, Covad and AOL Time Warner's RoadRunner network, forestalling the possibility of unwary subscribers becoming conduits for further viral infection. "Users should not be asked to protect themselves any more than they should be asked to go buy seat belts and airbags and install them in their own cars," says Alan Paller, research director for the SANS Institute, a security training facility. "That's got to come with their service, even if it comes with an added price." (Washington Post 28 Aug 2003)

*Category 23.5* *E-mail & instant messaging or chat*

2003-08-27 **sendmail vulnerability DoS denial service open source remote DNS Linux Unix free() fucntion attacks**

NIPC/DHS

August 27, SearchEnterpriseLinux.com — Sendmail vulnerable to DoS attacks. Versions 8.12.0 through 8.12.8 of the open-source mail transfer agent Sendmail are vulnerable to remote denial-of-service attacks, according to an alert issued by the FreeBSD Project. The vulnerability is in the code that implements DNS (domain name system) maps. An attacker sending a malformed DNS reply packet could cause Sendmail to call "free ()" on an uninitialized pointer. Such a call could cause a Sendmail child process to crash. Sendmail is widely implemented in enterprises as part of several Linux and Unix distributions. A patch is available on the Sendmail Website:
http://Sendmail.org/dnsmap1.html

*Category 23.5* *E-mail & instant messaging or chat*

2003-09-18 **instant mesasge NYSE Wall Street traders IM records Bank of America**

NewsScan

INSTANT MESSAGE: YOU'RE UNDER ARREST
The investigation of a Wall Street trading scandal (in which a former Bank of America broker has been charged with grand larceny and securities fraud) is the first case that has used a chain of evidence derived from the instant messaging records of licensed brokers and dealers. Instant messaging (IM) systems are now widely used on Wall Street and to a large extent have replaced traditional e-mail. One attorney who consults on electronic communications said a New York Stock Exchange executive's question about instant messaging was: "Wait a minute, is that what my 13-year-old daughter uses at home?" The answer: "I said yes — and your traders." (USA Today 18 Sep 2003)

---

*Category 23.5* *E-mail & instant messaging or chat*

2003-09-24 **Micorosoft MSN hat free expensive indentity requirements personal data accountability actions**

NewsScan

MICROSOFT LAUDED FOR CRACKING DOWN ON CHAT ROOMS
Child advocates are applauding a decision by Microsoft's MSN online service to crack down on its free chat rooms. Ernie Allen of the National Center for Missing & Exploited Children says: "There is no question but that chat rooms generally tend to be very dangerous places for children." MSN's move is intended to force users to identify themselves, so that they can be held accountable for their actions, and so that MSN can contact them when it gets complaints. Of course, ending support for free foreign chat rooms will also help Microsoft reduce MSN's financial loss. Technology analyst Rob Helm explains: "Maintaining any kind of online service is expensive. Putting chat on paid status in the U.S, and turning it off elsewhere is a step toward making MSN profitable." However, Microsoft spokesman Lisa Gurry says that cost savings were "not a factor" in the Microsoft chat-room decision. "This really is all about looking at delivering the safest online experience for folks using our services." (USA Today 24 Sep 2003)

---

*Category 23.5* *E-mail & instant messaging or chat*

2003-09-29 **chat ban india separatists internet yahoo groups forums**

NewsScan

CHAT GROUP BAN OF SEPARATIST GROUP AFFECTS ALL OF INDIA
A government ban on the Internet discussion group of a two-dozen member separatist movement has ended up blocking access to popular, unrelated Yahoo forums in nearly all of India. For technical reasons, Indian Internet service providers were unable to block just the separatist group's site and had to shut down every Yahoo discussion group. Businessman Sushil Devaraj says: "This is more like a dictatorship and goes against the concept of freedom of speech." Economics professor Rajeev Gowda of the Indian Institute of Management complains: "My students have a problem. I discuss my subject with them on Yahoo groups. We have not been able to do it. This heavy-handed action has affected a variety of users who have nothing to do with that group." (AP/Los Angeles Times 29 Sep 2003)

---

*Category 23.5* *E-mail & instant messaging or chat*

2003-09-30 **reuters microsoft messaging instant data voice financial services global communication**

NewsScan

REUTERS/MICROSOFT INSTANT MESSAGING DEAL
The Reuters news and information company and Microsoft will combine their two instant messaging systems as an offering for financial services companies. Reuters executive David Gurle says the goal is "to build a global communications infrastructure for the financial services industry. We want to provide the same functionality for which they now use the phone, but with the added element of data." (New York Times 30 Sep 2003)

---

*Category 23.5 E-mail & instant messaging or chat*

2003-10-25 **Windows Messenger exploit code Service MS03-043 Linux Unix crashes machines**

NIPC/DHS

October 25, TechWeb News — Attackers gearing up to exploit Windows Messenger security hole. An exploit code that takes advantage of a critical vulnerability in Microsoft's Windows Messenger Service is out in the wild and could prove as dangerous as this summer's MSBlaster worm if attackers decide to focus their efforts, security analysts said Friday, October 24. Released early last week, the exploit code — which has been crafted to run not only on attackers' Windows machines, but also on Linux and Unix boxes — crashes Windows systems not patched against the vulnerability released October 15 in Microsoft Security Bulletin MS03-043. What concerns security analysts is the speed with which this exploit was produced. The span between the disclosure of the vulnerability by Microsoft and proof of exploit code was just three days. Users can disable Windows Messenger Service by following the instructions in Microsoft's security bulletin:
http://www.microsoft.com/technet/treeview/?url=/technet/secu rity/bulletin/MS03-043.asp

*Category 23.5 E-mail & instant messaging or chat*

2003-11-14 **new vulnerability Eudora buffer overflow e-mail client spam**

NIPC/DHS

November 11, The Register — Eudora users warned over 'reply to all' trick. A buffer overflow vulnerability in Eudora version 5.x, the popular email client, creates a mechanism for hackers to compromise targeted PCs. The problem stems from a failure to properly verify the "
From:" and "Reply-To:" when users of vulnerable versions of Eudora select "Reply-To-All". This shortcoming creates a means for hackers to spam users with a maliciously constructed email designed to trigger this buffer overflow condition. Users should update to Eudora 5.1-Jr3 (Japanese) or Eudora 6.0 (English) in order to shore up their security defenses:
http://www.eudora.com/

*Category 23.5 E-mail & instant messaging or chat*

2003-11-19 **e-mail server flaw exploit spam relay Microsoft Exchange**

NIPC/DHS

November 14, CNET News.com — Mail server flaw opens Exchange to spam. Administrators of e-mail systems based on Microsoft's Exchange might have spammers using their servers to send unsolicited bulk e-mail, a consultant warned this week. Aaron Greenspan, a Harvard University junior published a white paper Thursday, November 13, detailing the problem. Greenspan's research concluded that Exchange 5.5 and 2000 can be used by spammers to send anonymous e-mail. He says even though software Microsoft provides on its site certifies that the server is secure, it's not. "If the guest account is enabled (on Exchange 5.5 and 2000), even if your login fails, you can send mail, because the guest account is there as a catchall," he said. "Even if you think you've done everything (to secure the server), you are still open to spammers." The guest account is a way for administrators to let visitors use a mail server anonymously, but because of security issues, the feature is generally not enabled. Exchange servers that had been infected by the Code Red worm and subsequently cleaned will still have the guest account enabled, Greenspan said.

*Category 23.5 E-mail & instant messaging or chat*

2003-11-25 **flaw vulnerability Microsoft Exchange Server 2003 kerberos authentication**

NIPC/DHS

November 24, ZDNet UK — Exchange flaw could open up user accounts. Microsoft is investigating what may be a serious flaw in Exchange Server 2003, only a month after the software's launch as part of Office System 2003. The bug appears to affect an Exchange component called Outlook Web Access (OWA), which allows users to access their in-boxes and folders via a Web browser. Consumers logging into their Web-based mailbox sometimes find themselves accessing another user's account, with full privileges, according to Matthew Johnson, a network administrator who reported the bug earlier this month on the NTBugtraq security mailing list. Microsoft has said it is investigating the issue and that the flaw appears to occur only when Kerberos authentication is disabled. Kerberos is the method that Microsoft uses for authenticating requests for services. For the moment, the company is advising customers to keep Kerberos authentication enabled, as it is by default, and may issue a patch or more information when its investigation is complete.

*Category 23.5 E-mail & instant messaging or chat*

2003-12-10 **Yahoo instant messaging flaw vulnerability executable code**

NIPC/DHS

December 08, CNET News.com — Yahoo answers IM security flaw. Yahoo has issued an update to its instant-messaging software, in order to address a security flaw found in the application. The company said the security issue was related to a buffer overflow, which is a common security vulnerability in computer programs written in C and C++ that allows more information to be added to a chunk of memory than it was designed to hold. Typical problems involved in an instant-messaging-related buffer overflow might include an involuntarily log-out of an IM session, a crash of browsing software applications, and a possible introduction of executable code. According to Yahoo, only a small percentage of the company's IM software users might be vulnerable as a result of the flaw. Yahoo said customers who changed their Explorer security settings from "medium" to "low" could be affected. The company said that even in that case, an attacker would have to lure a user of Yahoo IM to view malicious HTML code. Most often this would entail clicking a link sent through IM that leads back to a Web page hosting the code. Before changing an IE security setting to low, individuals are warned by the browser that the setting is considered "highly unsafe." Yahoo said it has not yet heard of any successful attacks based on the buffer flaw. The update is available on the Yahoo Website:
http://messenger.yahoo.com/messenger/security/

# 23.6 Web-site infrastructure, general Web security issues

*Category 23.6* *Web-site infrastructure, general Web security issues*

2003-01-15 **list top ten Web security vulnerabilities common HTTP exploits**

NIPC/DHS

January 13, Government Computer News — Open-source group names top 10 Web vulnerabilities. The Open Web Application Security Project has released a list of the top 10 vulnerabilities in Web applications and services. The group said it wants to focus government and private-sector attention on common weaknesses that require immediate remediation. In the longer term, this list is intended to be used by development teams and their managers during project planning," the report noted. "Ultimately, Web application developers must achieve a culture shift that integrates security into every aspect of their projects." OWASP is a volunteer open-source community project created to bring attention to security for online apps. The OWASP vulnerabilities are well known, but continue to represent significant risk because they are widespread. They can be exploited by code in HTTP requests that are not noted by intrusion detection systems and are passed through firewalls and into servers despite hardening. The complete report and list of vulnerabilities is available on the organization's Web site, www.owasp.org.

*Category 23.6* *Web-site infrastructure, general Web security issues*

2003-02-06 **Microsoft security bullentin Internet Explorer vulnerability patch**

NIPC/DHS

February 05, Microsoft — Microsoft Security Bulletin MS03-004: Cumulative patch for two vulnerabilities involving Internet Explorer's cross-domain security model. A flaw in Internet Explorer could allow a malicious web site operator to access information in another internet domain, or on the user's local system by injecting specially crafted code when certain dialog boxes were presented to the user. In the worst case, this vulnerability could allow an attacker to load a malicious executable onto the system and execute it. The attacker would have no way to force a user to a malicious web site. The vulnerability results because it is possible when using dialog boxes to bypass the cross-domain security model that Internet Explorer implements. A related cross-domain vulnerability allows Internet Explorer's showHelp() functionality to execute without proper security checking. In this scenario, the attacker could open a showHelp window to a known local file on the visiting user's local system and gain access to information from that file by sending a specially crafted URL to a second showHelp window. The attacker could also potentially access user information or run code of attacker's choice. Microsoft has assigned a risk rating of "Critical" to these vulnerabilities. A patch is available at the Microsoft website: http://www.microsoft.com/windows/ie/downloads/critical/81084 7/default.asp. Applying the patch, however, will disable the HTML Help functionality because HTML Help was one of the attack vectors. Users who apply this patch are also encouraged to download the HTML Help update after applying this cumulative patch in order to restore HTML Help functionality.

*Category 23.6* *Web-site infrastructure, general Web security issues*

2003-02-19 **list top ten Web security vulnerabilities common HTTP exploits**

NIPC/DHS

February 18, Government Computer News — Open Source group releases list of top 10 Web vulnerabilities. The Open Web Application Security Project released a list of the top ten vulnerabilities in Web applications and services on Tuesday. The group said it wants the list to focus government and private-sector attention on common vulnerabilities "that require immediate remediation." "Also, in the longer term, this list is intended to be used by development teams and their managers during project planning," the report reads. OWASP is a volunteer Open Source community project created to bring attention to Web application security. It patterned its list on the SANS Institute's and FBI's top 20 list of network vulnerabilities. Like the SANS-FBI list, the OWASP vulnerabilities are well known and have been recognized for years, but continue to represent significant risks because they remain common. They can be exploited by code in http requests that are passed through firewalls and into servers despite hardening and are not noted by intrusion detection systems. The complete report is available from the OWASP Website at www.owasp.org.

*Category 23.6 Web-site infrastructure, general Web security issues*

2003-03-06 **new vulnerability critical Macromedia Flash player Internet media software patch fix**

NIPC/DHS

March 04, IDG News Service — Macromedia reports critical hole in Flash player. Macromedia Inc. warned Monday of a "critical" security flaw in the latest version of its Flash animation player and advised users to install an updated to fix the problem. The security flaw affects Version 6 of the Macromedia Flash Player, which was released a year ago this month and has been installed on an estimated 75% of PCs worldwide, according to the company. The vulnerability affects the integrity of the player's "sandbox," which is supposed to act as a cordoned-off area where Flash code retrieved from the Web can be run safely, without access to a user's files. The flaw could allow a malicious hacker to run native code on a user's computer, outside the sandbox, possibly without the user's knowledge, according to information on the company's Web site. No users had reported having been affected by the problem as of Monday evening, a Macromedia representative said. Nevertheless, the company advised users to download a new version of the player — Version 6.0.79.0 — from its Web site immediately. The bulletin, with a link to the download site, is at www.macromedia.com/v1/handlers/index.cfm?ID=23821.

*Category 23.6 Web-site infrastructure, general Web security issues*

2003-03-10 **BIND domain name server vulnerability fix Internet Software Consortium**

NIPC/DHS

March 05, CNET News — Net consortium ties flaws to BIND. Domain name servers are used to match domain names to numerical Internet Protocol addresses. As the vast majority of these run BIND (Berkeley Internet Name Domain), the software essentially runs the Internet. The Internet Software Consortium (ISC), the group responsible for maintaining the software, released a new version of BIND on Monday, with their Web site billing it as a maintenance release. However, on Wednesday the site had been updated, saying that the ISC had been made aware of vulnerabilities in BIND, adding that upgrading was "strongly recommended." BIND 9.2.1 is vulnerable to a remote buffer overflow bug when installed with the "libbind" nondefault option. Previous versions may also be vulnerable to problems associated with the commonly used OpenSSL library, but again this is a nondefault installation option and has more to do with the SSL library than BIND itself. An updated version of BIND is available at the ISC website:
http://www.isc.org/products/BIND/.

*Category 23.6 Web-site infrastructure, general Web security issues*

2003-03-14 **new vulnerability buffer overflow Opera software browser fix**

NIPC/DHS

March 13, eSecurity Planet — Opera rushes out another security fix. Norway-based Opera Software has pushed out a new version of its Opera 7 browser because of issues surrounding security. The bug, which affects both versions 6.x and 7.x, was detected in the browser's handling of filenames when showing the "Download Dialog" box. "The problem is that very long filenames are handled incorrectly. This allows a malicious website to create a filename that causes a buffer overflow which can be exploited to execute arbitrary code," according to an alert from IT security services firm Secunia. In releasing the new Opera 7.03 version, the company confirmed the Secunia findings. Secunia warned that exploits for the vulnerability are in the wild for Windows, noting that "exploitation does not require user interaction as Web sites can spawn the "Download Dialog" automatically."

*Category 23.6 Web-site infrastructure, general Web security issues*

2003-03-18 **new vulnerability Internet Information Server IIS Microsoft buffer overflow advisory**

NIPC/DHS

March 17, Department of Homeland Security — Unchecked buffer in Microsoft Internet Information Server (IIS), Advisory 03-005. A security vulnerability is present in a Windows component used by WebDAV. A buffer overflow vulnerability exists in Microsoft IIS 5.0 running on Microsoft Windows 2000. Microsoft Windows 2000 and IIS Version 5.0 support the World Wide Web Distributed Authoring and Versioning (WebDAV) protocol. IIS 5.0 is installed and running by default on Microsoft Windows 2000 server products. An attacker could exploit the vulnerability by sending a specially formed HTTP request to a machine running Windows 2000 server and IIS Version 5.0. The request could cause the server to fail or to execute code of the attacker's choice. The code would run in the security context of the IIS service which, by default, runs in the LocalSystem context. Although Microsoft has supplied a patch for this vulnerability and recommends customers install the patch immediately, additional tools and preventive measures have been provided that customers can use to block the exploitation of this vulnerability while they are assessing the impact and compatibility of the patch. As an initial workaround Administrators can implement Microsoft's URL Scan tool to limit the lengths of URLs passed to the IIS system. Administrators are urged to update IDS signature files as relevant signatures become available; monitor FW, IDS, and other perimeter security devices for probes against port 80 and/or attempts to exploit this vulnerability; monitor information sources for additional alerts regarding possible attack activity; and report any relevant activity (increased port 80 probing or activity, web server crashes, etc.) to your agency Incident Response Capability and FedCIRC. The patch and additional information about this vulnerability are available on the Microsoft Website in Microsoft Security Bulletin MS03-007: Unchecked Buffer In Windows Component Could Cause Web Server Compromise:
http://www.microsoft.com/technet/treeview/default.asp?url=/t echnet/security/bulletin/MS03-007.asp See also CERT Advisory CA-2003-09: Buffer Overflow in Microsoft IIS 5.0 available at
http://www.cert.org/advisories/CA-2003-09.html

*Category 23.6 Web-site infrastructure, general Web security issues*

2003-03-26 **new exploit Microsoft Windows 200 flaw Internet Information Server IIS patch fix**

NIPC/DHS

March 24, CNET News.com — Program exploits Windows 2000 flaw. A Venezuelan security consultant has released a small program designed to compromise Microsoft Internet Information Service servers that haven't had a recent security hole patched. Monday's public release of the program's source code—known in security parlance as an exploit—will allow less technically knowledgeable system administrators to test for the existence of the vulnerability or allow less skillful miscreants to attack servers. "I released (the code) to enlighten the public and to promote system security for administrators unfamiliar with these exploits," said Rafael Nunez, information security consultant for Scientech de Venezuela and a former hacker. The flaw, which Microsoft said could be exploited through the World Wide Web Distributed Authoring and Versioning (WebDAV) component of Internet Information Service (IIS) 5.0, allows an attacker to take control of the server. Microsoft declined to comment on the issue, except to say that customers should patch their systems. Nunez stressed that system administrators need to patch their systems before a virus writer uses the vulnerability as a vector for a computer worm.

*Category 23.6 Web-site infrastructure, general Web security issues*

2003-04-04 **new vulnerabilities software Real RealPlayer Apple Quicktime heap corruption**

NIPC/DHS

April 02, CNET News.com — Holes found in RealPlayer, QuickTime. There are serious security holes in two popular digital media players: RealNetworks' RealPlayer and Apple Computer's QuickTime. In both cases, updates are available to remedy the problem. RealNetworks is warning that by creating a specifically corrupted Portable Network Graphics file, an attacker could cause "heap corruption." Doing so would allow the attacker to execute code on the victim's machine. The vulnerable software uses an older data-compression library within the RealPix component of the player, leaving the system vulnerable. The vulnerability affected the following versions of the software: RealOne Player, RealOne Player v2 for Windows, RealPlayer 8 for Windows, RealPlayer 8 for Mac OS 9, RealOne Player for Mac OS X, RealOne Enterprise Desktop Manager and RealOne Enterprise Desktop. Meanwhile, security firm iDefense warned this week of an exploitable buffer overflow vulnerability in versions 5.x and 6.0 of Apple's QuickTime Player that could affect computers with Microsoft's Windows. A URL containing 400 characters will overrun the allocated space on the system, allowing the attacker to assume control of the system, iDefense said.

*Category 23.6* *Web-site infrastructure, general Web security issues*

2003-04-07 **new vulnerability exploit patch fix Apache Web server denial-of-service**

NIPC/DHS

April 03, — Latest Apache release fixes DOS vulnerability. The latest release of Apache 2.0, version 2.0.45, fixes a number of security vulnerabilities including an as-yet-undisclosed flaw that could be used to launch a denial of service attack against machines running the Apache Web server, according to information released by the Apache Software Foundation (ASF). Apache 2.0 users are encouraged to upgrade. Other, lower priority security leaks and bug fixes were also included in the 2.0.45 release. However, a known DOS vulnerability that affects those systems running Apache on the OS/2 platform remains open. The latest Apache version was "too important" to delay release until the OS/2 fix could be included, the ASF said. OS/2 users will have to wait for the release of 2.0.46 to get a fix for that problem, the ASF said.

*Category 23.6* *Web-site infrastructure, general Web security issues*

2003-04-15 **XML security standard show intergration interoperability**

NIPC/DHS

April 11, IDG News Service — XML security standard touted at show. A group of application security vendors affiliated with the Organization for the Advancement of Structured Information Standards (OASIS) will next week announce a proposal for an XML standard for application vulnerabilities at the RSA Conference hosted by RSA Security in San Francisco. The group, made up of Citadel Security Software, GuardedNet, NetContinuum, SPI Dynamics and Teros, is promoting the development of the Application Vulnerability Description Language (AVDL), which is intended to standardize information about application vulnerabilities, enabling different products to share vulnerability information in a heterogeneous network environment, according to a statement released by the five companies. If widely adopted, the AVDL standards will enable customers to deploy diverse security technology to protect their network without having to sacrifice integration and interoperability, according to Wes Wasson, chief security strategy officer at NetContinuum.

*Category 23.6* *Web-site infrastructure, general Web security issues*

2003-04-24 **new patch exploit fix vulnerability Microsoft security bulletin Internet Explorer browser sofware**

NIPC/DHS

April 23, Microsoft — Microsoft Security Bulletin MS03-015: Cumulative Patch for Internet Explorer. This cumulative patch eliminates the following four vulnerabilities: 1) A buffer overrun vulnerability in URLMON.DLL; 2) A vulnerability in the Internet Explorer file upload control; 3) A flaw in the way Internet Explorer handles the rendering of third party files; 4) A flaw in the way modal dialogs are treated by Internet Explorer. In addition, this patch includes a fix for Internet Explorer 6.0 SP1 that corrects the method by which Internet Explorer displays help information in the local computer zone. This patch also sets the Kill Bit on the Plugin.ocx ActiveX control in order to ensure that the vulnerable control cannot be reintroduced onto users' systems and to ensure that users who already have the vulnerable control on their system are protected. Like the previous Internet Explorer cumulative patch released with bulletin MS03-004, this cumulative patch will cause window.showHelp( ) to cease to function if you have not applied the HTML Help update. Microsoft has assigned a risk rating of "Critical" to this vulnerability and a patch is available at the Microsoft website.

*Category 23.6* *Web-site infrastructure, general Web security issues*

2003-05-01 **crackers wreak havoc physica world ACM conference privacy electronic society web-based order forms google attack**

NewsScan

MALICIOUS CRACKERS COULD WREAK HAVOC IN PHYSICAL WORLD
Researchers participating in a recent ACM conference on privacy in an electronic society have described how automated order forms on the Web could be exploited to send tens of thousands of unwanted catalogs to a business or an individual. The resulting deluge not only would pose an inconvenience to the victim, but likely would swamp the local post office charged with delivery, said Avi Rubin, technical director of the Information Security Institute at Johns Hopkins University. "People have not considered how easily someone could leverage the scale and automation of the Internet to inflict damage on real-world processes." Using Google to locate online order forms and simple software to fill in fields such as "name" and "address," "it could be set up to send 30,000 different catalogs to one person or 30,000 copies of one catalog to 30,000 different recipients," said Rubin. The technique could also be used to exploit the increasingly common Web-based forms used to request repair service, deliveries or parcel pickups. Rubin and his fellow researchers suggested Web sites could take steps to prevent such attacks, including setting up online forms so that they cannot easily be picked up by a search engine, or using HTML coding to create an online form so it no longer contains easily recognized field names, such as "name." Another strategy could be to include a Reverse Turing Test — a step in each form that requires human input. (Science Daily 1 May 2003)

*Category 23.6 Web-site infrastructure, general Web security issues*

2003-05-29 **MS03-018 Microsoft Security Bulletin patches CSS Cross Site Scripting redirection buffer overrun IIS 4.0 5.0 5.1**

NIPC/DHS

May 29, Microsoft — Microsoft Security Bulletin MS03-018: Cumulative Patch for Internet Information Service. This patch supercedes all previous patches released for IIS 4.0 and IIS 5.0. It also fixes the following vulnerabilities affecting IIS 4.0, 5.0 and 5.1: a Cross-Site Scripting (CSS) vulnerability affecting IIS 4.0, 5.0 and 5.1 involving the error message that's returned to advise that a requested URL has been redirected; a buffer overrun that results because IIS 5.0 does not correctly validate requests for server side includes; a denial of service vulnerability that results because of a flaw in the way IIS 4.0 and 5.0 allocate memory requests when constructing headers to be returned to a web client; a denial of service vulnerability that results because IIS 5.0 and 5.1 do not correctly handle an error condition when an overly long WebDAV request is passed to them. This patch, rated "Important," requires the patch from Microsoft Security Bulletin MS02-050 to be installed.

*Category 23.6 Web-site infrastructure, general Web security issues*

2003-06-04 **MS03-020 cumulative patch internet explorer buffer overflow arbitrary code malicious functionality window.showHelp() update Microsoft Security Bulletin**

NIPC/DHS

June 04, Microsoft — Microsoft Security Bulletin MS03-020: Cumulative Patch for Internet Explorer. This cumulative patch includes the functionality of all previously released patches for Internet Explorer 5.01, 5.5 and 6.0, and eliminates two vulnerabilities: a buffer overrun vulnerability that occurs because Internet Explorer does not properly determine an object type returned from a web server, and a flaw that results because Internet Explorer does not implement an appropriate block on a file download dialog box. It could be possible for an attacker to exploit this vulnerability to run arbitrary code on a user's system. This cumulative patch will cause window.showHelp( ) to cease to function if you have not applied the HTML Help update. Microsoft has assigned a risk rating of "Critical" to this patch.

*Category 23.6 Web-site infrastructure, general Web security issues*

2003-06-25 **Internet Explorer IE flaw unearth worm microsoft buffer overflow vulnerability BugTraq**

NIPC/DHS

June 25, CNET News.com — IE flaw could unearth worm. A vulnerability in Microsoft's Internet Explorer could result in the creation of a serious Internet worm, security experts have warned. However, there is no proof that the vulnerability foretells the execution of arbitrary code. The buffer overflow vulnerability is triggered by a malicious Java script that can be embedded in an HTML document. When a Web page or HTML file containing the malicious script is viewed by Internet Explorer, versions 5 and 6, the buffer is overrun and the browser crashes. The code was posted to the BugTraq security mailing list early Sunday morning. Microsoft wasn't pleased with the premature revelation of the vulnerability before its security teams got a chance to look into the matter. There is currently no patch unavailable.

*Category 23.6 Web-site infrastructure, general Web security issues*

2003-07-09 **Apache http server denial service DoS open-source bug fix**

NIPC/DHS

July 09, internetnews.com — DoS holes plugged in Apache HTTP Server. The Apache Software Foundation on Monday released a new version of its open-source Web server project to plug four potentially serious security holes. The latest update to the Apache 2.0 HTTP Server (version 2.0.47) is described as a security and bug fix release to plug holes that could lead to denial-of-service attacks. The Foundation warned that the SSLCipherSuite directive being used to upgrade from a weak ciphersuite to a strong one could result in the weak ciphersuite being used in place of the strong one. The previous Apache HTTP Server version also contains a bug in the prefork MPM where certain errors returned by accept() on rarely accessed ports could cause temporal DoS. Another DoS security vulnerability, caused when target host is IPv6, was also patched. Apache explained that ftp proxy server can't create IPv6 socket. The Apache Foundation also warned older versions of the server would crash when going into an infinite loop because of too many subsequent internal redirects and nested subrequests.

*Category 23.6* *Web-site infrastructure, general Web security issues*

2003-10-20 **Microsoft Internet Explorer buy music online complaint Justice Department**

NewsScan

CHALLENGE TO THE WEB WEAVED BY MICROSOFT
The U.S. Justice Department and 19 states have complained to U.S. District Judge Colleen Kollar-Kotelly about a design feature of Windows that compels consumers who buy music online to use only Microsoft's Internet Explorer browser and guides them to a Microsoft Web site. The dispute may become the first test of the Microsoft antitrust settlement approved by a federal court in October 2002. In response, a Microsoft executive said, "We believe that the use of Internet Explorer by the Shop-for-Music-Online link in Windows is consistent with the design rules established by the consent decree, and we will continue to work with the government to address any concerns. At issue is a design feature in Windows XP called "Shop for Music Online," which lets consumers purchase compact discs from retailers over the Internet, but when consumers click the link to buy music, Windows opens Microsoft's browser software even if consumers have indicated that they prefer using rival browser software. (AP/San Jose Mercury News 20 Oct 2003)

*Category 23.6* *Web-site infrastructure, general Web security issues*

2003-11-02 **website abandoned sites weblogs y2k out-of-date content dissapear**

NewsScan

WEB LITTERED WITH ABANDONED SITES
The Web is cluttered with pages and whole sites long ago forgotten by their creators — political campaigns from yesteryear, personal projects that lost their pizzazz, and even Y2K sites that commemorate a catastrophe that never happened. And while it's easy to imagine losing interest in the effort required to update and maintain a Web site, the same phenomenon is evident among the Web's latest obsession — blogging. One study of 3,634 weblogs found that two-thirds had not been updated for at least two months and about 25% hadn't changed since the day they were launched. "Some would say, 'I'm going to be too busy but I'll get back to it,' but never did," says Jeffrey Henning, chief technology officer with Perseus Development Corp., which conducted the study. But while some users resent slogging through out-of-date content, others complain that sites disappear too quickly. "I do hear pretty frequently not so much that there's deadwood, but that sites go away without a trace," says Steve Jones, a communications professor at the University of Illinois at Chicago. (AP/Tampa Bay Online 2 Nov 2003)

*Category 23.6* *Web-site infrastructure, general Web security issues*

2003-11-13 **new critical vulnerability Microsoft security bulletin Internet Explorer browser software patch fix exploit**

NIPC/DHS

November 11, Microsoft — Microsoft Security Bulletin MS03-048: Cumulative Security Update for Internet Explorer. There are three vulnerabilities that involve the cross-domain security model of Internet Explorer, which keeps windows of different domains from sharing information. These vulnerabilities could result in the execution of script in the My Computer zone. After the user has visited a malicious Website or viewed a malicious HTML e-mail message an attacker who exploited one of these vulnerabilities could access files on a user's system, and run arbitrary code on a user's system in the security context of the user. Another vulnerability involves the way zone information is passed to an XML object within Internet Explorer. This vulnerability could allow an attacker to read local files on a user's system. Finally, there is a vulnerability that involves performing a drag-and-drop operation during dynamic HTML (DHTML) events in Internet Explorer. This vulnerability could allow a file to be saved in a target location on the user's system if the user clicks a link. No dialog box would request that the user approve this download. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that system administrators install this patch immediately.

*Category 23.6* *Web-site infrastructure, general Web security issues*

2003-11-25 **Web browser software Opera security flaw vulnerability exploit**

NIPC/DHS

November 24, CNET News.com — Opera update seals security holes. A new version of Opera, released Friday, November 21, fixes two vulnerabilities in the Web browser. The vulnerabilities, disclosed to the BugTraq security mailing list, allow rogue Web sites to take control of a victim's computer by exploiting weaknesses in the way the browser handles "skin" files, or configuration files that can change the look of a program. An advisory, written by Jouko Pynnonen of Finland, describes scenarios that would allow an attacker to seize control of systems running Opera, all of which require some degree of user interaction to be successfully exploited. "In order to be exploited, these vulnerabilities require the victim to visit a Web page created by a malicious user," he wrote. Though Pynnonen says one vulnerability affects Windows systems only, the second vulnerability, a buffer overflow, will allow an attacker to take control of Linux-based systems. "The directory traversal problem doesn't exist on Linux...Other versions weren't tested," the advisory read, noting also that "the buffer overflow can be produced on Linux, too."

*Category 23.6 Web-site infrastructure, general Web security issues*

2003-11-28 **vulnerability scripting Internet Explorer browser software hacker**

NIPC/DHS

November 25, The Register — Scripting flaws pose severe risk for IE users. A set of five unpatched scripting vulnerabilities in Internet Explorer creates a mechanism for hackers to compromise targeted PCs. The vulnerabilities, unearthed by Chinese security researcher Liu Die Yu along with Proof of Concept exploits, enable malicious Websites and viruses to bypass the security zone settings in IE6. Used in combination, the flaws might be exploited to seize control of vulnerable PCs. Microsoft has yet to patch the flaws. But users can protect themselves against the flaws by disabling active scripting or by using an alternative browser. Thomas Kristensen of Secunia said the five distinct vulns could used in combination to install executables. Secunia advises all IE users to disable active scripting. The drawback of this workaround is that with some Websites certain functions won't work unless scripting is enabled. IE users should define any sites they need to use as trusted so that they can continue to use scripting on those sites alone, Kristensen said. The original advisory is available here: http://www.secunia.com/advisories/10289/

*Category 23.6 Web-site infrastructure, general Web security issues*

2003-12-12 **new vulnerability flaw exploit Internet Explorer browser software**

NIPC/DHS

December 12, eWEEK — Internet Explorer spoofing vulnerability found. Security researchers confirmed a vulnerability in Internet Explorer 6 Tuesday, December 9, that could let an attacker display a fake URL in the browser's address bar in an attempt to disguise the real domain, an advisory from security company Secunia Ltd said. Using the security hole, an attacker could trick users into providing sensitive information or download malicious software by leading them to think that they are visiting a trusted site, the advisory said. A Microsoft spokesperson on Wednesday said that the company knows of no exploits of the reported hole or of any users being affected but said in a statement that it is "aggressively investigating the public reports." Microsoft may provide a fix through its monthly patch release cycle or a separate patch, depending on the outcome of the investigation, the spokesperson said. The Secunia advisory is available here: http://www.secunia.com/advisories/10395

# 23.7 VoIP

*Category 23.7* *VoIP*

2003-02-24 **Session Initiation Protocol SIP new vulnerabilities exploit software CERT CC advisory**

NIPC/DHS

February 21, CERT/CC — CERT Advisory CA-2003-06: Multiple vulnerabilities in implementations of the Session Initiation Protocol (SIP). The Session Initiation Protocol (SIP) is a developing and newly deployed text-based protocol that is commonly used in Voice over IP (VoIP), Internet telephony, instant messaging, and various other applications. Numerous vulnerabilities have been reported in multiple vendors' implementations of the SIP. These vulnerabilities may allow an attacker to gain unauthorized privileged access, cause denial-of-service attacks, or cause unstable system behavior. SIP-enabled products from a wide variety of vendors are affected. Other systems making use of SIP may also be vulnerable but were not specifically tested. Not all SIP implementations are affected. Detailed instructions for resolving this issue may be found in this advisory on the CERT/CC Website. To determine if your product is vulnerable please refer to CERT/CC Vulnerability Note VU#528719 at http://www.kb.cert.org/vuls/id/528719

# 24.1 Windows 9x/Me

*Category 24.1* *Windows 9x/Me*

2003-02-27 **Microsoft security bulletin Millenium Edition ME vulnerability**

NIPC/DHS

February 26, Microsoft — Microsoft Security Bulletin MS03-006: Flaw in Windows Me Help and Support Center could enable code execution . A security vulnerability is present in the Windows Me version of Microsoft's Help and Support Center. Users and programs can execute URL links to Help and Support Center by using the "hcp://" prefix in a URL link instead of " http://". The vulnerability results because the URL Handler for the "hcp://" prefix contains an unchecked buffer. An attacker who successfully exploited this vulnerability could cause code of his or her choice to be executed as though it originated on the local machine. Such code could provide the attacker with the ability to take any desired action on the machine, including adding, deleting or modifying data on the system or running any code of the attacker's choice. Microsoft assigned a risk rating of "Critical" to this vulnerability. A patch is available at the Microsoft website.

# 24.2 Windows NT/2K/XP

*Category 24.2* *Windows NT/2K/XP*

2003-02-06 **Microsoft security bulletin unchecked buffer vulnerability**

NIPC/DHS

February 05, Microsoft — Microsoft Security Bulletin MS03-005: Unchecked buffer in Windows Redirector could allow privilege elevation. A security vulnerability exists in the implementation of the Windows Redirector on Windows XP because an unchecked buffer is used to receive parameter information. By providing malformed data to the Windows Redirector, an attacker who successfully exploited this vulnerability could cause the system to fail, or could cause code of the attacker's choice to be executed with system privileges. Code running with system privileges could provide the attacker with the ability to take any desired action on the machine, such as adding, deleting, or modifying data on the system, and creating or deleting user accounts. This vulnerability cannot be exploited remotely. Windows XP systems that are not shared between users would not be at risk. The vulnerability could only be exploited by an attacker who had valid credentials to interactively log onto the computer. Microsoft has assigned a severity rating of "Important" to this vulnerability. A patch is available at the Microsoft website.

*Category 24.2* *Windows NT/2K/XP*

2003-03-12 **CERT CC advisory Windows Shares Serve Message Block 2000 XP target**

NIPC/DHS

March 11, CERT/CC — CERT Advisory CA-2003-08: Increased Activity Targeting Windows Shares. Over the past few weeks, the CERT/CC has received an increasing number of reports of intruder activity involving the exploitation of Null (i.e., non-existent) or weak Administrator passwords on Server Message Block file shares used on systems running Windows 2000 or Windows XP. This activity has resulted in the successful compromise of thousands of systems, with home broadband users' systems being a prime target. Recent examples of such activity are the attack tools known as W32/Deloder, GT-bot, sdbot, and W32/Slackor. The presence of any of these tools on a system indicates that the Administrator password has likely been compromised, and the entire system is therefore suspect. With this level of access, intruders may exercise remote control expose confidential data; install other malicious software; change files; delete files; or launch attacks against other sites. Information on how to guard against these attacks may be found on the CERT/CC website.

*Category 24.2* *Windows NT/2K/XP*

2003-03-20 **new vulnerability Microsoft security bulletin Windows Script Engine**

NIPC/DHS

March 19, Microsoft — Microsoft Security Bulletin MS03-008: Flaw in Windows Script Engine Could Allow Code Execution. The Windows Script Engine provides Windows operating systems with the ability to execute script code. A flaw exists in the way by which the Windows Script Engine for JScript processes information. An attacker could exploit the vulnerability by constructing a web page that, when visited by the user, would execute code of the attacker's choice with the user's privileges. The web page could be hosted on a web site, or sent directly to the user in email. Exploiting the vulnerability would allow the attacker only the same privileges as the user. Computers configured to disable active scripting in Internet Explorer are not susceptible to this issue. Users whose accounts are configured to have few privileges on the system would be at less risk than ones who operate with administrative privileges. Automatic exploitation of the vulnerability by an HTML email would be blocked by Outlook Express 6.0 and Outlook 2002 in their default configurations, and by Outlook 98 and 2000 if used in conjunction with the Outlook Email Security Update. Microsoft has assigned a risk rating of "Critical" to this vulnerability. A patch is available at the Microsoft Website. Microsoft has also provided information about preventive measures customers can use to help block the exploitation of this vulnerability while they are assessing the impact and compatibility of the patch.

*Category 24.2* *Windows NT/2K/XP*

2003-03-27 **new vulnerability Remote Procedure Call RPC Microsoft denial-of-service advisory**

NIPC/DHS

March 26, Microsoft — Microsoft Security Bulletin MS03-010: Flaw in RPC Endpoint Mapper Could Allow Denial of Service Attacks. There is a vulnerability in the part of Remote Procedure Call (RPC) that deals with message exchange over TCP/IP due to incorrect handling of malformed messages. This vulnerabilty affects the RPC Endpoint Mapper process, which listens on TCP/IP port 135. To exploit this vulnerability, an attacker would need to establish a TCP/IP connection to the Endpoint Mapper process on a remote machine. Once the connection was established, the attacker would begin the RPC connection negotiation before transmitting a malformed message. At this point, the process on the remote machine would fail. The RPC Endpoint Mapper process is responsible for maintaining the connection information for all of the processes on that machine using RPC. Because the Endpoint Mapper runs within the RPC service itself, exploiting this vulnerability would cause the RPC service to fail, with the attendant loss of any RPC-based services the server offers, as well as potential loss of some COM functions. A patch is available at the Microsoft website for Windows 2000 and Windows XP. However, Microsoft is unable to provide a patch for this vulnerability for Windows NT 4.0 and users are encouraged to employ the workaround posted on the Microsoft website, which is to protect the NT 4.0 system with a firewall that blocks Port 135.

*Category 24.2* *Windows NT/2K/XP*

2003-04-10 **new vulnerability Microsoft security bulletin virtual machine flaw patch exploit fix**

NIPC/DHS

April 09, Microsoft — Microsoft Security Bulletin MS03-011: Flaw in Microsoft VM Could Enable System Compromise. The Microsoft VM is a virtual machine for the Win32 operating environment. The Microsoft VM is shipped in most versions of Windows, as well as in most versions of Internet Explorer. A new security vulnerability affects the ByteCode Verifier component of the Microsoft VM, and results because the ByteCode verifier does not correctly check for the presence of certain malicious code when a Java applet is being loaded. The attack vector for this new security issue would likely involve an attacker creating a malicious Java applet and inserting it into a web page that when opened, would exploit the vulnerability. An attacker could then host this malicious web page on a web site, or could send it to a user in e-mail. Corporate IT administrators could limit the risk posed to their users by using application filters at the firewall to inspect and block mobile code. Microsoft has assigned a risk rating of "Critical" to this vulnerability. A patch is available at the Microsoft website.

*Category 24.2* *Windows NT/2K/XP*

2003-04-17 **new vulnerability Microsoft security bulletin buffer overflow kernel message handling**

NIPC/DHS

April 16, Microsoft — Microsoft Security Bulletin MS03-013: Buffer Overrun in Windows Kernel Message Handling could Lead to Elevated Privileges. The Windows kernel is the core of the operating system. It provides system level services such as device and memory management, allocates processor time to processes and manages error handling. There is a flaw in the way the kernel passes error messages to a debugger. A vulnerability results because an attacker could write a program to exploit this flaw and run code of their choice. An attacker could exploit this vulnerability to take any action on the system including deleting data, adding accounts with administrative access, or reconfiguring the system. For an attack to be successful, an attacker would need to be able to logon interactively to the system, either at the console or through a terminal session. Also, a successful attack would require the introduction of code in order to exploit this vulnerability. Because best practices recommends restricting the ability to logon interactively on servers, this issue most directly affects client systems and terminal servers. Microsoft has assigned a risk rating of "Important" to this vulnerability. A patch is available at the Microsoft website.

*Category 24.2* *Windows NT/2K/XP*

2003-04-28 **Cisco Systems Secure Access Control Server Windows vulnerability patch fix**

NIPC/DHS

April 24, CNET News.com — Cisco flaw exposes Windows servers. A potentially critical vulnerability has been found in Cisco Systems' Secure Access Control Server for Windows servers, which is used to control devices such as routers in large networks. The buffer overflow glitch may allow an attacker to seize control of the Cisco service when it's running on Windows, according to Cisco. The Unix variant is not affected. Exploitation of the flaw could result in a malicious hacker gaining full control of a target company's security infrastructure, leaving it completely exposed. An exploit for the vulnerability is not known to be circulating, and ACS servers are usually deployed on network segments with limited physical access. Administrators of ACS systems block TCP port 2002 until they can deploy Cisco's fix. A patch is available at the Cisco Website: http://www.cisco.com/warp/public/707/cisco-sa-20030423-ACS.s html.

*Category 24.2* *Windows NT/2K/XP*

2003-05-01 **windows flaw patch security microsoft multi-processor machine crash 2000 XP**

NIPC/DHS

May 01, eWEEK — Microsoft updates patch for Windows flaw. Microsoft Corp. has released an updated patch for a security vulnerability discovered in Windows NT 4.0 in December. The new update fixes a flaw in the original patch that installed the wrong binaries on multi-processor machines, causing them to crash in some situations. The original vulnerability that the patch was meant to fix affected Windows 2000 and XP as well. But the problem that prompted the release of the new patch only occurs in machines running Windows NT 4.0 Terminal Services Edition. The revised bulletin and patch for this flaw are available on the Microsoft Website:
http://www.microsoft.com/technet/treeview/default.asp?url=/t echnet/security/bulletin/MS02-071.asp.

*Category 24.2* *Windows NT/2K/XP*

2003-05-07 **MS03-017 Microsoft Windows Media Player 7.1 XP malicious executable HTML e-mail outlook update code execution**

NIPC/DHS

May 07, Microsoft — Microsoft Security Bulletin MS03-017: Flaw in Windows Media Player Skins Downloading could allow Code Execution. A flaw exists in the way Microsoft's Windows Media Player 7.1 and Windows Media Player for Windows XP handle the download of skin files. An attacker could force a file masquerading as a skin file into a user's machine. This could allow an attacker to place a malicious executable on the system. In order to exploit this flaw, an attacker would have to host a malicious web site and then persuade a user to visit that site. An attacker could also embed the link in an HTML e-mail and send it to the user. If the user was not using Outlook Express 6.0 or Outlook 2002 in their default configurations, or Outlook 98 or 2000 in conjunction with the Outlook Email Security Update, the attacker could cause an attack that could both place, then launch the malicious executable without the user having to click on a URL contained in an e-mail. Microsoft has assigned a risk rating of "Critical" to this vulnerability, and a patch is available at the Microsoft website.

*Category 24.2* *Windows NT/2K/XP*

2003-05-28 **MS03-019 microsoft security bulletin ISAPI Extension Windows Media Service Denial Service NT4.0 Server IIS exploit**

NIPC/DHS

May 28, Microsoft — Microsoft Security Bulletin MS03-019: Flaw in ISAPI Extension for Windows Media Services Could Cause Denial of Service. When Windows Media Services are installed in Windows NT 4.0 Server or added through add/remove programs to Windows 2000, nsiislog.dll is installed to the Internet Information Services (IIS) Scripts directory on the server. A flaw in the way in which nsiislog.dll processes incoming requests could allow and attacker could send specially formed communications to the server that could cause IIS to stop responding to Internet requests. An attacker attempting to exploit this vulnerability would have to be aware which computers on the network had Windows Media Services installed on it and send a specific request to that server. Microsoft has assigned a risk rating of "Moderate" to this vulnerability and a patch is available at the Microsoft website.

*Category 24.2* *Windows NT/2K/XP*

2003-07-03 **Windows 2000 ShellExecute API hole buffer overflow vulnerability SecureNet Service MUA**

NIPC/DHS

July 03, eSecurity Planet — Windows 2000 ShellExecute API hole patched. Microsoft has issued a fix for a buffer overflow vulnerability in the Windows 2000 ShellExecute API after a security researcher warned the flaw could trigger denial-of-service attacks. According to research firm SecureNet Service (SNS), which reported the hole, Microsoft included a fix in Windows 2000 Service Pack 4. It affects Microsoft Windows 2000 Datacenter Server, Windows 2000 Advanced Server, Windows 2000 Server and Windows 2000 Professional. SNS said the problem was triggered when the pointer to an unusually long string was set to the 3rd argument of the Windows 2000 API Shell Execute() API function. SNS said that several applications containing Web browser, MUA and text editor were vulnerable to security hole.

*Category 24.2* *Windows NT/2K/XP*

2003-07-09 **MS03-025 windows message handling utility privilege elevation interactive processes**

NIPC/DHS

July 09, Microsoft — Microsoft Security Bulletin MS03-025: Flaw in Windows Message Handling through Utility Manager Could Enable Privilege Elevation. Microsoft Windows messages provide a way for interactive processes to react to user events and communicate with other interactive processes. A flaw in the way that the Microsoft Accessibility Utility Manager handles Windows messages results in a vulnerability because the control that provides the list of accessibility options to the user does not properly validate Windows messages sent to it. It's possible for one process in the interactive desktop to use a specific Windows message to cause the Utility Manager process to execute a callback function at the address of its choice. Because the Utility Manager process runs at higher privileges than the first process, this would provide the first process with a way of exercising those higher privileges. By default, the Utility Manager contains controls that run in the interactive desktop with Local System privileges. An attacker who had the ability to log on to a system interactively could run a program that could send a Windows message upon the Utility Manager process, causing it to take any action the attacker specified. This would give the attacker complete control over the system. Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators install the patch immediately.

*Category 24.2* *Windows NT/2K/XP*

2003-07-09 **MS03-024 buffer overrun data corruption Server Message Block SMB port 139 445**

NIPC/DHS

July 09, Microsoft — Microsoft Security Bulletin MS03-024: Buffer Overrun in Windows Could Lead to Data Corruption. When a client system sends an Server Message Block (SMB) packet to the server system, it includes specific parameters that provide the server with a set of "instructions." The server is not properly validating the buffer length established by the packet. If the client specifies a buffer length that is less than what is needed, it can cause the buffer to be overrun. By sending a specially crafted SMB packet request, an attacker could cause a buffer overrun to occur. If exploited, this could lead to data corruption, system failure, or it could allow an attacker to run the code of their choice. An attacker would need a valid user account and would need to be authenticated by the server to exploit this flaw. By default, it is not possible to exploit this flaw anonymously. The attacker would have to be authenticated by the server prior to attempting to send a SMB packet to it. Blocking port 139/445 at the firewall will prevent the possibility of an attack from the Internet. Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators consider installing the patch.

*Category 24.2* *Windows NT/2K/XP*

2003-07-16 **MS03-027 buffer windows shell system compromise attacker service pack 1 XP important**

NIPC/DHS

July 16, Microsoft — Microsoft Security Bulletin MS03-027: Unchecked Buffer in Windows Shell Could Enable System Compromise. An unchecked buffer exists in one of the functions used by the Windows shell to extract custom attribute information from certain folders. An attacker could seek to exploit this vulnerability by creating a Desktop.ini file that contains a corrupt custom attribute, and then host it on a network share. If a user were to browse the shared folder where the file was stored, the vulnerability could then be exploited. A successful attack could have the effect of either causing the Windows shell to fail, or causing an attacker's code to run on the user's computer in the security context of the user. This vulnerability only affects Windows XP Service Pack 1. Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators install the patch at the earliest opportunity.

*Category 24.2* *Windows NT/2K/XP*

2003-07-17 **flaw Windows Microsoft Server 2003 vulnerability**

NewsScan

MICROSOFT FLAW: A NEW STAGE OF DELIRIUM
Microsoft has acknowledged a critical vulnerability in most versions of its Windows operating system software, including its latest Windows Server 2003 software. The vulnerability (first pointed out by researchers in Poland known as the "Last Stage of Delirium Research Group") could be used by network vandals to seize control of a victim's Windows computer over the Internet, stealing data, deleting files or eavesdropping on e-mail messages. The Server 2003 software was sold under the highly promoted "Trustworthy Computing" initiative launched last year by Microsoft founder Bill Gates. The company urged customers to immediately apply a free software patch available from Microsoft's Web site. Internet Security Systems, an Atlanta-based computer firm, characterized the Windows flaw as "an enormous threat." (AP/San Jose Mercury News 17 Jul 2003)

*Category 24.2* *Windows NT/2K/XP*

2003-07-23 **MS03-029 denial service windows nt 4.0 server file management function**

NIPC/DHS

July 23, Microsoft — Microsoft Security Bulletin MS03-029: Flaw in Windows Function Could Allow Denial of Service. A flaw exists in a Windows NT 4.0 Server file management function that can cause a denial of service vulnerability. The flaw results because the affected function can cause memory that it does not own to be freed when a specially crafted request is passed to it. If the application making the request to the function does not carry out any user input validation and allows the specially crafted request to be passed to the function, the function may free memory that it does not own. As a result, the application passing the request could fail. By default, the affected function is not accessible remotely, however applications installed on the operating system that are available remotely may make use of the affected function. Microsoft has assigned a risk rating of "Moderate" to this issue and recommends that system administrators consider applying the security patch

*Category 24.2* *Windows NT/2K/XP*

2003-09-10 **Internet Operations Microsoft Operating Systems Remote procedure Call Server Service RPCSS NCSD DHS IAP DCOM RPC ports exploit vulnerabilities worm virus**

NIPC/DHS

September 10, U.S. Department of Homeland Security — Potential For Significant Impact On Internet Operations Due To Vulnerability In Microsoft Operating Systems' Remote Procedure Call Server Service (RPCSS). The National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) Directorate is issuing this advisory in consultation with the Microsoft. There are three vulnerabilities in the part of Remote Procedure Call (RPC) that deals with RPC messages for the Distributed Component Object Model (DCOM) activation—two that would allow arbitrary code execution, and one that would result in a denial of service. These particular vulnerabilities affect the DCOM interface within the RPCSS, which listens on RPC enabled ports. An attacker who successfully exploited these vulnerabilities could be able to run code with local system privileges on an affected system, or cause the RPCSS to fail. The attacker could be able to take any action on the system. DHS is concerned that a properly written exploit could rapidly spread on the Internet as a worm or virus in a fashion similar to the Blaster Worm. DHS and Microsoft recommend that system administrators install the patch immediately. Additional information is available on the Microsoft Website: http://www.microsoft.com/security/security_bulletins/ms03-03 9.asp

*Category 24.2* *Windows NT/2K/XP*

2003-09-17 **iDefense internet attack blaster like tool hacker access victims computer infection**

NewsScan

VANDAL WATCH
Security firm iDefense Inc. of Reston, Va., has found new Internet attack software being distributed via a Chinese Web site, and says they expect widespread attacks similar to the Blaster infection within days. Microsoft confirmed it was studying the new attack tool, which gives hackers access to victims' computers by creating a new account with the name "e" with a preset password. The tool includes options to attack two Windows 2000 versions that are commonly used inside corporations.
(AP/San Jose Mercury News 17 Sep 2003)

*Category 24.2* *Windows NT/2K/XP*

2003-09-19 **ATM Windows NT security issues hackers IBM OS/2 open technology hardware support cut-down version**

NewsScan

ATMs TO SWITCH OVER TO WINDOWS
Sixty-five percent of the automated teller machines in the U.S. will be running on a stripped down version of Windows NT within three years, according to a study by market researcher Celent. Currently most ATMs use IBM's OS/2 operating system, but banking industry officials say they now prefer Windows, which is more compatible with their internal corporate networks. "Because we are seeing so many mergers and acquisitions in the last few years, you have large banks running a fleet of ATM hardware," says Celent analyst Gwenn Bezard. "With open technologies [like Windows] it is easier to run different types of hardware on the same software." Banking officials generally dismiss worries over hackers disabling or corrupting ATMs across the country, but some security specialists continue to have doubts: "What Microsoft actually sells to the banks for ATM use is a cut-down version of Windows that doesn't contain things like Web servers. They have tried to cut out the unnecessary rubbish that clutters up the typical PC. How good a job they've done, I just don't know… So we definitely can't rule out the possibility that someone in the future writes a Slammer-style worm that causes thousands of ATMs to start spewing out cash," says British security expert Ross Anderson. (Wired.com 19 Sep 2003)

*Category 24.2* *Windows NT/2K/XP*

2003-11-13 **new critical vulnerability Microsoft security bulletin buffer overrun overflow workstation patch fix exploit**

NIPC/DHS

November 11, Microsoft — Microsoft Security Bulletin MS03-049: Buffer Overrun in the Workstation Service Could Allow Code Execution. A security vulnerability exists in the Workstation service that could allow remote code execution on an affected system. This vulnerability results because of an unchecked buffer in the Workstation service. If exploited, an attacker could gain System privileges on an affected system, or could cause the Workstation service to fail. An attacker could take any action on the system, including installing programs, viewing data, changing data, or deleting data, or creating new accounts with full privileges. If users have blocked inbound UDP ports 138, 139, 445 and TCP ports 138, 139, 445 by using a firewall an attacker would be prevented from sending messages to the Workstation service. Most firewalls, including Internet Connection Firewall in Windows XP, block these ports by default. Disabling the Workstation service will prevent the possibility of attack. Only Windows 2000 and Window XP are vulnerable to this attack. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that system administrators install the patch immediately.

*Category 24.2* *Windows NT/2K/XP*

2003-11-17 **Microsoft Windows exploit patch fix release**

NIPC/DHS

November 13, eWEEK — Windows exploits released. Microsoft Corp. released its monthly passel of patches on Tuesday, November 11, including one for a flaw in the Workstation service in Windows 2000 and XP. A successful exploitation would give the attacker complete control of the compromised PC, Microsoft said. Less than 24 hours after Microsoft issued the fix, two members of the BugTraq security mailing list posted exploit code for the vulnerability. The author of one of the exploits said the code had been tested only on a Windows 2000 machine with Service Pack 4 installed and the FAT32 file system running. The other exploit is designed for machines running Windows XP. However, experts said it would take little effort to adapt the code for other Windows machines. And, more importantly, the Workstation vulnerability appears to be a prime candidate for a worm.

*Category 24.2* *Windows NT/2K/XP*

2003-12-11 **security expert warning Microsoft Windows critical vulnerability TCP UDP**

NIPC/DHS

December 10, eWEEK — Security experts warn of new way to attack Windows. Security experts have found a new way to exploit a critical vulnerability in Windows that evades a workaround. Microsoft Corp. issued a patch for the vulnerability in November, but the security bulletin also listed several workarounds for the flaw, including disabling the Workstation Service and using a firewall to block specific UDP and TCP ports. Researchers at security company Core Security Technologies discovered a new attack vector that uses a different UDP port. This attack still allows the malicious packets to reach the vulnerable Workstation Service. An attacker who successfully exploits the weakness could run any code of choice on the vulnerable machine. An attacker doesn't have to individually address computers on the network, but can broadcast an attack. Such a tactic could actually create a worm that spreads faster than the SQL Slammer worm did last year. Microsoft urged customers to apply the patch. "Applying the patch does correct the problem," said Iain Mulholland, a security program manager for Microsoft.

# 24.3 UNIX flavors

*Category 24.3 UNIX flavors*

2003-01-08 **Linux consumer appliances cellular mobile telephones**

NewsScan

LINUX IN CELL PHONES
The Linux operating system, which is being used in an increasing variety of devices (including handhelds, digital video recorders, and wristwatches) will soon be used in cell phones, vying for market share with operating systems from PalmSource, Microsoft, and Symbian. The NEC corporation is working on the development of Linux-based cell phones with MontaVista Software, and is in talks with other cell phone makers to begin similar projects focused on the global and Japanese markets. NEC executive Scott Hedrick says, "One of our customers wants to move its entire product line to MontaVista Linux." (PC World 8 Jan 2002)
http://www.pcworld.com/news/article/0,aid,108556,00.asp

---

*Category 24.3 UNIX flavors*

2003-01-10 **Linux home computers appliances consumer electronics**

NewsScan

SONY EXEC: WINDOWS FOR THE OFFICE, LINUX FOR THE HOME
Sony president and chief operating officer Kunitake Ando told an audience at the Consumer Electronics Show in Las Vegas that, although his company has a working partnership with Microsoft, Sony sees the Linux operating system, rather than Microsoft's Windows, as the standard for transferring digital entertainment from device to device in the home. He predicted that the TV set will be reborn as an "always on, interactive device" that will serve as a broadband networking hub for high-speed communications between all electronic systems in the home, from a large-screen digital screen to a handheld device. Sony's plan for doing that features a TV set-top box called Cocoon that is Linux-based, Internet-connected, and complemented by a hard-disk drive. (San Jose Mercury News 9 Jan 2003)

---

*Category 24.3 UNIX flavors*

2003-01-16 **Linux operating system data centers corporations study prediction open source**

NewsScan

LINUX: THE RISE OF THE PENGUIN
Linux will emerge as the dominant operating system in corporate data centers, according to a new study by Goldman Sachs, which says the ascendance of the open source software will enable IT managers to take advantage of lower-cost, higher-performance Intel-based servers, and to avoid "premium-priced proprietary systems." The report, titled "Fear the Penguin," predicts that eventually, Linux-based systems will displace those running on Unix and RISC processors: "Many observers confine Linux's enterprise opportunity to the market for low-end 'edge' servers such as file, print, Web and e-mail servers. But we are confident that the technical developments and market forces are in place for it also to become the dominant OS on the higher-end servers of the enterprise data center." The winners in this scenario will be "independent PC semiconductor companies (Intel and AMD) and Intel-based server businesses (Dell)." The emergence of Linux is also expected to buoy the fortunes of "open" infrastructure software vendors, such as BEA Systems, BMC Software, Oracle and Veritas. However, with regard to archrival Microsoft, Linux will "hamper the movement of Windows into the enterprise data center, an area that Microsoft has only recently begun to target for growth," by providing an easier migration path from current Unix-based systems. "This shift will limit Windows' market opportunity in the data center for both its OS and its applications that run on that platform," concludes the study. (NewsFactor Network 15 Jan 2003)
http://www.newsfactor.com/perl/story/20471.html

---

*Category 24.3 UNIX flavors*

2003-01-21 **Linux operating system sales**

NewsScan

LINUX ACCOUNTS FOR $2 BILLION OF HP's SALES
Carly Fiorina, the chief executive of Hewlett-Packard, the world's top seller of personal computers, says that the Linux operating system now accounts for fully $2 billion of HP sales. That $2 billion figure contrasts with virtually no sales at all a mere five years ago. Of course, the increasing importance of Linux goes beyond HP, and market research groups such as IDC say that Linux installations grew 35% last year, in spite of the fact that corporate information technology budgets were in most cases flat or declining. (Reuters/San Jose Mercury News 21 Jan 2003)

---

*Category 24.3* *UNIX flavors*

2003-02-05 **Linux training certification network administration universities colleges**

NewsScan

LINUX CERTIFICATION VS. WINDOWS CERTIFICATION
Red Hat, which sells Linux software, has developed a training course that academic institutions can use to teach Linux and certify their graduates as skilled Linux technicians. Red Hat says that "the costs and legal burden of proprietary [read: Microsoft] software are becoming unsupportable," and so believes that their courses will be very competitive against Microsoft's MSCE training program. The Red Hat instructional program will allow students to gain certified experience in subjects such as system administration, network engineering, C or C++ programming, databases, Web development, PC repair, and forensic computing. (The Inquirer 4 Feb 2003)
http://www.theinquirer.net/?article=7600

---

*Category 24.3* *UNIX flavors*

2003-03-19 **Linux vulnerability open source Samba file server**

NIPC/DHS

March 17, CNET News.com — Linux firms urge users to plug Samba hole. The open-source community is urging customers to patch their systems to close a hole in a software component that allows Windows programs to store and retrieve files on Linux and Unix servers. Known as Samba, the software can be found on many workstations and servers running any one of the variety of flavors of Linux and Unix, including systems running Apple OS X. The flaw occurs in the code that reassembles data that the software receives from the Internet, according to the advisory. By sending the server a specially crafted data packet, an attacker could overload the memory used by the Samba software and cause the application to run code of the intruder's choice. Members of the Samba team planned to announce the vulnerability on Tuesday, but they released information over the weekend because some believed a Web site break-in in Germany may have been attributed to the software. Several Linux editions—including Debian, Gentoo, and SuSE—released patches for the problem. Apple Computer noted in an advisory that Samba is not enabled by default with Mac OS X and Mac OS X Server, but the company plans to issue a patch for version 10.2.4. Red Hat hasn't yet released a patch but will do so soon, the company said in a statement.

---

*Category 24.3* *UNIX flavors*

2003-04-08 **US military hacking fund open source software DARPA secure**

NIPC/DHS

April 06, The Globe and Mail (Canada) — U.S. military funds Calgary hacker. Theo de Raadt, a hacker from Calgary, Canada, has received a $2-million grant from the U.S. Defense Advanced Research Projects Agency (DARPA), the R&D arm of the U.S. military. For this grant, DARPA is interested in testing the security of commercial software systems against the security of open source software projects. de Raadt leads development of OpenBSD, an open-source computer operating system. OpenBSD, a derivative of the Unix operating system, is widely considered by computer experts to be the most resistant to unauthorized use. "We were convinced OpenBSD was the best platform to use as a basis for further securing open source," said Jonathan Smith, a professor of computer and information science at the University of Pennsylvania. Because DARPA does not directly fund projects outside the United States, it is Smith's computer science department that received the grant, although most of the money flows through to de Raadt's project. Although Microsoft Corp., whose Windows products are the world's dominant operating system products, and many other commercial software vendors are paying new attention to the security of their products, that renewed interest has done little to improve their products so far, de Raadt said.

---

*Category 24.3* *UNIX flavors*

2003-04-09 **vulnerability Samba file server Windows Linux Unix patch fix FreeBSD Sun Solaris**

NIPC/DHS

April 07, CNET News.com — Samba flaw threatens Linux file servers. The Samba Team released a patch on Monday for the second major security flaw found in the past few weeks in the open-source group's widely used program for sharing Windows files between Unix and Linux systems. The security problem could easily let an attacker compromise any Samba server connected to the Internet. The vulnerability is already being used by online attackers to compromise vulnerable servers, the company warned in an advisory. The Samba software that runs on major Linux distributions as well as FreeBSD and Sun Microsystems' Solaris operating system were affected. Security firm Digital Defense found the vulnerability. However, in an added twist to the situation that could make the threat more serious, while Digital Defense noted that some hackers obviously knew of the method by which the vulnerability could be exploited, it also mistakenly posted its own exploit onto its Web site.
A patch is available on the Samba Website:
http://us1.samba.org/samba/samba.html.

---

*Category 24.3* *UNIX flavors*

2003-04-10 **Linux operating system cheap changing business operation**

NewsScan

RISE OF LINUX IS CHANGING THE LANDSCAPE
The growing appeal of Linux as an alternative to rival operating systems such as Microsoft's Windows and Sun Microsystems' Solaris is changing the dynamics of the computer software business. Although currently relegated to "back-office" operations that handle e-mail, Web pages, file-sharing and printing, Linux is primed to begin making inroads into the higher echelons of business computing, such as telecom billing and airline reservation systems. A recent Garner report says that "businesses are coming to regard Linux as a worthy alternative to Unix and Windows." That trend has proven a boon for IBM, which embraced Linux in 1999 and now offers it across its entire product range, from lowly PCs to mighty mainframes. Also benefiting are Hewlett-Packard and Dell, both of which have been successful selling Linux servers. But the blossoming of Linux could prove toxic to Sun, which has seen some of its high-end Solaris server customers migrate to inexpensive Linux-run machines. Sun has compensated by offering its own cheap boxes running Linux alongside its more powerful Solaris-based ones, but many in the industry predict the dual strategy is "doomed." (The Economist 10 Apr 2003)

*Category 24.3* *UNIX flavors*

2003-06-04 **Novell Unix patent copyright operating system SCO SEC**

NewsScan

NOVELL CLAIMS UNIX PATENTS, COPYRIGHTS NEVER TRANSFERRED
Conflicting claims of Unix intellectual property ownership have come to light, with Novell saying it sold SCO Group broad rights to the Unix operating system but retained the copyrights and patents. According to a 1995 contract, Novell sold "all rights and ownership of Unix and UnixWare" to SCO's predecessor, the Santa Cruz Operation. But the asset purchase agreement filed with the SEC specifically excludes "all copyrights" and "all patents" from the purchase. "This agreement is kind of murky. You end up with a lot of questions, to put it mildly," says one intellectual property lawyer. The question of Unix patent and copyright ownership is central to SCO's attempt to force companies using Linux software to pay royalties for Unix software code that SCO says was illegally incorporated into Linux. On May 14, SCO sent letters to 1,500 of the world's largest corporations warning them that using Linux could open them up to legal liability for infringement. SCO CEO Darl McBride acknowledged last week that the contract contained "conflicting statements," but added: "It doesn't make sense. How would you transfer the product but not have the copyright attached? That would be like transferring a book but only getting the cover." Novell CEO Jack Messerman, meanwhile, said his company is basing future operating system products on Linux: "Novell is an ardent supporter of Linux and the open-source development community." (CNet News.com 4 Jun 2003)

*Category 24.3* *UNIX flavors*

2003-06-17 **SCO unix IBM AIX operating system lawsuit**

NewsScan

SCO SUES IBM OVER UNIX LICENSE
The SCO Group has revoked IBM's license to use Unix. SCO is claiming in a lawsuit that IBM illegally used Unix in its AIX operating system. IBM seems unruffled by the lawsuit. Its spokesman says: "As we have said all along, our license is irrevocable, perpetual, and can not be terminated." (Reuters/USA Today 17 Jun 2003)

*Category 24.3* *UNIX flavors*

2003-11-12 **attack hack Linux kernel operating system Trojan horse development code**

NIPC/DHS

November 06, CNET News.com — Attempted attack on Linux kernel foiled. An unknown intruder attempted to insert a Trojan horse program into the code of the next version of the Linux kernel, stored at a publicly accessible database. The public database was used only to provide the latest beta, or test version, of the Linux kernel to users of the Concurrent Versions System (CVS), a program designed to manage source code. The changes, which would have introduced a security flaw to the kernel, never became a part of the Linux code and were never a threat, said Larry McVoy, founder of software company BitMover and primary architect of the source code database BitKeeper, Thursday, November 6. An intruder apparently compromised one server earlier, and the attacker used his access to make a small change to one of the source code files, McVoy said. The change created a flaw that could have elevated a person's privileges on any Linux machine that runs a kernel compiled with the modified source code. The recent incident raises questions about the security of open-source development methods, particularly how well a development team can guarantee that any changes are not introducing intentional security flaws. While Microsoft code has had similar problems, closed development is widely considered to be harder to exploit in that way.

*Category 24.3* *UNIX flavors*

2003-11-24 **Debian GNU Linux attack hacker cracker open-source operating system backdoor kernel**

NIPC/DHS

November 21, eWEEK — Debian Linux under attack by hackers. An unknown cracker compromised several machines belonging to the Debian Project, including servers that house the project's bug-tracking system and security components. Officials from the project said last week they are working to restore all of the affected machines. Debian is an open-source operating system that uses the Linux kernel and also includes a number of packages and tools from the GNU Project. This is the second such attack against an open-source project in recent weeks. Someone tried to insert a backdoor into the Linux kernel two weeks ago.

*Category 24.3* *UNIX flavors*

2003-12-03 **Linux security new critical vulnerability kernel operating system**

NIPC/DHS

December 01, eWEEK — Researchers find serious vulnerability in Linux kernel. Security professionals took note of a critical new vulnerability in the Linux kernel that could enable an attacker to gain root access to a vulnerable machine and take complete control of it. An unknown hacker recently used this weakness to compromise several of the Debian Project's servers, which led to the discovery of the new vulnerability. This discovery has broad implications for the Linux community. Because the flaw is in the Linux kernel itself, the problem affects virtually every distribution of the operating system and several vendors have confirmed that their products are vulnerable. The vulnerability is in all releases of the kernel from Version 2.4.0 through 2.5.69, but has been fixed in Releases 2.4.23-pre7 and 2.6.0-test6. RedHat Inc. and the Debian Project have both released advisories warning customers of the issue and providing information on fixes. Products from other vendors, including, MandrakeSoft S.A., SuSE Linux AG and Caldera International Inc., are also vulnerable.

*Category 24.3* *UNIX flavors*

2003-12-08 **vulnerability fix flaw patch Gentoo operating system Linux**

NIPC/DHS

December 05, ZDNet UK — Patch fixes flaw behind Gentoo attack. The team responsible for Rsync, an open-source file-transfer program, has released a fix for a security flaw used in the recent compromise of a Gentoo Linux project server. The attacker used a flaw in Rsync along with a recently-announced bug in the Linux kernel to penetrate the security of the Gentoo machine, which was subsequently taken offline for analysis. The attack and compromise of Gentoo's server came after several machines belonging to the Debian Linux project were breached by attackers last month. Gentoo and Debian are both distributions of the open-source operating system based on the Linux kernel. The flaw in Rsync versions 2.5.6 and earlier cannot be used on its own to remotely gain administrator, or root, access to a Rsync server, but could be used with the kernel flaw for a full remote compromise—as was apparently the case with Gentoo's Rsync server. The exploit does not work unless Rsync is being used as a server. Users are recommended to immediately upgrade to Rsync version 2.5.7, a version of the Linux kernel later than 2.4.23, and turn off the "use chroot = no" option in Rsync. Additional information available here: http://rsync.samba.org/

# 24.4 TCP/IP & HTTP

*Category 24.4* *TCP/IP & HTTP*

2003-01-16 **buffer overflow vulnerabilities Internet Software Consortium ISC BIND**

NIPC/DHS

January 16, CERT/CC — VU#284857: Buffer overflows in ISC DHCPD minires library. During an internal source code audit, developers from the Internet Software Consortium (ISC) discovered several vulnerabilities in the error handling routines of the minires library, which is used by NSUPDATE to resolve hostnames. These vulnerabilities are stack-based buffer overflows that may be exploitable by sending a DHCP message containing a large hostname value. Note: Although the minires library is derived from the BIND 8 resolver library, these vulnerabilities do not affect any current versions of BIND. At this time, CERT is not aware of any exploits. The ISC has addressed these vulnerabilities in versions 3.0pl2 and 3.0.1RC11 of ISC DHCPD. More information may be found on the ISC Website:
http://www.isc.org/

*Category 24.4* *TCP/IP & HTTP*

2003-07-16 **MS03-026 buffer overrun RPC remote procedure call interface code execution DCOM 135 changing viewing deleting data installing programs unauthorized**

NIPC/DHS

July 16, Microsoft — Microsoft Security Bulletin MS03-026: Buffer Overrun In RPC Interface Could Allow Code Execution. Remote Procedure Call (RPC) is a protocol used by the Windows operating system which provides an inter-process communication mechanism that allows a program running on one computer to seamlessly execute code on a remote system. There is a vulnerability in the part of RPC that deals with message exchange over TCP/IP which results because of incorrect handling of malformed messages. This vulnerability affects a Distributed Component Object Model (DCOM) interface with RPC, which listens on TCP/IP port 135. This interface handles DCOM object activation requests that are sent by client machines to the server. To exploit this vulnerability, an attacker would need to send a specially formed request to the remote computer on port 135. If successful, an attacker could then run code with Local System privileges on an affected system and then be able to take any action on the system, including installing programs, viewing changing or deleting data, or creating new accounts with full privileges. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that system administrators install the patch immediately.

*Category 24.4* *TCP/IP & HTTP*

2003-07-17 **flaw vulnerability Windows Cisco Microsoft routers**

NewsScan

YESTERDAY A MICROSOFT FLAW, TODAY A CISCO FLAW
Cisco, which makes communications routers and switches, has found a flaw in its software that could be used by network vandals to cause widespread outages; the company has released a free patch to fix the flaw in its Internetworking Operating System. No vandals have exploited the vulnerability up to this point, and Cisco says: "We literally have people working around the clock right now to get this situation taken care of." According to the company, the vulnerability could only be exploited by sending a "rare sequence" of data packets to a device running IOS, the equivalent of Windows for routers and switches.
(AP/San Jose Mercury News 17 Jul 2003)

*Category 24.4* *TCP/IP & HTTP*

2003-09-03 **MS03-034 NetBIOS information Disclosure BNBS NetBT Name Service UDP port 137 Internet Browser query**

NIPC/DHS

September 03, Microsoft — Microsoft Security Bulletin MS03-034: Flaw in NetBIOS Could Lead to Information Disclosure. Under certain conditions, the response to a NetBT Name Service (NBNS) query may, in addition to the typical reply, contain random data from the target system's memory. This data could, for example, be a segment of HTML if the user on the target system was using an Internet browser, or it could contain other types of data that exist in memory at the time that the target system responds to the NBNS query. An attacker could seek to exploit this vulnerability by sending a NBNS query to the target system and then examine the response to see if it included any random data from that system's memory. If best security practices have been followed and port 137 UDP has been blocked at the firewall, Internet based attacks would not be possible. Microsoft has assigned a risk rating of "Low" to this vulnerability and a patch is available on the Microsoft website.

*Category 24.4* *TCP/IP & HTTP*

2003-12-11 **Internet Protocol IPv6 security implementation IPSec**

NIPC/DHS

December 10, Government Computer News — IPv6 will need security, too, experts warn. Security has been one of the selling points for the new Internet protocol, but IPv6 is not inherently secure, say those planning its implementation. The Internet Engineering Task Force is still working on IPv6 security elements and "many of them need to be tested in the real world," security consultant Richard Graveman said Wednesday, December 10, at the U.S. IPv6 Summit in Arlington, VA. One of the key security elements in IPv6 is IPSec encryption, which is mandatory in the new protocol. But security is more than IPSec, Graveman said. "Downloading an encrypted virus and installing it is just as bad as downloading an unencrypted virus," he said. Good encryption will not stop hackers either, he said. "You don't break good crypto, you go around it," he said, so proper implementation of IPv6 and a secure platform still are key to securing networks. Latief Ladid, president of the IPv6 Forum, said warned that hackers already are studying the new protocols and are uncovering security flaws.

*Category 24.4* *TCP/IP & HTTP*

2003-12-11 **Moonv6 Internet Protocol IPv6 security testing network**

NIPC/DHS

December 09, Government Computer News — Moonv6 testing to continue. Initial ten-day testing in October on the nation's largest native IPv6 network by the Department of Defense (DoD) and the University of New Hampshire demonstrated IPv6 linkage of academic and military sites from New Hampshire to San Diego. Time was short, and there was a dearth of applications written for the new Internet Protocol. "We had a limited number of vendor implementations to work with," said Ben Schultz, managing engineer of the University of New Hampshire's interoperability laboratory. Opportunities to test security also were limited, he said Tuesday, December 9, at the U.S. IPv6 Summit in Arlington, VA. Under those constraints, the File Transfer Protocol, Hypertext Transfer Protocol, Secure HTTP, Telnet and Domain Name System applications worked, Schultz said. The Moonv6 test bed is a collaboration by JITC, the university lab and the North American IPv6 Task Force. The second phase of testing, scheduled to run from February 2 to April 14, will dig deeper into security, mobility and routing protocol testing, as well as network stability and management, JITC's Major Roswell Dixon said.

# 24.5 LAN OS

*Category 24.5* *LAN OS*

2003-01-09 **protocol vulnerability note CERT IEE 802.3 Ethernet information leakage**

NIPC/DHS

January 06, CERT/CC — CERT Vulnerability Note VU#412115: "Network device drivers reuse old frame buffer data to pad packets". The Ethernet standard (IEEE 802.3) specifies a minimum data field size of 46 bytes. If a higher layer protocol such as IP provides packet data that is smaller than 46 bytes, the device driver must fill the remainder of the data field with a "pad". For IP datagrams, RFC1042 specifies that "the data field should be padded (with octets of zero) to meet the IEEE 802 minimum frame size requirements." Researchers from @stake Inc., a digital security company in Cambridge, Mass, have discovered that, contrary to the recommendations of RFC1042, many Ethernet device drivers fail to pad frames with null bytes. Instead, these device drivers reuse previously transmitted frame data to pad frames smaller than 46 bytes. This constitutes an information leakage vulnerability that may allow remote attackers to harvest potentially sensitive information. Depending upon the implementation of an affected device driver, the leaked information may originate from dynamic kernel memory, from static system memory allocated to the device driver, or from a hardware buffer located on the network interface card.

*Category 24.5* *LAN OS*

2003-06-13 **windows 2003 server third-party device drivers TCP transmissions Chris Taget NGS data leakage**

NIPC/DHS

June 13, vnunet — Flaws expose Win Server 2003. Several third-party device drivers that ship with Windows Server 2003 contain a vulnerability that causes them to leak potentially sensitive data during TCP transmissions. Security experts have criticized many of the vendors for failing to act quickly enough to guide users to fixes, and warned that the flaw could lead to attacks through local area networks (LANS). The so-called Etherleak flaw, first identified in January, occurs when messages transmitted between two machines are padded with arbitrary data in order to bring their byte size in line with the accepted standard. Chris Taget of security consultancy NGS Software warned that the vulnerability could be extremely serious and suggested that "IT directors should find out whether their vendors have updated the driver to resolve the issue."

# 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-01-09 **wireless Internet LAN networking WiFi Denver airport tested secured**

NIPC/DHS

January 06, Computerworld — American Airlines secures wireless LANs in Denver. Last January it was discovered that the wireless local area networks (LANs) American Airlines Inc. had been operating at their Denver International Airport (DIA) terminal were highly vulnerable to hackers. White Hat Technologies Inc., a Colorado-based security firm, found they had been operating without any encryption and had even pasted the IP addresses of curbside terminals on the monitors. A test at DIA on December 20 by White Hat was unable to detect a single airline wireless network operating without encryption protection, said Thubten Comerford, CEO of White Hat. In addition, American had not only removed the IP addresses from its OneStop self-service kiosks, but it had also added Cisco Systems Inc.'s Lightweight Extensible Authentication Protocol (LEAP) authentication technology on top of the standard 40-bit Wired Equivalent Privacy (WEP) encryption. LEAP is an authentication algorithm that leverages the 802.1x framework and provides dynamic, per-user WEP keys to protect data in transit. On the downside, Comerford said the recent test of the DIA facility still managed to pick up a suspected rogue access point (AP), as well as a significant number of vulnerable wireless transmissions emanating from public traveler lounges and frequent-flier clubs throughout the airport. "The biggest danger at DIA is the sniffing of sensitive information being transmitted by travelers. Few, if any, airports have addressed this security vulnerability, [and] few airports or airlines warn travelers of the danger of using the wireless networks," Comerford said.

---

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-01-15 **wireless WiFi technology security implications concerns**

NIPC/DHS

January 14, Government Computer News — Spread of handheld devices raises security questions. Wireless security is a major concern for agencies that deal with ever-more tech-savvy employees bringing to work handheld devices that don't mesh with federal security guidelines, said CDW Government Inc. president James R. Shanks. As agencies are working to bolster network security, the proliferation of wireless devices is raising new security challenges, said Shanks. The potential mobilization of military troops for a war with Iraq is "adding fuel to the fire," Shanks said. Meanwhile, agencies also are working to merge a vast range of applications for use on wireless devices and figure out how to manage the applications from central servers. Some companies that develop wireless software have met with standards writers to better align their products to meet federal and commercial security needs, said Larry S. Kirsch, senior vice president of CDWG. And a few companies have begun to pitch products that inventory and update network administrators when any user taps into the server via a wireless device.

---

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-01-15 **cellular mobile telephone Wi-Fi networks**

NewsScan

COMPANIES SEEK TO LINK CELLULAR, WI-FI NETWORKS
A triad comprising Avaya, Proxim and Motorola is developing a mobile device capable of roaming between cell phone networks and Wi-Fi hotspots. "Our vision is to connect the various spaces, be they public hotspots, private hotspots or office networks," says Motorola official Bo Pyskir. Wi-Fi networks have a range of about 300 feet and offer transmission rates of up to 11mbps, while cellular networks cover enormous distances, but crawl at less than 56kbps when sending data like e-mail or Web pages. The effort currently underway at the three companies includes development of a Motorola phone that uses both Wi-Fi and cell phone networks, networking equipment and software from Avaya, and a new kind of Wi-Fi access point from Proxim. Early trials of prototypes are expected to start sometime in the second half of this year, with a commercial release in about 12 to 18 months. (CNet News.com 14 Jan 2003)
http://news.com.com/2100-1033-980582.html

---

*Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-01-29 **wireless Bluetooth cellular mobile telephones**

NewsScan

HYPERTAG SYSTEM LINKS CELL PHONES TO BILLBOARD ADS
Hypertag, based in Cambridge, England, has developed cheap, smart tags that can beam Web site links to mobile phones, giving passersby additional information about the poster, billboard or shop to which the tag is attached — for instance, links could lead to descriptions of historic monuments or exhibits in a museum, or contact information for products advertised on an outdoor kiosk. Hypertag CEO Jonathan Morgan says 40% of modern cell phones can already accept information sent via infrared technology, and added that his company was also working on a Bluetooth version , which would transfer data via short-range radio link. Many wireless firms see location-based information services as a potentially lucrative revenue stream, but the technological limitations of such systems are still being overcome. "The granularity of GPS and cell-ID is rather large," says Morgan, "and you have to have a lot of infrastructure behind it to make it work." By contrast, the Hypertag system is cheap to use ("It is just like using a remote control on the TV," says Morgan) and the tags can be attached to ads adjacent to each other without muddling the data streams. (BBC News 26 Jan 2003)
http://news.bbc.co.uk/1/hi/technology/2687179.stm

---

*Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-02-27 **Wi-Fi wireless networks consumer hotels**

NewsScan

MARRIOTT, INTEL CUT DEAL FOR WI-FI ACCESS IN HOTELS
Marriott International and Intel are launching a joint marketing campaign to promote the availability of Wi-Fi access at 400 Marriott, Renaissance, Courtyard, Residence Inn and other hotels. "Customers are making decisions about where they stay based on where this technology is available," says Lou Paladeau, Marriott VP in charge of technology development. "If you don't have it, you're not getting them in the door." Wi-Fi hotspots will be located in lobbies, meeting rooms, and other public spaces. Guests will pay $2.95 for the first 15 minutes of service, and 25 cents a minute thereafter. Marriott estimates that 10% of its guests have Wi-Fi capability. About 19% of laptops sold last year came with Wi-Fi circuitry included, according to IDC, which estimates that percentage will grow to 91% by 2005. (Wall Street Journal 27 Feb 2003)

---

*Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-03-03 **Department Homeland Security DHS wireless security ISAC analysis**

NIPC/DHS

February 28, Government Computer News — Wireless security on DHS agenda. Four groups in the Information Sharing and Analysis Center (ISAC) for the information and communications sectors, a public-private security forum, are meeting to evaluate commercial wireless security. The Cellular Telecommunications Industry Association (CTIA), Telecommunications Industry Association, Information Technology Association of America, and United States Telecom Association, have begun meeting with the National Infrastructure Simulation and Analysis Center and other Energy organizations, said Kathryn Condello, vice president of operations for CTIA. The ISAC currently has no industrywide way to review security gaps in the networks and services of wireless carriers. But that's just what the Department of Homeland Security will likely need to know to toughen security as more government employees adopt mobile devices and agencies integrate wireless platforms into their programs. Individual companies "know what their problems are," said Condello, who spoke yesterday on a panel about asset security at the Armed Forces Communications and Electronics Association's homeland security conference. But expanding individual assessments to a competitive telecom market with a half-dozen major carriers, each operating its own distinct network elements, is "really tough," Condello said. "That's a lot of data points."

---

*Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-03-11 **WiFi wireless ISP Internet service provider**

NewsScan

MCDONALD'S JUMPS ON WI-FI BANDWAGON
McDonald's announced ten stores in Manhattan will begin offering one hour of Wi-Fi high-speed Internet access to anyone who buys a combination meal, and plans to extend the program to 300 McDonald's restaurants in New York, Chicago and a yet-unannounced California town. "You can come in and have an extra value meal and send some e-mail," says a McDonald's spokeswoman. McDonald's joins more than 400 Borders bookstores, hundreds of hotels and a couple of U.S. airports where Wi-Fi access will be available by summer. (AP 11 Mar 2003)

---

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-03-13 **Wi-Fi wireless ISP Internet service provider**

NewsScan

WI-FI SEAL OF APPROVAL
The Wi-Fi Alliance, a trade group whose members include a number of major technology companies (Cisco, Dell, Intel, etc.) is putting a Wi-Fi logo ("Wi-Fi" stands for wireless fidelity) at places where the network card of any kind of laptop will be able to connect reliably to the network. Wi-Fi Alliance board member Andrea Vocale, a Cisco executive, says: "The pervasiveness of Wi-Fi is what it's about. We want the experience to be the same, with one standard everywhere." The Wi-Fi Alliance's site is http://www.wifizone.org. (AP/San Jose Mercury News 13 Mar 2003)

---

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-03-17 **Wi-Fi ISP Internet service provider**

NewsScan

PAYPHONES SEEK NEW LIFE AS INTERNET TERMINALS
Bell Canada is in the midst of a pilot program that offers customers in Toronto, Montreal and Kingston free Wi-Fi Internet access through hotspots originating in 16 former payphone booths located in airports, hotels, libraries, train stations and other public transit locales. As with regular Wi-Fi access, customers must be within 100 feet of the booth to use the signal. Bell Canada spokesman Don Blair says the company has received positive feedback so far: "We've received phone calls and e-mails from people using the service. The are very positive responses from users, as well as a lot of calls from location providers — people wanting to offer (wireless Internet) hotspots to their customers." Meanwhile, in Singapore, InfiniTech has a different idea for resuscitating the payphone booth. The company is looking for U.S. partners to help roll out booths where people could recharge their cell phones when their batteries run down. Users would deposit coins and then recharge their phones.
(Wired.com 17 Mar 2003)
http://www.wired.com/news/wireless/0,1382,58050,00.html

---

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-03-27 **wireless Wi-Fi network communication infrastructure unguarded protection**

NIPC/DHS

March 26, Government Computer News — Wireless infrastructure goes unguarded. The national wireless infrastructure "is one of the most important and least protected parts" of U.S. communications capability, a technology strategist said today. David Porte, an executive with technology incubator Astrolabe Innovations of Cambridge, Mass., said the World Trade Center attacks on September 11, 2001, were a case in point. Porte spoke at a Newport, R.I., conference sponsored by the National High-Performance Computing and Communications Council. The trade center towers housed hubs for multiple types of communications, he said: broadcast, land-line telecommunications and cellular phones. Yet when the towers fell, "cell phones became the primary means of national security communications," Porte said. The result was widespread congestion with a ripple effect that ended in loss of many communications spokes, he said. Lack of wireless interoperability also interfered with government communication in that crisis. The wireline infrastructure, although the first to go down on September 11, "was the first to recover because of built-in redundancy," he said. Porte encouraged greater density of cells and wireless hubs, saying, "Government and industry need to get wireless ready for emergencies."

---

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-04-09 **802.16 Wi-Fi wireless technology vendor support**

NewsScan

NEW WIRELESS STANDARD BUILDS SUPPORT
A new wireless standard — 802.16 — is gaining support, with Intel, Proxim and Fujitsu announcing yesterday they'd joined an industry group called WiMax, which is charged with helping to certify equipment based on the new standard. Unlike the increasingly popular WiFi standard, which is generally limited to a 300-foot radius from the base station antenna, 802.16 technology has a range of more than 31 miles. That means it can be used to extend broadband access to rural and remote locations that currently aren't served. "We believe it's the next big thing in the wireless broadband arena," says Margaret LaBrecque, president of WiMax and an Intel manager. WiMax says its goal is to ensure that 802.16 equipment from different companies will be able to communicate with each other. Analysts expect products using 802.16 to be available during the second half of 2004 and carriers may introduce high-speed Internet service based on the standard in 2005. (Wall Street Journal 9 Apr 2003)

---

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-04-15 **UPS tracking multiple protocols networks**

NewsScan

UPS DEVICE CONNECTS SIX WAYS
United Parcel Service is giving its drivers new handheld devices that connect to six different wireless networks. The Delivery Information Acquisition Device (DIAD) connects via infrared, WiFi, Bluetooth, GPS, and two cell networks: CDMA1x and GSM/GPRS. "It reminded me of 'shock and awe,'" says telecom analyst Jeff Kagan. "There are just so many different kinds of weapons, tools and technologies." A UPS manager says the handheld's battery, which is about the same size as a typical laptop battery, has enough power to last through normal workday because a driver likely would use only two connections at a time — for instance, using Bluetooth to read a packing slip and then connecting to a cell phone network to send information back to UPS headquarters. (CNet News.com 15 Apr 2003)

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-04-28 **WiFi technology compete cellular wireless phone**

NewsScan

WHY WIFI WON'T COMPETE WITH CELLULAR ANYTIME SOON
Business Week columnist Andy Reinhardt says despite the recent buzz over WiFi technology, there are fundamental limitations that will restrict its ability to break into the voice communications market. "Just look at roaming. In the mobile world, a fantastically complex system of databases and electronic billing is completely hidden from consumers, whose handsets magically switch from one network to another as they move around. Not so for WiFi, where going online from an unfamiliar hot spot is no easy feat. WiFi will definitely siphon off some of the revenues the Bell-heads [traditional phone companies] want to score from mobile data. But as long as users have to fiddle with Internet protocol settings and quirky, unpredictable connections, WiFi will remain a niche occupied by the technoscenti." (Business Week Online 28 Apr 2003)

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-05-08 **Wi-Fi security violators LAN hacker virus attacks Delaware Department Technology sniffer software**

NIPC/DHS

May 08, Washington Technology — State CIO hunts for Wi-Fi security violators. The new Delaware Department of Technology and Information has employed sniffer software to see whether state agencies have deployed wireless fidelity, or Wi-Fi, networks that meet state standards for such networks. Each month the department checks a different location for non-standard, or "illegal," use of a Wi-Fi local area network. During the course of one such check, the department discovered a serious violation, Delaware Chief Information Officer Tom Jarrett Jarrett said "I told the agency to cease and desist or in two days I would take them off the network." Because the agency was "running wide open" with Wi-Fi, they were putting the entire network community at risk from hacker and virus attacks, he said.

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-05-20 **GPS data stop wireless attacs Yi-Chi Hu Adrian Perrig Carnegie Mellon wormhole Ad-Hoc networks**

NIPC/DHS

May 20, New Scientist — GPS data could stop wireless network attacks. U.S. computer researchers Yi-Chin Hu and Adrian Perrig of Carnegie Mellon University, PA, and David Johnson at Rice University, TX have revealed that a "wormhole attack" could be used to knock a vulnerable network out of action or defeat a wireless authentication system. "Ad-hoc" wireless computer networks, which are used to extend the range of wireless LAN networks, and are used by the military and emergency services, could be severely disrupted using the technique. But the same researchers have also devised a radical scheme designed to counter it. The researchers propose defending networks against the attack by attaching identifying tags to each packet. They suggest tagging packets with GPS information or a timestamp based on a synchronized network clock. Both could be used to verify that a packet genuinely comes from another nearby node and not one intercepted much further away. The threat and countermeasure are outlined in the paper "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks" presented at the Twelfth World Wide Web conference in Bucharest, Romania.

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-06-18 **IEEE new wi-fi standard 802.11g**

NewsScan

IEEE RATIFIES NEW WI-FI STANDARD
The new 802.11g wireless standard, which has now been approved by the Institute of Electrical and Electronics Engineers (IEEE), is likely to prompt a new surge of interest in WiFi, the technology which uses a radio signal allowing laptops and other mobile devices to connect to the Internet through access points called "hot spots" located in cafes, airports, etc. The 802.11g standard will allow wireless transmission at speeds four to five times faster than the current standard, and make it possible to send bigger files (e.g., videos) and connect more computers to an access point. (Chicago Sun-Times 18 Jun 2003)

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-06-25 **wireless networking security school password protection**

NewsScan

[WIRELESS]...NEEDS TO BE WATCHED FOR SECURITY BREACHES
Using a laptop with a wireless card outside the main office of a Palo Alto, California school district, a reporter was able to gain access to such data as grades, home phone numbers and addresses, emergency medical information, student photos , and psychological evaluations. Unlike the majority of the district's information, the documents available on this wireless network were not password-protected. Superindent Mary Frances Callan says: "I don't see this as such a huge news story." The real story, says Callan, is the great progress represented by the network itself, which was made possible by new software purchases, employee training sessions, and technology-use policies. (Palo Alto Weekly 25 Jun 2003)

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-06-26 **pda corporate scheme end user Wi-Fi support bluetooth**

NewsScan

PDAs IN THE CORPORATE SCHEME OF THINGS
Handheld computers are in evidence everywhere in corporate America — yet they typically belong to individual employees rather than to the corporations that employ them. (Gartner Research analyst Todd Kort says that only 28% of all PDA's worldwide were purchased by businesses.) Microsoft is hoping that its new Windows Mobile software for the Pocket PC handheld operating system will bring that percentage up to a much higher level. Gartner's Kort says, "Most of the cool stuff is under the hood. The average end user isn't going to be immediately aware that any kind of major changes have taken place. What they're doing is a lot of things to satisfy IT managers." IT departments "don't want those support calls," so Microsoft has created a new configuration manager for automatically detecting and connecting to Wi-Fi and Bluetooth networks and allowing users to connect wirelessly without having to deal with any complicated configurations or setups — and without having to ask for help. (Information Week 26 Jun 2003)

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-07-02 **Cisco Systems Aironet flaw access point wireless Vigilante 1100 wi-fi 300 foot radius zone computer network**

NIPC/DHS

July 28, CNET News — Cisco releases fix for Aironet flaw. Cisco Systems has patches for a pair of security flaws that were discovered in its Aironet 1100 access points. One flaw would have allowed an attacker to use a "classical brute technique to discover account names, according to security troubleshooter Vigilante. said the second flaw could freeze the access point and bring down the wireless access Cisco posted advisories on the flaws Monday, July 28. "To date, Cisco is not aware active exploitations of the vulnerability," a Cisco representative said in a statement. Cisco Aironet 1100 Wi-Fi access point creates a 300-foot radius zone where laptops wirelessly connect to the Web or a corporate computer network. Additional information available on the Vigilante Website:
http://www.vigilante.com/inetsecurity/advisories/VIGILANTE-2 003002.htm

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-07-03 **Wi-Fi encryption eavesdropping AirDefense POP e-mail passwords**

NIPC/DHS

July 03, SecurityFocus — Study: Wi-Fi users still don't encrypt. Two days of electronic eavesdropping at the 802.11 Planet Expo in Boston last week sniffed out more evidence that most Wi-Fi users still aren't getting the message. Security vendor AirDefense set up two of its commercial "AirDefense Guard" sensors at opposite corners of the exhibit hall at the Boston World Trade Center, the site of the conference. The company provided attendees with ample notice of the study. "There were huge signs throughout the place saying AirDefense is monitoring all conference traffic." They found that users checking their e-mail through unencrypted POP connections vastly outnumbered those using a VPN or another encrypted tunnel. Only three percent of e-mail downloads were encrypted on the first day of the conference, 12 percent on the second day. That means the other 88% could easily be intercepted by eavesdroppers using commonly-available tools, compromising both the e-mail and the user's passwords.

---

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-07-31 **Sony Playstation wireless LAN**

NewsScan

SONY'S GAME PLAN
Sony's new handheld PlayStation console will come with wireless capability that allows gamers in close proximity to play together and download game characters. "We will be using some challenging technologies," including wireless LAN (local area network), says Sony Computer Entertainment president Ken Kutaragi. "The PSP is a product with huge potential, following the PlayStation and PlayStation 2. The video game market may change in a big way." The new device, set to debut in the fourth quarter of 2004, will process data at blazing speeds 10 times faster than the original PlayStation console. PSP games will come in the form of high-capacity optical discs created especially for the new device, and the PSP will also be able to play movies and music. The move pits Sony directly against Nintendo, which produces the market-leading GameBoy Advance device. (Reuters/CNet 30 Jul 2003)

---

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-08-29 **Wi-Fi ship short transmission radio satellite Internet**

NewsScan

SHIP-TO-SHORE WI-FI
For years, mariners have been reliant on pricey maritime radio and satellite services for connectivity afloat, but Wheat Wireless Services of Reston, Virginia is now selling a tweaked version of Wi-Fi Internet access that is functional up to 30 miles offshore. The boat receiver is a 4-foot antenna, and the Wi-Fi service piggybacks off T1 lines in data centers along the coast beamed from radio towers up to 300 feet tall perched atop coastal structures. The service isn't cheap — it costs $7,500 for installation and another $500 a month for unlimited Internet access — but that's pocket change for wealthy yacht owners and cruise lines, says In-Stat/MDR analyst Daryl Schooler. "Basically, they're delivering more than a T1 worth of bandwidth to people. Satellite is slower than that and could be tens of thousands of dollars a month." Two casino ships have signed up for Wheat's service, but not to provide their passengers with Internet access. "They want people to gamble," says Wheat CEO Forrest Wheat. "They don't want them to surf the Internet. (The Internet service) is for the crew." (Wired.com 29 Aug 2003)

---

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-11-07 **wireless Wi-Fi security protocol vulnerability**

NIPC/DHS

November 06, InternetNews.com — Weakness found in Wi-Fi security protocol. Wireless security expert Robert Moskowitz has detected a glaring weakness in the interface design of a Wi-Fi Protected Access (WPA) protocol deployed in numerous Wireless LAN products. According to a research paper written by Moskowitz, the weakness could allow intruders to crack poorly chosen passphrases via offline dictionary attacks. The paper means that Wi-Fi hardware products that ship with WPA might be less secure than the older Wireless Encryption Protocol (WEP), which it replaced in 2002. The WPA standard was designed to improve upon the security features in wireless networks. The weakness only takes effect when short, text-based keys are used and does not reflect a fault in the WPA protocol. The weakness can be avoided if WLAN hardware manufacturers build units with the ability to generate random keys that can be copied and pasted across systems. Manufacturers can also restrict the ability to enter weak keys by requiring passphrases with numerous characters instead of words that can be found in the dictionary. Moskowitz warned that dictionary based programs used to crack passwords are heavily used by criminal hackers. The paper is available online:
http://wifinetnews.com/archives/002452.html

---

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-12-05 **Cisco Systems wirelss LAN security alert Wi-Fi SNMP vulnerability**

NIPC/DHS

December 04, VNUNet (UK) — Cisco issues wireless Lan security alert. Cisco has warned firms using its Aironet access points running Cisco IOS operating software of a security flaw that allows hackers to gain full access to wireless networks. The vulnerability allows hackers to steal Wired Equivalent Privacy (Wep) encryption keys. The issue arises if the wireless Lan device's 'SNMP-server enable traps wlan-wep' command is enabled. "Under these circumstances, an adversary will be able to intercept all static Wep keys," Cisco said in a statement. If the command is switched on, which Cisco stressed is disabled by default, the access point will broadcast any network static Wep keys in cleartext to the SNMP server every time a key is changed or access points rebooted. Affected hardware models are the Cisco Aironet 1100, 1200 and 1400 series. Cisco has posted a workaround advising companies with deployments of these devices to disable this command, adding that any dynamically set Wep key will not be disclosed. The problem only applies to wireless Lan kit running its IOS software, so Aironet access point models running VxWorks are not affected. Customers are advised to upgrade their IOS version to a patched system. Cisco's advisory and workaround are available here:
http://www.cisco.com/warp/public/707/cisco-sa-20031202-SNMP- trap.shtml

---

*Category 24.6* *WAP, WEP, Wi-Fi, Bluetooth, 802.11*

2003-12-19 **wireless Internet test Rutgers WINLAB NSF**

NIPC/DHS

December 17, Rutgers University — Rutgers area to become test track for wireless Internet. The Wireless Information Network Laboratory (WINLAB) at Rutgers, The State University of New Jersey, has won a $5.45 million, four-year grant from the National Science Foundation (NSF) to construct and operate a facility for researchers around the nation to test the next generation of wireless and mobile networks. This wireless networking test bed will include both a large-scale "radio grid emulator" laboratory and a "field trial" system in and around the Rutgers campus and nearby Central New Jersey communities. The project is called the Open Access Research Testbed for Next-Generation Wireless Networks. Rutgers is managing the project in collaboration with Columbia University, Princeton University, Lucent Bell Labs, IBM Research, and Thomson Inc. The two-tiered project will include a new wireless system emulation laboratory to be headquartered at the Technology Centre of New Jersey. An indoor radio grid of about 625 stationary and mobile nodes will give researchers throughout the country remote access for testing of future network concepts under a variety of computer-generated topologies and radio conditions. The field test network will include about 50 nodes running a configurable mix of third generation high-speed cellular, along with wi-fi wireless access.

---

# 24.8 MAC OS

*Category 24.8* *MAC OS*

2003-10-29 **Macintosh Operating System X @Stake systemic flaws buffer overflow exploitable Apple patches released**

NIPC/DHS

October 29, ZDNet Australia — Three flaws discovered in Mac OS X. Security-research company @Stake has warned of three vulnerabilities affecting the Mac OS X operating system. The first details "systemic" flaws in the way OS X handles file and directory permissions, while the second details a kernel level vulnerability that does not affect default installations of the operating system. The third involves a buffer overflow condition that may be remotely exploitable. Apple has not yet released patches for the security issues. Mac users are advised to upgrade to the latest Apple operating system, which is not vulnerable to the flaws, for a fee. The full advisories are available online:
http://www.atstake.com/research/advisories/2003/

*Category 24.8* *MAC OS*

2003-10-31 **Apple Powerbook LCD white spots unexplained**

NewsScan

WHITE SPOTS ON POWERBOOK SCREENS
The new 15-inch-screen PowerBooks have unexplained white blotches showing up on the LCD screens. Some customers say they sent their laptops in for repair, only to see the spots reappear when the systems came back. A statement from Apple says: "The new 15-inch PowerBook has been a big hit with customers since its introduction last month. However, some customers are reporting the appearance of faint, white spots on their displays after using the system for a short period of time, and Apple is investigating these reports right now. Any customers experiencing this problem should contact AppleCare." (San Jose Mercury News 31 Oct 2003)

*Category 24.8* *MAC OS*

2003-11-24 **Apple OS X security patch vulnerability exploit fix Jaguar**

NIPC/DHS

November 20, Macworld.co.uk — Apple releases security patches. Apple Computer Inc. has released security updates for Mac OS X Panther 10.3.1 client and server systems and Mac OS X Jaguar 10.2.8 client and server operating systems. The Panther update includes the following updated components: OpenSSLzlib "gzprintf()" function, an update to the open-source lossless compression library used by Darwin, the kernel of Apple's OS. The Jaguar update improves a number of components, including document formatting system, groff; Unix macro processor component, gm4; and Mail w/CRAM-MD5 authentication (used to debug common authentication services). It also improves OpenSSL (a robust, commercial-grade, full-featured, and open-source toolkit with a general-purpose cryptography library that implements the Secure Sockets Layer); Personal File Sharing; QuickTime for Java; and the zlib "gzprintf()" function. Both updates are available for download from Apple's Website:
http://www.info.apple.com/support/downloads.html

*Category 24.8* *MAC OS*

2003-12-24 **patch fix flaw vulnerability Apple Mac OS X DHCP Jaguar buffer overflow**

NIPC/DHS

December 22, CNET News.com — Apple issues patch for Mac OS X hole. Apple Computer has issued a security update that, among other fixes, closes a hole in Mac OS X that could have allowed hackers to take control of a computer under particular circumstances. The patch essentially changes the default settings for connecting to a Dynamic Host Communication Protocol (DHCP) server on Mac OS X 10.2.8. (aka "Jaguar"), Mac OS X 10.3.2 (aka "Panther") and the corresponding server versions of these operating systems. A DHCP server assigns a TCP/IP address to a computer and, under the earlier default settings, a Mac running one of the above-listed OSes would accept data from DHCP servers found on a local area network. If a hacker inserted a malicious DHCP server on a local network, he or she could then exploit Apple's earlier default setting to embed malicious software on a computer or use the computer as a drone for coordinated attacks on other systems. Apple's security update also fixes a buffer overflow vulnerability in a file system, plugs another vulnerability in Panther that could cause denial-of-service requests and in general improves the security features of the affected OSes. Additional information available on Apple's Website:
http://docs.info.apple.com/article.html?artnum=61798

# 24.9 Peer-to-peer networking

*Category 24.9 Peer-to-peer networking*

2003-03-29 **US military peer-to-peer P2P technology battlefield Iraq**

NewsScan

P2P GOES TO WAR
The U.S. military is using peer-to-peer technology to plan battlefield operations in Iraq and coordinate humanitarian aid to that country. Microsoft's NetMeeting software and programs from Groove Networks and Appian Corp. are part of the Defense Department's shift away from massive central computer servers toward more flexible systems that enable users to work on joint projects and share information. For instance, commanders in the Persian Gulf use collaboration software to chart their progress, drawing on one another's maps during videoconferences several times a day, says J.P. Angelone, who heads the enterprise capabilities center at the Defense Information Systems Agency. One advantage is that data are kept on individuals' computers — when a participant disconnects from the network, he can keep working on his personal version of the material. Logging in again automatically sends the updated material to other participants. "It's helpful because you reduce the physical distance to connect. If you've got a command or a tactical unit in the area of responsibility, there's no sense coming all the way back to tap into a server," says Angelone. The Defense Information Systems Agency has installed basic collaboration tools at more than 63 sites worldwide, and the trend toward P2P use likely will continue because such systems are more resistant to attack and can be faster and easier to use than traditional, server-based systems. (Los Angeles Times 29 Mar 2003)

---

*Category 24.9 Peer-to-peer networking*

2003-06-01 **Altnet KaZaA peer-to-peer p2p users networking authorized sharing awards**

NewsScan

ALTNET AND KAZAA PUSH LEGIT P2P NETWORK
Sharman Networks' Kazaa and Brilliant Digital Entertainment's Altnet are teaming up to launch a new phase of peer-to-peer networking, harnessing the capacity of tens of millions PCs to swap authorized copies of games, songs and movies. Giving people an incentive to trade in legitimate files could create a powerful new business model for the entertainment industry and reduce file-swapping networks' role as hubs of online piracy, says Altnet CEO Kevin Bermeister. "The minute you begin shifting unauthorized files out of people's shared folders, the peer-to-peer networks (as sources of copyright infringement) begin to disappear. Lawsuits are the stick approach. This is the carrot." Customers who sign up for the new service will agree to install high-security file-swapping software and host files that are authorized for distribution through the network. "Peer Points" will be awarded each time someone uploads a file, with the points redeemable for a variety of bonuses ranging from free access to paid content to sweepstakes entries for big-ticket items such as cars or cash. The new Altnet service and a revamped version of the regular Kazaa file-swapping software are expected to be released in test form later this week. (CNet News.com 1 Jun 2003)

---

*Category 24.9 Peer-to-peer networking*

2003-10-10 **P2P peer-to-peer networking Simson Garfinkel MIT technology copyright infringement**

NewsScan

P2P: SALVATION OR SCOURGE?
Internet gadgeteer and author Simson Garfinkel says peer-to-peer technology may have gained a bad name in recent years, but it could solve many of the current Internet's traffic congestion and security problems. "Peer-to-peer could overcome many of the fundamental problems that are facing the Internet today — problems of centralized control, vulnerable servers, and the difficulty that most organizations have scaling. On the other hand, peer-to-peer could also make the Internet's security problems worse, by allowing hackers to create large-scale attack networks. Peer-to-peer could be a boon for the artists and the recording industry, giving them a way of publicizing and distributing their intellectual property for far less than they do now. Yet better peer-to-peer systems could further hurt the recording companies — and not just through copyright violations... The real threat that peer-to-peer poses to the record labels is that it could make them obsolete. At the end of the day, peer-to-peer technology is about increasing the reliability and the redundancy of Internet-based systems. That's why the recording industry is afraid of it — because peer-to-peer can be used to create networks that the industry can't shut down. But peer-to-peer can also be used to create networks that earthquakes, wars and terrorists can't shut down. Ultimately, I think that we're better off trying to strengthen the Internet rather than trying to make it weaker." (MIT Technology Review/Wall Street Journal 10 Oct 2003)

---

*Category 24.9 Peer-to-peer networking*

2003-12-09 **hackers pirates theft Trojan horses peer-to-peer P2P Kazaa**

NIPC/DHS

December 08, New York Times — Hackers steal from pirates, to no good end. Rogue programs known as "Trojan horses" are used by hackers to mask their identities by using unwitting people's computers as relay stations. It had been assumed that investigators could ultimately shut down a system by identifying the server computer used as the initial launching pad. But computer expert Joe Stewart has said that a program called Backdoor.Sinit uses the commandeered machines to form a peer-to-peer network like the Kazaa program used to trade music files. Each machine on the network can share resources and provide information to the others without being controlled by a central server machine. When there is no central machine, "these tactics make it impossible to shut down," he said. Rings of infected computers have been used to send spam, present online advertisements for pornographic Websites, or trick people into giving up information like credit card numbers. "Sinit appears to have been created as a money-making endeavor," Stewart said. "This Trojan is also further evidence that money, not notoriety, is now the major driving force behind the spread of malware these days." On Websites frequented by hackers, spammers and people who identify themselves as practitioners of credit card fraud, the remote-access networks, or "radmins," are offered openly.

# 24.A Secure processors

*Category 24.A* *Secure processors*

2003-10-11 **laptop crash protection IBM ThinkPad freefall crash chip**

NewsScan

IBM TOUTS LAPTOP CRASH PROTECTION
Two of IBM's new ThinkPad laptop models come with a chip designed to detect when a laptop is in freefall (if it's been knocked off a table for instance), and automatically stops the hard drive from reading or writing data — activities that IBM says make it especially vulnerable to crashing completely. The crash chips are included in the ThinkPad R50 and T41 models, which start at $1,529 and $1,649 respectively. (AP 11 Oct 2003)

# 25.1 Remote control, RATs, reprogramming, auto-updates

*Category 25.1* *Remote control, RATs, reprogramming, auto-updates*

2003-03-10 **Windows root kit remote administration back door penetration stealth exploit**

NIPC/DHS

March 05, SecurityFocus — Windows root kits a stealthy threat. A Windows root kit called "ierk8243.sys" was discovered on the network of Ontario University last January. It has since been dubbed "Slanret", "IERK," and "Backdoor-ALI." A root kit is an assembly of programs that subverts the Windows operating system at the lowest levels, and, once in place, cannot be detected by conventional means. Also known as "kernel mode Trojans," root kits are far more sophisticated than the usual batch of Windows backdoor programs. Greg Hoglund, a California computer security consultant, believes intruders have been using Windows root kits covertly for years. He says the paucity of kits captured in the wild is a reflection of their effectiveness — not slow adoption by hackers. Once Slanret is installed on a hacked machine, anti-virus software won't pick it up in a normal disk scan. That said, the program is not an exploit — intruders have to gain access to the computer through some other means before planting the program. Despite their increasingly sophisticated design, the current crop of Windows root kits are generally not completely undetectable, and Slanret is no exception. Because it relies on a device driver, booting in "safe mode" will disable its cloaking mechanism, rendering its files visible. And in what appears to be an oversight by the kit's author, the device driver "ierk8243.sys" is visible on the list of installed drivers under Windows 2000 and XP, according to anti-virus company Symantec Security Response. Hoglund says future Windows root kits won't suffer from Slanret's limitations. And while he says the risk can be reduced with smart security policies — accept only digitally-signed device drivers, for one — ultimately, he worries the technique may find its way into self-propagating malicious code.

# 25.2 Jamming

*Category 25.2* *Jamming*

2003-09-11 **jamming phone cameras iceberg systems safe have technology picture cell picture imaging capabilities**

NewsScan

TECHNOLOGY JAMS CELL PHONE CAMERAS
A new product from Iceberg Systems, dubbed Safe Haven, is designed to block a camera cell phone's ability to snap pictures. The imaging system is then reactivated when the cell phone leaves the Safe Haven-protected area. The product uses hardware transmitters with a small piece of control software loaded into a camera phone handset to disable the imaging capability, and Iceberg Systems managing director Patrick Snow says his company is in talks with handset manufacturers interested in testing the technology. Safe Haven could prove popular with businesses that operate secure sites — Samsung and LG Electronics have already barred employees from using camera phones in research and manufacturing facilities for fear sensitive data could be stolen. Snow says the system could also be tweaked to eliminate other annoying cell phone intrusions, such as loud ringtones in a theater or text-messaging in school. Meanwhile, analysts predict there will be some 1 billion camera phones in use within five years. (CNet News.com 11 Sep 2003)

# 25.3 RFI, HERF, EMP/T

*Category 25.3* *RFI, HERF, EMP/T*

2003-02-04 **Wi-Fi wireless radio-frequency interference RFI radio frequency interference jamming radar military national security spectrum**

NewsScan

PENTAGON AND INDUSTRY IN TUG-OF-WAR OVER RADIO SPECTRUM
The U.S. Defense Department, citing national security reasons, is seeking new limits on wireless Internet technology such as the Wi-Fi systems increasingly found in airports, homes and offices, and places like Starbucks. The Pentagon says that the low-power radio emissions may jam as many as ten types of military radar systems. Industry powerhouses such as Intel and Microsoft insist, however, that military and civilian uses of wireless communications technology can coexist peacefully, and that in Europe there are smart wireless Internet devices that can sense the nearby use of military radar and automatically yield the right of way. Wireless industry executive Rich Redelfs of Atheros says: "The idea is to get the world on a single page, and Europe is way ahead of the U.S. in understanding these interference issues." However, Defense Department officials consider the technology unproven and want the Federal Communications Commission to delay releasing for civilian use additional radio frequencies in the 5-gigahertz range. (New York Times 17 Dec 2002)

PACT PREVENTS WIRELESS INTERFERENCE WITH MILITARY CHANNELS
The U.S. Defense Department and a group of high-tech manufacturers have struck a deal aimed at preventing future interference with military radar from next-generation wireless devices. Under the compromise, wireless device makers will build in technology to detect and actively avoid military radars that operate on similar frequencies. In return, Defense officials will support proposals to nearly double the amount of wireless spectrum available, particularly that used for "Wi-Fi" computing. Ed Thomas, chief engineer for the Federal Communications Commission, called the pact "good for the Department of Defense and good for the industry." (Wired.com 3 Feb 2003)
http://www.wired.com/news/wireless/0,1382,57528,00.html

*Category 25.3* *RFI, HERF, EMP/T*

2003-08-27 **RSA RFID block information collection tags**

NewsScan

RSA SECURITY's PLANS FOR RFID BLOCKING TECHNOLOGY
RSA Security has developed a blocking technique that disrupts the transmission of information contained in RFID tags and prohibits data collection. The technique is still in the drawing board stage, but the company plans to make prototype chips and see if any manufacturing groups are interested in making the processors, according to chief RSA researcher Ari Juels. Juels says the RSA technology would enable the RFID tags to be used, but that the blocking feature would allay the privacy concerns that have derailed recent deployment plans. "This is not meant to be a hostile tool. It balances consumer privacy and retail use in a profitable way. Tags are too useful to completely disable them." (CNet News.com 27 Aug 2003)

# 26.1 Radiation

*Category 26.1* *Radiation*

2003-09-30 **3G wireless signals sick headache nausea**

NewsScan

3G WIRELESS SIGNALS COULD MAKE YOU SICK
Radio signals used for next-generation (3G) wireless services can cause headaches and nausea, according to a study conducted on behalf of the Netherlands ministries for Economic Affairs, Health and Telecommunications. The study compared the impact of radiation from base stations used for current wireless services with those for new 3G networks, which transfer data at a faster rate. "If the test group was exposed to third-generation base station signals there was a significant impact. They felt tingling sensations, got headaches and felt nauseous," says a spokeswoman for the Dutch Economics Ministry. The Dutch government said follow-up research was needed. Previous research on health effects of mobile phones, primarily second-generation, has been inconclusive, but a long-term study conducted by the International Agency on Research on Cancer is expected to yield results next year. (Reuters 30 Sep 2003)

# 26.2 Toxic materials

*Category 26.2 Toxic materials*

2003-01-10 **recycling toxic materials**

NewsScan

U.S. TECH COMPANIES RANK LOW IN RECYCLING EFFORTS
The Silicon Valley Toxics Coalition (SVTC) has released its annual Computer Report Card comparing the environmental records of 28 high-tech firms, and reports that most U.S. companies lag behind their Japanese competitors when it comes to recycling equipment and safe disposal of hazardous substances used in the manufacturing process. Of the companies surveyed, only Fujitsu received a passing grade. It's one of a handful of Japanese companies that has sought to eliminate toxic chemicals by developing and using lead-free products. "The leadership continues to be by and large the Japanese companies, and the U.S. companies tend to be far behind," says SVTC founder Ted Smith. "A lot of (U.S. manufacturers') initiatives are piecemeal and not really designed to address the vast majority of consumer concerns. There is still an enormous amount of computer waste being exported to China." The Computer Report Card notes that some U.S. companies use a double standard when it comes to recycling. Divisions located in Europe and Japan, where safe recycling is mandated by law, have implemented programs but their U.S. operations have not. Meanwhile, Congressman Mike Thompson (D-Calif.) has introduced a bill that would require the EPA to create grants for private and governmental organizations to develop computer recycling programs and the National Electronics Product Stewardship Initiative is working on a nationwide plan for recycling obsolete electronic devices. (Wired.com 10 Jan 2003)

*Category 26.2 Toxic materials*

2003-02-06 **computer recycling waste toxic materials**

NewsScan

HP OFFERS CONSUMER INCENTIVES FOR COMPUTER RECYCLING
Hewlett-Packard will offer e-coupons exchangeable for HP products when users recycle old computer hardware through the company. The coupons will range from $20 to $50 in value, depending on the amount a consumer spends on recycling services, which cost from $17 to $30 depending on the size of the equipment to be recycled. An HP executive said: "This is a way to learn what our customers want. Do they even want an incentive? Or do they just want to fill out a form and leave a box on their doorstep? We know that waste is a growing problem in the industry, but no one has really studied what consumers want to do to get rid of their computers." (AP/San Jose Mercury News 6 Feb 2003)

*Category 26.2 Toxic materials*

2003-02-26 **high technology computer waste toxic materials recycling**

NewsScan

E-WASTE RECYCLERS UNITE!
A group of 16 electronics recycling firms has signed an "Electronics Recycler's Pledge of True Stewardship," vowing to uphold stricter standards for processing electronic waste, including old computers, cell phones, TV sets and monitors, which contain hazardous materials such as lead and mercury. "We hope the pledge will really set the standard for how electronics recyclers operate their business," says David Wood, organizational director of the Computer TakeBack Campaign. "We hope that attention around it will raise the performance of other companies that are not presently signers." The companies have pledged not to dump discarded electronics into landfills, and to prevent their export to foreign countries. They also say they'll stop using prison labor to dismantle and recycle or refurbish old electronic devices. The group's actions come in response to startling results reported last year in a study, "Exporting Harm: The High-Tech Trashing of Asia." That study, produced by the Silicon Valley Toxics Coalition and the Basel Action Network, found that 50% to 80% of e-waste collected in the U.S. is shipped to developing countries like China, India and Pakistan. (Wired.com 26 Feb 2003)

*Category 26.2* *Toxic materials*

2003-03-05 **toxic materials recycling waste**

NewsScan

'REVERSE PRODUCTION' SYSTEM RECYCLES ALL
A study underway at Georgia Tech could offer a model for responsible recycling of electronic waste. Researchers have developed a "reverse production" system that enables every raw material contained in e-waste — metals such as lead, copper, aluminum and gold, as well as plastics, glass and wire — to be recovered and reused. Scientists say such "closed loop" manufacturing offers a win-win situation for manufacturers and consumers, and the project is generating buzz abroad, with officials in Taiwan and Belgium expressing interest in the system. Key to the process is chemical engineer Matthew Realff's design for a means to separate metals, as well as different qualities of plastics from crushed, ground-up components. From this work, new industries could be created to recover value not only from e-waste, but also from automobiles and other durable goods, says Realff. (Science Daily 4 Mar 2003)

# 27.1 Vulnerability assessment

*Category 27.1 Vulnerability assessment*

2003-09-12 **vulnerability scada systems grid electric hacker shut down North America back doors**

NewsScan

VULNERABILITY OF ELECTRIC GRID SYSTEM
Researchers say that "back doors" in the digital relays and control room technology managing direct electricity flow in North America is vulnerable to computer viruses and hackers. Cybersecurity researcher Eric Byres of the British Columbian Institute of Technology in Vancouver says: "I know enough about where the holes are. My team and I could shut down the grid. Not the whole North American grid, but a state, sure." He's frustrated because he's contacted a well-known manufacturer — whom he declined to name for security reasons — and urged that the weakness be fixed before hackers found it. Gary Seifert, a researcher with the Energy Department's Idaho National Engineering and Environmental Laboratory, defines the problem this way: "We have a plethora of intelligent electrical devices going into substations and power stations all over the United States. What's to keep somebody from accessing those devices and changing the settings?... We're still going to have back doors no matter how hard we try. You can't keep them out but you hope to slow them down." (AP/USA Today 12 Sep 2003)

# 27.5 Honeypots

*Category 27.5 Honeypots*

2003-02-03 **exposed vulnerable server high attack rate honeypot**

NIPC/DHS

January 29, Silicon.com — Exposed server is a magnet for hack attacks. The amount of hacking activity on the Internet has been revealed after one company set up an anonymous 'dummy test' server—and found it was maliciously attacked 467 times within 24 hours of being installed. The server, which contained no data and had no public profile, was attacked every single day over the next three weeks. PSINet Europe ran the test on an unprotected server at its Internet Data Center in Amsterdam, and registered a total of 626 malicious attacks over the three week period. A significant number of attacks originated from broadband or cable ISPs. PSINet's report into the experiment says that: "High bandwidth links do not only provide end users with faster download times—they also allow hackers to attack a wider target audience with a wider array of tools." PSINet also found that the bulk of the attacks originated from the United States and Western Europe and not in the most commonly expected areas of the former Eastern Bloc countries. Within Europe, Germany, Italy, the Netherlands and the UK were the most popular locations, while the countries most associated with attackers—Russia, Bulgaria and Romania—did not even feature. The findings of the PSINet Europe test are backed up by figures from the Gartner Group, which reported that 90 per cent of security breaches occur as a result of networks being incorrectly configured and managed.

# 28.1 Spyware, Web bugs & cookies

*Category 28.1* *Spyware, Web bugs & cookies*

2003-11-19 **Spyware UK ThreatLab Clearswift recording confidential data anti-spyware Ad-Ware Pest Patrol**

NewsScan

SPYWARE IN THE CROSSHAIRS
After several years of mounting concern, worries over "spyware," which surreptitiously deposits information-stealing software on computers, are coming to a head. Last summer, a corporate IT manager's nightmare came true when an e-mail sent to a British credit card and finance company carried a secret software program capable of recording confidential corporate data and sending it over the Net. "The good old days of script kiddies and geeks are well gone," says Pete Simpson, manager of the ThreatLab division of U.K. security firm Clearswift. "These are criminal gangs, and the motive is clearly profit." In response to the growing threat, legislation has been introduced in Congress that would outlaw both corporate spyware and the annoying kind that comes bundled with free software programs such as Kazaa and is used to deliver advertising. But in a report released Tuesday, the Center for Democracy and Technology argued against any legislation that specifically targets spyware, noting that most of the worst software-spying practices are already illegal. Rather, consumers would be better served by a broad-ranging privacy bill that would force all software programs to give clear notice when they are collecting information and give consumers the option to turn them off or easily uninstall them. Meanwhile, the Consortium of Anti-Spyware Technology Vendors, led by the creators of the spyware-battling Ad-Aware and Pest Patrol software programs, is developing standard definitions of "spyware," "adware," and other annoyances in an effort to present "best practices" recommendations to companies hoping to avoid being blocked by their software. (CNet News.com 19 Nov 2003)

# 28.3 Keystroke loggers

*Category 28.3* *Keystroke loggers*

2003-02-10 **spying keystroke logger criminal prosecution case Boston College**

NIPC/DHS

February 06, CNET News — Ex-student accused of spying on campus. A former Boston College student was indicted on Thursday for allegedly installing keystroke-recording software on more than 100 campus computers and accessing databases containing personal information on other students, staff and faculty. The case may be the first criminal prosecution of a person accused of unlawfully installing a key-logging device, which is designed to capture and record what a computer user types, including passwords and other private information. "I am very concerned about (key-logging software) given the enormous number of public access computers at schools, copy shops and libraries," said John Grossman, chief of the Massachusetts attorney general's corruption, fraud and computer crimes division. According to the attorney general's office, Boudreau began to install key-logging software around April 2002 and used intercepted information to add money to a stored-value card used in the campus dining and bookstore system. Boudreau is not, however, accused of misusing credit card numbers or profiting from selling any private information he allegedly gleaned. Universities have grown more worried about the possibility of key-loggers monitoring their systems, with the University of Illinois at Urbana-Champaign warning that the "Secret Service has advised us about several nationwide computer intrusions/hacking incidents." The charges against Boudreau include unauthorized access to a computer system, wiretapping, and breaking into a building at night "with intent to commit a felony." The last charge alone carries a penalty of up to 20 years in state prison.

*Category 28.3* *Keystroke loggers*

2003-03-07 **criminal hackers keystroke loggers bank accounts theft**

NewsScan

SUSPECTS STEAL MONEY VIA KEYSTROKE MONITORING SOFTWARE
Two Japanese men were arrested for allegedly hacking into people's bank accounts and stealing $136,000. The men are accused of downloading software that detects the keystrokes made by a computer user and installed it on PCs at Tokyo cybercafés. They then figured out the passwords that five previous customers had used to access their bank accounts online, and transferred a total of $141,000 from those accounts to another bank. One of the men, 27-year-old Goro Nakahashi, then used an alias to withdraw $136,000. If charged with theft, the two could face up to 10 years in prison. According to the Asahi newspaper, the men allegedly tried to use about 100 computers at 13 different Internet cafes around Tokyo. (AP 7 Mar 2003)
http://apnews.excite.com/article/20030307/D7PKA2180.htm

*Category 28.3* *Keystroke loggers*

2003-05-12 **Fizzer stealth worm KaZaA file-sharing P2P crackers Vxers anti-virus PC update Europe**

NIPC/DHS

May 12, The Register — Fizzer stealth worm spreads via KaZaA. An Internet worm called "Fizzer" is spreading through the KaZaA P2P file-sharing network and as an executable file via e-mail. Reuters reported Monday that businesses in Asia were the first to report the attack, followed by reports of tens of thousands of infections in Europe. Fizzer is especially dangerous because it installs a keyboard-logging program that intercepts and records all keyboard strokes in a separate log file. To transmit this information, Fizzer loads a backdoor utility that allows crackers/VXers to control a computer via IRC channels. Additionally, the worm regularly connects with Web page located on the Geocities server from which it attempts to download updated version of its executable modules. In an attempt to foil detection, Fizzer also attempts to shut down an array of widely used anti-virus programs that might be running on a victim's PC. Computer users should keep their anti-virus software updated.

*Category 28.3* *Keystroke loggers*

2003-10-10 **hacker security fraud Drexel University investment keystroke**

NewsScan

HACKER CHARGED WITH SECURITIES FRAUD
A 19-year-old student at Drexel University in Pennsylvania is being charged by the Securities & Exchange Commission (SEC) of fraud and identity theft for hacking into someone's investment account and making a complex and illegal trade. The student is accused of using a program called the Beast to monitor every keystroke typed on the target machine, and by doing so was able to obtain the log-in and password for the investor's online brokerage account with TD Waterhouse. (New York Times 10 Oct 2003)

*Category 28.3* *Keystroke loggers*

2003-10-10 **spyware covert monitoring eavesdropping keylogger RAT fraud spam law enforcement parents ethics**

NYT
http://www.nytimes.com/2003/10/10/technology/10SPY.html?th=&pagewanted=print&position=

Rick Eaton, founder of TrueActive, altered his monitoring product to remove its "silent deploy" feature, which allowed secret installation of the surveillance software on the target machine via e-mail and without permission. He did so on ethical grounds. In contrast, more than a dozen other keystroke loggers persist in providing facilities for surreptitious installation.

# 28.4 Cell / mobile phones / GPS (as tracking devices)

*Category 28.4* *Cell / mobile phones / GPS (as tracking devices)*

2003-06-17 **prevent theft gps matsushita bicycle**

NewsScan

BIKE HAS GPS TO PREVENT THEFT
An electric bicycle produced by National Bicycle, a Matsushita company, will have a Secom global positioning system (GPS) designed to guard against theft. The battery will simultaneously supply electricity to the bicycle and recharge the portable GPS unit. (Japan Today 17 Jun 2003)

# 28.6 RFID tags

*Category 28.6* *RFID tags*

2003-07-21 **surveillance radio frequency RFID GPS Wozniak WiFi**

NewsScan

WOZNET: APPLE COFOUNDER COMES BLAZING BACK
Beginning with an interest in finding a way to track his lost dogs, Apple co-founder Steve Wozniak developed location-monitoring technology using electronic tags and designed to help people keep track of their animals, children or property. The new company, Wheels of Zeus, is touting WozNet as a simple and inexpensive wireless network that uses radio signals and global positioning satellite data to keep track of a cluster of inexpensive tags within a one- or two-mile radius of each base station. Its low-power network will complement rather than compete with other wireless technologies such as radio-frequency I.D. tags used in stores and factories and higher speed Wi-Fi and cellular data networks. WozNet, with data rates of no more than 20,000 bps, will be able to transmit a very small amount of digital information even through environments subject to radio interference, and will be able to location information from global positioning system (GPS) satellites. (New York Times 21 Jul 2003)

*Category 28.6* *RFID tags*

2003-07-25 **Intel Alzheimer RFID patient tracking artificial intelligence system**

NewsScan

INTEL, ALZHEIMER'S ASSOCIATION TEAM UP ON PATIENT CARE
Intel has formed a consortium with the Alzheimer's Association to fund research on new ways to improve the care of Alzheimer's patients, such as using a combination of sensors and wireless technologies to monitor the patient, thereby freeing up the caregiver to tackle some chores. "If you are a caregiver, this is really empowering technology," says Eric Dishman, director of proactive research at Intel. Intel says it is also investigating the use of radio frequency identification (RFID) tags on items that the patient uses every day, such as a coffee cup or plate. The tags could track activity patterns for each object, and a link to an artificial intelligence system could generate prompts via the radio or TV on what to do with it (i.e., instructions for making coffee or washing a dish and putting it away). The Everyday Technologies for Alzheimer Care will fund more than $1 million worth of new research. (San Jose Mercury News 25 Jul 2003)

*Category 28.6* *RFID tags*

2003-10-03 **tracking books RFID people privacy EFF**

NewsScan

TRACKING LIBRARY BOOKS OR TRACKING PEOPLE?
The Electronic Frontier Foundation (EFF), which concerns itself with civil liberties issues in cyberspace, is expressing dismay over a plan by the the San Francisco Public Library use RFID technology to track books. A RFID (radio frequency identification) chip would be inserted into each library book, and would send out electromagnetic waves that would allow tracking of the book's location. San Francisco's city librarian Susan Hildreth says the RFID devices will help streamline inventory and prevent loss, and explains that tracking people is not the goal; "It will not allow us to track people to their home or any location." Hildreth's response has failed to satisfy Electronic Frontier Foundation Lee Tien, who worries: "We're talking about the imbedding of location trafficking devices into the social fabric." (AP/USA Today 3 Oct 2003)

# 29.2 Cybersyndromes

*Category 29.2* *Cybersyndromes*

2003-01-23 **impolitness etiquette wireless e-mail laptop computers audience inattention rudeness**

NewsScan

WIRELESS AND RUDE
The increasing availability of wireless networks is creating new opportunities for rudeness — or, theoretically, politeness. One wireless enthusiast admits, "When I speak to a room of people with laptops, they all have their heads buried in their laptops. Many of them are taking notes of what we're saying, but I think many of them are just trying to catch up with their e-mails." Etiquette expert Sue Fox adds: "If you're doing other work — talking on a phone, working on a computer — I think it's ill manners. It's very rude." (USA Today 23 Jan 2003)

*Category 29.2* *Cybersyndromes*

2003-02-12 **computer game psychology sociology community**

NewsScan

COMPUTER GAMES ARE GOOD FOR YOU
Playing computer games can be beneficial, say researchers studying the complex social interactions inherent in the popular online multiplayer shoot-em-up Counter-Strike. Professor Talmadge Wright and colleagues at Loyola University in Chicago say that Counter-Strike is much more than just racking up "kills," with the strategies and tactics used by many regular players approaching the complexity of those used in chess. And although much of the banter reflects the typical trashtalk of teenage boys, it's a mistake to dismiss the gamers as misguided misanthropes. "The most common emotion when people are playing is laughter," says Wright. In fact, games like Counter-Strike that rely on trust and cooperation give rise to strong communities and friendships, he adds. "It gives people an option of actively participating in some kind of fantasy role they could not do in real life that allows them to play with their own feelings. It is an area that's bricked off from everyday life that you can enter and leave at will. It offers you a way to play with things you may be scared of in a safe way where there are very few consequences." For these reasons the games are good for players, says Wright, who suggests that many studies of game-playing have been skewed by hidden agendas. "There's a cultural motif that underlies the critiques that go on around this, the idea of mindless activity is given short shrift in culture where productivity is given the highest praise." (BBC News 12 Feb 2003)
http://news.bbc.co.uk/1/hi/technology/2744449.stm

*Category 29.2* *Cybersyndromes*

2003-02-24 **data recovery disk drive crash psychological counselling**

NewsScan

PSYCHOLOGICAL HELP FOR COMPUTER MELTDOWN VICTIMS
Here's the latest in data recovery services — DriveSavers, a technology firm that specializes in recovering data from even the most devastated computer system, employs a full-time crisis counselor to help customers work through their trauma. "People get upset — very, very upset," says Kelly Chessin. "They yell. They cry. They need someone to listen to them and let them vent. That's what I'm here for." When customers go berserk on the phone, Chessin steps in and tries to help them calm down before an engineer comes on the line to discuss the technical aspects of the problem. Chessin says her experience working for a suicide hot line is invaluable in helping distraught customers deal with data disaster. "It's similar. But when people call a hot line, you need to help them find their own solutions. Now I can offer solutions to people's problems." Another difference? People who seek help from DriveSavers frequently call Chessin back to thank her for being there. "That's really nice," she says. (San Francisco Chronicle 23 Feb 2003)

*Category 29.2* *Cybersyndromes*

2003-03-04 **text messaging children spelling**

NewsScan

TEXT MESSAGE ESSAY BEWILDERS BRITISH TEACHER
A 13-year-old's "How I Spent My Summer Vacation" essay proved to be almost indecipherable to her poor teacher. "I could not believe what I was seeing. The page was riddled with hieroglyphics, many of which I simply could not translate," the teacher told the Daily Telegraph newspaper. The girl's essay began: "My summr hols wr CWOT. B4, we used 2go2 NY 2C my bro, his GF & thr 3 :- kids FTF. ILNY, it's a gr8 plc." For those who had trouble reading that, here's a translation: "My summer holidays were a complete waste of time. Before, we used to go to New York to see my brother, his girlfriend and their three screaming kids face to face. I love New York. It's a great place." The text messaging craze is partially to blame for a decline in grammar and written English abilities, says Judith Gillespie of the Scottish Parent Teacher Council. "Pupils think orally and write phonetically." (Reuters/CNN 3 Mar 2003)

*Category 29.2* *Cybersyndromes*

2003-03-17 **spell checker software errors dependence**

NewsScan

BEWARE THE SPELLCHECKER
A study at the University of Pittsburgh reveals that the ubiquitous spellchecker software may be doing as much harm as good, when it comes to writing. In the study, 33 undergraduate students were asked to proofread a one-page business letter — half of them using Microsoft Word, with its spell- and grammar-checking features and the other half using only their brains. Without the software, students with higher SAT verbal scores made, on average, five errors, compared with 12.3 errors made by students with lower scores. However, using the software, the two groups made about the same number of errors — 16 vs. 17. Dennis Galletta, a professor of information systems at the Katz Business School, says people have come to rely on spellchecking software too completely. "It's not a software problem, it's a behavior problem." (AP 14 Mar 2003)
http://apnews.excite.com/article/20030314/D7POQ7R80.htm

# 29.3 Digital divide

*Category 29.3* *Digital divide*

2003-01-07 **online polls digital divide bias non-random sampling**

NewsScan

ONLINE POLLS REFLECT CONSERVATIVE OUTLOOK
While both Democrats and Republicans were likely to turn to the Internet as a source of news and political information during last fall's midterm elections, Republicans were much more likely to register their views in online polls, according to a study by the Pew Internet and American Life project. Nearly half of the Republicans who went online in search of election news said they liked to participate in online polls, compared with 23% of Democrats. The bottom line is that Web sites operating online polls should take those results with a grain of salt, says Lee Rainie, director of the Pew project. "They very much skew toward more conservative views. People who rely on Internet polls are relying on a false indicator." (Wired.com 6 Jan 2003) http://www.wired.com/news/politics/0,1283,57093,00.html

---

*Category 29.3* *Digital divide*

2003-03-19 **digital divide accessibility Internet**

NewsScan

MORE UNDERSERVED CHILDREN ARE GETTING ONLINE
Almost two-thirds of American children between the ages of 2 and 17 logged onto the Net last year, with a whopping 205% increase among African-American children, according to a new report from the Corporation for Public Broadcasting. The disparities between higher and lower income children still exist, but the study found that 58% of African American children and 50% of Hispanic children now use the Internet from some location — either home, school or the local library. The study, based on a series of surveys conducted last year by technology market research firm Grunwald Associates, also found that digital media use among children ages 6-17 is now approaching parity with television viewing. According to the report, children spend 3.1 hours per day watching TV and 2.9 hours a day surfing the Web, playing video games or using the computer for non-Internet activities. Among teenagers, computer use actually outstrips TV viewing — 3.5 hours vs. 3.1 hours per day. An electronic version of the report "Connected to the Future" is available at cpb.org/ed/resources/connected. (Corporation for Public Broadcasting 19 Mar 2003)

---

*Category 29.3* *Digital divide*

2003-04-17 **Internet usage evasion elderly digital divide**

NewsScan

PEW STUDY OF INTERNET EVADERS
A study by the Pew Internet and American Life Project has found that 42 % of American adults are not connected to the Internet, even though two out of three of those people have relatives or close friends who do. In addition, the study's authors label as "Net Evaders" 20% of the nonusers who live in Internet-connected homes where other relatives go online. And then there's a category of "Net Dropouts" to characterize the 17% of nonusers who tried the Net and didn't like it. The director of the Pew project says of the Net Dropouts: "Some grew disillusioned with the online world. They decided it was just a time swamp, or they never found what they wanted." [They have our full sympathies. If the poor wretches never found NewsScan, who can blame them for jumping ship?] (New York Times 17 Apr 2003)

---

*Category 29.3* *Digital divide*

2003-06-26 **Wi-Fi poorer nations wireless internet**

NewsScan

WIRELESS GIVES POORER NATIONS CHANCE TO CATCH UP…
In a speech prepared for a UN conference on the social implications of wireless communications technologies, UN Secretary-General Kofi Annan declared that wireless Internet access has "a key role to play everywhere, but especially in developing countries and countries with economies in transition… It is precisely in places where no infrastructure exists that Wi-Fi can be particularly effective, helping countries to leapfrog generations of telecommunications technology and infrastructure and empower their people." (Reuters 26 Jun 2003)

---

*Category 29.3* *Digital divide*

2003-07-15 **MIT search engine poor countries e-mail connectivity**

NewsScan

A SEARCH ENGINE FOR THE WORLD'S POOR
Researchers at MIT are designing a search engine geared to the needs of computer users in the world's disadvantaged countries, most of whom have only sporadic access to the Web at what are often less-than-optimal bandwidths. "Let us assume you are in Malawi," says professor Saman Amarasinghe of MIT's Laboratory for Computer Science, "and the computer lab does not have access to the telephone line all the time. If you want to find some new information about malaria, you are prompted with a message that says 'we are going to send a query through e-mail, is it OK?'. At night, when the phone line is available, the teacher can dial out and send the queries." The request is routed to computers at MIT, which then perform the search and filter the results, choosing the most relevant. These results are then sent back to the computer in Malawi. "Next morning the teacher can connect, download that e-mail and when the students arrive, they can browse through those pages the way they would if they had full Internet connectivity." Amarasinghe says most search engines are geared toward Western users who are cash-rich but time-poor. "The idea is that developing countries are willing to pay in time for knowledge. In the West when we surf we want the information in the next two seconds. We are not willing to wait." (BBC News 15 Jul 2003)

*Category 29.3* *Digital divide*

2003-12-19 **internet illiteracy language non-english population technology**

NewsScan

GLOBAL INTERNET USE LIMITED BY LANGUAGE, ILLITERACY
According to the International Telecommunication Union, about 70% of the world's Internet users live in countries that make up only 16% of the world's population — statistics that reinforce complaints aired at last week's U.N World Summit on the Information Society that despite the Internet's global reach, most of the material is inaccessible to the vast non-English-speaking population of the world. And while international development efforts have included linking villages and schools in developing nations to the Internet, once people are connected, there must be compelling information available in native languages and in accordance with local customs. "Getting the technology into people's hands is one thing. Getting people to use it is key," says Daniel Wagner, director of the University of Pennsylvania's International Literacy Institute. The solution involves more than just translating Web sites into other languages. To address the problem of population illiteracy, South Africa is developing speech recognition, text-to-speech and other voice technologies, starting with Zulu. Bulgaria, South Korea and other countries are producing government sites in native languages. And the Canadian government is looking at adapting its internal search engine to include materials in Inuktitut, the Inuit language, as well as French and English. "The point is to produce more content that is useful," says Bernardo Sorj, an advisor to Brazilian urban assistance group Viva Rio. "If people go on the Internet and do not find good content for themselves, then they go to pornography." (AP 19 Dec 2003)

# 29.4 Online & electronic voting

*Category 29.4* *Online & electronic voting*

2003-01-22 **online Internet election voting**

NewsScan

INTERNET ELECTION
The tiny village of Anieres, Switzerland, made Swiss history by holding that country's first legally binding [online] election. The 323 citizens who cast their votes by Internet were required to type in a series of security codes and their date and place of birth. An additional 370 Anieres residents voted by mail, and 48 actually went to the polls. (AP/Chicago Sun-Times 20 Jan 2003) http://www.suntimes.com/output/news/cst-nws-net20.html

*Category 29.4* *Online & electronic voting*

2003-01-28 **electronic voting analysis flaws problems resources**

http://www.nwfusion.com/newsletters/sec/2003/0127sec1.html

E-Voting (1): Not Ready Yet

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Electronic voting has been proposed in a number of precincts in the USA. One of the most extensive archives of discussions about this issue is the RISKS FORUM DIGEST edited by Peter G. Neumann of SRI Intl. Entering “vote” as a keyword in the search engine available through at < http://catless.ncl.ac.uk/Risks/ > brings up 303 entries starting with Volume 1 Number 1 [henceforth notated as “v(n)” for the volume and number] in 1985; additional articles can be found using other related keywords such as “voting” and “election.”

One of the most recent contributions comes from Jonathan Kamens, writing in RISKS 22(39) (23 Nov 2002). He describes a system that allows a voter to mark a paper ballot and then feed it in through an electronic reader. Kamens points out that the card-reading voting system proposed for Boston MA has fundamental problems:

* There is no way for a voter to verify that the system is correctly registering the voter's choices on the ballot.

* If the card reader indicates that a card has not successfully been registered, a voter can be given a second card -- but the invalid one goes straight into a locked ballot box. If there's a recount, someone could get both their ballots counted.

In general, e-voting systems can include any or all of the following functions, each requiring increasing degrees of security:

* Automatic reading and tallying of votes made on paper ballots;

* Accepting votes using electronic input devices such as electric pens, touch-screens, and keyboards;

* Remote voting at a distance.

E-voting systems need to include at least the following security characteristics:

1) Remote voting requires identification, authentication and authorization PLUS guarantees of complete privacy as well as measures to prevent fraudulent exclusion of valid voters and fraudulent acceptance of repeated votes by individuals.

2) Electronic data entry should include all the measures developed in the last 40 years of data processing to reduce the likelihood of user error; such measures include

a) feedback to the user to be sure that what was entered was what was recorded;

b) error checking and alerts to prevent obvious blunders such as voting for two people for the same position if that is not permitted;

c) provision of overrides so that voters can deliberately spoil their ballot if that's what they want to do;

3) Fail-safe redundancy so that no single point of failure or even widespread denial-of-service attacks could wipe out voter's intentions;

4) Cryptographically strong local and remote audit trails to keep multiple independent records of all votes; such files could include checksums that are calculated using the preceding record's checksum as input to the hashing algorithm (to reduce the ease of fraudulent tampering with the records).

One of the most serious questions raised about e-voting is independent of security: it’s the issue of equal access. Will widespread e-voting lead to increased disparity between the voting patterns of richer and poorer people among the electorate? Will e-voting be yet another example of what has been called the “digital divide?”

* * *

In the next article in this two-part sequence, I will look at some detailed analyses of e-voting with special attention to security.

* * *

For further reading:

Bonsor, K. (2002). How E-Voting Will Work. < http://www.howstuffworks.com/e-voting.htm/printable >

Burke, L. (2000). Report says E-Voting Is Unsafe. < http://www.wired.com/news/politics/0,1283,37504,00.html >

Cranor, E. (1996). Electronic Voting: Computerized polls may save money, protect privacy. _ACM Crossroads Student Magazine_ < http://www.acm.org/crossroads/xrds2-4/voting.html >

Digital Divide Network < http://www.digitaldividenetwork.org/content/sections/index.cfm >

Election.com – The Global Election Company < http://www.election.com/us/index.htm >

Electronic Frontier Foundation “E-voting” Archive < http://www.eff.org/Activism/E-voting/ >

*Category 29.4* *Online & electronic voting*

2003-01-30 **electronic voting analysis flaws problems resources**

http://www.nwfusion.com/newsletters/sec/2003/0127sec2.html

E-Voting (2): Security Analyses

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the first of these two short articles, I've been introducing e-voting. In this part, I summarize some key analyses of the security issues surrounding remote voting via the Internet.

In a July 2002 article posted on the BBC Web site, commentator Bill Thompson comments on a recent Green Paper proposal by Robin Cook, Leader of the House of Commons. Cook includes two methods for increasing the involvement of the public in government decision-making: "For the government, the two strands that make up e-democracy are ways to enhance participation (e-participation) and electronic voting (e-voting)." Thompson argues that the vulnerabilities of any e-voting system built in the next few years should preclude any use of such insecure technology. He writes that the consequences of fraud would be so serious that large amounts of investment would be profitable if they swayed the direction of an election. For example, "If we all use trusted processors then why not set up a production line to manufacture your own hacked chips? It would only cost a few tens of millions of euros. If all code has to be signed by some digital authority, why not spend a few million bribing the senior staff?"

A much longer and more detailed analysis of e-voting is from the respected scientist Avi Rubin of AT&T Labs. Rubin neatly summarizes the issues as follows [I have added the asterisks as bullets and slightly changed the punctuation]: "There are many aspects of elections besides security that bring this type of voting into question. The primary ones are

* coercibility – the danger that outside of a public polling place, a voter could be coerced into voting for a particular candidate.

* vote selling – the opportunity for voters to sell their vote.

* vote solicitation – the danger that outside of a public polling place, it is much more difficult to control vote solicitation by political parties at the time of voting.

* registration – the issue of whether or not to allow online registration, and if so, how to control the level of fraud."

Rubin then analyses the voting platform, the communications infrastructure, social engineering, and specialized devices (by which he means "tamper-resistant devices, such as smart cards." He discusses in some detail how programmatic attacks (viruses, worms, denial-of-service [DoS] attacks) could easily alter election results. Just imagine the consequences of, say, carefully-written Trojan horse programs, targeted DoS attacks on particular precincts on election day; Rubin writes, "In some close campaigns, even an untargeted attack that changes the vote by one percentage point could sway the election." According to the notes in the source HTML for the document, that sentence was written a few weeks before the contested US presidential election of 2002. I strongly recommend Dr Rubin's paper as foundation reading for anyone interested in e-voting.

Finally, I direct your attention to the immensely valuable annotated bibliography on electronic voting prepared by Rebecca Mercuri, PhD, Professor of Computer Science at Bryn Mawr College. Dr Mercuri has a distinguished record of contributions to the technical analysis of electronic voting; her Web site (see below) has many pages of news, essays, pointers to other e-voting sites, lists of her own and other scholarly works on the subject, and even pointers to e-voting humor.

* * *

I hope that these two short articles will increase readers' interest in the trustworthiness of e-voting and that some of you will be able to contribute to a more informed discussion of this critically important issue in the future of representative democracy. I'm sure that I will be hearing from e-voting technology vendors clamoring for attention; if possible, I'll write a follow-up column with some of their remarks.

* * *

For further reading:

Legon, J. (2002). Electronic elections: What about security? Voters put touch screens to the test. < http://www.cnn.com/2002/TECH/ptech/11/05/touch.screen/ >
[Note to avoid ambiguity: the string /11/ in this URL uses the numeral "one"]

Mercuri, R. (2002). Electronic Voting. < http://www.notablesoftware.com/evote.html >

Rubin, A. (2000). Security Considerations for Remote Electronic Voting over the Internet. < http://avirubin.com/e-voting.security.html >

Thompson, B. (2002). Why e-voting is a bad idea. < http://news.bbc.co.uk/1/hi/sci/tech/2135911.stm >
[Note to avoid ambiguity: the string /1/ in this URL uses the lowercase form of the letter "L"]

*Category 29.4* *Online & electronic voting*

2003-02-03 **electronic e-voting security risk debate**

NIPC/DHS

January 30, SecurityFocus — E-voting security debate. Some respected computer scientists and security experts in California's Silicon Valley say the risks posed by malicious hackers, equipment failure or subtle programming errors make fully-electronic voting systems a bad idea. "There's no voter-validated record, so Trojan horses or accidents can happen without any evidence that anything has gone wrong," correctly," says Peter Neumann, a scientist at SRI International, a non-profit research institute. Electronic voting systems usually featuring touch screens and simple ATM-like interfaces. By some estimates one out of five votes were cast electronically last November. The systems are not connected to the Internet; instead, voters' ballots are typically stored on an internal hard drive until the polls close. Then they're copied a portable disk or a non-volatile memory card and taken to a central counting facility. It's the paperless nature of the transaction that bothers critics. "The problem is that…it's really up to the company that wrote the software to say that there were no errors or deliberate tampering that interfered with the vote," says David Dill, a computer science professor at Stanford University. The computer scientists say they'd be happier, but not convinced, if companies making the electronic voting systems released their code for public review. On Friday they are going to attempt to persuade Santa Clara County to embrace a system in which electronic voting stations print a hard copy of the voter's ballot. The voter can then review the printout before manually depositing it in a ballot box.

*Category 29.4* *Online & electronic voting*

2003-02-24 **online voting**

NewsScan

LORRIE CRANOR ON INTERNET VOTING
In an interview with John Gehl for the ACM online weekly publication Ubiquity, Dr. Lorrie Faith Cranor of ATT Labs-Research, an expert on technology policy issues, says: "I am afraid that Internet voting will be a reality, and I think it's a bad idea, which surprises people. Usually people think that because I have done Internet voting work, I must be excited that Internet voting is progressing. It's one of those things that the more you know about, the less you like it." What does she dislike about Internet voting? "For one thing, there are huge security risks, especially when people are talking about Internet voting from home or from work as opposed to, say, going to a polling place that happens to be connected to the Internet. That's no fun. If we have to go to the polling place it really doesn't matter if it's connected to the Internet or whatever because we still had to go to a polling place. So when people, especially in the press, talk about Internet voting they're talking about voting from anywhere; from home in your pajamas is the classic example. That means voting over the existing insecure Internet using the existing insecure computers in my house that might have viruses or mis-installed software on them. I think that it is really dangerous, especially in elections where there's something really important at stake." (Ubiquity Feb 2003)
http://www.acm.org/ubiquity/interviews/l_cranor_2.html

*Category 29.4* *Online & electronic voting*

2003-07-12 **e-voting security experiment 2004**

NewsScan

INTERNET VOTING IN 2004
The Secure Electronic Registration and Voting Experiment, which involved only 84 voters in 2000, is set to balloon next year when as many as 100,000 citizens in the military and living abroad will have the option of casting their votes via the Internet. The Pentagon-run SERVE program will be limited to eligible voters from South Carolina and Hawaii, as well as residents from selected counties in Arkansas, Florida, Minnesota, North Carolina, Ohio, Pennsylvania, Utah and Washington. If the test proves successful, the $22-million program could be expanded to include 6 million voters in the military and their dependents, as well as nonmilitary citizens living abroad. Some observers have voiced security concerns over electronic voting, however. "It wouldn't take much for some smart hacker to send around a virus that lays in wait for someone to issue a vote," says a project manager for the Center for Public Integrity. Meanwhile, Polli Brunelli, director of the Pentagon's Federal Voting Assistance Program, says her office is taking unprecedented security measures to ensure system integrity. "With this population, we have made the casting of the Internet ballot as safe, if not safer, than with the mail-in ballots. If we reach a point where things are vulnerable and we can't guard against that, we won't go forward." (AP 12 Jul 2003)

*Category 29.4* *Online & electronic voting*

2003-07-24 **impersonation e-voting software flaw election system**

NewsScan

SERIOUS FLAWS IN ELECTRONIC VOTING SYSTEMS
Johns Hopkins University experts say that high-tech voting machine software from Diebold Election Systems has flaws that would let voters cast extra votes and allow poll workers to alter ballots secretly. Aviel D. Rubin, technical director of the Information Security Institute at Johns Hopkins, led a team that examined the Diebold software, which has about 33,000 voting machines operating in the United States. Adam Stubblefield, a colleague of Rubin's, said that "practically anyone in the country — from a teenager on up — could produce these smart cards that could allow someone to vote as many times as they like." Diebold has not seen the Institute's report and would not comment on it in detail, but a company spokesman said: "We're constantly improving it so the technology we have 10 years from now will be better than what we have today. We're always open to anything that can improve our systems." Peter G. Neumann, an expert in computer security at SRI International, said the Diebold code was "just the tip of the iceberg" of problems with electronic voting systems. [Side note: see the interview of Peter Neumann by John Gehl in the archives of the ACM online publication Ubiquity: [http://www.acm.org/ubiquity/interviews/p_neumann_3.html.] (New York Times 24 Jul 2003)

---

*Category 29.4* *Online & electronic voting*

2003-09-11 **electronic voting glitch faulty system fraud Diebold Election Systems Inc.**

NewsScan

DEBATE OVER ELECTRONIC VOTING
During California's March 2002 primary, absentee vote tallies from one county seem to have been sent to an Internet site operated by Diebold Election Systems Inc., the company that manufactured the voting machines used in the election. Activist critics of electronic voting systems say the glitch is new evidence that the technology is intrinsically faulty, but Diebold executive Deborah Seiler says that Diebold engineers may have published the results as part of a test performed days, weeks or months after the county primary (regardless of the time stamp shown): "These activists don't understand what they're looking at." Seiler insists that the company has a system of checks and balances to safeguard against fraud, but that explanation doesn't satisfy Kim Alexander, president of the California Voter Foundation, who charges: "In our quest to deliver faster, more accurate election results, we've left the voting process wide open to new forms of attack and mismanagement." (AP/San Jose Mercury News 11 Sep 2003)

---

*Category 29.4* *Online & electronic voting*

2003-09-12 **voting internet poll tax dean al sharpton howard vote**

NewsScan

SHARPTON CALLS INTERNET VOTING A 'HIGH-TECH POLL TAX'
Democratic presidential candidate Al Sharpton has protested a Democratic Party plan that would, for the first time, allow Internet voting in Michigan's presidential caucus — and is challenging front-runner Howard Dean to stand with him. Sharpton wrote to Dean: "Perhaps it is due to the fact you governed a state with virtually no people of color living within its borders that you are unaware that this is a racially biased proposal." (Vermont is nearly 98% white.) A Dean spokesman said that Dean supports the concept of Internet voting or anything that will people to the polls "as long as it's coupled with the need to insure access to African Americans and others when it might not be available." Calling the scheme a "high-tech poll tax," Sharpton explained: "A grandmother in a housing development is going to have to go downstairs and walk five blocks to vote. Who do you think is going to get more of the vote? Democracy is about equal access. This is not equal access. It really is a high-tech poll tax." (AP/USA Today 12 Sep 2003)

---

*Category 29.4* *Online & electronic voting*

2003-11-04 **electronic voting information leakage hacker stanford diebold e-mail servers machines**

NewsScan

ELECTRONIC VOTING DISPUTE
The Electronic Frontier Foundation and Stanford University's Cyberlaw Clinic are suing Diebold Inc., a manufacturer of electronic voting machines, to stop it from issuing threats to groups that publish company documents leaked by a hacker; the hacker broke into Diebold's servers in March (using an employee's ID) and copied thousands of company announcements and internal e-mails. The intruder e-mailed the data to voting activists, some of whom published stories on their Web logs denouncing Diebold. A California advisory panel has refused to certify new Diebold voting machines, pending a determination of whether uncertified software and hardware was used in a recent election. (AP/Los Angeles Times 4 Nov 2003)

---

*Category 29.4* *Online & electronic voting*

2003-11-09 **electronic voting machines proprietary source code secret touch-screen ballot fraud**

NYT
http://www.nytimes.com/2003/11/09/business/yourmoney/09vote.html?th=&pa
gewanted=print&position=

Walden O'Dell wrote a letter in mid-August 2003 to 100 wealthy friends inviting them to a Republican fund-raiser. He included the line, "I am committed to helping Ohio deliver its electoral votes to the president next year." Unfortunately, Mr O'Dell is also the CEO of the Diebold company, makers of paperless voting machines. A political storm has erupted over these machines, which have no independent audit trail or means of convincing a voter that his or her vote is being recorded accurately. Accusations of bias led Mr O'Dell to protest in September 2003, "I'm not doing anything wrong or complicated, but it obviously did leave me open to the criticism I've received."

---

*Category 29.4* *Online & electronic voting*

2003-11-18 **EFF Electronic Frontier Foundation Diebold leaked documents security problems**

NewsScan

ELECTRONIC VOTING LAWSUIT
The Electronic Frontier Foundation, a civil liberties advocacy group, says it fears legal threats from Diebold Inc., the maker of electronic voting systems. Diebold has asked a U.S. district court in San Jose to bar Diebold from sending cease-and-desist letters to activists who have published links to leaked documents about alleged security problems with the company's equipment. Diebold's response is that the company has never had an intention to stifle intent to free speech or place onerous burdens on Internet service providers, but that it strenuously objects to the "wholesale reproduction" by activists of 13,000 pages of internal, proprietary documents. Diebold's attorney argues: "The plaintiffs advocate an open-source code system for elections code. These materials were intended to be secret and private and proprietary." (AP/Washington Post 18 Nov 2003)

---

*Category 29.4* *Online & electronic voting*

2003-11-20 **voting online internet democrats dean clark michigan poor blacks portesting**

NIPC/DHS

MICHIGAN DEMS WANT INTERNET VOTING
Democrats in Michigan want to increase turnout in their presidential caucus by allowing Internet voting. All of front-runner Howard Dean's opponents except Wesley Clark are protesting the plan, saying that Internet voting puts blacks and the poor at a disadvantage by making access difficult. Under the plan, registered Michigan Democrats who want to vote by mail or Internet will request an absentee ballot from the state party ahead of time; they will then be sent a ballot that can either be returned by mail or used to obtain a code that will allow voting by Internet. Donna Brazile, former Gore strategist, says that with improvements that have bee made to the Internet voting system, "the access argument sort of melts away." (AP/USA Today 20 Nov 2003)

---

*Category 29.4* *Online & electronic voting*

2003-12-01 **Diebold voting machines leaked documents EFF Electronic Frontier Foundation forum public discussion internet security holes**

NewsScan

DIEBOLD BACKS OFF — AT LEAST FOR AWHILE
After considerable controversy, the Diebold company, which makes electronic voting machines, has agreed not to sue voting rights advocates who published leaked documents about alleged security breaches on their machines. Dozens of students, computer scientists and Internet service providers were sent cease-and-desist letters and threatened with law suits Electronic Frontier Foundation attorney Wendy Seltzer says, "This is a huge victory that shows we have weapons on our side to protect free speech from overbearing copyright laws so that the Internet remains a forum for public discussion. We're trying to hammer home that you can't go around making idle threats that aren't backed up by the law." But a Diebold executive says the company will continue to monitor the online proliferation of the leaked documents, and may file lawsuits against others who publish the data.(AP/USA Today 1 Dec 2003)

---

*Category 29.4* *Online & electronic voting*

2003-12-08 **secure voting machines sufficient enough intrusion hackers**

NewsScan

SECURITY CONCERNS ABOUT VOTING MACHINES
Diebold and other companies that make electronic voting machines are joining forces to make the case that electronic voting technology is sufficiently secure to withstand intrusion by hackers. A number of computer experts have argued that the new machines have security problems, and that they should be equipped to provide companion paper records for auditing purposes. Paper printers could add $500 to the cost of each machine. (Washington Post 8 Dec 2003)

# 31.1 Surveys, studies, audits of security

*Category 31.1* *Surveys, studies, audits of security*

2003-01-23 **identity theft statistics growth reports**

NewsScan

IDENTITY THEFTS DOUBLED LAST YEAR
The number of identity thefts doubled in 2002, with 162,000 reports of identity theft compared to 86,000 the previous year. However, the Federal Trade Commission says that the rise in identity theft complaints does not necessarily mean an increase in actual crimes — it may simply reflect an increasing public awareness of the problem and a greater likelihood that such incidents are now being reported. But an official of the Michigan State Police points out that many former violent criminals are now using the Internet for identity theft: "They are switching over to white-collar crime because it's more lucrative and they know they will get less time. Identity theft is not necessarily a sophisticated crime." (New York Times 23 Jan 2003)

*Category 31.1* *Surveys, studies, audits of security*

2003-01-28 **cellular mobile telephone driving danger attention study**

NewsScan

CELL PHONE USE CAN IMPAIR VISION WHILE DRIVING
Researchers at the University of Utah have found that drivers using cell phones, even hands-free devices, experience a decrease in the ability to process peripheral vision, creating a potentially lethal "tunnel vision." This "inattention blindness" slows reaction time by 20% and resulted in some of the 20 test subjects missing half the red lights they encountered in simulated driving. "We found that when people are on the phone, the amount of information they are taking in is significantly reduced," says associate professor David Strayer. "People were missing things, like cars swerving in front or sudden lane changes. We had at least three rear-end collisions." The Utah study is only the latest investigation into the effects of driving and cell phone use, and most of the others have also demonstrated some degree of impairment. And while most studies have focused on the distractions of dialing or holding a phone, the Utah research tried to focus on the distractions caused by having a conversation. New York is the only state to have instituted laws against the practice, but 30 more states have similar legislation pending. (CNet News.com 27 Jan 2003)
http://news.com.com/2100-1033-982325.html

*Category 31.1* *Surveys, studies, audits of security*

2003-02-03 **criminal hacker attacker vulnerabilities survey study**

NewsScan

CYBER ATTACKS DOWN, VULNERABILITIES WAY UP
The level of cyber attacks dropped for the first time in the second half of 2002, falling by 6%, according to Symantec's Internet Threat Report. But at the same time the number of vulnerabilities shot up significantly, with 2,524 new vulnerabilities reported in 2002, 81.5% over 2001. Power and energy companies saw the highest level of hacking and cracking attempts over the last six months of last year, with financial companies second. South Korea was cited as the source of many of the attacks, both because of the increased use of broadband Internet access in the country, as well as its usefulness as a hopping-off point for hackers. Hacking incidents from South Korea grew 62% between July and December last year. (The Register 3 Feb 2003)
http://www.theregister.co.uk/content/55/29149.html

*Category 31.1* *Surveys, studies, audits of security*

2003-02-04 **cyber attacks hacking Internet vulnerability report**

NIPC/DHS

February 03, eWeek — Cyber attacks decline; vulnerabilities surge. The number of attacks on Internet-connected machines decreased over the past six months while the number of software vulnerabilities continued to skyrocket, according to a new report. This supports the conventional wisdom that most attackers search for a few vulnerabilities to exploit and will abandon their efforts if these vulnerabilities are unavailable," the report concludes. The report, published by Symantec Corp., of Cupertino, Calif., is based on data from more than 400 companies. The company said it recorded more than 2,500 newly identified vulnerabilities in various software products during all of 2002, an 81.5 percent increase over the previous year. Several factors may have contributed to this increase, including the huge jump in recent years in the number of researchers looking for vulnerabilities. Once again, attackers in the United States were by far the most eager to exploit those vulnerabilities and accounted for more than 35 percent of all of the attacks during the reporting period. South Korea, China, Germany and France rounded out the top five. However, the South Koreans appear to have the most attackers per capita among countries with the largest online populations, launching 23.7 attacks per 10,000 Internet users. The U.S. is not in the top 10 on this list.

*Category 31.1* *Surveys, studies, audits of security*

2003-02-04 **network attacks vulnerabilities corporate increase rise fall vulnerabilities**

NewsScan

RISING NUMBER OF NETWORK ATTACKS AND VULNERABILITIES
The Internet security firm Symantec says that the number of cyber attacks on corporate networks rose 20% in the second half of last year compared to the same period the previous year. The good news, though, is that the number actually declined by 6% compared to the first six months of 2002. The number of vulnerabilities to such attacks jumped 81%, comparing the last half of 2002 to the last half of the previous year; however, Symantec chief technology officer Robert Clyde noted that the increased number of vulnerabilities may be largely the result of a greater tendency of companies to admit their problems: "It could be that more vendors are reporting vulnerabilities as they are patched." (Reuters/San Jose Mercury News 4 Feb 2003)

*Category 31.1* *Surveys, studies, audits of security*

2003-02-11 **cyber terrorism cyberspace threats infrastructure protection international**

NIPC/DHS

February 07, Medill News Service — Don't underestimate cyberterrorists, experts warn. The Internet is becoming a new battleground for warfare, according to experts concerned about the potential of a cyberattack to cripple the public infrastructure. The recent Slammer worm, which blocked Internet traffic and crippled some corporate networks for most of a weekend, is just a watered-down version of a cybercrisis that could disrupt everything from banks to water supplies, critics say. In the Mideast conflict, pro-Palestinian hackers have successfully taken down Web sites of the Israeli Parliament, the Israeli Defense Force, the Foreign Ministry, the Bank of Israel, the Tel Aviv Stock Exchange, and others, according to a report by Dartmouth College's Institute for Security Technology Studies. Dartmouth's study charts how political cyberattacks often precede physical attacks. Cyberattacks after U.S.-led military action are "extremely likely" and could possibly be catastrophic, according to the report. Information systems—like electrical infrastructures, water resources, and oil and gas—should be considered likely targets, it warns. While cyberattacks can take a variety of forms and may originate from terrorist groups or targeted nation states, they are more likely to be launched by sympathizers or thrill-seekers, according to the institute's report.

*Category 31.1* *Surveys, studies, audits of security*

2003-03-07 **survey forecast US firms disaster recovery business continuity unprepared calamity**

NIPC/DHS

March 04, eSecurity Planet.com — Survey says U.S. firms unprepared for disasters. A large percentage of U.S. companies are unprepared to face business and IT outages caused by a severe calamity, according to the results of a survey released by research firm Gartner Dataquest Tuesday. The survey found that one third of U.S. businesses face the loss of critical data or operational capability in the wake of a disaster, unless investments toward disaster preparedness planning are made. Tony Adams, principal analyst for Gartner Dataquest's IT Services group, said "Preparation is the key, and without adequate investment for protection of critical systems, the repercussions of disasters will be lengthier and more costly." But cost is one of the primary reasons many of the companies surveyed cited for not having a disaster preparedness plan. "IT managers are not investing appropriately in disaster plans because they do not have a budget to accomplish their needed readiness," Adams said. Most disaster preparedness experts say that sophisticated real-time remote backup capabilities are the foundation of disaster recovery plans. In other words, it's all about redundancy. In the wake of September 11, 2001, Lee Clarke, associate professor of Sociology at Rutgers University — and an expert in organizations, technology and disasters — told Internetnews.com that the redundancy must be "meaningful." For instance, Clarke noted that many of the organizations in the World Trade Center had their disaster facilities in one of the other towers or buildings that were part of the complex.

*Category 31.1* *Surveys, studies, audits of security*

2003-03-17 **NIST NSA security configuration IT profile document**

NIPC/DHS

March 10, Government Computer News — NIST and NSA draft safe-IT profiles. The National Institute of Standards and Technology (NIST) has partnered with the National Security Agency (NSA) to draw up Protection Profiles-basic security recommendations for 10 hardware and software areas. NSA also is developing implementation guides for configuring operating systems securely. A 2,000-page guide for Microsoft Windows 2000 is finished, and a guide for Windows XP is in beta evaluation, said William Billings, chief of operational network evaluation for NSA's Systems and Network Attack Center. In addition, the Defense Information Systems Agency's (DISA) soon-to-be-released Gold Disk tool will apply security configurations to operating systems. The Gold Disk is part of DISA's Security Technical Implementation Guidelines (STIGs), which parallel the NSA guides. Profile development, which began about two years ago, already is complete for OSes, firewalls, intrusion detection systems, tokens and public-key infrastructures. Profiles should be ready by mid-2003 for wireless systems, browsers, databases, virtual private networks and biometric products.

*Category 31.1* *Surveys, studies, audits of security*

2003-03-25 **cyber security lack United States US infrastructure protection**

NIPC/DHS

March 24, Federal Computer Week — States need cybersecurity focus. A Zeichner Risk Analytics LLC study released today found 36 state governments have failed to prepare, adopt and implement acceptable cybersecurity policies, which could have damaging consequences to citizen services, communication systems and critical utilities if the nation were to undergo cyberattacks. Following a yearlong review, the study found that only 14 states and the District of Columbia are in full compliance with the Gramm-Leach-Bliley Act of 1999, which requires federal agencies and states to prepare cybersecurity guidance for financial institutions. Fourteen other states have pending legislation and/or regulations for compliance, while 22 states have little or no cybersecurity activity. The study recommended that: 1) States adopt the National Association of Insurance Commissioners nationwide proposal, which provides an approach similar to that of states in compliance with the Gramm-Leach-Bailey Act; 2) States create a single, nationwide process for developing cybersecurity laws and policies; 3) A single public-private "focal point is badly needed" to coordinate strategy.

*Category 31.1* *Surveys, studies, audits of security*

2003-04-02 **software piracy declines Software Business Alliance**

NewsScan

SOFTWARE PIRACY RATES FALLING WORLDWIDE
A report by the Software Business Alliance and market research firm IDC says that software piracy rates (measured by the amount of business installed without a license) have declined in many countries since 1996: down by 30% in Egypt; 28% in Ireland; 14% in Colombia; 20% in South Korea. Pointing out that reductions in piracy rates lead to increased sales and improved government economies, the authors of the report say that the countries with most to gain from curbing software piracy are ones where the rates are highest: China (92%) and Russia (87%). The U.S. has the lowest piracy rate (25%). (San Jose Mercury News 2 Apr 2003)

*Category 31.1* *Surveys, studies, audits of security*

2003-04-03 **critical infrastructure protection challenges Homeland Security**

NIPC/DHS

February 28, General Accounting Office — Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors. The General Accounting Office has released report GAO-03-233 titled "Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors." With computer interconnectivity comes a threat: both physical and cyber assets are potentially vulnerable to computer-based attack. In response, Presidential Decision Directive 63 (PDD 63, May 1998) called for a range of actions to improve the nation's ability to detect and respond to serious infrastructure attacks. GAO examined four specific agencies—the Departments of Health and Human Services, Energy, and Commerce, and the Environmental Protection Agency—and found that the agencies have made progress in implementing several PDD 63 requirements. However, none of the agencies has fully implemented all requirements. GAO also examined private-sector groups known as Information Sharing and Analysis Centers (ISACs) for five specific industry sectors—information technology, telecommunications, energy, electricity, and water supply. ISACs serve as clearinghouses for their sectors to share information. For other suggested activities, such as establishing baseline statistics on computer security incidents, progress is mixed. Both the agencies and the ISACs identified challenges and obstacles to undertaking CIP activities. Agency-identified challenges included coordinating security efforts for critical assets with the General Services Administration, which may often be responsible for protecting agency facilities that house critical assets. The ISACs identified obstacles to information sharing, both between the sectors and the government and within the sectors. In particular, they noted concerns that information reported to the government could be subject to public release under the Freedom of Information Act.

*Category 31.1* *Surveys, studies, audits of security*

2003-04-07 **warning survey study Web server Microsoft Internet Information Server vulnerability HTTP Netcraft**

NIPC/DHS

April 02, Security News Portal — 75% of all web servers running MS IIS 5.0 are vulnerable to exploitation. Three-quarters of web sites running Microsoft's Internet Information Server 5.0 software to serve web pages have the WebDAV protocol enabled and thus remain open to a serious vulnerability which was announced by Microsoft last month, the latest web server survey from Netcraft says. Microsoft issued a security alert on March 17 regarding a buffer overflow vulnerability which allows attackers to execute arbitrary code on Windows 2000 machines. The survey found 767,721 IPs running IIS 5.0 and offering WebDAV and 273,496 IPs running IIS 5.0 with the protocol turned off. The monthly survey looks at web server software usage on internet-connected computers, collecting and collating as many hostnames as can be found providing an HTTP service. Each is systematically polled with an HTTP request for the server name. The March survey received responses from 39,174,349 sites. Additional information may be found on the Netcraft Website:
http://news.netcraft.com/archives/2003/03/

*Category 31.1* *Surveys, studies, audits of security*

2003-04-09 **Internet fraud crime triples**

NewsScan

INTERNET FRAUD COMPLAINTS TRIPLE
Complaints about fraudulent schemes perpetrated over the Internet tripled in 2002 from the previous year, with the most common grievance being auction fraud, followed by non-delivery of promised merchandise, credit card fraud and fake investments. According to a report from the Internet Fraud Complaint Center, which is run by the FBI and the National White Collar Crime Center, the 48,252 complaints referred for prosecution in 2002 represent only a fraction of the crimes authorities believe are occurring. The center also received almost 37,000 other complaints that did not constitute fraud, but involved such things as spam, illegal child pornography and computer intrusions. The report says 80% of known fraud perpetrators and about 71% of complainants are male. Fraud complaints originated in all parts of the country, with a third coming from California, Florida, Texas and New York. One of the most persistent scams described in the report is the infamous "Nigerian letter," which urges victims to pay an upfront fee (characterized as a bribe to the government) in order to receive non-existent funds from the "Government of Nigeria." There were 16,000 complaints related to that scam in 2002, up from 2,600 in 2001. (AP 9 Apr 2003)

*Category 31.1* *Surveys, studies, audits of security*

2003-04-10 **critical infrastructure protection information security progress report**

NIPC/DHS

April 08, The General Accounting Office — Information Security: Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures. On April 8, the General Accounting Office (GAO) published report GAO-03-564T titled “Information Security: Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures.” Significant information security weaknesses at 24 major agencies continue to place a broad array of federal operations and assets at risk of fraud, misuse, and disruption. Although recent reporting by these agencies showed some improvements, GAO found that agencies still have not established information security programs consistent with the legal requirements. For example, periodic testing of security controls is essential to security program management, but for fiscal year 2002, 14 agencies reported they had testing the controls of less than 60 percent of their systems. Further information security improvement efforts are also needed at the governmentwide level, and these efforts need to be guided by a comprehensive strategy in which roles and responsibilities are clearly delineated, appropriate guidance is given, adequate technical expertise is obtained, and sufficient agency information security resources are allocated.

*Category 31.1* *Surveys, studies, audits of security*

2003-04-14 **Federal Bureau Investigation FBI technology investment return Interner crime fraud thwart security privacy**

NIPC/DHS

April 10, National Journal — FBI director says tech investments are paying off. FBI Director Robert Mueller on Thursday highlighted the bureau's success in thwarting terrorist attacks, counterintelligence operations and confronting cyber crime in his budget presentation to the Senate Commerce, Justice and State Appropriations Subcommittee. After counterterrorism and counterintelligence, Mueller said that tackling cyber crime was the bureau's third priority area. "Unfortunately, we are seeing explosive growth in cyber crime-both traditional crimes such as fraud and copyright infringement that have migrated online, and new crimes like computer intrusions and denial of service attacks," he said. Over the past six years, the number of such cases grew from 113 to 2,300. The FBI's Cyber Program would "focus on identifying and neutralizing: 1) individuals or groups conducting computer intrusions and spreading malicious code; 2) intellectual property thieves; 3) Internet fraudsters; and 4) online predators that sexually exploit or endanger children," he said. The agency has been consolidating those operations into a new Cyber Division at its headquarters, and its total budget request for fiscal 2004 is $234 million to protect against cyber-based attacks and high-tech crimes, including 77 new agents.

*Category 31.1* *Surveys, studies, audits of security*

2003-04-17 **Internet Insecurity Index RSA study survey statistics mathematics**

NIPC/DHS

April 15, AtNewYork.com — "Internet Insecurity Index" unveiled at conference. Online encryption firm RSA Monday launched its "Internet Insecurity Index" — a simple one-to-ten scale that measures how secure electronic data is each year. Given the amount of attacks, Jim Bidzos of RSA currently ranks 2003 at about a 6 and a half. Bidzos pointed to more than 62,000 hacking incidents last year as a rally cry for better safeguards. In addition to commonplace server strikes, Bidzos said ATM and wireless networks are the new target of hackers. "Part of the price is not having security designed in the first place," Bidzos said. "We found 30 percent of ISPs have no info security plans in place with 33 percent deciding that online security is not a priority." The threat index also identifies last year's $59 billion in data theft as a major impact on how safe the Internet is. The one bright area, according to RSA's index report was the U.S. government. Bidzos said the creation of the Department of Homeland Security and a national strategy to secure cyberspace marked a turning point in how the government is dealing with online threats. California's move to require companies to publicly disclose security breaches may also have a major impact on how well companies secure their networks and data.

---

*Category 31.1* *Surveys, studies, audits of security*

2003-05-07 **Spam Email virus British ISP BT Openworld monitor 25 million**

NIPC/DHS

May 07, Net4Nowt — BT Email: 41% Spam and 1 in 220 has Virus. British ISP BT Openworld monitored mails sent by its customers between March 17, 2003 and March 23, 2003. Of more than 25 million emails scanned, nearly 11 million were detected and trapped as spam. This equates to a weekly average of 41 per cent. Thursday was the most popular day for spamming, with more than four million examples detected. Sunday polled the highest percentage of spam with the proportion rising to 51 percent of all messages sent. To make matters worse, the filters also detected over 113,000 viruses - one for every 220 mails sent.

---

*Category 31.1* *Surveys, studies, audits of security*

2003-05-20 **women dominate text-messaging UK competent**

NewsScan

WOMEN DOMINATE TEXT MESSAGING IN UK
A survey by the Mobile Data Association found that a full 74% of female respondents said they'd used text messaging in the last two minutes, compared with 26% of males, and about half the women said they'd prefer receiving a sentimental text message to a card on special occasions. Two-thirds of the women described themselves as test-messaging competent, compared with only a third of the men. Text messaging the UK reached an all-time high in March, when 1.7 billion messages were sent. (BBC News 20 May 2003)

---

*Category 31.1* *Surveys, studies, audits of security*

2003-05-27 **OMB federal IT security Office Management Budget systems progress agencies GISRA**

NIPC/DHS

May 27, Government Computer News — OMB: federal IT security's better but still not good enough. Agencies have made progress in evaluating and securing systems, but serious and pervasive problems persist, according to the Office of Management and Budget (OMB). OMB released its second report to Congress last month under the Government Information Security Reform Act. The report compares the performance of 14 departments and 10 independent agencies in fiscal 2002 with baseline data collected in 2001. Despite across-the-board improvements in eight areas, more than a third of federal systems overall still have not been assessed for risk and lack up-to-date security plans, and less than half have been certified and accredited for use. The 2001 GISRA report identified government-wide areas of weakness: lack of performance measures and senior management attention, poor security education and awareness, failure to include security in IT capital planning, failure to ensure security of contractor services, and poor information sharing.

---

*Category 31.1* *Surveys, studies, audits of security*

2003-05-29 **cyber-attack survey companies organizations authorities FBI computer crime negative publicity**

NIPC/DHS

May 29, eWEEK — Cyber-attack costs down, says survey. The percentage of organizations that detected unauthorized use of their systems fell to 56 percent from 60 percent a year earlier, according to the latest "Computer Crime and Security Survey" from the Computer Security Institute and the FBI. The 2003 survey also shows that companies are still failing to report most of their intrusions and attacks to law enforcement. Only 30 percent of the survey's respondents said they had contacted the authorities after an attack, a drop from 34 percent a year ago. Negative publicity and fear that competitors would use the information to their advantage were the top two reasons organizations cited for failing to talk to law enforcement after an attack. Among the most frequently seen attacks, viruses, laptop misuse and unauthorized access by insiders continued to lead the way, according to the survey. The 530 organizations surveyed reported $201.8 million in losses this year; in 2002, 503 respondents lost $455.8 million.

*Category 31.1* *Surveys, studies, audits of security*

2003-05-30 **technical errors government sites web bug Business Internet Group San Francisco applications server blank pages content Keynote Systems internal**

NIPC/DHS

May 30, Government Computer News — Study finds technical errors in government sites. A survey of 41 federal Web sites found that 68 percent will present some sort of bug within the first 15 minutes of a visit, according to the Business Internet Group of San Francisco. Most glitches were application server and Web server errors such as blank pages, embedded content errors and the 500 internal server error, the survey found. Diane Smith, the group's research director, said she selected the sites because they are used in the Keynote Government Internet Performance Index from Keynote Systems Inc. of San Mateo, Calif. The index includes sites of 10 Cabinet departments, the White House, both houses of Congress and several large agencies. Smith said she visited each Web site for up to 15 minutes and explored as if she were unfamiliar with the agency. She stopped exploring at the first error, even if the 15 minutes were not yet up. Twenty-five of the buggy sites had blank pages and internal server errors. Smith said she found three other sites with data errors, such as a wrong page link or bad data returned from a database query.

*Category 31.1* *Surveys, studies, audits of security*

2003-06-02 **Software piracy 2002 vietnam russia ukraine indonesia china BSA pirate piracy illegal copy**

NewsScan

SOFTWARE PIRACY DOWN IN 2002
Global business software piracy declined slightly last year, thanks to increased education efforts and more aggressive tactics by the software industry, according to a report released Tuesday by the Business Software Alliance. The study estimates that 39% of business software installed on computers worldwide in 2002 was not legally obtained, with the most common violation being purchasing a single legal copy and installing it on several computers, said Robert Holleyman, president and CEO of the BSA. To combat that scenario, the alliance is continuing to circulate brochures on piracy and is conducting amnesty campaigns urging businesses to pay for additional copies without threat of prosecution. In addition, companies like Microsoft have instituted new restrictions, requiring special activation codes for its software that are tied to a single computer. It's too early to tell how well these strategies have worked in reducing piracy, said Holleyman. The country with the largest percentage of illegal software was Vietnam (95%), followed by China (92%), and Indonesia, Russia and the Ukraine, all at 89%. (AP/Wall Street Journal 2 Jun 2003)

*Category 31.1* *Surveys, studies, audits of security*

2003-06-04 **boradband risk vulnerability hackers firewall homeland security**

NewsScan

BROADBAND BROADENS RISK AS WELL AS PERFORMANCE
A study of 120 broadband users conducted by the National Cyber Security Alliance (a group of business and government entities) has found that although 77% think their systems are protected from outside hackers, fewer than 60% had installed firewalls to keep their systems safe. "The disconnect means we have to do more to educate people," says Alliance spokesman Keith Nahigan, who is also a consultant to the national Office of Homeland Security. Despite the vulnerability of their systems, 86% of broadband users keep sensitive information on their computers. Broadband systems are "always-on" and Nahigan notes: "When you have your connection open all day and all night, it's easier for hackers to get in." (New York Times 4 Jun 2003)

*Category 31.1* *Surveys, studies, audits of security*

2003-06-09 **kids spam symantec research statistics age study**

NewsScan

KIDS GET SPAMMED, TOO
A new study by Applied Research probably won't surprise anyone, but it does highlight the consequences of the current spam-run-amok Internet culture. According to the research, which was commissioned by Internet security firm Symantec, more than 80% of kids (aged 7 to 18) get "inappropriate" unsolicited commercial e-mail on a daily basis, and their spam looks just like yours: sweepstakes offers (80%), "relationship-related" e-mail (62%), financial come-ons (61%), weight-loss ads (55%), pharmaceutical ads (51%), and, of course, p*rn (47%). Symantec has characterized spam as a new summer hazard, right up there with sunburns and insect bites. Almost half of the 1,000 respondents said they were online more than two hours a day in the summer, compared with only 23% during the school year. (CNet News.com 9 Jun 2003)

*Category 31.1* *Surveys, studies, audits of security*

2003-06-12 **spam hackers symantec virus threats**

NewsScan

COMPANIES WORRY MORE ABOUT SPAM THAN HACKERS
Businesses are far more concerned about the rising flood of spam that's engulfing their networks than they are about run-of-the-mill hackers, according to a survey of 2,800 silcon.com readers. But the biggest worry is over virus attacks, with 71% of respondents citing viruses as the biggest threat to their businesses. Symantec's Kevin Chapman says he's not surprised by the results. "Spam has now gone way beyond the quick and easy 'hit the delete button and it's gone' solution. It's now a really big problem. From the employees' point of view it is about productivity and the sheer annoyance of dealing with all these e-mails. For the employer it is about bandwidth and other network resources issues." But aside from productivity and bandwidth concerns, there's another consequence that could be lurking out there, says Martino Corbelli, marketing director for SurfControl. "Some of these spam e-mails have completely inappropriate content which can create serious problems for the employer on a legal basis. There may be somebody who feels they should be protected from p*rnographic content, for example, and in some cases they may be prepared to sue their employer if they feel they are being exposed to offensive material on the company's network." (Silicon.com 12 Jun 2003)

*Category 31.1* *Surveys, studies, audits of security*

2003-07-07 **security major universities 80% policy importance hijack school computers launch attacks EDUCAUSE**

NIPC/DHS

July 07, Network World — University net execs face variety of security challenges. A recent Emory University survey of 13 major U.S. universities found that 80% agreed that network security policies are very important, but only half of them are taking steps to combat the growing flood of security breaches. Staffing and budgeting were cited as the main obstacles. A new worry is the legal liabilities created for a university when someone hijacks a school computer and uses it to launch attacks against networks and computers elsewhere on the Internet. "Desktops and laptops are not professionally administered," says Rodney Petersen, of EDUCAUSE, a nonprofit group focused on advancing higher education through IT. "The freedom to allow faculty, staff, and students to alter system configurations and install software make PCs particularly vulnerable," he says.

*Category 31.1* *Surveys, studies, audits of security*

2003-07-09 **NIST security products standardization intrusion detection systems effectiveness analyze systems**

NIPC/DHS

July 09, Washington Technology — NIST: Security products need standardization. Despite wide use across government, intrusion detection systems have no standard metrics to measure their performance, according to a new report by the National Institute of Standards and Technology. The report "An Overview of Issues in Testing Intrusion Detection Systems" concluded that there are no comprehensive and scientifically rigorous methodologies to test the effectiveness of intrusion detection systems, which monitor and analyze systems and network traffic for possible hacker attackers or misuse. The report may be viewed here:
http://csrc.nist.gov/publications/nistir/.

*Category 31.1* *Surveys, studies, audits of security*

2003-07-21 **identity theft crime impersonation fraud credit cards social security**

NewsScan

IDENTITY THEFT: A CRIME THAT PAYS?
The number of victims that have fallen prey to identity thieves is severely underreported, according to a study by Gartner Research, which estimates that 3.4% of U.S. consumers — about 7 million adults — have suffered ID theft in the past year. Moreover, identity thieves generally get away with it — arrests are made in only one out of every 700 cases. "The odds are really stacked against consumers," says Gartner VP Avivah Litan. "Unfortunately, they are the only ones with a vested interest in fixing the problem." Typically, victims of ID theft learn of the crime a year or more later after it happens — long after the trail has gone cold. "It is different from payment fraud, where the thief takes a credit card number and consumers are innocent until proven guilty. With identity theft, it is the opposite: Consumers are thought to be guilty until proven innocent," says Litan. "There is a serious disconnect between the magnitude of identity theft that innocent consumers experience and the [financial] industry's proper recognition of the crime. Without external pressure from legislators and industry associations, financial services providers may not have sufficient incentive to stem the flow of identity crimes." (CNet News.com 21 Jul 2003)

---

*Category 31.1* *Surveys, studies, audits of security*

2003-07-29 **Farm Internet access broadband**

NewsScan

WHAT ARE THEY DOING DOWN ON THE FARM?
Answer: surfing and sending e-mail. An Agriculture Department survey has found that 48% of the 2 million farms in the U.S. are connected to the Internet. The next big push will be to upgrade from dialup to broadband connections. Because the scarcity of rural subscribers doesn't justify the cost of laying cable or building rural areas, Congress last year passed a farm bill pushed by President Bush, that provided $100 million in loans and loan guarantees over the next six years to encourage companies, cities and counties to invest in broadband in rural areas. (AP/San Jose Mercury News 29 Jul 2003)

---

*Category 31.1* *Surveys, studies, audits of security*

2003-09-04 **colleges vigilant viruses blaster U.S. infected computers log on campus students**

NewsScan

COLLEGES MORE VIGILANT AGAINST VIRUSES
Reeling from the recent rash of computer viruses, U.S. colleges and universities are taking unusually aggressive steps against further infection by returning students. University of North Texas technicians report they're eradicating viruses from about 10 PCs every hour, charging students a mandatory $30 cleaning fee for the service. Students cited for infectious computers must show proof they've been fixed before they can log back onto the campus network. Vanderbilt University reports about 25% of returning students have infected computers and Oberlin College IT director John Bucher says his department found viruses on nine out of every 10 Windows-based PCs owned by students. Meanwhile, some schools managed to avert catastrophe by filtering e-mails and using antivirus software. Duke University computer security officer Christopher Cramer says his school filtered out 2.5 million infected e-mail messages, limiting the damage to only a few dozen PCs, and Temple University's mandatory use of Symantec's antivirus software kept the infection rate down to about 400 PCs out of 35,000 students. "If it had been 10-fold, it would have crashed the network," says Temple chief information security officer Ariel Silverstone. (AP 4 Sep 2003)

---

*Category 31.1* *Surveys, studies, audits of security*

2003-09-04 **indetity theft account credit card stolen personal information bank internet transaction**

NewsScan

VICTIMS OF IDENTITY THEFT AND ACCOUNT THEFT
The Federal Trade Commission says that the personal credit information of about 3.3 million U.S. consumers has been used last year to open fraudulent new bank, credit card or utility accounts or to commit other crimes, and that an addition 6.6 million people fell victim to account theft to steal from the victim's existing accounts. Half of all victims knew the method by which the thieves had obtained the personal information. About 25% of the victims said the information had been stolen through either the mail or the loss of a wallet, and 13% percent said it had been stolen in the course of a purchase or another transaction. (New York Times 4 Sep 2003)

---

*Category 31.1* *Surveys, studies, audits of security*

2003-09-11 **Net Attack ports ISP block internet worms malicious program SANS Institute Inc. customers**

NIPC/DHS

September 11, IDG News Service — Study: ISPs should block 'Net attack ports. Internet service providers (ISPs) should block access to communications ports on their customers' computers which are commonly exploited by Internet worms and other malicious programs, according to a report by Johannes Ullrich of the SANS Institute Inc. Leaving the ports open offers little to customers, while needlessly exposing them to infection and making it more likely that ISPs will be overwhelmed by future virus outbreaks, the report said. Many ISPs already block some or all of the ports named, while others offer customers free personal firewall software to install on their home computers. However, home Internet users often lack the technical knowledge necessary to install and configure a firewall, Ullrich said. The report is available on the SANS Institute Website: http://www.sans.org/rr/special/isp_blocking.php

*Category 31.1* *Surveys, studies, audits of security*

2003-09-15 **big brother syndrome IM U.K. UK work job personal use colleagues**

NewsScan

IM-ING HABITS DIFFER IN U.S., U.K.
Using Instant Messenger at work to flirt with colleagues, complain about the boss and gossip about co-workers are among the most common IM themes — at least in the U.K., where 65% of survey respondents say they use IM for personal purposes during work hours. "If you're leaning forward and typing away at your machine, who's to know what you're typing about," says Nigel Hawthorn, whose cybersecurity firm, Blue Coat Systems, conducted a poll of some 300 firms in the U.K. and the U.S. Half the British respondents admitted to spicing up their IMs with abusive language; 40% used IM-ing to conspire with colleagues during conference calls; and nearly a third confessed to "making sexual advances" via IM. U.S. respondents, meanwhile, were much more circumspect in their IM habits, with fewer than one in five using IM to comment on senior management or to flirt. The difference, says Hawthorn, is probably attributable to the Big Brother syndrome. While nearly 60% of Brits were pretty sure their bosses couldn't monitor their IM activities, 71% of U.S. respondents believed — correctly — that their IM messages could be traced back to them. (Reuters 15 Sep 2003)

*Category 31.1* *Surveys, studies, audits of security*

2003-09-17 **europe download movie music free file sharing spending money in CDs**

NewsScan

EUROPE'S DOWNLOADERS ARE DIFFERENT
Unlike most Internet downloaders in the U.S., who tend to be teenagers trolling for free tunes, European downloaders are avid music and video fans, as well as regular shoppers who don't mind spending money on CDs in stores. "They are more likely to listen to digital radio and visit artist Web sites," says Jupiter Research analyst Mark Mulligan. "There is compelling evidence that this group is the bedrock community for those willing to pay for legitimate (online) music services in the future." And unlike the U.S. situation, where record labels are waging an all-out war on music swappers, in Europe, labels are pursuing a gentler approach, promoting industry-backed services and educating consumers that downloading copyrighted material is illegal. Europeans also tend to download more videos than their U.S. counterparts — 15% said they downloaded a movie every month from a free file-sharing service with Spain topping the list at 38%. In contrast, about 12% of U.S. Internet users download a video file each month. Mulligan says Hollywood should take note and avoid the hardline tactics of the music industry. "I think there's definitely an opportunity for television companies and movie studios alike to harness an emerging pattern of consumption here." (Reuters 17 Sep 2003)

*Category 31.1* *Surveys, studies, audits of security*

2003-10-01 **music download piracy RIAA lawsuit copyright infringement**

NewsScan

MUSIC DOWNLOADING NUMBERS FALL
The lawsuits filed in September by the Recording Industry Association of America (RIAA) against 261 people accused of illegally downloading copyrighted material seem to have been largely responsible for a 40% decrease in usage of the file-swapping service Kazaa. A typical user reaction is this one given by a 27-year-old marketing consultant in New York: "I've been holding off. I don't want to get sued. I was never a big user per se, but I do have a ton of music files." However, Chicago intellectual property lawyer Leonard Rubin suggests that the RIAA's victory may be short-lived: "The record companies are winning a skirmish, but it's still an open question as to whether they're winning the war. What they're not doing is figuring out how to either restore some favor among music lovers, or work with the system to figure out some way to please these people who they are now offending."(San Jose Mercury News 1 Oct 2003)

*Category 31.1* *Surveys, studies, audits of security*

2003-10-07 **cyber crime organized Internet Britain scam fraud pornography**

NewsScan

CRIMINALS GO WHERE THE ACTION IS: THE INTERNET
Len Hynds, the head of Britain's National Hi-tech Crime Unit (NHTCU), says that organized crime syndicates have stepped up their presence on the Internet, operating extortion rackets, child pornography rings and elaborate financial scams: "Organized crime is turning to the weakest element in the chain, which is the people. It's the hands on the keyboard on either end of the transaction that is the actual weak point. Organized crime in all its guises is extremely flexible. It does spot the new and lucrative opportunity." One urgent problem is the increase in child pornography online, and Hynds says his group is taking the problem very seriously: "We are focusing on the organized groups that are making money out of peddling child pornography on the Internet. We are doing that in partnership with business and industry. We've deployed officers from this office overseas to physically remove children to places of safety." (USA Today 7 Oct 2003)

*Category 31.1* *Surveys, studies, audits of security*

2003-10-21 **employee net usage Internet work monitor survey**

NewsScan

WORKERS PLAYING ON THE NET
About half of the employees polled in an annual survey conducted for Websense admit they spend time accessing non-work-related Web sites during the work day, with the time spent joy-surfing averaging about 3.4 hours a week. The top recreational lure was news, cited by 77% of the survey respondents, followed by personal e-mail (52%), shopping (51%), online banking (47%), and investing (35%). Predictably, male employees accessed sports sites a lot more often than female (47% vs. 17%). And what do the bosses think about all this? Seventy-two percent of managers at large companies expressed concern over their workers' surfing habits, while only 54% at smaller companies saw it as a problem. (Wall Street Journal 21 Oct 2003)

*Category 31.1* *Surveys, studies, audits of security*

2003-10-22 **Spam hurt e-mail use messages block millions businesses web list link attachment Pew American Life Project**

NIPC/DHS

October 22, Reuters — Spam beginning to hurt e-mail use, report says. Half of all Internet users say "spam" e-mail messages has made them less trusting of all e-mail in general, according to a report released Wednesday, October 22 by the Pew Internet and American Life Project. One in four say they now use e-mail less because of spam. The group's June survey of 1,400 Internet users found that most feel they can do little to block the billions of unwanted pitches that arrive in their inboxes on a daily basis. Spam now comprises roughly half of all e-mail messages, according to several estimates, costing businesses billions of dollars in wasted bandwidth and lost productivity. Most respondents said they did not post their e-mail addresses to Web sites in an effort to keep off spammers' lists, and many said they used filters to block spam at work or home. But others admitted to behavior likely to perpetuate the problem. Some 7% said they had bought a product or service that was offered in an unsolicited e-mail, while one-third said they had clicked a link to get more information. Two-thirds said they had clicked a link to be removed from a spammer's e-mail list, an activity consumer advocates say is likely only to generate more spam.

*Category 31.1* *Surveys, studies, audits of security*

2003-10-23 **Kansas Health Department Environment High Risk Information Systems Protection fraud disruption bioterrorism password-cracking tools 11 hours 90 percent cracked anti-virus software**

NIPC/DHS

October 23, The Lawrence Journal (Kansas) — Kansas Department of Health and Environment computers at 'high risk'. The Kansas state agency in charge of protecting the public's health and safety is having trouble protecting its own computers and information system, according to an audit released Wednesday, October 22 by the Legislative Division of Post Audit. Operations of the Kansas Department of Health and Environment (KDHE) "were at an extremely high risk of fraud, misuse or disruption," the auditors concluded. KDHE is a large regulatory agency that collects records and information about Kansans. The agency is the leader for dealing with hazardous wastes, epidemics, immunizations and, most recently, the state's bioterrorism program. Using a standard password-cracking software, auditors were able to determine more than 1,000 employee passwords, which is about 60 percent of the total, in three minutes. Ninety percent of the passwords were cracked within 11 hours. During a lunch hour, auditors easily walked into empty offices where computers were logged on to the network and unlocked. The audit also revealed that many agency computers were infected with computer viruses that could send files and passwords to computer addresses outside the agency, and some 200 computers had no anti-virus software installed. After meeting with auditors, KDHE officials "acted strongly and swiftly to address these problems," according to the audit report.

*Category 31.1* *Surveys, studies, audits of security*

2003-10-24 **Internet fraud identity theft report FTC**

NewsScan

INTERNET FRAUD UPDATE
The Federal Trade Commission says that complaints of Internet-related identity theft more than tripled last year, to 2,352 last year from the year before. Jay Foley of the Identity Theft Resource Center says, "Online fraud is becoming as big an issue for eBay and AOL as security is for Microsoft." Typically, eBay covers buyers or sellers for up to $200 (or $500 for some listings) if an item is not delivered or is in bad condition, though there is a $25 processing fee. Posting safety tips for eBay transactions are listed at at www.ebay.com/securitycenter. (USA Today 24 Oct 2003)

*Category 31.1* *Surveys, studies, audits of security*

2003-10-27 **cyber crime Brazil laboratory hacker syndicate legislation**

NewsScan

CYBERCRIME: THE BRAZILIAN CONNECTION
Brazil has become a laboratory for cybercrimes such as identity theft, credit card fraud, and online vandalism. Hacker Assunção Marcos Flávio says: "If things go on like this, there'll be no more bank holdups with guns. All robberies will be done over the Net." Already, police in cities such as São Paulo, Rio de Janeiro and Brasília are finding it difficult to keep pace with hacker syndicates. Ronaldo Tossunian of the electronic crime division of the São Paulo police department points a finger at Brazilian law-makers: "We don't have the specific legislation for these crimes like they do in America and Europe. Just breaking in isn't enough to make an arrest, which means there's no deterrent." Brazil's hackers are as strong and resourceful as they are because they have little to fear legally. (New York Times 27 Oct 2003)

*Category 31.1* *Surveys, studies, audits of security*

2003-10-29 **enormous data pile up UC Berkeley report**

NewsScan

WHOLE LOTTA DATA PILING UP
A study conducted at UC Berkeley reports that in 2002 people around the globe created enough new information to fill 500,000 U.S. Libraries of Congress (which is the equivalent of a stack of books 30 feet high per person). Berkeley Professor Peter Lyman says that how and to what extent all that information is used will be the subject of another study. (USA Today 29 Oct 2003)

*Category 31.1* *Surveys, studies, audits of security*

2003-12-04 **movie piracy indeustry MPAA Motion Picture Association of America web sites copying difficult**

NewsScan

MOVIE PIRACY CONTINUES DESPITE INDUSTRY EFFORTS
Although film industry efforts to make illegal copying more difficult, piracy appears to have increased from previous years. The Motion Picture Association of America (MPAA) estimates that there are now 200,000 Web sites offering movies pirated by "ripping crews" (who recruit members around the world to obtain, edit, transfer and store films); these ripping crews are frequently assisted by people connected to the movie industry itself, such as cinema employees, workers at post-production houses and friends of Academy members. The MPAA and California law enforcement officials are planning how to enforce a new state law barring the illegal recording of motion pictures in movie theaters. (Los Angeles Times 4 Dec 2003)

*Category 31.1* *Surveys, studies, audits of security*

2003-12-17 **virus worm cleanup expense Britain UK study**

NIPC/DHS

December 16, SearchSecurity.com — Cost of virus cleanups goes up in Britain. Malicious code attacks are costing enterprises in the UK four times as much as they did in 2002, according to a recent study by Britain's Corporate IT Forum. The forum, an organization of IT professionals from some of the UK's largest blue-chip companies, estimates that each incident costs an average of $213,000 in man-hours and related costs. In contrast, a 2002 survey conducted by Britain's Department of Trade and Industry (DTI) and PricewaterhouseCoopers put the per-incident price tag at $52,000. Three quarters of the administrators recently surveyed reported an average of 365 man-hours lost. Of those, one-third reported an average of 3,080 man-hours lost. The report determined that enterprises with sturdy incident-response teams and procedures suffered fewer malicious code outbreaks and were able to trim costs. Most infections, it was determined, came from systems integrated with business partners and contractors.

*Category 31.1 Surveys, studies, audits of security*

2003-12-29 **cybercrime doubled scammers nigerians cash-sharing partnerships Internet Fraud**

NewsScan

CYBERCRIME MORE THAN DOUBLED IN 2003
This past year the Internet proved a lucrative haven for phishers, online auction scammers and Nigerians proffering cash-sharing partnerships, according to statistics from the Internet Fraud Complaint Center, which reports it received more than 120,000 online fraud complaints in 2003. That translates to an increase of 60% since 2002, when 75,000 complaints were processed. The Center provides cybercrime victims with a convenient process for filing complaints, which it then analyzes and routes to the appropriate FBI field office or local law enforcement agency for further action. (The Register 29 Dec 2003)

# 31.2 Estimates, guesses, predictions, forecasts concerning security

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-01-07 **cyber terrorism threat estimate overrated national security**

NIPC/DHS

January 07, Computerworld — Think Tank says the threat of cyberterrorism is overrated. A research paper released last month by the Center for Strategic &International Studies (CSIS), a Washington-based Think Tank, argues that computer networks and critical infrastructures are distinct entities and that the threat from cyberterrorism is far less serious than the government and the media contend. "While many computer networks remain very vulnerable to attack, few critical infrastructures are equally vulnerable," argues James A. Lewis, a CSIS analyst. "Computer network vulnerabilities are an increasingly serious business problem, but their threat to national security is overstated." However, Brenton Greene, deputy director of the National Communications System, an executive-branch agency responsible for maintaining and restoring communications during times of national crisis, said the physical and cyber aspects of critical infrastructure protection can't be separated. Major physical events will have digital ramifications and vice versa, said Greene. That's also the conclusion of the recently released annual report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, led by former Virginia Governor James S. Gilmore. "Cyberspace has been isolated and specialized, thus limiting its perceived relevance to day-to-day outcomes and even its relevance to what are viewed as clear and present homeland security threats," the commission stated.

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-01-07 **outsourcing concern secure coding vulnerablities threat**

NIPC/DHS

January 06, New York Times — Experts see vulnerability as outsiders code software. As American companies increasingly move their software development tasks out of their own offices to computer programming companies here and abroad, new concerns are being raised about the security risks involved. The companies providing outsourcing services say that they take all necessary precautions to limit risk. But the question of whether the booming business in exporting high-tech jobs is heightening the risk of theft, sabotage or cyberterrorism from rogue programmers has been raised in discussions at the White House, before Congress and in boardrooms. "I can't cite any examples of this happening - but what that means is we haven't found any," said James Lewis, director of the technology program at the Center for Strategic and International Studies in Washington. While operations in some countries, like the United States, Britain and India, are considered generally safe for such software outsourcing, nervousness is beginning to grow at companies and in the government about the possibility of abuse by hackers, organized crime agents and cyberterrorists in nations like Pakistan, the Philippines and Russia. It is easy to see why companies find the economics of outsourcing compelling; cost savings can be 25 to 40 percent. Forrester Research of Cambridge, Massachusetts, predicted in a recent report that the acceleration in outsourcing would result in 3.3 million American jobs' moving offshore by 2015. Forrester estimates that 70 percent of these jobs will move to India, 20 percent to the Philippines and 10 percent to China.

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-01-14 **malware viruses worms instant messaging predictions**

NewsScan

BRACE FOR ONSLAUGHT OF NEW VIRUSES
Computer users will be plagued with a host of new viruses this year, particularly worms deployed into instant messaging systems, predicts a senior technology consultant with UK-based Sophos. "Virus writers are most interested in creating the next super Windows worm, spread by e-mail or instant messaging, as these mass-mailing viruses carry the greatest impact," says Graham Cluley. "We expect more executable e-mail-aware worms this year, while more viruses are written which use instant messaging services." Sophos also expects to see an increase in the number of so-called "Backdoor Trojans," which can open up holes in operating systems so that crackers can control them from a remote location. Windows users are particularly at risk, as nine out of 10 of last year's top viruses were spread via e-mail on Windows platforms, with the most prolific being the Klez worm. So far, PDAs and mobile phones have remained largely free of virus problems, says Cluley. "There is no indication yet that we will see an avalanche of new viruses affecting mobile devices — virus writers are not interested in targeting the mobile phone until it becomes more developed and has a bigger, common platform." (Reuters 14 Jan 2003)

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-01-17 **music piracy sales projections prediction copyright intellectual property infringement**

NewsScan

AND THE MUSIC GOES 'ROUND AND 'ROUND — AND DOWN AND DOWN
As a result of music piracy over the Internet coupled with a general economic downturn, the music industry is reeling — global recorded music sales are set to fall this year for the fourth straight year. Media analyst Michael Nathanson says, "2003 will be the tipping point. The fundamentals continue to deteriorate and consolidation will have to happen." Industry critics say that the business of selling physical copies of music is hopelessly out-of-date in the Internet age, and music company executive are bewailing the creation of new generations of music fans who simply refuse to pay for music, when they can skirt laws to get it free on the Internet. Jay Berman, the chief executive of the trade association IFPI (International Federation of the Phonographic Industry), sees the challenge this way: "This is a time when different sectors of the music industry, for all their diverging interests, have one big common interest: namely to develop a new online music business and to fight piracy." (Reuters/USA Today 17 Jan 2003)

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-02-11 **Moore's Law growth technology density cost computational power nanotechnology**

NewsScan

MORE LIFE IN MOORE'S LAW
Moore's Law, which predicts that the number of transistors on a chip will double every two years, will "slow down" a bit in the coming years, says Intel co-founder Gordon Moore, for whom the law is named. "You really get bit by the fact that the materials are made of atoms." Alternatives to conventional chipmaking techniques, such as nanotechnology, are still in development, but haven't evolved to the point that they can take on silicon, says Moore, who notes that crafting single transistors is one thing, but "housing a billion of them on a chip is another." Still, scientific ingenuity has overcome conventional thinking in the past: "I remember we didn't think we could go beyond 1 micron because of optical lithography." (CNet News.com 9 Jul 2002)
http://news.com.com/2100-1001-942671.html?tag=fd_top

MOORE'S LAW GOOD FOR ANOTHER 10 YEARS
Moore's Law — the theory espoused by Intel co-founder Gordon Moore that the number of transistors on a computer chip would double every 18 months or so — is still valid, says Moore, who sees "no apparent roadblocks" for at least another decade. "It gets complicated and expensive, but the technological solutions seem to be there? Even if we get to the point where we can't squeeze any more [transistors] in there, we'll be putting billions of transistors on a chip. It's certainly not the end of creativity in the industry." Moore predicted that growth in the semiconductor industry would equal growth in the world's gross domestic product by 2017 if the industry continues at its current pace. (AP 10 Feb 2003)
http://apnews.excite.com/article/20030211/D7P4C9S81.htm

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-02-12 **National Infrastructure Protection Center NIPC global hacking advisory**

NIPC/DHS

February 11, NIPC — Advisory 03-002: National Infrastructure Protection Center "Encourages Heightened Cyber Security as Iraq - US Tensions Increase". The NIPC is issuing this advisory to heighten the awareness of an increase in global hacking activities as a result of the increasing tensions between the United States and Iraq. Attacks may have one of several motivations: 1) Political activism targeting Iraq or those sympathetic to Iraq by self-described "patriot" hackers; 2) Political activism or disruptive attacks targeting United States systems by those opposed to any potential conflict with Iraq; 3) Criminal activity masquerading or using the current crisis to further personal goals. Regardless of the motivation, the NIPC reiterates such activity is illegal and punishable as a felony. The U.S. Government does not condone so-called "patriotic hacking" on its behalf. Further, even patriotic hackers can be fooled into launching attacks against their own interests by exploiting malicious code that purports to attack the other side when in fact it is designed to attack the interests of the side sending it. During times of potentially increased cyber disruption, owners/operators of computers and networked systems should review their defensive postures and procedures and stress the importance of increased vigilance in system monitoring.

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-02-13 **forecast prediction cyber attack terrorism Internet subvert financial network**

NIPC/DHS

February 11, Newsday — In cyber-attack, the system bends, doesn't break. Experts met last weekend at the annual CyberCrime convention in Mashantucket, CT to model a scenario where cyber-terrorists decide to strike first in a potential cyber-war against unspecified enemies. Richard Hunter of Gartner, the research firm that proposed and conducted the high-tech war games, says the "significant" threat to the Net is not its collapse, but the possibility that terrorists could build an undetectable control network on top of it to monitor and filter Internet traffic. Then, Hunter said, the terrorists could "subvert the Internet and take it for their own purposes." At the same time he noted that diligent maintenance of computer networks in the private and public sector would prevent 90 percent of those attacks, and suggested a seat-belt law-like model could prod slackers into cleaning up their network acts. As it turns out, the greatest potential threat against the country's infrastructure is one against the nation's financial networks — an attack that requires little technical savvy, Hunter said. Terrorists with clean credentials could buy or even start a bank and get access to the financial clearing house. Done the day after Thanksgiving, the biggest shopping day of the year, and also the day when Social Security checks and half of private corporation paychecks are processed, the terrorists could then introduce a massive onslaught of fraudulent bills into the system, causing it to choke on all the unacceptable volume.

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-02-24 **cyber terrorism alert United Kingdom UK**

NIPC/DHS

February 20, The Times — Firms in the United Kingdom warned of IT terrorists. Terrorist groups may try to infiltrate the computer systems of some of Britain's biggest companies, government departments and emergency services if a war is launched against Iraq, the Home Office of the United Kingdom has cautioned. Stephen Cummings, director of the National Infrastructure Security Co-ordination Centre (NISCC), said key IT systems were under threat of cyber attack by Islamic extremists. He said: "There will be groups attacking U.S. Government and defense websites and similar groups carrying out activity against the websites of any country involved in military action." Cummings urged businesses to step up security ahead of a possible war in the Gulf. He gave warning that terrorist groups might try to infiltrate activists into the IT departments of leading firms. "My view is that terrorist groups have identified the potential value in having people inside organizations rather than just responding passively as they have done in the past. There are already non-cyber examples of this," he said. Since NISCC was set up three years ago to monitor the threat of electronic attack against the UK, the number of digital attacks on "critical" organizations has soared. Cummings said that "there have been companies perceived to be in line with U.S. support for Israel in the past which have been attacked by pro-Palestinian groups. We could expect to see the same thing again from different sources."

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-02-28 **mobile phone handheld device hacking spread**

NIPC/DHS

February 26, ZDNet (Australia) — Experts say mobile phone hacking may spread. United States-based security company @stake has released a security advisory detailing a Denial of Service (DoS) vulnerability in the Nokia 6210 GSM mobile phone. "This is a good example of why all newly introduced product functionality should be reviewed to ensure that no new security vulnerabilities will also be introduced. A cursory source code audit would find an error of this type," the advisory said. The vulnerability is not serious — affected users can simply "reboot" their phones — but it could be a sign of worse things to come. John Papandriopoulos, a wireless communications researcher based in Melbourne, Australia, says that current generation handsets are not necessarily a popular target because there's little that can be done even if an attacker is able to compromise them. "I think it's more likely that the motivation would be to inconvenience people," he said. As for a mobile phone worm, spreading by sending itself to phonebook entries, John says this isn't likely to happen for some time. However, as standardized client software becomes a standard feature on mobile handsets it's only a matter of time before malicious hackers start paying more attention to wireless worms, according to security consultant Daniel Lewkovitz of Sydney, Australia.

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-03-17 **cyber crime India infrastructure threat Central Bureau of Investigation CBI FBI**

NIPC/DHS

March 14, SiliconIndia.com — Cyber crime a threat to Indian infrastructure. The director of the Central Bureau of Investigation (CBI) in India said that cyber crime and organized corruption have assumed serious proportions. "Cyber crimes like hacking, e-mail fraud and other information security breaches linked to computers are turning out to be very serious problems," P.C. Sharma told journalists during a visit to Assam, India. Fears have been expressed that a new breed of criminals could damage telecommunications or rail links, disrupt power supplies and harm other important parts of India's infrastructure using cyber tools. The CBI has launched a massive drive to tackle the threat, honing the skills of its elite officers and modernizing the agency's computer network. Experts from the U.S. Federal Bureau of Investigation (FBI) visited India last year and trained policemen in dealing with cyber offences.

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-03-19 **CERT CC Internet net attack forecast warning**

NIPC/DHS

March 17, eWEEK — More net attacks loom, CERT says. The recent rash of Internet worms has produced an army of hundreds of thousands of compromised machines that could ultimately be used to launch a massive distributed-denial-of-service attack at any time, according to security officials. Officials at the CERT Coordination Center said the organization is monitoring at least five large networks of compromised machines installed with so-called bots. The bots connect compromised PCs or servers to Internet Relay Chat servers, which attackers commonly use to execute commands on the remote systems. At least one of these networks has more than 140,000 machines, officials said. CERT's dire warning is underscored by last week's emergence of the Deloder and Code Red.F worms. While neither worm does any immediate damage to infected machines, both install back doors that enable attackers to use compromised machines for future, much more damaging operations, such as DDoS attacks. At the heart of this new trend, according to security experts, are poor security practices. But more important is the mistaken belief by corporate IT that once crises such as those caused by Code Red or SQL Slammer die down, the trouble's over. In fact, after an initial flurry of advisories, warnings and patches, there are often months or years of sustained infections and residual DDoS attacks, Marty Lindner of CERT said. Also problematic are the many affected machines belonging to home users, few of whom do any logging of the activity on their PCs. As a result, attackers can easily hide their tracks by using these anonymous computers, according to the experts.

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-03-19 **Department Homeland Security DHS system threat attack forecast warning Iraq war**

NIPC/DHS

March 18, Government Computer News — DHS warns about systems threats as war looms. The Department of Homeland Security (DHS) on Tuesday reminded Internet users to be vigilant for cyberattacks in light of the ultimatum President Bush issued Monday that Iraqi President Saddam Hussein leave his country or face military invasion. The department and other federal agencies are monitoring "the Internet for signs of a potential terrorist attack, cyberterrorism, hacking and state-sponsored information warfare," a Homeland Security statement said. "Industry and public Internet users are reminded of the importance of employing sound security practices and reporting unusual activity or intrusion attempts to DHS or local law enforcement."

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-03-20 **virus worm malware cost business survey study estimates**

NewsScan

THE COST OF VIRUSES
Based on an analysis of 306 U.S. companies, computer-security company ICSA Labs says that disaster-causing viruses in 2002 cost an average of $81,000 each, compared to $69,000 in 2001. A "disaster" is defined in the company's report as having affected at least 25 machines and causing significant financial loss or damage to data. ICSA Labs says a stronger breed of viruses has increased a victimized company's recovery costs. (Dow Jones/AP/San Jose Mercury News

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-03-28 **music piracy downloading file-sharing recording industry**

NewsScan

INTERNET VS. RECORDING INDUSTRY
Media analyst Eric Garland of Big Champagne has told California lawmakers that the growth of music file-sharing on the Internet is "fundamentally unstoppable," because 61 million Americans and millions more worldwide are already downloading music and only 9% of them think they're doing something wrong. "We see only one trend. More people are downloading more copyrighted material." Garland's advice for the recording industry is to embrace digital distribution rather than institute lawsuits or education campaigns, but such advice is not well-received by industry executives, who are routinely urged by Internet enthusiasts to accommodate to technological realities. Phil Corwin, a lobbyist for Internet music service Kazaa, told the same group of state legislators: "The record business, in the digital revolution, has been a day late and a dollar short." [A dollar may not be the final figure.] The fight goes on. (AP/San Jose Mercury News 28 Mar 2003)

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-04-02 **Chinese criminal hacker attack hacking US UK Websites vandalism defacement Iraq war prediction warning forecast**

NIPC/DHS

March 31, Washington Post — DHS: Chinese hack attacks likely. Chinese hacker groups are planning attacks on U.S.- and U.K.-based Web sites to protest the war in Iraq, the Department of Homeland Security (DHS) warned in an alert Monday. The hackers are planning "distributed denial-of-service" attacks, which render Web sites and networks unusable by flooding them with massive amounts of traffic. They also are planning to deface selected Web sites, according to the alert, though the government said it did not know when the attacks would occur. The DHS said it got the information by monitoring an online meeting that the hackers held last weekend to coordinate the attacks.

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-04-15 **cyber attacks physical damage repercussion virtual network bank account idea**

NIPC/DHS

April 14, New York Times — Cyberattacks with offline damage. Most experts think of cyberattack as something that will happen in the virtual world, with effects on computer networks or access to bank accounts. But in a new paper, Aviel D. Rubin of the Information Security Institute at Johns Hopkins University, describes cyberattacks involving the use of online tools against the offline world. Using tools that have been published by search engines like Google that allow programmers to automate searches on a large scale, the paper describes a relatively simple program that could set the victim up to receive catalogs from hundreds of thousands of Web sites that have sign-up forms. Rubin's attack could be enormously disruptive to the target, and could paralyze the local post office that has to deal with the onslaught. As the report notes, the exploit could be used as a diversion to accompany a deadly terrorist act, like mailing an envelope containing anthrax spores. The paper can be found at www.avirubin.com/scripted.attacks.pdf

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-04-16 **cyber terrorism chances increase CERT incidents**

NewsScan

CYBERATTACK STATISTICS: UP, UP AND AWAY
Although computers have up to this point been spared a major cyberattack from terrorists or rogue nations, there have been plenty of smaller acts of vandalism by individual troublemakers. The Computer Emergency Response Team (CERT) tracked 52,658 online security incidents in 2001, more than double the number reported in the previous year, and more than four times the number reported the year before that. Figures for 2002 are not yet available. (Reuters/USA Today 16 Apr 2003)

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-04-21 **warning threat security RSA conference**

NIPC/DHS

April 18, CNET News.com — New attack may draw government intervention. Security experts warned Thursday that business executives need to take network protection more seriously before a major cyberattack results in government intervention. Although the Bush administration has indicated it doesn't intend to dictate how companies should handle security, another Code Red or Nimda incident could change that stance, Roger Cressey, president of Good Harbor Consulting, said during a panel discussion this week at the RSA Conference in San Francisco. "If we do have a major cyberincident, there will be a critical mass of pressure for regulation, and (Congress) will take out a sledgehammer when a scalpel is needed," Cressey said. Two months ago, the Bush administration released the National Strategy to Secure Cyberspace, a document that mainly suggested solutions for protecting the Internet and critical infrastructure. The only mandates in the document were directed at government agencies. That's the correct approach, Lawrence Dietz of Symantec said at the panel. Instead, Dietz said, the government should wield its wallet and put restrictions on companies that want to do business with federal agencies.

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-04-29 **security terrorism uncertainty Department Homeland Security DHS cost-benefit analysis**

NIPC/DHS

April 25, Computerworld — Lack of terrorist activity leads to complacency. The changing of the cybersecurity guard at the Department of Homeland Security (DHS), coupled with complacency on the part of some corporate executives, has put a higher premium on information-sharing and cooperation between the private sector and the government. Michael Hershman of Virginia-based security consulting firm Decision Strategies LLC says companies have started to slow their efforts to boost security because there has been no terrorist activity recently. "I'm afraid that they may be drawing back into complacency," he said last week at a U.S. Chamber of Commerce conference in Washington that addressed the roles and responsibilities of the government and private sector in homeland security efforts. "Corporations in America have spent billions of dollars for security, with very little cost-benefit analysis," said Hershman.

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-04-30 **cyber-crime warning National High Tech Crime Unit NHTCU Great Britain InfoSecurity Europe**

NIPC/DHS

April 30, vnunet — British law enforcement issues stark cyber-crime warning. The head of the National High Tech Crime Unit (NHTCU) of the Great Britain has called on businesses to take cyber-crime more seriously. Detective superintendent Len Hynds told delegates attending the Infosecurity Europe 2003 show that cyber-crime is no different from any other criminal activity and needs to be treated as such. Hynds's remarks came as the NHTCU released the results of a survey on UK cyber-crime. Three quarters of the 150 UK businesses surveyed had suffered some form of high-tech crime. More than one in five companies didn't even conduct regular security audits.

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-05-05 **Nemertes Research IT security government regulations companies corporate real-world requirements**

NIPC/DHS

May 05, Network World — Corporate security spending not in line with real-world requirements. Technology research firm Nemertes Research last week released its "Effective Security Solutions" report, which says the average 2% to 3% of the overall IT budget that companies allocate for security will not adequately prepare most of them for government regulations, new applications and/or Web services architectures. Johna Till Johnson of Nemertes Research says companies must spend at least 5% of their overall IT budgets on security to comply with government regulations passed in the past eight years or so. The security requirements in legislation such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach-Bliley Financial Modernization Act of 1999, the Sarbanes-Oxley Act of 2002 and ongoing Department of Homeland Security initiatives, represent a significant concern for companies currently underspending, says Johnson. "The fine print in these pieces of legislation has the CEO or the security officer potentially going to jail if found in violation of these acts," she says.

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-05-05 **DHS CIO Pearl Harbor digitally Steven Cooper government IT safeguard risk chat online**

NIPC/DHS

May 05, InformationWeek — DHS CIO: no 'digital Pearl Harbor' likely. "It's highly unlikely that the United States will experience a crippling "digital Pearl Harbor," the CIO of the Department of Homeland Security (DHS) says. "While this is a possibility, the probability is relatively low," Steven Cooper said in an online chat sponsored by The Washington Post. "We have done a lot in the federal arena to provide multilayered security for our digital environments and continually 'red team' our networks and applications to find vulnerabilities." The government spends millions of dollars on technology to safeguard IT, and Cooper said he isn't overly concerned about individuals who might compromise the government's IT infrastructure. "I would agree that it is always a risk," Cooper said. "However, all personnel working in the department, including contractors, must pass a security clearance and additional reviews and background checks, depending on level of clearance."

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-05-05 **security offshore coding U.S. software companies economy rish India Pakistan Russia China Techo-Security Conference**

NIPC/DHS

May 05, Computerworld — Offshore coding work raises security concerns. IT professionals are raising questions about the U.S. software industry's reliance on overseas software developers, arguing that the practice puts companies and the U.S. economy at risk. A recent study by Gartner Inc. predicts that by 2004, more than 80% of U.S. companies will consider outsourcing critical IT services, including software development, to countries such as India, Pakistan, Russia and China. But some users at last week's Techno-Security Conference in Myrtle Beach, S.C., said the trend needs to be reconsidered in light of recent changes in the global security environment. Of particular concern is the work that is being sent to China. While not yet a major provider of outsourcing services, China has a significant economic espionage program that targets U.S. technology, the users noted. Also of concern are countries in Southeast Asia, particularly Malaysia and Indonesia, where terrorist networks are known to exist.

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-05-07 **emergency backup systems information data FEMA Federal Management Agency WTC World Trade Center Pentagon attacks**

NIPC/DHS

May 07, National Journal — IT officials emphasize need for emergency backup systems. Many government offices must do better at backing up their information systems to preserve important data and ensure "continuity of operations" in the event of a terrorist attack, several federal technology officials said on Tuesday at a homeland security conference sponsored by the Armed Forces Communications and Electronics Association. FEMA's continuity-of-operations plan for many other systems typically amounts to "a pile of tapes" containing archived data, said Robert Coxe, deputy CIO of the Federal Emergency Management Agency (FEMA). Redundant communications and information systems proved invaluable after the attacks on the World Trade Center and the Pentagon, according to Lt. General Harry Raduege of the Defense Information Systems Agency. He recalled that one military agency avoided major data losses during the Pentagon attack because its computer systems had "double backup" capabilities. But he said officials in another Pentagon organization had stored "everything they had" on only one system that was destroyed in the attack. "They lost every bit of that data," he said.

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-05-15 **e-mail instant message GoToMyPC.com impression management idle bankruptcy**

NewsScan

THE NEW WHITE-COLLAR CRIME: TECHNO-SLACKING
It's getting easier than ever to convince your customers, supervisors and employees that you're hard at work — firing off e-mail messages and opening files on your office PC while you're really attending your kids' soccer game or sleeping in. Services like GoToMyPC.com enable users to manipulate their office computers by remote control — even going so far as to move the cursor on the screen, open documents and print them on the networked office printer. E-mail timers allow workers to compose messages during the day and then queue them to be sent hours after they've gone to bed, giving the impression that they're up burning the midnight oil. Instant Message software can be reconfigured so that the "idle" message that pops up signaling inactivity is disabled, making users look perpetually available. And BlackBerry aficionados can change their settings to make on-the-road e-mail look like it came straight from the office PC. Psychologists call these activities "impression management," but other see signs of a disturbing trend: "If you're out playing golf, and you look like you've spent four hours in the office… If everybody does that, the company goes bankrupt," says Stuart Gilman, director of the Ethics Resource Center in Washington. A recent survey conducted by the Society for Human Resource Management found that 59% of HR professionals had personally observed employees lying about the number of hours they'd worked, and 53% said they'd seen employees lying to a supervisor, a jump of eight percentage points in six years. (Wall Street Journal 15 May 2003)

---

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-06-03 **digital pearl harbor Carnegie Mellon SEI software engineering institute disgruntled insiders foreign terrorsits greatest cuyber security threat terrorism Al-Qaeda steganography**

NIPC/DHS

June 03, National Journal — Computer security officials discount chances of 'digital Pearl Harbor'. The notion that the cyberterrorism against the United States could create a "digital Pearl Harbor" is fading three computer-security experts said Tuesday. Casey Dunlevy of Carnegie Mellon's Software Engineering Institute (SEI), and Richard Hunter of Gartner Group, said disgruntled insiders, not foreign terrorists, pose the greatest cybersecurity threat to companies. "But could [cyber terrorism] be a force multiplier in terrorist attacks" by, for example, disabling all traffic lights after a bombing? "I think we have to consider that," said Dunlevy. He said computers recovered from Afghanistan demonstrated al Qaeda's use of steganography, a technique for embedding secret data within pictures or text. "We will eventually see a cyber element to terrorist activity," Dunlevy said. But both he and Hunter said terrorist groups also are likely to continue to engage in money laundering and cybercrime as a means of purloining resources.

---

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-06-04 **PKI Public Key Infrastructure Tim Polk NIST businesses IT security momentum encryption**

NIPC/DHS

June 04, Post Newsweek Tech Media — PKI momentum builds, program manager says. A dozen years after the start of the federal push for a public-key infrastructure, the technology is gaining momentum, and more agencies will be using PKI in a matter of months, a federal program manager predicts. By year's end, Tim Polk, the PKI program manager at the National Institute of Standards and Technology, estimated, eight to 10 agencies will be heavily engaged in PKI, nearly twice the number involved today. Polk spoke today at a conference on IT security in Washington sponsored by the research and advisory firm Gartner Inc. As governments and businesses move from paper to electronic documents, PKI holds promise as an effective way to protect and validate those documents and verify identities. PKI also is being used with employee identification smart cards.

---

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-06-12 **security software viruses Trend Micro**

NewsScan

SECURITY SOFTWARE BUSINESS DUE FOR A SHAKE-UP
As the nature of computer viruses changes, the business of selling security software is changing, too, says Steve Chang, head of antivirus software firm Trend Micro. With viruses morphing into ever-more-complex forms, antivirus firms will need to shift from selling software to selling security services aimed at minimizing customers' downtime. Chang says the security software industry used to compare itself to the pharmaceutical business, developing new antidotes for each virus that cropped up. But the ubiquity of the Internet and the advent of such virulent viruses as Nimda, Slammer and Bugbear have changed all that. Now, the ability of a company to avoid infection depends as much on the security measures taken by other companies it does business with and employees working in their home environments as on its own vigilance. That means companies increasingly are seeking an ongoing service which, in addition to protecting them from malicious attacks, speeds up the recovery time following a security breach so that everyone can get back to work. "You buy a drill because you want a hole," says Chang, "not because you want a drill. Customers do not want a security product. They just want to improve their productivity without downtime." (BBC News 12 Jun 2003)

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-07-11 **surveys estimates data disaster disconnect IT vulnerable**

NewsScan

BUSINESS/TECHNOLOGY DISCONNECT ON DATA DISASTER
U.S. business executives may be a bit overly optimistic in their estimates of the impact a major data disaster would have on their operations. A survey sponsored by data storage firm EMC indicates that only 14% of senior business executives regard their company's data as very vulnerable, compared to 52% of senior IT executives. And only 9% of business execs said it would take three days or more to get back to normal following a data disaster, compared with 23% of tech executives. "Our customers tell us that their greatest challenge isn't backing up their information — it's recovering and resuming operations in a timely manner. We don't believe U.S. business leaders are being misled by their IT teams. Instead, it is likely a misperception that, if the data is backed up, there is no issue," says an executive VP for EMC. Meanwhile, European executives were more in synch with their IT counterparts regarding the likely vulnerability of their data — 40% of business executives and 44% of technology executives regarded their data as very vulnerable. (CNet News.com 11 Jul 2003)

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-07-30 **outsourcing litigation bill**

NewsScan

TECH EXODUS: 500,000 JOBS MOVING OVERSEAS
One out of 10 jobs in the U.S. computer services and software sector could move overseas by the end of next year, according to a new report from Gartner Inc. And while professionals in the computer industry will be especially hard-hit, IT jobs in other sectors such as banking, health-care and insurance will feel the impact also, with one in 20 being exported to emerging markets such as Russia, India or other countries in Southeast Asia. "Suddenly we have a profession — computer programming — that has to wake up and consider what value it really has to offer," says Gartner VP and research director Diane Morello. Morello estimates that based on her preliminary calculations, at least 500,000 jobs will be lost to offshore outsourcing by then end of 2004. The trend toward "offshore outsourcing" is heating up as a political issue, with legislators in five states proposing bills that would require workers hired under state contracts be American citizens or fill a special niche that citizens cannot. (Reuters/CNN.com 30 Jul 2003)

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-08-04 **country coded computer worms Jonath Wignall information warfare internet protocol**

NIPC/DHS

August 04, New Scientist — Country-coded computer worms may be ahead. Jonathan Wignall of the UK's Data and Network Security Research Council highlighted techniques that worm creators might use to make their code spread more effectively during a presentation at the security conference Defcon 11 in Las Vegas, NV, on Sunday, August 3. One of these techniques could also limit a worm's geographic range, which would turn a computer worm into an effective weapon for information warfare, he said. Instead of attacking internet-connected computers at random it could be used to attack a specific country. After infecting a host computer, a worm normally scans randomly for further machines that could be infected. But Wignall says a worm could download a prepared list of internet protocol (IP) addresses to attack from a single server or a group of machines. This would prevent duplicate requests being sent to each machine, a common cause of bottlenecking with existing worm design. Nicholas Weaver, a computer scientist at the University of California in Berkeley says this is just one way that a worm could, in theory, be used to target a specific country. Another way is to avoid computers running a particular language, he says.

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-08-28 **computer viruses anti-virus worms predictions propagate Sobig.F Microsoft Windows operating systems target fight**

NIPC/DHS

August 28, Washington Post — Fight against viruses may move to servers. Computer viruses are becoming so aggressive and sophisticated that they may soon be able to elude anti-virus programs installed on individual computers, according to many in the security industry. Analysts say the speed with which viruses and worms now propagate require technologies that predict outbreaks before they happen. Such predictive systems require intensive computing power beyond the capacity of desktop machines. Computer worms and viruses are getting more sophisticated, are spreading faster and are capable of doing more damage than those of the past. Viruses such as Sobig.F can change during their attacks by receiving updates and new instructions from other computers. Some analysts point out that while no software or hardware is perfect, it's much easier to spread viruses when so much of the computing world depends on the Microsoft Windows operating system. Advocates of the Unix, Linux, Macintosh and other operating systems argue that they are more secure than Windows, but others note that those systems simply have not been targeted as much.

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-09-01 **Digital vandalism internet government computer virus attachs security experts breaches terrorist damaging**

NIPC/DHS

September 01, New York Times — Digital vandalism spurs a call for oversight. The Internet is not subject to government oversight, and many see the Internet's openness as crucial to its success as a platform for innovation. But the increasing severity of computer virus attacks may have muted the antiregulatory reflex. Some security experts now advocate direct regulation, in the form of legislation that makes software companies liable for damage caused by security flaws in their products. Advocates of increased regulation say a California law that requires companies conducting business in the state to disclose computer security breaches if they result in unauthorized access to residents' personal information could serve as a model. A survey released Sunday, August 31, by the Pew Internet and American Life Project said that nearly 60 percent of Internet users say they favor the government's requiring American corporations to disclose more information about their vulnerabilities. Half of those surveyed said they worried about terrorists damaging the Internet.

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-09-02 **attack anti-virus software market growth**

NewsScan

SOFTWARE MAKERS FIND SILVER LINING TO NET VANDALISM
Business analysts expect to see continued growth in the anti-virus market, and Sarah Friar of Goldman Sachs predicts the market will climb 18% to $2.6 billion this year and improve to $2.8 billion in 2004: "This last wave of viruses perked people up to say, 'My God, I need to protect my computer.'" Nitsan Hargil of investment bank Friedman Billings Ramsey adds: "Fear sells, especially among consumers, who aren't as well-protected as corporations." Since August 11th, Symantec shares are up 22%, Network Associates shares up 30%, and Trend Micro shares up 33%. (USA Today 2 Sep 2003)

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-09-11 **unpatched holes Internet Explorer Microsoft new vulnerabilities Thor Larholm former black hat heighten security**

NIPC/DHS

September 11, Sydney Morning Herald (Australia) — Thirty unpatched holes in IE, says security researcher. As Microsoft releases details of new vulnerabilities, it is yet to tackle the 30 unpatched holes in Internet Explorer which have been documented by well-known security researcher Thor Larholm. Larholm, a former black hat and now a senior security researcher with a private company, said on Friday, September 12, that seven more vulnerabilities had been added to the list he maintains, all of them having been discovered by Chinese researcher Liu Die Yu. "One of these new vulnerabilities exploits a new attack vector that has surfaced in IE lately, namely misdirecting user input," Larholm said. According to Larholm, "This allows you to redirect a user's mouseclick to (for example) the OK button on a dialog asking for security confirmation by moving the browser window prior to the mouse being released. This resurrects the debate on whether to disable some core functionality to heighten security. Similarly, several of the vulnerabilities that remain unpatched are known to be under active investigation by the Microsoft Security Response Center, and I am confident that a secure patch is being prepared for prompt release."

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-09-29 **spam estimates marketing filtering masking blocking**

TechWeb http://www.techweb.com/wire/story/TWB20030929S0020

Gartner Group estimated that spam would be 50% of all e-mail on the 'Net by the end of 2003 and 60% by mid-2004. They also found that permission-based, well-designed, targeted e-mail could produce as much as a 15% response rate — much higher than the 1% for banner ads and the fraction of a percent for broadcast print mail advertisements.

David Legard, writing in Network World, summarized the Gartner findings as follows (quoting):

* E-mail marketers no longer have to comply with 36 state laws and, although the bill requires a valid opt-out mechanism, it does not make clear who should be responsible for implementing the unsubscribe or do-not-contact request.

* Businesses, ISPs and vendors filtering inbound e-mail will have to develop increasingly sophisticated technology and practices to decide between legitimate advertising material and spam, both of which will have to carry the 'ADV' tag in the subject line

* Disreputable spammers will ignore the legislation and if they feel under threat, will use offshore ISPs beyond the reach of U.S. jurisdiction to send material.

---

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-10-01 **virus threat damage Microsoft software Symantec report**

NewsScan

NEW VIRUSES USE 'BLENDED THREATS' TO WREAK DAMAGE
Computer viruses are increasing in frequency, speed and sophistication, according to the latest Internet Security Threat Report from Symantec, adding that hackers are using "blended threats" that combine various types of viruses to carry out their attacks. Not surprisingly, the target of most of these attacks is Microsoft software, says Tony Vincent, Symantec's lead global security architect. "There's a continued focus by the bad guys on vulnerabilities based on Microsoft's Web server product and Internet Explorer." The report also cites a narrowing gap between the discovery of a potential vulnerability and the launch of a virus designed to exploit it. "The speed of propagation of blended threats is also increasing. Symantec expects to see greater worm propagation resulting in overloads to network hardware, crippling network traffic, and seriously preventing both individuals and businesses from using the Internet." (Reuters 1 Oct 2003)

---

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-10-19 **cyber crime Bucharest Romania litigation defraud US**

NewsScan

CYBERCRIME HOTSPOT: BUCHAREST
There now exists a loosely organized network of young Romanians conspiring with other accomplices in Europe and the U.S. to defraud consumers through bogus Internet purchases, extort cash from companies after hacking into their systems, and release worms and viruses. Romanian lawmaker and former programmer Varujan Pambuccian says: "We want a good name for our country. I'm very angry that Romania is so well-known for ugly things — for street dogs, street children and hackers." Mihai Radu, a computer security expert in Bucharest, believes that Romania's law enforcement officials are not up to the job of defeating the vandals: "The Romanian police aren't qualified. They don't have the tools, the skills, the software." (AP/San Jose Mercury News 19 Oct 2003)

---

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-12-02 **worm network cell phone handset vulnerability Internet enabled**

NIPC/DHS

November 28, New York Times — Beware the worm in your handset. As more consumers begin surfing the Web and sending e-mail messages on cellphone and hand-held devices, along comes a new worry: worms and viruses spread via Internet-enabled handsets. The problem is still small, with only a few cases reported globally. But as operating systems in cellphones become standardized, hackers will probably begin focusing on vulnerabilities in those systems as they have with personal computers. And as cellphones and personal digital assistants connect to the Internet at ever faster speeds, more users will be able to download files with attachments—some of which may be infected. Asia, where high-speed networks and text messaging on mobile phones are common, is the most vulnerable to these threats. As carriers in Europe and North America adopt similar technology, they will confront the same kinds of hazards. Telecommunications companies currently spend as much as $8 billion a year fixing handsets with programming errors, faulty mechanics and other problems. Now some are scrambling to prevent virus attacks that could cost carriers millions of dollars more in repairs and lost business.

---

*Category 31.2* *Estimates, guesses, predictions, forecasts concerning security*

2003-12-04 **computer virus crime authors successful Microsoft piracy**

NIPC/DHS

December 03, Reuters — Web virus authors 'winning battle' — Microsoft. Creators of computer viruses are winning the battle with law enforcers and getting away with crimes that cost the global economy some $13 billion this year, a Microsoft official said Wednesday, December 3 at a cybercrime conference in Germany. Counterfeit centers are shifting from California and Western Europe to countries including Paraguay, Colombia and Ukraine said David Finn. In Asia, pirate plants have emerged in Vietnam, Macao, and Myanmar (Burma) in addition to more established facilities in Indonesia, Malaysia and Thailand. "So far they are getting away with it...Very few have been identified or prosecuted or punished," Finn said. He cited estimates by Business Week that financial damage this year from bugs like the Blaster worm and the SoBig.F e-mail virus, which crashed systems and disrupted Internet traffic around the world, would total some $13 billion. The cost of protecting networks against such cyberattacks was put at $3.8 billion. Finn said "we shouldn't be surprised" if terror organizations were looking to recruit computer expertise. Len Hynds, head of the National High-Tech Crime Unit in Britain, said gangs were recruiting people with IT skills not only to help them commit cybercrime but to secure their own communications networks and avoid detection. He said companies needed to recruit more carefully.

# 31.3 New technology with security implications

*Category 31.3 New technology with security implications*

2003-01-09 **smart wireless watch download**

NewsScan

MICROSOFT'S 'SMART' WRISTWATCH
Microsoft took the wraps off its new "smart" wristwatch that delivers custom-tailored data, such as sports scores, weather reports or traffic updates, via a new wireless network that Microsoft is cobbling together by leasing existing FM spectrum. Initially, the watches will work in 100 cities covered by the network. In order to access information, the wearer just checks the different "channels" on the watch to determine the best route home or how warmly to dress in the morning. The souped-up watches, made by Fossil, Citizen Watch and the Finnish firm Suunto, are expected to be available late this year, priced in the $100 to $250 range. The wristwatches are part of Microsoft's "Smart Personal Objects Technology" or SPOT initiative, which eventually will also include "smart" alarm clocks and refrigerator magnets. (Wall Street Journal 9 Jan 2003)

*Category 31.3 New technology with security implications*

2003-01-15 **surveillance privacy camera telephone**

NewsScan

CAMERA/CELL PHONES RAISE NEW PRIVACY ISSUES
Citing its customers' need for privacy, a chain of Hong Kong health clubs has banned the use of mobile phones in its locker rooms. At issue is the new generation of phones that can record and transmit video and still photos. Analysts say the new policy at Physical is one of the first cases they've heard of connected with the new cell phone capabilities. Fitness First, another Hong Kong chain that competes with Physical, is also considering a ban on cell phone use in some areas, and in nearby Macau, the use of the new camera-equipped cell phones has become an issue for the territory's 11 casinos. A spokeswoman for the casino company says traditional cameras are now prohibited in the establishments but that cell phones, which are extremely popular in Hong Kong, have yet to be forbidden. "This is something new that's come up. We have inspectors watching. Should they find anyone using these phones, because it's just like a camera, they will delete whatever photos were taken."
(Reuters/CNet 14 Jan 2003)
http://news.com.com/2100-1033-980530.html

*Category 31.3 New technology with security implications*

2003-01-28 **location surveillance tracking objects people children wireless radio GPS**

NewsScan

FORGETFUL BOOMERS SPAWN MARKET FOR MEMORY AIDS
A stream of new products is hitting the shelves, aimed at solving one of life's daily annoyances: locating everyday objects such as keys or glasses that always seem to go missing just when you're in a hurry to leave. The products range from a FINDIT keychain that beeps after the user claps three times to the Sharper Image's "Now You Can Find It!" — a collection of plastic tags that can be attached to potentially elusive items, and then beep when users hit a button on the central device (of course, for it to work, users must make sure not to misplace the central device). The device and tags communicate with each other via radio frequency waves, and require that the user be within several meters of the hidden object's location. A handful of companies are also marketing GPS-enabled "kid finder" watches and pagers, and plans are underway to put homing devices on everything from luggage to pacifiers. Most ambitious of all, perhaps is the DIPO device, made by a French company of the same name, that not only finds an object but notifies the owner if it is about to be left behind. The central device — the size of a small cell phone — checks every few seconds to ensure that all tagged objects are within a certain radius — say, five meters. If it notices that the tag on the Palm Pilot, for instance, has moved outside the radius, it will beep or vibrate to remind the user to take it along. DIPO started out as the brainchild of the company's absent-minded CEO, Bruno Enea, who says, "I kept losing my credit card. I always forgot my passport. I realized I had to do something about this problem." (Wall Street Journal 15 Oct 2002)

RADIO FREQUENCY IDENTIFICATION (RFID) TAGS READY TO GO
A number of new consumer products from companies such as Gillette, Procter & Gamble, and Prada will come with embedded RFID (radio frequency identification) "tags" (actually, tiny computer chips), that will contain scannable information such as the product's serial number. The goal is to dramatically improve inventory processes, and other big companies poised to join the RFID movement are Johnson & Johnson, Coca-Cola, Pepsi, Home Depot and Target. Within a year or two RFID tags will be included in all kinds of products, including Michelin and Goodyear tires (to tell where a tire was made). Privacy groups are expressing fears that thieves will buy or make chip scanners that can crack security controls to scan shoppers' bags and know what they bought. (USA Today 28 Jan 2003)

*Category 31.3 New technology with security implications*

2003-02-10 **electrical power lines broadband communications network**

NewsScan

POWER COMPANIES TEST BROADBAND TECHNOLOGY
Energy utility Ameren Corp. and other power companies are testing technology that would deliver high-speed Internet access over their power lines, making every home electrical outlet an always-on Web connection. The FCC has applauded the energy companies' efforts, with chairman Michael Powell saying the technology "could simply blow the doors off the provision of broadband." But existing broadband providers and others are skeptical, saying that while they consider the technology intriguing, talk about it has been around for years, with nothing to show for it. "I think they're a long way from proving it, let's leave it there," says Larry Carmichael, a project manager with the Electric Power Research Institute. "The tests to date have been so small as far as looking at the financial and technical viability. It's still at the very early stage of development." (AP 10 Feb 2003)
http://apnews.excite.com/article/20030210/D7P3R6801.htm

*Category 31.3 New technology with security implications*

2003-02-13 **pen handwriting capture replay biometrics**

NewsScan

IT'S ALL IN THE SCRAWL: PENS THAT READ
Two companies, Logitech and Seiko, have developed pens that can be used to translate your handwriting into a computer. Here's how the $170 Logitech Io pen works: A pinhole camera next to the tip of the pen records your movements as you write on paper, and a microprocessor then turns this information into handwritten notes and diagrams (as many 40 pages worth). Later, you can insert the pen into a small desktop stand which communicates to a Windows personal computer through a USB connector. The handwriting is stored as a dumb graphic, but you can make simple editing changes and can e-mail the notes to someone else. (New York Times 13 Feb 2003)

*Category 31.3 New technology with security implications*

2003-03-07 **autonomic computing self-repair artificial intelligence**

NewsScan

IBM ZEROES IN ON AUTONOMIC COMPUTING IBM has established a new Autonomic Computing group, which will focus on R&D and product development in self-diagnosing computers that can take steps to fix themselves. The goal is to free up users from routine maintenance and repair tasks so that they can concentrate on other things. "The end game is to deliver a computing environment that is online all the time as a utility," says Nick Donofrio, senior VP of technology and manufacturing at IBM. "It sounds far-fetched right now, only because it's a lot of hard work." But ultimately, says Donofrio, "for consumers it means incredibly available data and a much richer (online) environment." IBM has been working on autonomic computing for more than a year, and has already incorporated the technology in several products, such as its newest DB2 Version 8 database software. The Autonomic Computing group hopes to expand use of the technology in IBM's products and create open standards for an autonomic computing architecture that would apply across computing platforms and manufacturers. (CNet News.com 20 Oct 2002)
http://news.com.com/2100-1001-962623.html?tag=fd_top_1

AUTONOMIC COMPUTING
IBM says it has developed software that allows networked computer systems to automatically adjust to unexpected demand surges by turning on additional computers on the network. This kind of capability is known as autonomic computing, which IBM also calls "on-demand" computing. As an example of on-demand computing, IBM says that if an airline is hit by a flood of customer responses to a special fare sale, it would take the system only a minute to note the changing load requirements and add another computer to handle the new demand. (Reuters/San Jose Mercury News 7 Mar 2003)

*Category 31.3 New technology with security implications*

2003-03-27 **e-mail traffic monitoring terrorist criminal activity logs**

NewsScan

E-MAIL TRAFFIC PATTERNS SIGNAL WHO'S IN CHARGE
A new technique developed at Hewlett-Packard's research labs in Palo Alto can quickly identify online communities and the key people in them. "If the CIA or another intelligence agency has a lot of intercepted e-mail from people suspected of being part of a criminal network, they could use the technique to figure out who the leaders of the network might be," says researcher Joshua Tyler. Tyler and his colleagues analyzed communications patterns using the lab's log of nearly 200,000 internal e-mails sent by 485 employees over a couple of months. They plotted lines between people who had exchanged at least 30 e-mails with each other, and found the grid included 1,110 links between 367 people. The researchers then used a computer algorithm that looks for critical links that form bridges between separate groups, which revealed 66 communities within the lab. To identify the leader in each community, they plotted the same network of e-mails using a standard algorithm that tries to arrange the connections in the least tangled way. This step identified the managers, who tended to cluster in the middle. "This approach puts in the middle the people who have the most diverse range of contacts in the organization — and these tend to be the leaders," says Tyler, who adds that the technique could be used to identify the ringleaders in criminal or terrorist gangs. (New Scientist 27 Mar 2003)

*Category 31.3 New technology with security implications*

2003-04-18 **Cisco WiFi telephone**

NewsScan

CISCO'S WIFI PHONE DUE OUT IN JUNE
Cisco plans a June rollout for its 7920 portable phone, which will use a WiFi network to connect. A future update will combine conventional cellular and WiFi capabilities in one handset. Meanwhile, the competition is heating up as similar phones are planned by Motorola, Avaya and WiFi equipment maker SpectraLink. However, the short battery life of these "multimodal" devices likely will prove a technological hurdle for companies planning to tackle the market, says an Aberdeen Group analyst, who based his criticism on his own experience with a Toshiba WiFi-enabled handset that needed recharging after only 75 minutes of use. (CNet News.com 18 Apr 2003)

*Category 31.3 New technology with security implications*

2003-04-21 **new tool counterterrorism search find pattern recognition database**

NIPC/DHS

April 17, Government Computer News — Data management system gets new analysis tool. An automated data analysis tool will power a new FBI counterterrorism database, letting bureau analysts easily pore through more than 1 billion documents. The tools, ClearTags and ClearResearch, will draw patterns from terrorism-related intelligence collected from several sources into a centralized data mart that's part of the agency's modernized Trilogy network. The applications are intended to ease information sharing between the FBI and organizations at the CIA and Department of Homeland Security. The tools will also give intelligence officers a quicker method for scanning various databases at the Bureau of Alcohol, Tobacco and Firearms, Defense Department, Drug Enforcement Agency, State Department, and state and local agencies.

*Category 31.3 New technology with security implications*

2003-04-29 **Microsoft digital newspapters intellectual property rights**

NewsScan

MICROSOFT TARGETS DIGITAL NEWSPAPERS
Microsoft is developing software geared toward delivering digital newspapers, said chairman Bill Gates at the Newspaper Association of America's annual convention Tuesday. The new software will enable newspapers also to provide services like video messaging and bill-payment to readers across a variety of devices. Publishers who continue to view their Web sites as an add-on feature of their print operations are ignoring the next generation of readers, said Gates. "We see the online newspaper as one where it takes all the strengths [of current newspapers] and then adds in new capabilities." Readers not only will be able to read about an upcoming concert, but also will have the ability to hear audio clips and purchase tickets, added Gregg Brown of Microsoft's e-periodicals team. (AP/Wall Street Journal 29 Apr 2003)

*Category 31.3* *New technology with security implications*

2003-05-06 **bill gates microsoft security system hard-wired technology protect medical records**

NewsScan

GATES ON MICROSOFT'S NEW SECURITY SYSTEM: USE IT OR DON'T IT
Microsoft's Bill Gates thinks people should have no fears about the company's new hard-wired security technology — but reminds them that they don't have to use it unless they want to: "This is a mechanism that if people want to use, for example, to protect medical records, they can use it. It's a lot of work to do this stuff, and we think consumers will want those privacy guarantees. If they don't want them, then fine, ask me about our other work." Chipmakers Intel and AMD are working on the hardware aspects of the technology, which will provide the creators or owners of digital content a very high level of control over that content, allowing it to be viewed only by trusted employees or paying customers, and locking out snoops and vandals. Microsoft is calling its technology "Next Generation Secure Computing Base." (AP/San Jose Mercury News 6 May 2003)

---

*Category 31.3* *New technology with security implications*

2003-05-10 **Verizon Wi-Fi wireless payphone urban areas terminals Bell Canada Lawrence Babbo**

NewsScan

VERIZON TO TRANSFORM PAYPHONES TO WIFI TERMINALS
Verizon Communications, following the lead of Bell Canada, is planning to install WiFi terminals in payphones located in busy urban areas, according president Lawrence Babbo. "All of our payphone people have already told us (that the phones would make good wireless access points.) That will probably be the vehicle we use, probably in Manhattan." Verizon already offers WiFi equipment to its DSL customers, and last November began offering WiFi connectivity to small and medium-sized businesses. Bell Canada has been testing the concept at payphones in Toronto and Montreal, and several independent phone companies are interested in following suit. (AP 10 May 2003)

---

*Category 31.3* *New technology with security implications*

2003-05-28 **hacker university michigan rollback techonology track transactions administrators system authorized ReVirt backup restore intruders**

NIPC/DHS

May 28, SC Infosecurity News — Hacker damage reversal technology revealed. The University of Michigan is developing a rollback technology that allows administrators to track all transactions on a system, whether authorized or not, and reverse those transactions when required. The ReVirt technology is still way off completion but, according to Peter Chen, associate professor of electrical engineering with university, several commercial products can record all changes made to a hard drive, allowing users to restore their systems to a previous backup point. But, he said, none of these products allow system administrators to replay an intruder's actions on a step-by-step basis.

---

*Category 31.3* *New technology with security implications*

2003-05-29 **pornography tiny storage device videos photos law enforcement**

NewsScan

TINY DEVICES OFFER LAW ENFORCEMENT CHALLENGE
Portable storage drives continue to gain popularity among child pornography collectors. The typical drive is as small as a cigarette lighter yet holds 128 megabytes of data and costs only $100 or less; it device plugs directly into most PCs, and can store entire movies or hundreds of digital photos. Sgt. Art Martinez of the San Mateo County Sheriff's Department in California explains that the devices offer a completely new challenge to law enforcement officers: "A lot of officers will look at them and don't know what they are. It's just another thing that we need to be looking for." (San Jose Mercury News 29 May 2003)

---

*Category 31.3* *New technology with security implications*

2003-06-12 **privacy problems 3rd generation image capable cell phones**

NewsScan

3RD-GENERATION PRIVACY PROBLEMS
In Australia, that country's Royal Life Saving Society (a lifesaving and lifeguarding organization) intends to ban 3rd-generation image-capable cell phones from swimming pool changing rooms: "We, as operators and as providers of guidelines to the industry in this particular case, we just want to make sure that people are aware. We make every reasonable step to make sure that the privacy of individuals and, as I say, the private parts of individuals are not exposed where they don't want them to be exposed," says a spokesman for the Society. The potential for mischief with the new technology is apparent from the remarks of a student who reported: "One of my mates who's got one actually, as a joke, said that you could stand on the elevators and take photos up girls' skirts, which I thought was a bit much. He was only joking, he wasn't being serious, but, sure enough, the potential is there." Australia's privacy commissioner, Malcolm Crompton, says: "We need the social debate to make sure we use these technologies the way we want them to be used, we need to demand that technologies are developed the right way, we need laws in place, as appropriate, to back up those social norms." (ABC News Australia 12 Jun 2003)

*Category 31.3* *New technology with security implications*

2003-06-16 **RECONFIGURABLE chip designs laptops**

NewsScan

RECONFIGURABLE CHIP DESIGN
A coming trend in chip design will be the use of software that can, in an instant, reconfigure a microchip's circuitry. Paul Master of QuickSilver, which has created a prototype the chip, says: "Until now, the hardware had to match the problem. Now we can change that." Possible uses of reconfigurable chips will include: cell phones that can work anywhere in the world; portable computers that can wirelessly and automatically connect to the Internet using the most suitable radio frequency; and consumer electronics devices that can easily adjust to every new technical standard in digital sights and sounds. (New York Times 16 Jun 2003)

*Category 31.3* *New technology with security implications*

2003-06-18 **united airlines E-Mail domestic flights attachments**

NewsScan

UNITED TO OFFER E-MAIL ON DOMESTIC FLIGHTS
By the end of the year, United Airlines will become the first domestic airline to offer e-mail on all of its domestic flights. Industry analyst Jonathan Gaw of IDC says the service will be a good attraction for business users, who both need their e-mail and who can expense it." For $15.98 a flight, a passenger will be able to send and receive e-mail and attachments, by connecting a laptop computer to a jack on the Verizon Airfone handset available throughout the plane. (Baltimore Sun 18 Jun 2003)

*Category 31.3* *New technology with security implications*

2003-06-23 **cell phone commerce buy stuff bookings paying**

NewsScan

EUROPEAN PAY-BY-CELL-PHONE PLANS
Four of Europe's top wireless carriers have created a new clearinghouse for taking payments for small purchases directly from mobile phone customers. Using the slogan "Pay for stuff with your mobile," the promoters are saying: "Our aim is for you to see it on music Web sites, when making a flight booking, or even when paying a bus fare." The carriers are Britain's Orange SA and Vodafone, Spain's Telefonica Moviles, and Germany's T-Mobile. (AP/San Jose Mercury News 23 Jun 2003)

*Category 31.3* *New technology with security implications*

2003-09-10 **internet control VoIP voice phone PC household equipment 802.11 wireless**

NewsScan

VINT CERF ON THE FUTURE OF VOIP
Vint Cerf, senior VP of Internet Architecture and Technology for MCI, talks about the next-generation phone services based on VoIP (voice over Internet protocol) that are now being rolled out: "You can show up at a hotel and register your normal telephone number — as long as you can plug in your PC to an Internet service. What that means is your visibility in the communications world is now portable. Wherever you are, your communications are (there also). You can control where things go. If someone's trying to send a fax, you can vector that to your e-mail as an attachment or vector it to a different fax machine. There's an incredible amount of interaction over what had been completely separate services." Looking to the future, Cerf says the most important next-generation service is the ability to use the Internet as a household control system. "If you're like me, you have consumer equipment with remotes around the house. I can't figure out which one's which. And once I get the right one, the batteries are dead. Why not Internet-enable everything? Then it's possible to just have a single radio-based device, maybe 802.11-enabled, that lets you interact with all those appliances. You don't even have to be home. Obviously there are some security issues involved. You need strong authentication to make sure some 15-year-old next door won't reprogram your house." (CNet News.com 10 Sep 2003)

*Category 31.3* *New technology with security implications*

2003-09-18 **Intel wireless future radio peer-to-peer mesh network access technology WiMax 802.16**

NewsScan

INTEL BETS ON WIRELESS FUTURE
Intel chief technology officer Patrick Gelsinger says the chip giant is focusing on a wireless future and is contributing to a "renaissance of the radio" through research in antennas, networks and other technology. At this week's Intel Developer Forum, Gelsinger demonstrated Intel's MIMO (multiple input, multiple output) antenna technology, which adds multiple antennas to both transmitters and receivers to improve performance significantly. He told participants that the company is also exploring the concept of a "mesh" network, which enables devices on a wireless network to communicate more easily using the same idea behind peer-to-peer networks. "We want to make wireless 'the' access technology. Simply put, no more copper," said Gelsinger. Future plans also call for new chips based on the 802.16 WiMax standard. WiMax, or Worldwide Interoperability for Microwave Access, is being touted as a broadband wireless access alternative to cable, DSL and other last-mile technologies. (CNet News.com 18 Sep 2003)

*Category 31.3* *New technology with security implications*

2003-10-02 **security risk overlook telephone VoIP voice over IP**

NewsScan

OVERLOOKED SECURITY RISK: THE TELEPHONE
As corporate phone systems become increasingly complex and computerized, criminals are finding new ways to infiltrate company networks, and the problem becomes magnified as businesses turn to IP-based phone systems. "This is the first time that a computer virus can stop your telephones from working," says PricewaterhouseCoopers senior manager Mark Lobel. "There is a whole new class of attacks that can occur. The essence of the problem is that everyone is looking at this as a new technology for voice — the way we're sending voice communications is absolutely new. But the data is still riding on the same infrastructure that was pounded by recent problems like SoBig." To counteract the threats, phone system administrators need to be much more vigilant about password management and may even consider locking out certain country codes. "In fact, you should probably consider the risk associated with VoIP systems to be as high as the threats to your organization's most sensitive data. If someone in your IT department gets paged when your firewall goes down, they should also be paged when 40 new voicemail boxes mysteriously appear on your IP system," says Lobel. (E-Commerce Times 2 Oct 2003)

*Category 31.3* *New technology with security implications*

2003-10-19 **self-destructing e-mail Microsoft Office 2003**

NewsScan

MICROSOFT TOUTS SELF-DESTRUCTING E-MAIL
Microsoft's new Office 2003 software, set to debut on Tuesday, will include an e-mail feature that can be used to time-stamp messages, directing them to delete themselves on a certain date. In addition, senders will be able to restrict forwarding and printing of messages by the recipient. The new Information Rights Management software could run into opposition from U.S. regulators, who view destroying e-mail as on a par with shredding documents. Earlier this year, Morgan Stanley was fined $1.65 million for failing to keep e-mail records, despite the company's claim that it due to oversight rather than a deliberate attempt to evade financial investigation. (BBC News 19 Oct 2003)

*Category 31.3 New technology with security implications*

2003-10-21 **stereo Japan download online music copyright intellectual property**

NewsScan

NEW STEREO LINKS DIRECTLY TO ONLINE STORE
Four major Japanese electronic makers have unveiled a prototype of a next-generation audiovisual system that downloads music directly from the Internet without a PC and is expected to hit the shelves in Japan early next year. Officials from Sony, Sharp, Pioneer and Kenwood said there are no plans to distribute the Linux-based device outside Japan. The test models from Any Music Planning sport Ethernet ports and LCDs automatically set to access a Web site run by LabelGate, a Japanese online music store. Users can browse, download, store and play songs, which can also be recorded on mini-disc or transferred to other devices. "Ultimately, our dream is to make the service a worldwide standard," says Any Music CEO Fujio Noguchi. (AP 21 Oct 2003)

*Category 31.3 New technology with security implications*

2003-10-30 **superfast new processor Israeli company Enlight electron computation**

NewsScan

COMPUTING AT THE SPEED OF LIGHT
Israeli tech firm Lenslet has developed a superfast processor called EnLight that uses light rather than electrons to perform calculations at 8 trillion arithmetic operations per second. EnLight's optical circuits use a process called vector matrix-multiplication, which allows calculations to be performed on 256 optical inputs. The beams from these lasers are then added or multiplied together when shone on a device called a spatial light modulator, and the output is read by an array of light detectors. Lenslet founder Aviram Sariel notes that EnLight "is not a general purpose processor like a Pentium," but his company plans to custom-build the processors to perform a specific set of tasks for each client. Prices could range in the tens of thousands of dollars for each EnLight processor. (New Scientist 30 Oct 2003)

*Category 31.3 New technology with security implications*

2003-10-30 **USB flash drives data leakage security policies precautions**

Network World Fusion Security Newsletter
http://www.nwfusion.com/newsletters/sec/2003/1027sec1.html &
http://www.nwfusion.com/newsletters/sec/2003/1027sec2.html

Gone in a Flash

by John Bumgarner, MA, CISSP, GCIH, IAM, SSCP
& M. E. Kabay, PhD, CISSP

In the movie "The Recruit," (Touchstone Pictures, 2003) an agent for the Central Intelligence Agency (played by Bridget Moynahan) downloads sensitive information onto a tiny USB flash drive. She then smuggles the drive out in the false bottom of a travel mug. Could this security breach (technically described as "data leakage") happen in your organization?

Yep, it probably could, because most organizations do not control such devices entering the building or how they are used within the network. These drives pose a serious threat to security. With capacities currently ranging up to 2 GB (and increasing steadily), these little devices can bypass all traditional security mechanisms such as firewalls and intrusion detection systems. Unless administrators and users have configured their antivirus applications to scan every file at the time of file-opening, it's even easy to infect the network using such drives.

Disgruntled employees can move huge amounts of proprietary data to a flash drive in seconds before they are fired. Corporate spies can use these devices to steal competitive information such as entire customer lists, sets of blueprints, and development versions of new software. Attackers no longer have to lug laptops loaded with hacking tools into your buildings. USB drives can store password crackers, port scanners, key-stroke loggers, and remote-access Trojans. An attacker can even use a USB drive to boot a system into Linux or other operating system and then crack the local administrator password by bypassing the usual operating system and accessing files directly.

On the positive side, USB flash drives are a welcome addition to a security tester's tool kit. As a legitimate penetration tester, one of us (Bumgarner) carries a limited security tool set on one and still has room to upload testing data. For rigorous (and authorized) tests of perimeter security, he has even camouflaged the device to look like a car remote and has successfully gotten through several security checkpoints where the officers were looking for a computer. So far, he has never been asked what the device was by any physical security guard.

This threat is increasing in seriousness. USB Flash drives are replacing traditional floppy drives. Many computers vendors now ship desktop computers without floppy drives, but provide users with a USB flash drive. Several vendors have enabled USB flash drive support on their motherboard, which allows booting to these devices. A quick check on the Internet shows prices dropping rapidly; Kabay was recently given a free 128 MB flash drive as a registration gift at a security conference. The 2 GB drive mentioned above can be bought for $849 as this article is being written; 1GB for $239; 512 MB for $179; 256 MB for $79; and 128 MB for $39.

In the next part of this two-part series, John and I will look at preventive measures for safe use of these devices.

* * *

In the last column, security expert John Bumgarner and I looked at the potential for data leakage introduced through the use of small portable USB flash drives.

To counter the threats presented by USB Flash drives organizations need to act now. Organizations need to establish a policy which outlines acceptable use of these devices within their enterprises.

* Organizations should provide awareness training to their employees to point out the security risk posed by these USB Flash drives.

* The policy should require prior approval for the right to use such a device on the corporate network.

* Encrypting sensitive data on these highly portable drives should be mandatory because they are so easy to lose.

* The policy should also require that the devices contain a plaintext file with a contact name, address, phone number, e-mail address and acquisition number to aid an honest person in returning a found device to its owner. On the other hand, such identification on unencrypted drives will give a dishonest person information that increases the value of the lost information – a bit like labeling a key ring with one's name and address.

* Physical security personnel should be trained to identify these devices when conducting security inspections of inbound and outbound equipment and briefcases.

Unfortunately, the last measure is doomed to failure in the face of any concerted effort to deceive the guards because the devices can easily be secreted in purses or pockets, kept on a string around the neck, or otherwise concealed in places where security guards are unlikely to look (unless security is so high that strip-searches are allowed). That doesn't mean that the guards shouldn't be trained, just that one should be clear on the limitations of the mechanisms that ordinary organizations are likely to be able to put into place.

Administrators for high security systems may have to disable USB ports altogether. However, if such ports are necessary for normal functioning (as is increasingly true), perhaps administrators will have to put physical protection on those ports to prevent unauthorized disconnection of connected devices and unauthorized connection of flash drives.

Because without appropriate security, these days your control over stored data may be gone in a flash.

* * *

John Bumgarner < mailto:john.bumgarner@cyberwatchinc.com > is President of Cyber Watch, Inc. < http://www.cyberwatchinc.com >, a security consulting firm based in Charlotte, NC. John has a rich background in national security and international intelligence and security work.

*Category 31.3* *New technology with security implications*

2003-10-30 **DRM copy management BMG sales boos Anthony Hamilton music CD**

NewsScan

COPY-MANAGED CD BOOSTS SALES FIGURES
BMG Entertainment is cautiously optimistic about its latest experiment in discouraging music copying. The new Anthony Hamilton album, "Comin' From Where I'm From," hit the shelves in late September on a CD with built-in "copy management" technology. Buyers were limited to making three copies of the CD, and BMG says so far, the Hamilton album has experienced a slower-than-average sales drop-off — 23% vs. the typical 40-60% after the first week. "I know my science well enough to know that correlation does not mean causation," says Jordan Katz, senior VP of sales at BMG's Arista label. "I would not go out on a limb and say this was the only reason [sales] were down only 23%. However, I would say it was a contributing factor." The CD also allows users to e-mail songs to friends, who can download and play them on their computers for 10 days before they expire. A lack of buyer backlash against the technology has prompted Katz to put the copy management software on at least two more upcoming releases. (Washington Post 30 Oct 2003)

*Category 31.3* *New technology with security implications*

2003-11-12 **ibm linux desktop operating system simplified computing scott handy**

NewsScan

IBM'S LINUX STRATEGY
IBM vice president Scott Handy says, "There is a lot of interest in Linux on the desktop from customers; this is definitely a trend with traction." IBM is now using Linux as the desktop operating system in a simplified computing environment that delivers, updates and maintains desktop applications over high-speed corporate networks. "The discussion with customers usually starts with Linux. But the huge gains come from using this server-based architecture, which is made possible by these Internet technologies. And Linux is one of them." Handy says IBM's Linux solutions could be easily adopted by bank branch offices, sales people, insurance agents, auto dealers and others. (New York Times 12 Nov 2003)

*Category 31.3* *New technology with security implications*

2003-11-18 **cell phone secure conversation freedom phone XDA microsoft**

NewsScan

NEW CELL PHONE OFFERS SECURE CONVERSATION
German-based Cryptophone has developed a mobile handset that guarantees your conversation won't be tapped into by unscrupulous competitors or your local law enforcement officials. And while some observers say such phones could promote nefarious activities by the criminal crowd, privacy lobbyists say the new device is more of a "freedom phone" than a "terror phone." "It's a tremendous step forward, because the level of surveillance by authorities is breathtaking," says Simon Davies, director of the U.K.'s Privacy International. The Microsoft-based XDA handheld computer phone sells for about €3,499 (about $4,121) for two handsets, a price point that ensures the gadgets will be targeted at the corporate market. "Not many average consumers will pay that kind of money. The people who will be using it are in business," says Ian Brown, director of the Foundation for Information Policy Research in Britain. (Reuters 18 Nov 2003)

*Category 31.3* *New technology with security implications*

2003-12-09 **Internet Protocol Voice VoIP Time Warner digital data plug regular phones**

NewsScan

TIME WARNER TO OFFER VOIP
The cable unit of Time Warner has developed a plan to send telephone calls using Internet protocol (VoIP) technology. VoIP sends phone calls as digital data over the Internet and lets customers plug regular phones into modems connected to the cable wire in their homes. Still, the chief executive of Time Warner Cable is not ready to declare victory over traditional phone companies, because those companies have the overwhelming share of the local telephone market, and "they're going to be around for a long time." (New York Times 9 Dec 2003)

*Category 31.3* *New technology with security implications*

2003-12-16 **ipass T-mobile wi-fi wireless internet Ken Denman HotSpot mobile**

NewsScan

T-MOBILE TEAMS WITH IPASS ON WI-FI ROAMING
T-Mobile USA and iPass, two of the top U.S. wireless Internet access providers, have inked a Wi-Fi roaming agreement that will enable mobile workers to access the T-Mobile HotSpot network through the iPass virtual network. The move could spark broader adoption of Wi-Fi technology by corporations, which have lagged behind consumers in Wi-Fi use. Part of the reluctance on businesses' part has stemmed from security concerns, but they also have been waiting for the emergence of a nationwide service with broad coverage and enhanced reliability before jumping on the Wi-Fi bandwagon. "The Wi-Fi vision of both iPass and T-Mobile are in synch," says iPass chairman and CEO Ken Denman. "Both companies believe the addition of the T-Mobile HotSpot network to the iPass global Wi-Fi network of business-oriented venues represents a major step closer to the tipping point of Wi-Fi by the enterprise." (Financial Times 16 Dec 2003)

# 32.1 Censorship in the USA

*Category 32.1* *Censorship in the USA*

2003-02-20 **online content filter Internet law child pornography ISP Internet service provider**

NewsScan

OPPOSITION TO SOFTWARE FILTERING LAW
The Washington-based civil liberties group Center for Democracy and Technology is considering a legal challenge to a Pennsylvania law that threatens fines on any company providing Internet access to Web sites with child pornography rather than fines on the pornographic sites themselves. CDT associate director Alan Davidson says, "It's sort of this weird world where we're not prosecuting the people producing child pornography," and instead harassing Internet service providers whose existence is necessary for the stability of the Internet. (AP/San Jose Mercury News 20 Feb 2003)

---

*Category 32.1* *Censorship in the USA*

2003-03-04 **children Internet SCOTUS constitutionality free speech pornography violence law**

NewsScan

SUPREME COURT TO REVIEW INTERNET FILTER LAW
The U.S. Supreme Court has agreed to consider the constitutionality of the Children's Internet Protection Act, which requires that libraries receiving federal funding for Internet access must install software filters to prevent children from being exposed to pornography and excessive violence. A coalition of libraries, library users and Web sites successfully challenged the law at the appellate level, where the court ruled that filters were "blunt instruments" that would suppress not only pornography and violence but constitutionally protected speech presented on legitimate sites. It is now being argued that the lower court was wrong when it viewed the case as a first amendment case, and should instead have treated it as one involving the government's broad discretion to decide whether material is sufficiently worthwhile for the government to required to support it with public funds. The government argues that to assert otherwise is to argue that public libraries engage in prior restraints when they fail to provide pornographic magazines or XXX videos to their patrons." (New York Times 13 Nov 2002)

SOFTWARE FILTERING CASE GOES TO SUPREME COURT
Tomorrow the U.S. Supreme Court will hear arguments in a case challenging the constitutionality of the Children's Internet Protection Act of 2001, which requires any library that receives federal money to block access to online pornography and obscenity. In support of the Act, U.S. Solicitor General Ted Olson says that libraries are being asked merely to use the same kind of discretion they've always used in managing their print collections: "Public libraries have broad discretion to decide what material to add to their collections. The use of filtering software to block access to online pornography falls well within the permissible limits of that discretion. (USA Today 3 Mar 2003)

---

*Category 32.1* *Censorship in the USA*

2003-04-16 **free speech censorship hacking information techniques lecture**

NIPC/DHS

April 14, CNET News.com — Court blocks security conference talk. Washington D.C.-based education software company Blackboard convinced a Georgia state court to block a pair of students from presenting information at a security and hackers' conference on how to break into and modify a university electronic transactions systems. Blackboard argues that the restraining order blocked the publication of information gained illegally, which would have harmed the company's commercial interests and those of its clients. But organizers of the Interz0ne conference in Atlanta contend that Georgia Institute of Technology's Billy Hoffman and University of Alabama's Virgil Griffith's free speech rights were abridged. The information set to be presented was gleaned after one of the students had physically broken into a network and switching device on his campus and subsequently figured out a way to mimic Blackboard's technology, the company told the judge. Because that alleged act would be illegal under the federal and state laws, publication of the resulting information should be blocked, it argued. A hearing on a permanent injunction against publication or presentation of the work will be held in Georgia state court Wednesday.l

---

# 32.2 Censorship outside the USA

*Category 32.2* *Censorship outside the USA*

2003-03-06 **Internet content filtering pornography**

NewsScan

THE AUSTRALIAN APPROACH TO SPAM
Clive Hamilton, the head of an Australian public think tank, thinks that Australia's method of Internet regulation, managed by the Australian Broadcasting Authority, is essentially useless. Referring to a survey finding that 84% of boys ages 16-17 are exposed to pornography on the Internet, Hamilton complained: "The Internet industry has convinced the government that there is little that can be done to prevent pornography coming in from overseas. But this is false. Mandatory filtering by Internet service providers (ISPs) would severely restrict the availability of pornography." Labor information technology spokeswoman Kate Luncy disagrees: "The cost this would place on ISPs would be prohibitive and Internet speeds would be significantly reduced. The end result for consumers would be a slower, more expensive Internet." (The Age 4 Mar 2003)

# 33.1 Acceptable use policies

*Category 33.1* *Acceptable use policies*

2003-01-24 **Internet access office work appropriate use economics**

NewsScan

CRACKDOWN ON OFFICE SURFING COULD AFFECT WEB PROFITS
Office workers with corporate broadband networks have long enjoyed high-speed access to online entertainment, shopping and other personal pursuits, but a widespread crackdown on non-work-related Internet use may be looming, driven by cost-cutting efforts and increased scrutiny of workers' surfing habits. "I think it was an issue of productivity — people were spending too much time on these sites. I know people who were bidding on eBay all day long," says one office worker who admits to logging on to online dating sites several times a week. According to Websense, an estimated $85 billion in productivity is lost annually to workers wasting time on the Net. But the corporate backlash is bad news for Web sites courting broadband users at a time when nearly 87% of people accessing the Net from work are using a broadband connection, compared with about 28% from home. Companies that stand to lose from the crackdown include game sites like "The Sims," e-commerce hot spots like eBay, online dating sites like Matchmaker.com, and news and entertainment outlets offering rich media formats such as video and audio clips. "Given that about 40% of the activity (in many of these areas) is coming from work, if (blocking) became a pervasive practice in the workplace, it would impact the business," says a Bear Stearns analyst. A network performance analyst at a Fortune 10 company argues that companies have to take steps to protect their network resources: "If you're looking at a company with an $82 million IT budget, and 10% of the network is going to nonwork uses, you're saving $8 million if you can stop it." (CNet News.com 24 Jan 2003)

---

*Category 33.1* *Acceptable use policies*

2003-02-06 **appropriate use productivity work telecommuting Internet access home**

NewsScan

PEOPLE WHO PLAY AT WORK, WORK AT HOME
What employers lose in productivity when workers goof off, bidding on eBay and circulating jokes, is made up in the home, according to a survey by the University of Maryland and Rockbridge Associates. The study found that employees with Web access both at home and at work spend an average of 3.7 hours a week doing personal online chores in the office. Those same employees, however, spend an average of 5.9 hours a week at home catching up on work. "I think what this says is the Internet is actually helping business productivity," says Roland Rust, director of the Center for eService at the U. of Md.'s Robert H. Smith School of Business. Rust warns that, based on his findings, employers should think twice about banning personal online activities in the office. (Wall Street Journal 6 Feb 2003)

---

*Category 33.1* *Acceptable use policies*

2003-02-13 **copyright intellectual property piracy violations guide policy employers corporations**

NewsScan

FILM, MUSIC GROUPS TARGET WORKPLACE PIRATES
The Recording Industry Association of America and the Motion Picture Association of America have published a guide for employers, asking major corporations to curb illicit file-swapping by workers on company time. The guide, titled "A Corporate Policy Guide to Copyright Use and Security on the Internet," requests that businesses advise employees against copyright abuse using corporate computer systems and warns that such abuse is illegal, damages corporate reputations, increases corporate network security risks, and can put organizations at risk of legal liability. The guide cites a case in which an Arizona company paid a $1 million settlement in April 2002 to the RIAA after workers were found to be accessing and distributing thousands of music files via the company server. (Reuters 13 Feb 2003)

---

*Category 33.1* *Acceptable use policies*

2003-03-14 **copyright intellectual property rights education awareness**

NewsScan

INTERNET BOOKENDS: #1, KAHN ON COPYRIGHT
Internet co-founder (with Vint Cerf) Bob Kahn is head of the Corporation for National Research Initiatives (CNRI), which he founded in 1986. In an interview with John Gehl for the ACM online publication Ubiquity, Kahn talks about the state of the Internet, including the need for more education about copyright law: "We [at CNRI] have been promoting copyright and, more generally, intellectual property protection in the network probably as much as anybody in the research world. CNRI built a system for the U.S. Copyright Office to manage the registration of copyright claims and the attendant submission of copyright information and digital objects online; the system is called CORDS (cords.loc.gov). In my view, one of the problems that has not been satisfactorily dealt with in this country is the widespread lack of respect for the value of intellectual property. People think that they can do anything they want with intellectual property just because they themselves don't happen to see any cost associated with accessing it on the net and, perhaps sending it to others or otherwise using it. I think this is clearly an educational issue as much as it is a constitutional issue." (Ubiquity 13 Mar 2003)
http://www.acm.org/ubiquity/interviews/r_kahn_1.html

---

*Category 33.1* *Acceptable use policies*

2003-03-18 **copyright infringement intellectual property workplace piracy monitoring employers liability**

NewsScan

RECORD LABELS WARN COMPANIES OF 'SIGNIFICANT LEGAL DAMAGES'
The Recording Industry Association of America has sent letters to about 300 companies, informing them that their computers were being used by workers for illegal file-swapping and threatening "significant legal damages" for employers and employees alike. The new tactic is the RIAA's first systematic effort to tackle digital music piracy that occurs using corporate networks, following a similar effort to enlist universities in the fight against illegal file-sharing. Copyright law experts said companies might be liable for piracy on their networks if they know about it and don't intervene, but it's unclear whether companies have an obligation to police their networks and remove unauthorized copies of songs without being asked to. "I think what they're trying to do is get people thinking 'Gee, I'm in this gray area, and I don't want to be the guy who gets fingered for the test case,'" says one intellectual property attorney. "As a corporation, do you really want to be in the news defending the right of your employees to have pirated music on your network?" About 35% of the letters went to information technology companies, 20% to healthcare firms, 20% to manufacturers, and the rest to miscellaneous industries. (Los Angeles Times 18 Mar 2003)

---

*Category 33.1* *Acceptable use policies*

2003-03-26 **pornography library government computer usage trial**

NIPC/DHS

LIBRARY PORN CASE GOES TO TRIAL
A group of librarians in the Minneapolis library system has filed a federal lawsuit against that system, alleging that administrative failures have created an intimidating, hostile and offensive workplace. "We were living in hell, and they were unwilling to acknowledge the problem," says one librarian. The dispute arose in 1997, soon after the Minneapolis libraries installed Internet access, and a number of library visitors began displaying on publicly accessible computer images of "virtually every imaginable kind of human sexual conduct." (AP/USAToday 26 Mar 2003)

---

*Category 33.1* *Acceptable use policies*

2003-04-22 **copyright infringement University Pennsylvania student accounts revoked**

NewsScan

PENN STATE PULLS THE PLUG ON STUDENTS' ACCOUNTS
Pennsylvania State University has suspended the Internet accounts of about 220 students after investigations showed they were using the school's broadband network to trade in "publicly listed copyright infringing materials." The school said connections will be restored once the copyrighted files have been removed from the systems. The move came about a month after the school had issued a warning to its 110,000 students, alerting them that illegal trading of copyrighted materials was against the law, and just weeks after the Recording Industry Association of America slapped four students at Rensselaer Polytechnic Institute, Princeton University and Michigan Technological University with lawsuits. (Internet News 22 Apr 2003)

---

*Category 33.1* *Acceptable use policies*

2003-09-12 **state workers e-mail privacy publicity pubilc documents private business venture first amendment advocates**

NewsScan

STATE WORKERS' PRIVATE E-MAIL IS PRIVATE
The Florida Supreme Court ruled Thursday that state workers' private e-mails cannot be treated as public documents just because they are created or stored on government computers. The ruling came in a case brought by the St. Petersburg Times, which had sued the city of Clearwater for access to the e-mail records of two city employees who had exchanged messages regarding a private business venture. The city allowed the workers to determine which e-mails should be made public, a decision challenged by the newspaper and First Amendment advocates. Florida Attorney General Charlie Crist expressed disappointment with the ruling: "If the taxpayers pay for the computers, they ought to have the right to see what's on them." St. Pete Times attorney George Rahdert noted that the 1967 law covering public records was written before electronic communications were commonplace. "The problem is public records law is kind of paper-bound. It doesn't really account for the way that people are communicating important information." (St. Petersburg Times 12 Sep 2003)

---

*Category 33.1* *Acceptable use policies*

2003-10-03 **peer-to-peer copyright infringement file-sharing University of Florida**

NewsScan

U. OF FLORIDA PULLS THE PLUG ON P2P USERS
Students returning to the University of Florida this fall have discovered a new utility on the school network: Icarus (Integrated Computer Application for Recognizing User Services), a open-source program developed by campus personnel to thwart students' obsession with peer-to-peer file-sharing. Last spring, the university received about 40 notices of copyright violations per month and at peak times 90% of all the traffic on the housing network was P2P. "We needed something to stem the flow. We were spending too much time tracking people down," says Robert Bird, supervisor of network services for UF's housing department, who reports that the debut of Icarus has reduced P2P use by 90%. When students first register on the UF network, they must pledge not to share copyright files. Icarus then scans their computer, flags any worms, viruses or file-sharing software, and gives instructions on how to disable those programs. First-time offenders receive a pop-up warning and are disconnected from the campus network for 30 minutes, but a repeat performance results in being disconnected for five days. Third-time violators are subject to the school's judicial process and are cut off form the network indefinitely. The new system has some students grumbling, but most seem resigned to the new restrictions. "While file-sharing is nice, it's not worth risking college or your future," says one. (Wired.com 3 Oct 2003)

---

*Category 33.1* *Acceptable use policies*

2003-11-05 **personal surfing good thing increase productivity lower stress**

NewsScan

PERSONAL SURFING AT WORK CAN BE A GOOD THING
Here's a new book that turns conventional wisdom about personal surfing on company time on its head. Claire Simmers and Murugan Anadarajan have co-authored a human resources guide to worker Web use that indicates a looser attitude toward personal surfing can yield some beneficial side effects. "Personal Web usage in the workplace has a negative perception, especially among administrators who often see it as inefficient and creating a decrease in work productivity," says Simmers. But according to the authors' research, personal surfing at work can result in better time management, lower stress levels, improved skill sets and a happier balance between work and personal life. (AP 5 Nov 2003)

---

# 33.2 Spam

*Category 33.2* *Spam*

2003-01-06 **spam consumer attitudes**

NewsScan

SURPRISE — MOST E-MAIL USERS HATE SPAM
In an anticlimactic finding, a Harris Interactive poll released Friday reveals that 96% of the 2,221 respondents find unsolicited commercial e-mail annoying, and nearly three quarters of those favor making spam illegal. Pornographic spam messages were deemed most troublesome, according to 90% of respondents, while 79% cited mortgage and loan come-ons as objectionable. Less annoying (but not by much) were investment opportunity and real-estate spam. Meanwhile, consumers needn't look for a break from spam mail any time soon — despite a recent crackdown by the Federal Trade Commission on fraudulent schemes advertised on the Internet, the incidence of spam continues to grow. According to anti-spam software maker Brightware, unsolicited messages made up 40% of all e-mail in November — up from 13% a year earlier. The Senate Commerce Committee passed a bill last May to set guidelines for unsolicited e-mail, but no further action has been taken by the full Senate. (Wall Street Journal 3 Jan 2003)

---

*Category 33.2* *Spam*

2003-04-29 **spam zombies relay junk e-mail Trojan horses proxy crime**

NIPC/DHS

April 25, SecurityFocus — Rise of the spam zombies. Pressed by increasingly effective anti-spam efforts, senders of unsolicited commercial e-mail are using Trojan horses to turn the computers of innocent netizens into secret spam zombies. One of those programs, popped up last week. "Proxy-Guzu" arrives as a spam, and when executed by an unwitting user, the Trojan listens on a randomly-chosen port and uses its own built-in mail client to dash off a message to a Hotmail account, putting the port number and victim's IP address in the subject line. The spammer then routes as much e-mail as he or she likes through the captured computer, knowing that any efforts to trace the source of the spam will end at the victim's Internet address. "As a general rule it's legal to send someone an e-mail even if they don't want it," says Mark Rasch, a former Justice Department computer crime attorney. "But once you break into their computer and get their computer to send e-mail to someone else, then you're violating federal and state computer crime laws."

---

*Category 33.2* *Spam*

2003-04-30 **spam spyware adware relay viruses hijack Outlook ICSA**

NewsScan

SPAMMERS USE VIRUSES TO HIJACK COMPUTERS
As efforts to tackle junk e-mail ramp up, unscrupulous spammers increasingly are hiding their identities by taking over innocent users' accounts using e-mail messages that resemble computer viruses. Like many other viruses, these programs exploit weaknesses in Microsoft's popular Outlook e-mail package. One of the first hijacking programs to emerge was called "Jeem," which contained a hidden e-mail engine that enabled it to route messages via the infected computer. Another, called Proxy-Guzu, comes as a spam message with an attachment. When the unsuspecting recipient clicks on the attachment, the computer contacts a Hotmail account and transmits information about the infected machine, making it possible to route e-mail through that machine. "Spammers are beginning to use virus-like techniques to cover themselves," says Larry Bridwell, content security programs manager at ICSA Labs. "Spam is one of the two things that the security industry is going to be asked to deal with. The other is adware or spyware." (BBC News 30 Apr 2003)

---

*Category 33.2* *Spam*

2003-05-01 **spam cell phones text messages 2025551212@cellphonecarrier.com telemarketers**

NewsScan

SPAM HEADING FOR CELL PHONES
The spam that now accounts for as much as three-quarters of total e-mail volume is heading for a cell phone near you, according to a panel of telecom experts at a forum on spam held Thursday. Federal law prohibits most telemarketers from dialing cell phones, but there are no laws preventing them from sending text messages to addresses like 2025551212@cellphonecarrier.com. Because many text messaging services carry a per-message charge, the cost to consumers could mount quickly. Text messaging has yet to catch on in the U.S., and it may never happen if spammers start exploiting it, said phone-company officials. Wireless spam is already a problem in Japan, where text messaging has been a popular feature for years. "As data traffic over wireless networks continues to grow, so will spam," warned an NTT executive. (Reuters 1 May 2003)

---

*Category* *33.2* *Spam*

2003-05-20 **spammer your computer money issue hijacking backdoor software**

NewsScan

ARE YOU A SPAMMER?
Hundreds of thousands of computers are now being used without their owners' knowledge to forward spam around the world. William Hancock, chief security officer of Cable & Wireless, says: "This is not about a hacker trying to show off, or give you a hard time. This is about money. As long as there are people who want spam to go out, this is not going to go away." And how do the hijacked victims feel? They usually feel ignorant and in the dark. A network abuse engineer with Earthlink explains, "People are shocked. Someone will say, 'I thought my computer was running a little slow, but I had no idea it was being used to send spam.'" A common way for spammers to pull this trick off is to use a backdoor in the software used to link several computers or "proxy servers." (New York Times 20 May 2003)

*Category* *33.2* *Spam*

2003-05-20 **hacker hijack computer remotely spam e-mailers messages bounce AOL KaZaA virus software computer**

NIPC/DHS

May 20, New York Times — Hackers hijack computers remotely in new surge of spam. As spam has proliferated many mass e-mailers have become more clever in avoiding the blockades by aggressively bouncing messages off the computers of unaware third parties. In the last two years, more than 200,000 computers worldwide have been hijacked without the owners' knowledge and are currently being used to forward spam, according to AOL and other Internet service providers. Last Thursday, 17 law enforcement agencies and the Federal Trade Commission issued a public warning about some of the ways spammers now commandeer computers to evade detection. Mostly, the spammers are exploiting security holes in existing software, but increasingly they are covertly installing e-mail forwarding software, much like a computer virus. In the last six months, an increasingly common trick has been for spammers to attach rogue e-mail-forwarding software to other e-mail messages or hide it in files that are meant to emulate songs on music sharing sites like KaZaA.

*Category* *33.2* *Spam*

2003-05-22 **spam battle Direct Marketing Association DMA e-mail advertisements $7 billion sales**

NewsScan

STUDY SHOWS SPAM PAYS
While the battle against spam intensifies, the Direct Marketing Association has just released figures showing that commercial e-mail advertisements generated more than $7 billion in sales last year. The DMA's study is intended to bolster its claim that commercial e-mail plays a significant role in the U.S. economy. According to the report, about 36% of e-mail users, or 21% of all adult Americans, have purchased a product or service as the result of receiving commercial e-mail over the past year, with purchases valued at an average of $168. About 9% of these e-mail users said they made their purchases as the result of unsolicited commercial e-mail. (Wall Street Journal 22 May 2003)

*Category* *33.2* *Spam*

2003-06-25 **spam E-Mail Ronnie Scelson spammer**

NewsScan

SPAMMER: 'I HATE SPAM AS MUCH AS THE NEXT GUY'
Ronnie Scelson, known as the Cajun King of Spam, sees himself as a good spammer, not a bad spammer: "I hate spam as much as the next guy. What I do is not illegal. It's the people who spam sex, Viagra, and get-rich-quick schemes that give commercial e-mailers a bad name. He says that the 60-70 million ads he send out each day all give customers the option to be removed from mailing lists, do not hide behind forged e-mail addresses, do not get routed through foreign relays, and always leave contact information. Scelson makes more than $30,000 a month when business is good, and lives a typical middle-class life — except that he keeps a 9mm gun close to him because his life is threatened so often by anti-spammers. (USA Today 25 Jun 2003)

*Category* *33.2* *Spam*

2003-07-28 **spam costs e-mail insfrastructure**

NewsScan

THE COSTS OF SPAM (NOT INCLUDING BLOOD PRESSURE MEDS)
Spam costs senders almost nothing, but takes a heavy toll on those who receive it. Ferris Research says the cost of spam is $10 billion in the U.S.; Nucleus Research pegs the figure at $87 billion. Is the problem being overblown? Wharton School marketing professor Peter S. Fader says: "I am deeply skeptical that these crude top-down methods are accurate. Hitting the delete key is far more efficient than carrying your physical mail from the mailbox over to the trash can." And he even sees an upside: "Spam, although it is a bad thing per se, is fostering the growth of the e-mail infrastructure." But that new infrastructure also comes with a price: Ferris Research says corporations will spend $120 million this year on antispam systems, and The Radicati Group claims the correct figure is closer to $635 million. Ah, what to do, what to do? America Online now discards, each day, nearly 2 billion e-mail messages flagged as spam — but then has to contend with complaints [including NewsScan] about "false positives" (mail falsely treated as spam). Ferris Research says: "We think companies lose $3 billion dealing with false positives." (New York Times 28 Jul 2003)

*Category* *33.2* *Spam*

2003-08-25 **spam spammer New Zealand give up threats**

NewsScan

NEW ZEALAND SPAMMER 'OUTED' — SAYS HE'LL GIVE IT UP
Shane Atkinson, a New Zealand man who was recently identified in a local newspaper as a major spammer, says he's giving up his business after being inundated with threatening phone calls and having his personal information posted on the Net. And while vigilantes may rejoice at such intimidation methods, industry analysts says the potential for wrongful targeting is too great and, in any event, there's always a steady supply of replacements. "You'll put a dent in it but somebody else will be there to take his place," says Gartner research director Maurene Caplan Grey. "The spam kings know how to get around the system. The only ones you'll frighten are the occasional spammers trying to make a few extra bucks this weekend." According to a recent estimate, about 200 spammers are responsible for 90% of the spam-mail sent out globally. Meanwhile, it's not just the spammers who profit from their activities; other beneficiaries include the providers of e-mail addresses, suppliers of spamming software, offshore Internet service providers and even legitimate spam-filtering software vendors. (TechNewsWorld/E-Commerce Times 25 Aug 2003)

*Category* *33.2* *Spam*

2003-09-02 **Spammer spiders chain letters collect e-mail addresses U.S. DoE Department Energy hoax advisory website web search usernames Spamfire**

NIPC/DHS

September 02, CNN — Spammers turn to chain letters to collect addresses. While not as efficient as "spiders" which automatically crawl the Web in search of addresses, computer experts warn that some spammers are using chain letters to collect e-mail usernames. "Chain letters are the ideal place to collect addresses. I've seen several hundred on one e-mail," said Bill Orvis, who maintains the U.S. Department of Energy's hoax advisory Web site. "Just by forwarding a message to a dozen friends, it only takes a few generations before you fill the network with messages," he said. Michael Herrick, whose Spamfire software helps individual users filter junk e-mail, doesn't think spammers are using chain letters in this way. Herrick, however, admits that the practice could be a good way to bypass e-mail filters which block messages from senders who are not known to the recipient. Spammers could use chain letters to discover the addresses of people with whom you frequently communicate. Spam purporting to be from someone in your address book would sneak by filters.

*Category* *33.2* *Spam*

2003-09-11 **you've got spam sex to get attention e-mail holidays tricks terminator for governor**

NewsScan

BREAKING NEWS: YOU'VE GOT SPAM
Analyst Matt Cain of META Group says that spammers "used to use sex to get your attention, then e-mails tied to holidays like Mother's Day. Now, it's topical come-ons" such as breaking-news headlines "The intent of every spammer is to try every trick to get you to open a message." And Ken Schneider of Brightmail thinks the trend will grow and grow: "You can be sure there will be substantially more spam during the presidential primaries next year. People will take advantage of any current event to make a buck." More than 20 million messages with references to the California recall — many of them hawking "Terminator for Governor" T-shirts and adult DVDs for another candidate — were sent in the past month, and 100 million are expected before the recall election is over. Gubernatorial candidate and porn star Mary Carey is angry that a distributor of adult DVDs is using her run for office to sell two of her films for $14.95. "I'm very upset, because it offends people, and they're profiting from my name." (USA Today 11 Sep 2003)

*Category* *33.2* *Spam*

2003-11-11 **christmas spam spammonger Clearswift cheap loans festive gifts**

NewsScan

ALL I WANT FOR CHRISTMAS IS… MORE SPAM?
While you're decking the halls with boughs of holly, spammongers are cooking up their own holiday plans, which (surprise!) involve sending even more spam than usual! Net filtering firms report that spammers are already altering their messages in an attempt to cash in on the festive season, offering more single products and high-tech gadgets such as DVD burners as potential gifts. Oh, and of course — more cheap loans to pay for it all! "Not only are spammers developing more and more cunning ways of getting around e-mail filtering technology, but their marketing strategy is clearly up to scratch, too," says Alyn Hockey, research director at Clearswift, a spam filtering firm. Clearswift reports that the number of spam e-mails offering cheap loans aimed at Christmas shoppers doubled in October as a percentage of overall spam. (BBC News 11 Nov 2003)

*Category* *33.2* *Spam*

2003-11-13 **Spam clogs blogs ISP prevent spammers viagra Comment Spam Manifesto bloggers e-mail accounts disabled**

NewsScan

SPAM CLOGS BLOGS
Most weblogs are designed to allow readers to post comments on entries, but that capability is being abused by spammers, who leave remarks like "Sounds great!" submitted by names like "Generic Viagra," complete with links to questionable sites. Howard Rheingold, a futurist who touts the power of online communities, worries that the recent invasion could derail the revolution in public discourse just as it's gathering steam. "It forces you to either turn off the comments and lose some of the value of the medium, or spend your time deleting spam," says Rheingold. Meanwhile, some inveterate bloggers are taking matters into their own hands. Adam Kalsey, who's run his own blog for the past three years, has penned a "Comment Spam Manifesto," which warns spammers: "What you failed to understand is that bloggers are smarter, better connected and more technologically savvy than the average e-mail user. We control this medium that you are now attempting to exploit. You've picked a fight with is and it's a fight you cannot win." Kalsey tracks spammers down and reports them to their ISPs and domain registers in an effort to get their accounts canceled. "The blog immune system does seem to be responding," he says, noting that he receives help from other bloggers in his spam-slamming activities. (AP 13 Nov 2003)

*Category* *33.2* *Spam*

2003-12-31 **spim instant messenger spam clogging users pornography e-mail marketers**

NewsScan

GET READY FOR SPIM
Instant messenger spam, dubbed "spim," is increasingly clogging users' computers, popping up with the real-time regularity of instant messages and annoying users who complain they're now receiving several messages a day. Users can either accept or decline the spim, which often contains a link to — what else? — a pornography site. Ferris Research estimates about 500 million spim messages were sent in 2003, double the number sent in the previous year. And while instant-messenger spam "isn't nearly the industry that e-mail spam is,… it's starting to increase," says the CEO of an antispam consulting firm. Experts warn that the recent crackdown on conventional spam may push illicit marketers to explore new avenues, including instant messaging. "The irony is that focusing like a laser on our No. 1 concern — spam — has painted e-mail spammers into a corner like never before and incited them to find other ways to try and reach our membership online," says an AOL spokesman. (Wall Street Journal 31 Dec 2003)

# 33.3 Antispam

*Category 33.3* *Antispam*

2003-03-06 **anti-spam research**

NewsScan

THE IETF APPROACH TO SPAM
The Internet Research Task Force — loosely affiliated with the Internet Engineering Task Force standards group — has formed an Anti-Spam Research Group, which will focus on the problem of spam proliferation and make suggestions on ways to change basic e-mail technology to foil the bulk e-mailers. "Once considered a nuisance, spam has grown to account for a large percentage of the mail volume on the Internet," says the group's Web site. "The purpose of the [research group] is to understand the problem and collectively propose and evaluate solutions to the problem." First steps will include classifying different kinds of spam and antispam proposals, and studying ways to track down spammers, who are often difficult to identify. A first meeting is set for March 20 at the IETF's San Francisco gathering. (CNet News.com 6 Mar 2003)
http://news.com.com/2100-1032-991305.html

*Category 33.3* *Antispam*

2003-03-24 **anti spam software developed challenge response**

NIPC/DHS

NEW ANTI-SPAM SYSTEM BEING DEVELOPED
A California start-up company created by well-known software designer Phil Goldman (formerly of Apple, General Magic, WebTV and Microsoft) has designed an e-mail service that takes a "challenge-response" approach to blocking spam. When a user receives a bulkmail message from an unknown source the system intercepts the message and requires the sender to give indication (by filling out a form) that the message is not an instance of spam. The service will cost $9.95 a year, so Forrester Research analyst Jim Nail note skeptically: "It's a really nice product, and it's pretty easy to use. The question is how big a market. Do people want to pay anybody anything for these features?" (New York Times 24 Mar 2003)

*Category 33.3* *Antispam*

2003-03-25 **Hotmail outgoing spam Microsoft**

NIPC/DHS

HOTMAIL TARGETS OUTGOING SPAM
To fight unsolicited bulk commercial e-mail, Microsoft's free Hotmail e-mail service has limited to 100 the number of messages that a user can send in a 24-hour period. The limit, which was imposed earlier this month, will not apply to Hotmail subscribers who purchase extra storage. (AP/San Jose Mercury News 25 Mar 2003)

*Category 33.3* *Antispam*

2003-04-22 **anti spam debate**

NewsScan

THE BEAUTY OF SPAM IS IN THE EYE OF THE BEHOLDER
Brightmail, which makes spam-filtering software for corporations and Internet service providers, says that 45% of the mail it now sees is spam (unsolicited bulk-distributed messages), and AOL says 2 billion spam messages are sent to its 35 million customers each day, accounting for more than 70% of the total AOL incoming traffic. But the spam creators are getting tired of having figures like these flouted as though spam was a bad thing. Bob Dallas of an e-mail firm in Ohio says, "We have allowed these spam cops to rise out of nowhere to be self-appointed police and block whole swaths of the industry. This is against everything that America stands for. The consumer should be the one in control of this." E-mail marketer Alyx Sachs thinks the same way Bob Dallas does: "These antispammers should get a life. Do their fingers hurt too much from pressing the delete key? How much time does that really take from their day?" (New York Times 22 Apr 2003)

*Category 33.3 Antispam*

2003-04-24 **anti spam hide from spammers preserve e-mail address**

NewsScan

HOW TO HIDE FROM SPAM-MONGERS
Researchers at the Center for Democracy and Technology have competed a study that seeks to answer the question: how do spammers find you? They found that e-mail addresses posted on Web sites or in newsgroups attract the most spam, because spam-mongers use harvesting programs such as robots and spiders to collect e-mail addresses listed in those places. So if you've ever provided your e-mail address as part of an eBay transaction, or responded to an online job listing, or participated in a discussion board, it's likely that your e-mail address is now making the rounds on junk e-mail lists. One way to avoid the harvesting in the first place, says the team, is to replace characters in an e-mail address with human-readable equivalents — for example jane@domain.com would become jane at domain dot com. Another successful evasion technique is to replace the characters in an e-mail address with the HTML equivalent. Over the course of the six-month study, 97% of the spam was sent to addresses that had been posted on public Web sites, especially those that were linked to major portals such as AOL and Yahoo. (BBC News 24 Apr 2003)

*Category 33.3 Antispam*

2003-04-24 **anti spam initivate markerters consortium e-mail productivity**

NewsScan

CONSORTIUM OF ONLINE MARKETERS ANNOUNCES ANTI-SPAM INITIATIVE
The E-mail Service Provider Coalition (ESPC), a consortium of online marketers such as DoubleClick and iMakeNews, is launching what it calls Project Lumos, which will provide a way for high-volume e-mail senders to have their mailings certified by ESPC to ensure they follow ethical practices. Under Project Lumos there will be four levels of accountability: certification to ascertain the mailer's identity; standardization of all sender info including identification and trackability; proof of sender ID in the SMTP message header; and various performance monitoring activities. The project seeks to accommodate the interests not only of the receivers of commercial e-mail, but also those of the senders of such mail. According to ESPC, "E-mail is indeed a killer app and has been a major component in the productivity and efficiency gains of the digital economy. But those gains will be lost if e-mail becomes unreliable as a communications tool. Businesses will not be able to use e-mail if they cannot have a reasonable assurance that their messages will be delivered." (ComputerWorld 24 Apr 2003)

*Category 33.3 Antispam*

2003-05-22 **fight spam internationally Bill Gates protecting American computers anti-spam business lost productivity**

NewsScan

THE NEED FOR INTERNATIONAL COOPERATION TO FIGHT SPAM
The president of Brightmail (a company that helps Internet providers block spam) predicts that by the end of this year half of all e-mail will be spam messages, and says that spam costs U.S. businesses $10 billion a year in lost productivity. Microsoft chairman Bill Gates has called for international organizations to join the anti-spam effort, and Sen. Charles Schumer (D,NY) says: "As soon as we tighten up our laws here and institute vigorous enforcement, those who want to violate our laws move abroad. A global agreement will ensure that anti-spam standards protecting American computers are enforceable both here and abroad." (AP/San Jose Mercury News 22 May 2003)

*Category 33.3 Antispam*

2003-05-27 **spam cure disease Cnet blocking software death e-mail**

NewsScan

SPAM'S CURE COULD BE WORSE THAN THE DISEASE
CNet columnist Declan McCullagh worries that the proliferation of spam-blocking software incorporating challenge-response technology could lead to the death of e-mail. Challenge-response systems require the human sending a message to perform a simple task such as clicking on a link or typing a special password to get past the barrier. The problem is, says McCullagh, that many challenge-response systems are poorly designed, and could causes big headaches for administrators of legitimate e-mail newsletters (such as NewsScan Daily) that go out to large numbers of people. "Big corporations may be able to afford to hire someone to sit in front of a computer and spend all day proving they're not a spam bot, but nonprofit groups, individuals and smaller companies probably can't," says McCullagh. Earthlink has already announced its intentions to make a challenge-response system available to subscribers by the end of May, and other ISPs may follow suit — a scenario that has veteran list operators concerned. Dave Farber, a computer scientist at the University of Pennsylvania who runs the "interesting people" list, says: "If I start getting a flood of challenges from Earthlink IPers that require my response I will most likely declare them spam and you will stop receiving IP mail. I fully expect this to be the case for almost all the legitimate mailing lists you are on and count on." Meanwhile, editors at the popular Macintosh newsletter TidBits, have told readers: "Be warned that we will not answer any challenges generated in response to our mailing list postings. Thus, if you're using a challenge-response system and not receiving TidBits, you'll need to figure that out on your own." (CNet News.com 27 May 2003)

*Category 33.3* *Antispam*

2003-06-02 **law school spam course seminar marketing e-mail**

NewsScan

LAW SCHOOL DISHES UP COURSE ON SPAM
Students at John Marshall Law School in Chicago will be able to bone up on the legal issues surrounding unsolicited commercial e-mail this fall, in what's reputedly the first law school course offered dealing exclusively with the subject of spam. "This seminar will investigate legal and policy issues raised by e-mail marketing and spam," reads the description for associate professor David Sorkin's seminar titled "Current Topics in Information Technology Law: Regulation of Spam and E-mail Marketing." Sorkin's course will address "litigation and legislation involving spam and e-mail marketing; the application of tort law and other traditional doctrines to spam; concerns related to constitutionality, jurisdiction, extraterritoriality, privacy, content and public policy; regulatory perspectives; issues faced by Internet service providers and legitimate e-mail marketers; legal aspects of blacklisting and other antispam measures; and other relevant issues." (CNet News.com 2 Jun 2003)

*Category 33.3* *Antispam*

2003-09-15 **anti-spam pay stop fighting Global Removal do-not spam list**

NewsScan

ANTI-SPAM EFFORT WOULD PAY SPAMMERS TO STOP
A new anti-spam service, called Global Removal, is taking a different approach to fighting spam — it's proposing to pay spammers for cooperating with their effort. Internet users fed up with junk e-mail would pay a $5 lifetime fee to have their e-mail addresses put on a Global Removal do-not-spam list. Addresses on the list would be cross-referenced and deleted from mailing lists maintained by Global's partners, which include more than 50 known spammers and an equal number of legitimate e-mail marketers. These partners would be rewarded for their diligence through an affiliate program, which would pay $1 for every new subscriber that they bring to the service. In order to avoid a new flood of spam touting Global Removal's service, the spammers would be allowed to send only one message to their purged mailing lists. "Despite the urban legend, these guys don't really want to keep these names on their lists if they know that the people aren't going to be receptive to advertising," says Global CEO Tom Jackson. "They can make more money for less effort through our program." Critics say the flaw in Global's sales pitch is that subscribers would still receive junk e-mail from spammers not affiliated with Global and that Global's spammers could always renege on their deal and go back to their old lists. One intellectual property lawyer says, "It's a little like paying protection money to mob bosses. There's precious little assurance about the comprehensiveness of the protection, or that the prices won't go up at the whim of the 'bosses.'" Still, if spammers "could be assured some minimum bit of income by not sending me mail, it's a better deal for them and a relief to me." (Wired.com 15 Sep 2003)

*Category 33.3* *Antispam*

2003-10-06 **spam fight legitimate e-mail unsolilicted**

NewsScan

FIGHTING SPAM: RAISE THE BRIDGE OR LOWER THE WATER?
Many software experts now believe that the best way to fight spam is not by targeting it directly but instead by concentrating on the identification of legitimate mail. VeriSign executive Nico Popp explains, "People have been spending all their time creating filters to find the bad guys. We want to turn that on its head and find ways to identify the good guys and let them in." The idea would be to develop the Internet equivalent of caller ID, with a technology that identifies senders and lets receivers presume that un-identified senders are sending junk mail. Richard Reichgut of AuthentiDate says, "It's not easy to change something as successful and widely used as e-mail. But the only way to fix e-mail is to have a strong way to know who is sending you mail." (New York Times 6 Oct 2003)

*Category 33.3* *Antispam*

2003-10-09 **spam elude antispam cracker unsolicited e-mail new methods**

NewsScan

NEW BREED OF 'SPACKERS' ELUDES ANTISPAMMERS
Computer crackers have joined forces with spammers to devise new ways of defrauding hapless Internet users. The latest technique enables spammers to create Web sites that are virtually untraceable, making it impossible for antispammers to shut down those sites by conventional means. Typical of the scam is a group in Poland currently advertising "invisible bulletproof hosting" for $1,500 a month, which provides its clients protection from network sleuthing tools such as 'traceroute' and 'whois' by routing traffic through thousands of hijacked computers (most of them home computers running Windows and having broadband connections). The technique is effective. "You're not going to have much success trying to follow IP addresses through hacked hosts," says one security researcher. "About all you can do is follow the money — sign up for whatever it is they're selling and try to figure out who's behind the whole thing." Fueling the new tactics is an influx of "engineers who have been laid off or fired, and people who really know what they're doing with networking and DNS," says Steve Linford, head of the Spamhaus Project. "Hackers used to detest spammers, but now that spamming has become such a big business, it's suddenly cool to be a spammer." (Wired.com 9 Oct 2003)

*Category* *33.3* *Antispam*

2003-10-21 **spam decoy Yahoo mail Address Guard base name junk**

NewsScan

YAHOO DEPLOYS E-MAIL DECOYS
Yahoo now offers its e-mail customers a new way to evade spam — its AddressGuard feature allows subscribers to create a fictitious "base name" and then up to 500 variations on that name that can be used in online shopping and banking transactions as well as online community discussions. If an address starts to draw spam, it can be discarded and another one selected. Yahoo's anti-spam arsenal also includes new spam-blocking software along with the option to receive e-mail only from known sources. Yahoo has also changed its rule on viruses, now requiring users to scan all attachments before downloading them. Yahoo VP Brad Garlinghouse says the company has to keep tweaking its technical defenses because legal battles can't do the job alone. "Legislation and litigation, it's something of a whack-a-mole problem," he says, referring to the arcade game where players are challenged to hit an ever-increasing number of pop-up figures. An August survey of Yahoo users found that 77% said they would rather clean a toilet than sort through the junk e-mail in their in-box. (Reuters 21 Oct 2003)

*Category 33.3* *Antispam*

2003-11-09 **spam fraud blacklist lawsuits investigation blocking spoofing DDoS zombie**

NYT
http://www.nytimes.com/2003/11/09/business/yourmoney/09spam.html?th=&pagewanted=print&position=

The Spamhaus Project <http://www.spamhaus.org/> was profiled in a New York Times article by Saul Hansell in November 2003. One of the best indications that the group of volunteers running this project have been effective is that they have often been assaulted by spammers using DDoS attacks.

Notes from the Web site:

* Spamhaus tracks the Internet's Spammers, Spam Gangs and Spam Services, provides dependable realtime anti-spam protection for Internet networks, and works with Law Enforcement to identify and pursue spammers worldwide.

* The Spamhaus Block List (SBL) is a realtime blocklist of spam sources and spam services. The SBL can be used by almost all modern mail servers, by setting your mail server's anti-spam DNSBL feature (sometimes called "Blacklist DNS Servers" or "RBL servers") to query sbl.spamhaus.org. Use of the SBL is free for users with normal mail servers (but networks with heavy email traffic should see DataFeed).

* The Spamhaus Exploits Block List (XBL) is a realtime database of IP addresses of illegal 3rd party exploits, including open proxies (HTTP, socks, AnalogX, wingate, etc), worms/viruses with built-in spam engines, and other types of trojan-horse exploits.

* The Register Of Known Spam Operations (ROKSO) database collates information and evidence on the known spammers and spam gangs, hard-line spam operations that have been terminated by a minimum of 3 consecutive Service Providers for serious spam offenses. ROKSO assists ISP Abuse Desks and Law Enforcement Agencies.

The section on ROKSO has the following information:

200 Known Spam Operations responsible for 90% of your spam.

90% of spam received by Internet users in North America and Europe can be traced via redirects, hosting locations of web sites, domains and aliases, to a hard-core group of around 200 known spam operations, almost all of whom are listed in the ROKSO database. These spam operations consist of an estimated 500-600 professional spammers loosely grouped into gangs ("spam gangs"), the vast majority of whom are operating illegally, and who move from network to network seeking out Internet Service Providers ("ISPs") known for lax enforcing of anti-spam policies.

These are the spammers you definitely do NOT want on your network.

Many of these spam operations pretend to operate 'offshore' using servers in Asia and South America to disguise the origin. Those who don't pretend to be 'offshore' pretend to be small ISPs themselves, claiming to their providers the spam is being sent not by them but by their non-existent 'customers'. Some set up as fake networks, pirate or fraudulently obtain large IP allocations from ARIN/RIPE and use routing tricks to simulate a network, fooling real ISPs into supplying them connectivity. When caught, almost all use the age old tactic of lying to each ISP long enough to buy a few weeks more of spamming and when terminated simply move on to the next ISP already set up and waiting.

ROKSO is a "3 Strikes" register. To be listed in ROKSO a spammer must first be terminated by a minimum of 3 consecutive ISPs for AUP violations. IP addresses under the control of ROKSO-listed spammers are automatically and preemptively listed in the Spamhaus Block List (SBL).

For Law Enforcement Agencies there is a special version of this ROKSO database which gives access to records with information, logs and evidence too sensitive to publish here.

*Category 33.3* *Antispam*

2003-11-22 **Spam murder threat Charles Booher kill five years prison 22 calibre**

NewsScan

GETTING SOME RAGE OUT: MAN THREATENS MURDER AFTER GETTING SPAMMED
A few months ago 44-year-old Charles Booher, a self-described non-violent person, went bonkers after receiving too much spam, and sent a series of e-mail messages threatening to kill the spammer. Now Booher's been charged with 11 violations of interstate communications, for which he could be sentenced to five years in prison and a $250,000 fine if found guilty. His current thoughts: "If I could go back, I wouldn't have done it. I would have realized sooner that I needed to shut my Web site down, to shut down my e-mail, and to re-evaluate the way I was using the Internet." In one of the messages he told the spammer: "I will locate you, disable you using a quick 22 calibre shot to your lower spine and then duck tape... I am going to cut into the left side of your brain using a power drill and an ice pick." Reflecting on the messages he sent to the spammer, Booher now says: "It felt like I was just getting some rage out." (San Jose Mercury News 22 Nov 2003)

*Category 33.3* *Antispam*

2003-12-02 **spammers anti-spam groups targeted e-mail worms Spamhaus Project Steve Linford**

NewsScan

SPAMMERS TARGET ANTI-SPAM GROUPS WITH E-MAIL WORM
Virus experts say a new worm, dubbed W32/Mimail-L, has been unleashed by a vengeful spammonger intent on paralyzing anti-spam groups via a crippling barrage of data — a so-called denial of service attack. "It's the third Mimail variation to come after us, except this one is trying to do more," says Steve Linford, founder of the Spamhaus Project. The nasty worm comes as an attachment to an e-mail from "Wendy" who describes an erotic encounter and then offers photos. Clicking on the attachment launches the worm. In a new twist, a follow-up e-mail is sent to the infected user announcing that an order for a CD containing child pornography images will be sent to their mailing address. Virus experts say the impact of this latest worm has been minimal, compared with the problems caused by last summer's plague of viruses, "but what this shows is that there is more evidence that virus writers and spammers are now colluding," says Sophos senior technology consultant Graham Cluley. (Reuters 2 Dec 2003)

# 33.4 Authorization, access controls

*Category 33.4* *Authorization, access controls*

2003-02-24 **authorization confidentiality privacy control data leakage**

NewsScan

MICROSOFT PUTS A LOCK ON CORPORATE COMMUNICATIONS
Alarming organizations that encourage employee whistle-blowing on corporations engaged in wrongdoing, Microsoft has developed new technology called Windows Rights Management Services, which lets a company restrict which of its employees may access, download, print, or forward "company-sensitive" e-mail or Web material. Based on the XrML programming language, the software was created within Microsoft's Trustworthy Computing initiative focused on improving the security and privacy of information. But corporate accountability watchdogs are appalled. Joanne Royce of the nonprofit Government Accountability Project says, "It sounds to me like just another way to restrict the free flow of information. In a way it sounds like it won't hinder whistleblowers per se, because they won't even get to see this stuff." Michael Kohn of the National Whistleblower Center in Washington, D.C., calls the new technology "ludicrous" and warns, "You create a whole secret society within a corporation. Anyone who is within that circle is unlikely to be a whistleblower." (AP/USA Today 21 Feb 2003)

# 34.1 Net filters

*Category 34.1* *Net filters*

2003-04-07 **pornographic sites blocked Pakistan**

NewsScan

PAKISTAN FILTERS 1800 SITES TO BLOCK PORNOGRAPHY
On the order of the Pakistani government, Pakistan Telecommunications is blocking at least 1800 Web sites described as pornographic. Hafiz Muhammed Taqi, a religious leader in that country, says: "This is one good move on the part of the present government. The young generation should be saved from sinking neck-deep in the filth of pornography and vulgarity;" however, Web software engineer Farhan Parpia, skeptical of the effectiveness of such filters, note that "curbing porn sites is as difficult as blocking the wind. You block one, and dozens more come up like mushrooms." (AP/USA Today 7 Apr 2003)

---

*Category 34.1* *Net filters*

2003-06-24 **pronography child library block pornographic sites web**

NewsScan

COURT UPHOLDS LAW REQUIRING SOFTWARE FILTERS IN LIBRARIES
The U.S. Supreme Court, in a 6-3 opinion, has upheld provisions in the Children's Internet Protection Act that require public libraries to install anti-pornography software filters, if those libraries are to receive federal grants and subsidies. All nine justices agreed that there was no constitutional problem in a decision to restrict children's access to pornographic material, and that software filters are blunt instruments that inevitably block more material than the statute contemplates; still, the majority did not view this over-blocking as an infringement of the First Amendment rights of adult library patrons. To the argument that adults might be embarrassed by having to ask librarians to unblock pornographic sites for their viewing, Chief Justice Rehnquist wrote that "the Constitution does not guarantee the right to acquire information at a public library without any risk of embarrassment." (New York Times 24 Jun 2003)

---

*Category 34.1* *Net filters*

2003-07-24 **libraries net filtering FCC CIPA software unblock**

NewsScan

LIBRARIES GET REPRIEVE ON NET FILTER DEADLINE
The Federal Communications Commission said yesterday that libraries will have an extra year to comply with the provisions of the controversial Children's Internet Protection Act (CIPA), which mandates that libraries accepting federal funding must install Internet filtering software. The new deadline is July 1, 2004. Opponents of the Act — including the American Library Association and the American Civil Liberties Union — have challenged CIPA, saying it violates free speech guarantees, but the U.S. Supreme Court ruled June 23 that CIPA did not infringe on First Amendment rights, noting "the ease with which patrons may have the filtering software disabled" by asking a librarian to unblock a particular site. (CNet News.com 24 Jul 2003)

---

*Category 34.1* *Net filters*

2003-12-11 **spam-filtering software free nonprofits Mailshell Inc. www.stopspamtoday.org**

NewsScan

FREE SPAM-FILTERING SOFTWARE FOR NONPROFITS
Mailshell Inc., maker of anti-spam software, is offering nonprofits and charities a holiday gift — free one-year subscriptions to its $30 software product. "Nonprofits can't necessarily avail themselves of cutting-edge technologies," says Mailshell marketing VP Eytan Urbas. "These are people who are working hard, a lot of them don't make a lot of money, for things they believe in. It feels like the right thing to do to support that." To avail themselves of Mailshell's offer, nonprofits with a 501(c)(3) designation should sign up by Friday at www.stopspamtoday.org. (AP 11 Dec 2003)

---

# 34.2 Usage monitoring, audit trails (employees, children)

*Category 34.2* *Usage monitoring, audit trails (employees, children)*

2003-01-21 **employee monitoring data theft prevention privacy simulations**

NewsScan

NEW WAY TO FOIL DATA THIEVES
Researchers at the State University of New York at Buffalo are developing software that tracks and analyzes how each computer user performs his or her routine tasks, such as opening files, sending e-mail or searching archives, to create individual profiles. The "user-level anomaly detection" software then alerts network administrators if a worker's behavior deviates from his or her profile so that they can monitor that employee's activities more aggressively. "The ultimate goal is to detect intrusions or violations occurring on the fly," says head researcher Shambhu Upadhyaya. "There are systems that try to do this in real time, but the problem is it results in too many false alarms." Some rival computer-security products also feature user profiling, but it's based on huge amounts of data flowing through entire networks. Upadhyaya says such detection systems are usually 60% to 80% reliable, whereas simulation tests indicate the new software would be up to 94% accurate. One information specialist says, "Other intrusion techniques require something like looking at audit logs after the damage has already occurred. The advantages offered by this approach is an intruder with malicious intent can be identified very early and a system operator can contain the damage, repair it in real time and shut out the intruder. This means that systems that have been attacked by an intruder maliciously might not necessarily be brought down." (Wired.com 20 Jan 2003)

---

*Category 34.2* *Usage monitoring, audit trails (employees, children)*

2003-02-20 **content filtering monitoring university college student network bandwidth file-swapping P2P peer-to-peer copyright intellectual property infringement violation piracy**

NewsScan

TECHNOLOGY TARGETS P2P PIRATES
A new technology, provided by Audible Magic, has been tracking file-swapping traffic on the University of Wyoming's network for the past several months, quietly noting every trade of an Avril Lavigne song or a "Friends" episode. The technology isn't yet blocking file trades, but that could come next, say university administrators who complain their networks are sometimes overwhelmed with file-swapping activity. "I don't really want to be looking that closely at what people are doing, and you'd probably just as soon not have me looking either," says a University of Wyoming network specialist who's helping to manage the Audible Magic project. "But it's getting to be the only way to control our bandwidth." Audible's technology goes beyond the conventional port-blocking and digital rights management efforts now used to control file-swapping. It allows a network operator to see exactly what files are being transferred by creating a copy of all the traffic flowing on a network, identifying those bits that are using FTP (file transfer protocol) or Gnutella technology, and then re-creating those files to identify them. The resulting reports give university network administrators a good look at what students are trading and in what quantities, and future steps could include selectively blocking such trades. "We believe that what this does is transform network devices to be content-intelligent," says Audible CEO Vance Ikezoye. "That will be important. You can't just say, 'Let's block peer-to-peer.'" (CNet News.com 20 Feb 2003)
http://news.com.com/2100-1023-985027.html

---

*Category 34.2* *Usage monitoring, audit trails (employees, children)*

2003-04-08 **computers monitor work habits Queen's University**

NewsScan

COMPUTERS TO WATCH YOU WHILE YOU WORK
With today's computer users increasingly overloaded by a combination of e-mail, instant messages and phone calls, researchers at the Human Media Lab at Queen's University in Ontario are designing technology that will enable a PC to gauge their user's attention level and sort out which messages and phone calls are important. "Today's digital lifestyle has the unfortunate side effect of bombarding people with messages from many devices all the time, regardless of whether they're willing, or able, to respond," says Human Media Lab director Dr. Roel Vertegaal. "We now need computers that sense when we are busy, when we are available for interruption, and know when to wait their turn — just as we do with human-to-human interaction." Techniques used to evaluate PC users' availability include an eye contact sensor that enables the PC to determine whether the user is present and whether he or she is looking at the screen. (BBC News 8 Apr 2003)

---

*Category 34.2 Usage monitoring, audit trails (employees, children)*

2003-06-17 **big brother company monitoring e-mail employees**

NewsScan

BIG BROTHER AT THE OFFICE
More than three out of four of the nation's largest companies monitor employee e-mails, Internet connections and computer files, because bosses are worried that their employees, instead of working, will use the Internet for pornography, online shopping, or Internet gambling. George Walls, a union president in Milwaukee, says that companies "are far more aggressive than they ever have been in the past. Virtually every minute of every day they can tell what you are doing. With all the monitoring, it is turning into an electronic sweatshop." Lisa Ellington, a call center worker, finds the situation "kind of insulting," and explains: "I am a good employee and don't have any reason to be stressed out by this. But it is human nature. You tense up. I pay bills, buy children's school clothes or order flowers. I know a lot of people did Christmas shopping. It gives you time to multitask and take care of things." (Milwaukee Journal Sentinenal/SJMN 17 Jun 2003)

# 35.1 Cybersquatting

*Category 35.1* *Cybersquatting*

2003-01-06 **DNS Domain Name System cybersquatting fraud theft lawsuit**

NewsScan

SEX.COM RULING COULD OPEN FLOODGATES ON REGISTRY LAWSUITS
A federal appeals court has asked California's Supreme Court to rule on whether Network Solutions Inc., the largest U.S. domain registry, must face a multimillion-dollar damage claim from the rightful owner of the sex.com domain name. The ruling could lead to a flood of lawsuits against domain registries, particularly NSI, from hundreds of people who claim their domain names were also stolen. The current case stems from a lawsuit filed in 1998 by Gary Kremen who registered the sex.com name with NSI in 1994. In October 1995, NSI received a letter purportedly from Kremen asking that the name be reregistered to a company headed by Stephen Cohen. NSI complied without attempting to verify the validity of the request, and then refused to undo the transfer when alerted to the fraud. Meanwhile Cohen, who was using the domain name for a lucrative porn business, fled the country before Kremen's lawsuit against him went to trial in 2001. Kremen, who is now using sex.com for his own porn business, was awarded $65 million in damages from Cohen for fraud (which he'll probably never collect) and is now requesting an additional $30 million from NSI for allowing the fraudulent transfer. (San Francisco Chronicle 4 Jan 2003)

*Category 35.1* *Cybersquatting*

2003-02-11 **.gov domain hijacking government Access One Network Northwest AONN**

NIPC/DHS

February 05, CNET News — GSA pulls suspicious .gov site. The General Services Administration (GSA), which runs the .gov registry, pulled the plug on a .gov Web site pending an investigation into the authenticity of the organization that controlled it. Until January 24, the AONN.gov Web site contained information about an agency calling itself the Access One Network Northwest (AONN), a self-described cyberwarfare unit claiming to employ more than 2,000 people and had the support of the U.S. Department of Defense. No federal agency called AONN appears to exist, and no agency with that name is on the official list of organizations maintained by the U.S. National Institute of Standards and Technology. The action could point to the first case of a .gov domain name hijacking. Cybersquatting, or registering a domain to which you may not be entitled, is hardly uncommon among the multitude of .com and .net domains. But there are no known cybersquatting incidents involving a governmental domain, according to the GSA. Claiming credit for the deleted .gov site is a man who calls himself Robert L. Taylor III. Taylor declined to explain how or when he secured a .gov domain for the group, calling AONN's operations "classified." A Pentagon representative said that AONN has no affiliation with the U.S. military and he had no knowledge of the organization. According to the official .gov registration rules, only organizations that appear in an official list of government agencies qualify for a .gov domain—and AONN is not on it. Registering a .gov domain name involves writing an authorization letter, printing it out, and then sending it to the ".GOV Domain Manager" in Reston, Virginia.

*Category 35.1* *Cybersquatting*

2003-06-13 **sex.com domain name ownership stephen cohen gary kremen**

NewsScan

S*X.COM RESTORED TO RIGHTFUL OWNER
The U.S. Supreme Court has rejected an appeal from cybersquatter Stephen Cohen, who had hijacked the lucrative s*x.com domain name from its original owner Gary Kremen, putting an end to six years of legal wrangling. The ruling, which upheld a lower court's award of $65 million in damages to Kremen, is viewed by legal experts as a landmark case because it holds domain registrar VeriSign accountable for allowing the ownership transfer to take place, based on a forged letter from Cohen. The case is also expected to set a precedent for treating an Internet address as legal property — a designation disputed by VeriSign, which could face fines of up to $200 million if found liable. Kremen now faces an uphill battle to claim his award, because Cohen is now a fugitive in Mexico. (BBC News 13 Jun 2003)

# 35.2 Trademarks vs DNS

*Category 35.2* *Trademarks vs DNS*

2003-06-19 **falwell sites name personal information privacy WIPO**

NewsScan

FALWELL WINS IN BATTLE OVER SITES USING HIS NAME
The Rev. Jerry Falwell has won his battle with an Illinois man who created parody Web sites using Falwell's name. Falwell had lodged a previous complaint about the sites with the World Intellectual Property Organization (WIPO), but WIPO ruled against him. Recently he learned that his own organization had trademarked the name Jerry Falwell several years ago when he was doing a television talk show. When that became known, the Illinois man decided to surrender the site names to Falwell, rather than face a lawsuit. (AP/Atlanta Journal-Constitution 19 Jun 2003)

*Category 35.2* *Trademarks vs DNS*

2003-11-06 **Microsoft domain name hotmail.co.uk forgets expires**

NewsScan

OOPS! MICROSOFT DROPS THE BALL ON U.K. HOTMAIL DOMAIN
Microsoft apparently forgot to renew its registration for hotmail.co.uk, sending the domain name back into the pool of available names. It was snapped up immediately by a do-gooder, who then contacted Microsoft to alert it to its oversight and arrange a transfer of ownership back to the software giant. However, these efforts to do the right thing were rebuffed and it was only when The Register contacted the company to inquire about the snafu that the matter was "escalated" to upper-level officials who then sought to work out a deal. By all accounts, hotmail.co.uk will be restored to the Microsoft fold within the next few days. (The Register 6 Nov 2003)

# 35.3 Politics of the DNS

*Category 35.3* *Politics of the DNS*

2003-03-21 **DNS Domain Name System governance policies politics**

NewsScan

NEW ICANN CHIEF TO CONTINUE POLICY FOCUS
Succeeding Stuart Lynn as CEO of the often-controversial Internet Corporation for Assigned Names and Numbers (ICANN), in-coming chief Paul Twomey says that in addition to focusing on technical coordination, the organization will also have to continue its efforts to deal with the policy issues such as intellectual property, privacy, and law enforcement: "The consequences of those technical issues flow into other arenas, like intellectual property, consumer protection, and privacy, potentially even into commercial relationships between infrastructure providers. The law enforcement issues are potentially issues like identification for Whois databases (which list information on domain name owners), identification of those people who are committing computer crimes, (and) ensuring that financial scams don't take place on the Internet." Twomey, an Australian, has been a consultant and government bureaucrat. (CNet News.com 19 Mar 2003)
http://news.com.com/2100-1028-993390.html

*Category 35.3* *Politics of the DNS*

2003-04-04 **forecast warning domain name system DNS work Internet future extension**

NIPC/DHS

April 04, Electronic Times — DNS pioneer warns of Internet security. When it comes to the Domain Name System (DNS), the database architecture at the heart of the Internet infrastructure for the last 20 years, "the majority of the work to be done still lies ahead of us," said Paul V. Mockapetris who co-invented DNS in 1983. Mockapetris received the 2003 IEEE Internet Award for his pioneering work on DNS on Tuesday. Mockapetris warned that efforts need to be made to improve its security especially since the October 2002 attacks on 9 of the Internet's 13 DNS root-name servers that contain the master domain list for DNS and the March 27th 2003 hacker attacks on the al-Jazeera network, part of which were DNS-based. Despite attacks that portend graver security breaches, Mockapetris noted that The Internet Engineering Task Force has not yet hammered out a standard after nearly a decade of work. With a security model for DNS in place, extensions could be built onto DNS that would relate to creating greater opportunities on the Internet including phone numbers for IP telephony, distribution of security keys and certificates, and no-call lists for telemarketers. But without it, there is a "real opportunity for fraud" as the hacker community climbs the technology ladder and puts the 30 million people with web domains at risk, according to Mockapetris.

*Category 35.3* *Politics of the DNS*

2003-04-27 **domain names non-English ICANN Chinese Japanese Korean**

NewsScan

NON-ENGLISH DOMAIN NAMES COMING SOON
The Internet Corporation for Assigned Names and Numbers (ICANN), is poised to approve technical standards that will enable registration of Internet domain names in Chinese, Arabic and other languages. "A great deal of progress has been made this week and I hope we will see progress as the weeks go by," said ICANN chairman Vinton G. Cerf at this week's meeting in Rio de Janiero. "The technical standards are ready. Now the policy work has to be done… The languages that are most advanced are Japanese, Chinese and Korean. Those groups have done a tremendous amount of work to translate their scripts into domain names." Currently, the core computers that handle online addresses understand only the 26 English letters, 10 numerals and a hyphen, along with a period for splitting addresses into sections. How soon users will be able to obtain domain names in other languages depends largely on the extent to which technicians using those languages have translated their alphabets into Internet protocol, said Cerf. (AP 27 Mar 2003)

*Category 35.3* *Politics of the DNS*

2003-06-27 **ICANN At-Large structures infrastructure personal information whois**

NewsScan

ICANN PLANS TO OPEN THE DOORS
The Internet Corporation for Assigned Names and Numbers (ICANN) has long been accused by critics of being a closed organization, but a reform movement begun under outgoing president Stuart Lynn (and continued by his successor, Paul Twomey) will allow organization of the individual Internet user community for informed participation in the organization. Applications will be accepted from groups seeking designation as "At-Large Structures." In a separate discussion, the group tried to wrestle with the question of how much personal data collected by Internet domain administrators should be publicly available. Twomey said, "Although no definitive policy was formed, a lot of healthy dialogue took place paving the way for future policy development." (Internet News 27 Jun 2003)

*Category 35.3* *Politics of the DNS*

2003-07-25 **domain name switch lawsuit sex.com**

NewsScan

NETWORK SOLUTIONS MAY BE LIABLE FOR SEX.COM SWITCH
A U.S. appellate court has ruled that Web registry Network Solutions may be liable for damages for its part in transferring the domain name "sex.com" from its rightful owner, Gary Kremen, to convicted forger Stephen Michael Cohen. In his ruling, Judge Alex Kozinski said that domain names should be treated as property, despite their virtual nature, comparing them to "a plot of land." "Exposing Network Solutions to liability when it gives away a registrant's domain name on the basis of a forged letter is no different from holding a corporation liable when it gives away someone's shares under the same circumstances. The common law does not stand idle while people give away the property of others," wrote Kozinski, who returned the case to the U.S. District Court in San Jose to be tried again. "This was a major victory, no doubt about it," said Kremen, who won a $65 million judgment against Cohen, but has been unable to collect because Cohen has fled the country. The case, which may garner landmark status for equating domain names with tangible property, likely will be retried within a year. (CNet News.com 25 Jul 2003)

*Category 35.3* *Politics of the DNS*

2003-09-22 **ICANN Verisgn site finder typographical errors URL site Internet Corporation For Assigned Names and Numbers**

NewsScan

ICANN ASKS VERISIGN TO SHELVE SITE FINDER SERVICE
ICANN (Internet Corporation for Assigned Names and Numbers) has issued a statement voicing "widespread expressions of concern" over the technical repercussions possible from VeriSign's recently launched Site Finder service. Site Finder steers Web users who make typographical errors while entering URLs to a site operated by VeriSign. Critics say the technical process by which VeriSign "hijacks" users could disrupt e-mail delivery as well as impair the ability of ISPs to block "spam" sent from non-existent Internet addresses — a common technique for reducing the volume of junk e-mail. In self-defense, some ISPs and software groups have developed patches that prevent the Site Finder software from working on their networks. (Wall Street Journal 22 Sep 2003)

*Category 35.3* *Politics of the DNS*

2003-10-06 **Versign DNS domain name ICANN site finder suspended**

NewsScan

VERISIGN AGREES TO SUSPEND SITE FINDER SERVICE
VeriSign and ICANN reached a temporary truce Friday, with VeriSign acquiescing to ICANN's demand that it suspend its controversial Site Finder service pending further technical review. ICANN could have fined VeriSign as much as $100,000 or even revoked its contract to manage the master list of .com and .net Internet domain names. Critics have charged VeriSign with undermining the collectivist culture of the Internet with the preemptive launch of its service, which redirects Web users who mistype a URL to the VeriSign Web site. "In the past when you made a dramatic change to the network structure that was the least bit potentially damaging, you went out through the community and you exposed what you were going to do and got reaction," says Carnegie Mellon computer science professor David Farber. VeriSign "just broke the whole process." In its defense, VeriSign executives say they notified ICANN of their plans ahead of time, but admitted that they sidestepped ICANN's lengthy approval process because it's too slow. In response, ICANN says it's "sympathetic to concerns" about its process and has proposed a more streamlined procedure for reviewing new services such as Site Finder. (Wall Street Journal 6 Oct 2003)

*Category 35.3* *Politics of the DNS*

2003-10-16 **Verisign DNS Network Solutions sale ICANN URL**

NewsScan

VERISIGN SHEDS NETWORK SOLUTIONS
VeriSign is selling its Network Solutions domain registrar business to Pivotal Private Equity for about $100 million, but plans to retain control over the .com and .net database that Network Solutions operates. The domain registration business has essentially become a commodity service as more registrars have entered the field. VeriSign has been in the news recently for its controversial Site Finder service, which redirects all mistyped URLs to a search page that it operates. It suspended the service under pressure from ICANN, which expressed concern over the technical ramifications of the Site Finder service, but VeriSign said Wednesday that it plans to restart the service after having found "no identified security or stability problems" in the system. (CNet News.com 16 Oct 2003)

*Category 35.3* *Politics of the DNS*

2003-11-06 **Internet address space**

NWF

The BBC reported in October 2003 that the Internet would run out of new IP addresses in 2005. Scott Bradner of Harvard University pointed out serious errors in the report. In contrast to the projections from the BBC, the consensus among Internet specialists predicts another 20 years to exhaust the 4B addresses under IPv4. Under IPv6, there will be an additional 64B addresses available.

*Category 35.3* *Politics of the DNS*

2003-11-11 **internet united states european commission ICANN Internet Corporation for Assigned Names and Numbers public resource**

NewsScan

WILL THE U.N. TAKE OVER THE INTERNET?
Some of the developing countries want to put management of the Internet under United Nations control. U.N. officials expect governments to continue talks on Internet governance with the aim of reaching accord by 2005. Brazil, India, South Africa, China and Saudi Arabia are dissatisfied with the current Internet regulator, the semi-private California-based ICANN (the Internet Corporation for Assigned Names and Numbers), and argue that the Internet is a public resource that should be managed by national governments and by intergovernmental organizations. But both the United States and the European Commission are standing behind the ICANN model, in the belief that to turn Internet regulation over to governments could threaten the existence of the borderless Internet. (Financial Times 11 Nov 2003)

*Category 35.3* *Politics of the DNS*

2003-12-10 **Internet domain name system DNS politics control ICANN**

NIPC/DHS

December 10, Washington Post — UN sets aside debate over control of Internet. In a last-minute meeting this weekend before the start of this week's World Summit on the Information Society in Geneva, Switzerland, representatives set aside a debate over whether national governments, rather than private-sector groups, should be in charge of managing and governing the Internet around the globe. UN member states instead will ask Secretary General Kofi Annan to put together a panel of experts from government, industry and the public to study the issue and draft policy recommendations before the high-tech summit reconvenes in Tunisia in 2005. Leaders had planned to wade into a debate over the way Website and e-mail addresses are doled out, standards are set for Internet security and the thorny question of how Internet-based transactions are taxed, among other things. Some developing nations have complained that the world's most visible Internet governance body — the U.S.-based, nonprofit Internet Corporation for Assigned Names and Numbers (ICANN) — hasn't adequately represented non-U.S. interests, and should be replaced with a governmental group overseen by the United Nations. ICANN has managed the Internet's global addressing system since 1998 under an agreement with the U.S. government.

# 37.1 Elementary & middle school

*Category 37.1 Elementary & middle school*

2003-11-20 **education children schools ethics cybercrime cheating parents**

St Peterburg Times <
http://www.sptimes.com/2003/11/20/Tampabay/Some_kids_turn_the_ta.shtml >

Winn Schwartau, author of many books on information warfare and of the popular new book, _Internet & Computer Ethics for Kids (and Parents & Teachers Who Haven't Got a Clue)_, was disappointed by the response of teenagers to a series of ethical challenges that were part of the Great American Teach-in in his son's school in Seminole Florida. For example, one question in the "Cyberethical Survivor Game" was, "You accidentally receive an e-mail with answers to next week's big test. Without them you could fail. No one will ever know if you peek." Although a few students strongly asserted that they would not cheat, hundreds of teenagers express their contempt for such a position. According to a report by Thomas Tobin of the St. Petersburg Times, "Boos and catcalls rained down from about 200 ... students, who made it clear during the spirited 40-minute game that they favored unfettered computer use, no parental controls and cheating."

# 37.2 High school

*Category 37.2* *High school*

2003-07-25 **hacking contest Japan cybercrime computer expertise**

NewsScan

JAPANESE GOVERNMENT SCRAPS HACKING CONTEST
Japan's Economy, Trade and Industry Ministry has canceled a national computer-hacking contest, bowing to an outpouring of angry mail and phone calls complaining that sponsoring such an event would just encourage cybercrime. The ministry said the "Security Koshien" contest was intended to foster computer expertise among high school and vocational students, and would have involved teams of students attempting to hack into opponents' systems while protecting their own from similar breaches. (AP 25 Jul 2003)

# 37.3 Undergraduate degrees

*Category 37.3 Undergraduate degrees*

2003-03-15 **digital forensics AS associate BSc bachelor baccalaureate online major**

http://digitalforensics.champlain.edu/

Champlain College officially approved a new major called Digital Forensics Technology. Commencing in the 2003-2004 academic year, Champlain College offers Associates of Science (A.S.) and Bachelor of Science (B.S.) degrees in Computer & Digital Forensics. This major combines aspects of computer and network technology, criminal justice, digital forensics methods, and other related fields. Individuals interested in the technical content of the Computer & Digital Forensics curriculum but who do not want to obtain a B.S. degree (such as those individuals who are pursuing a degree in another discipline or who already have a Bachelors degree) would be able to take a subset of the courses and earn a Professional Certificate. More information can be found in the program information sheet.

All of the courses for this curriculum are available on-line. For more information about the program, contact program director Gary Kessler.

---

*Category 37.3 Undergraduate degrees*

2003-05-23 **unviersity canada calgary virus writing education malware worms trojan horses**

NIPC/DHS

May 23, Sophos — Canadian university offering course in virus-writing. The University of Calgary in Canada is offering its students a course in malicious virus-writing this autumn. The course, titled "Computer Viruses and Malware," is described by university literature as focusing on "developing malicious software such as computer viruses, worms and Trojan horses that are known to wreak havoc to the tune of billions of dollars world-wide on an annual basis." The course professor, Dr. John Aycock, is said to have convinced the University authorities to allow virus writing to be part of the course in the belief that it will lead to a greater understanding of how to stop viruses.

---

*Category 37.3 Undergraduate degrees*

2003-05-27 **virus course writing skills student understand hackers criminals crackers motivation**

NewsScan

VIRUS WRITING 101
The University of Calgary is drawing fire for its decision to offer a class next fall in "Computer Viruses and Malware," giving students the opportunity to perfect their virus-writing skills. Ken Barker, head of Calgary's computer science department, defends the decision, saying the class will enable students to better understand the motivations of crackers who are responsible for the proliferation of malicious attacks against corporate networks and personal computers. "Somebody who is suggesting we are doing enough really has their head in the sand," says Barker. In response to concerns that the students' work could lead to more cracking incidents, school officials say they've taken extra precautions, with plans to use a closed network and prohibitions on students removing disks from the lab, which will be secured 24 hours a day. But it's the financial consideration that likely will keep students focused on preventing viruses rather than proliferating them, says Barker. "They are not really employable as virus writers," he notes. (CNet News.com 27 May 2003)

---

*Category 37.3 Undergraduate degrees*

2003-06-01 **Cyber Corps education Department of Defense's Information Assurance Scholarship Program stipend tuition students**

NIPC/DHS

June 01, Information Security — Cyber Corps' failing grades. Federal administrators are overhauling Cyber Corps because conflicting policies and management structures are making it increasingly difficult to place graduates of the infosec training program in government jobs. University coordinators say getting the first 50 Cyber Corps graduates into federal jobs proved extremely difficult. Federal agencies were unwilling to hire inexperienced security admins when more senior infosec positions went unfilled. Complicating the situation is the Office of Personnel Management (OPM), which is responsible for placing students but has little authority to compel placements. Officials are still working on details, but it has already been decided to reorganize Cyber Corps based on the Department of Defense's Information Assurance Scholarship Program. The government launched Cyber Corps in 2001 under the scholarship for service model. Students receive tuition and a stipend in exchange for serving in a summer internship and working at a government agency for up to two years. Cyber Corps has distributed nearly $30 million to upgrade university infosec programs and fund scholarships for 200 students at 13 universities certified as Centers for Academic Excellence by the National Security Agency.

---

# 37.4 Master's degrees

*Category 37.4* *Master's degrees*

2003-04-23 **cyberspace war games Internet warfare education US military academies**

NIPC/DHS

April 18, Monterey Herald — Cyberspace games teach real world lessons. On Thursday, 39 students at the Naval Postgraduate School (NPS) ended four days of mock Internet warfare that pitted a team made up of NPS, the Air Force Institute of Technology, and the U.S. Military, Naval, Air Force, Coast Guard and Merchant Marine academies against a team made up of the Army's Land Information Warfare unit and the Air Force's 92nd Aggressor Squadron. The object of the exercise is for each side to try to penetrate the other's computer systems, aiming to infect them with viruses, shut them down or take them over. The mock war in cyberspace draws students "who are interested in what a real-world situation is," said Marine Corps Capt. Eric Walters who led the Navy school team this year. Some of the team members are military officers enrolled in various information technology classes, others are civilians enrolled in the National Science Foundation's federal Cyber Service Corps scholarship program, which began in 2001. That program offers a two-year, full-ride scholarship in a computer science master's degree program aimed at safeguarding computer systems. Graduates are expected to serve two years with a U.S. government agency as specialists in safeguarding computer systems.

# 37.9 White papers

*Category 37.9* *White papers*

2003-06-06 **SQL Slammer Code ATM worm educate**

NewsScan

PUBLISHING THE SQL SLAMMER CODE: TRAINING OR EDUCATION?
Wired magazine has decided to include the code of the SQL Slammer worm to educate its readers on how worms work and how they cause damage. (SQL Slammer shut down Internet service providers in South Korea, disrupted plane schedules, and jammed ATM bank machines.) Symantec security director Vincent Wheeler warns that the publication of such code is "something you need to be cautious of, particularly in a broad-based magazine. You need to be aware of your audience and what you're saying to them." Blaise Zerega, Wired's managing editor, says that "the people who are in a position to wreak havoc on the Internet don't have to read about it on Wired." (Reuters/USA Today 6 Jun 2003)

# 38.1 Consumer profiling

*Category 38.1* *Consumer profiling*

2003-04-23 **privacy concern Amazon FTC COPPA**

NewsScan

TC ASKED TO INVESTIGATE AMAZON
A coalition of privacy and consumer groups has asked the Federal Trade Commission to investigate online retailer Amazon.com, and has charged Amazon with violating the Children's Online Privacy Protection Act of 1998 (COPPA) by allowing minors to post personal, identifying information. Chris Hoofnagle of the Electronic Privacy Information Center says, "When you find a posting that says, 'I'm Jane Done, I'm 11 and I'm from Hampsted, New York,' that's information that can be verified with the White Pages." Amazon's response is that its Web site is directed not at children but at adults: "We sell products for children to be purchased by adults." The company says it does not "knowingly solicit or collect personally identifiable information online from children under the age of 13 without prior verifiable parental consent." And if it receives such information anyway? Amazon says it removes it "as soon as we see it." (San Jose Mercury News 23 Apr 2003)

*Category 38.1* *Consumer profiling*

2003-06-27 **TV advertising ads private information TiVo data consumer**

NewsScan

TV ADVERTISING EXECS IN DENIAL OVER TIVO DATA
Television advertising has long relied on Nielsen ratings, which indicate how many viewers are watching a particular TV show, but not whether they're sticking around for the commercials, or heading off to the kitchen for a snack or channel-surfing to check on the baseball score. But the data service recently launched by TiVo offers a much more complete vision of what's happening in the home when the TV's on. It can track what viewers record, what they watch, when they change the channel and which commercials they skip. This ability to pinpoint viewer behavior has received a less than enthusiastic reception from advertisers. "This kind of information is the holy grail for marketers. But it's not the holy grail for advertising agencies and media companies, which have built an industry around the idea of getting a shallow message to a broad audience rather than a tailored message to a narrower one," says the chief strategy officer for interactive ad agency Avenue A. According to the TiVo data, genres like big-budget situation comedies (think "Friends") tend to have the lowest commercial-viewing rates because couch potatoes record them and skip through the commercials when they watch. Reality TV, news programs such as "60 Minutes" and "event" programming such as the Academy Awards do significantly better. With Forrester Research predicting that by 2007, more than half of American households will have either a personal video recorder such as TiVo or other on-demand services, advertisers will be forced get their heads out of the sand and come with a new business strategy. (Business Week Online 27 Jun 2003)

# 38.2 Trade in personal information

*Category 38.2* *Trade in personal information*

2003-02-10 **privacy personal information search engines**

NewsScan

THE GOOGLING OF AMERICA
The search engine Google is changing the kind of information Americans can find out about each other — information that once was the purview of private investigators or the extremely nosy. Now with one click, potential employers, salespeople, and just about anyone can find out every publicly reported detail of your past life, says Boston Globe columnist Neil Swidey. "Now, in states where court records have gone online, and thanks to the one-click ease of Google, you can read all the sordid details of your neighbor's divorce with no more effort than it takes to check your e-mail. 'It's the collapse of inconvenience,' says Siva Vaidhyanathan, assistant professor of culture and communication at New York University. 'It turns out inconvenience was a really important part of our lives, and we didn't realize it.'" (Boston Globe 2 Feb 2003)

---

*Category 38.2* *Trade in personal information*

2003-09-01 **selling personal data Do Not Call list personal information business privacy identity ownership**

NewsScan

WHO OWNS YOUR PERSONAL DATA ANYWAY?
Harvard Business School professor John Deighton says that instead of relying on regulators to protect their privacy through contrivances such as the "Do Not Call" list, consumers should capitalize on the value of their personal information and get something in return for allowing businesses to use it. With companies doing a brisk business in selling and reselling your data, it's time for individuals to get into the act, demanding rewards such as better customer service, price discounts or maybe just plain money. "The challenge is to give people a claim on their identities while protecting them from mistreatment. The solution is to create institutions that allow consumers to build and claim the value of their marketplace identities and that give producers the incentive to respect them. Privacy and identity then become opposing economic goods, and consumers can choose how much of each they would like to consume" says Deighton. (HBS Working Knowledge/CNet 1 Sep 2003)

---

*Category 38.2* *Trade in personal information*

2003-10-16 **search engine Google text data mining FBI**

NewsScan

TEXT-SEARCHING OR TEXT-MINING?
Whereas Google and other Web search engines retrieve information and display links to documents that contain certain keywords, text-mining programs dig deeper in order to categorize information, make links between seemingly unconnected documents, and provide visual maps that lead down new pathways of exploratory learning. Unlike data mining, text mining works on unstructured data — such as e-mail messages, news articles, internal reports, phone call transcripts, and so on. A good example of the problem it seeks to solve is suggested by the comment of researcher Randall S. Murch, who says: "I was an FBI agent for 20 years. And I have yet to see anyone who is able to model the way an agent thinks and works through an investigation." And a good example of the solution offered by text-mining is its use in the 1980s University of Chicago information scientist Don R. Swanson in studying the medical literature on migraines. Starting with the word "migraine," he downloaded abstracts from 2,500 articles from Medline and noticed a reference to a neural phenomenon called "spreading depression" — which prompted him to look for articles with that term in their titles, which in turn led him to the discovery that magnesium was often mentioned as preventing this spreading depression. Thus, as a result of text-mining he was able to hypothesize a link between headaches and magnesium deficiency — a link that was later confirmed by actual experiments. (New York Times 16 Oct 2003)

---

# 38.3 Industry efforts for privacy protection

*Category 38.3 Industry efforts for privacy protection*

2003-06-25 **bill gates orwell 1984 security homeland computers**

NewsScan

GATES: ORWELL GOT IT BACKWARDS
"Orwell's vision didn't come true, and I don't believe it will," Microsoft chairman Bill Gates said this week in a speech commemorating the 100th anniversary of the birth of George Orwell, the English author whose works included the dystopian novel "1984." That novel described a repressive society of the future dominated by a figure called Big Brother, whose image was displayed on screens throughout the land. Gates said that, contrary to Orwell's fears, "This technology can make our country more secure and prevent the nightmare vision of George Orwell at the same time... At a time of increased uncertainty about homeland security, computers must be available wherever and whenever we need them... Not so long ago, most people paid little attention to cybercrime, but today there's a broader recognition that IT security is vital to homeland security. We must build higher walls and stronger vaults, and government must continue to step up the priority given to this kind of crime while protecting the privacy of consumers." (AP/Los Angeles Times 25 Jun 2003)

---

*Category 38.3 Industry efforts for privacy protection*

2003-10-28 **Orbitz security breaches online travel agency customers junk e-mail unauthorized spammers**

NIPC/DHS

October 28, CNET News.com — Orbitz investigates security breach. Online travel agency Orbitz has notified law enforcement authorities about a recent security breach that has resulted in its customers' e-mail addresses falling into the hands of spammers, an Orbitz representative confirmed Tuesday, October 28. "A small number of customers have informed us that they have received spam or junk e-mail from an unknown party that apparently used unauthorized and/or illegal means to obtain their e-mail addresses used with Orbitz," spokeswoman Carol Jouzaitis said in a statement. "There is no evidence that customer password or account information has been compromised," she said. Orbitz found no indication that credit card information had been compromised, Jouzaitis added. Orbitz became aware of the problem "in the last day or so," Jouzaitis said.

---

*Category 38.3 Industry efforts for privacy protection*

2003-12-19 **RIAA music dowloaders Verizon copyrighted privacy**

NewsScan

APPEALS COURT STRIKES DOWN RIAA STRONGARM TACTICS
A U.S. appeals court has ruled that the strongarm tactics used by the Recording Industry Association of America to track down music downloaders are illegal. The RIAA had sought to force Internet service providers, including Verizon, to divulge the names of subscribers suspected of downloading copyrighted music files without permission. Verizon argued that existing copyright law does not give the recording industry the authority to enforce its subpoenas and said the RIAA's actions violated Verizon customers' privacy. A lower court had earlier upheld the RIAA's actions, but this latest ruling sided with Verizon: "In sum, we agree with Verizon that [the 1998 copyright law] does not by its terms authorize the subpoenas issued here," wrote Chief Judge Douglas Ginsburg. (Reuters/CNN.com 19 Dec 2003)

---

# 38.4 International agreements on security, privacy, Net law

*Category 38.4* *International agreements on security, privacy, Net law*

2003-02-12 **European cybersecurity agency proposal cope cyber crime co-ordination**

NIPC/DHS

February 10, IDG News Service — European cybersecurity agency proposed. The European Commission Monday proposed the creation of a Europe-wide network and information security agency. The European Network and Information Security Agency is to serve as an advice center for the fifteen member states on matters relating to cybersecurity, such as computer viruses, Erkki Liikanen, commissioner for the information society, said. Until now, viruses have largely been propagated by young individuals and amateurs, but in the post-September 11 era there is a risk of worse attacks, he said. Mobile Internet connections, through mobile phones in particular, are expected to increase the risk of serious attacks, Liikanen said. The Commission has earmarked a ï¿½24.3 million ($26.3 million) budget for the agency over a five-year period, with an additional $9 million planned to include the 10 new member states, mainly from Central Europe, in May 2004. Individual member states have already established crisis units (known as Computer Emergency Response Teams) in an effort to cope with increasing cyber crime. However, the current system lacks central coordination. The agency is due to start operating next January. The governments of the 15 member states will decide on a location later this year, Liikanen said.

---

*Category 38.4* *International agreements on security, privacy, Net law*

2003-09-16 **internet management ICANN international body UN intergovernmental organizations**

NewsScan

BATTLE IS BREWING OVER NET MANAGEMENT
Two camps with opposing views on Internet management are emerging, setting the stage for discord at the upcoming UN-backed World Summit on the Information Society in December. "Some governments are arguing that the management of things like (Internet protocol) addressing, global domain names and privacy should be done by an intergovernmental organization because the feel the Internet is a public resource, and they have responsibility over public resources," says Mohammed Sharil, chairman of the government advisory committee for ICANN (the Internet Corporation for Assigned Names and Numbers). "Then there are some governments who feel that the Internet should be managed by an international body. International by definition means everyone is involved, from governments to private sector and civil society. Whereas intergovernmental gives an indication that only governments are involved and not necessarily people." Sharil says many countries in the Asia-Pacific region prefer an independent international managing body, whereas some in Europe and the Middle East favor an intergovernmental organization. The issue is currently under debate as the wording of a key article to be adopted at the summit is hammered out. "Positions are shifting all the time," says Sharil, who adds that ICANN will not take a position on the subject. (Reuters/CNet 16 Sep 2003)

---

*Category 38.4* *International agreements on security, privacy, Net law*

2003-11-14 **windows media player europe commission brad smith audiovisual software**

NewsScan

MICROSOFT TO EUROPE: 'WE CAN WORK THINGS OUT'
After concluding Microsoft's defense in the antitrust case brought against it by the European Commission, Microsoft general counsel Brad Smith told reporters: "I do really want to underscore one thing, which is that we come to Brussels not only to discuss the issues but to work things out." The Commission has threatened to fine Microsoft as much as 10% of its global sales and force the company to remove its Media Player audiovisual software from Windows. But Microsoft seems to be hoping to work out a deal similar to the out-of-court settlement it reached with the U.S. Justice Department in November 2001. (Los Angeles Times 14 Nov 2003)

---

*Category 38.4* *International agreements on security, privacy, Net law*

2003-12-09 **international computer crime cooperating fighting cyberspace**

NIPC/DHS

December 07, — Cybercops and robbers growing trickier on World Wide Web. When the World Summit on the Information Society convenes in Geneva, Switzerland, December 10 to 12, leaders will seek to build on their success in developing better cross-border guidelines to fight online crime. Investigators say organized crime rings and terror groups are using the Internet to expand their reach and exploit the Web's anonymity to stay one step ahead of the law. Internet experts are particularly concerned about the potential for "cyber terrorism" in which the Internet is used to shut down computer networks, potentially disabling vital infrastructure at banks, airports and emergency services. "It is not at all unusual for a regional conflict to have a cyber dimension, where the battles are fought by self-appointed hackers operating under their own rules of engagement," said Dorothy Denning, a cyber terrorism expert at the Naval Postgraduate School in Monterey, CA. "A rash of cyber attacks have accompanied the conflict between Israel and the Palestinians, the conflict over Kashmir, and the Kosovo conflict, among others." Denning said that for now, at least, studies indicated that anything more than irritating cyber attacks were still difficult for most extremists to mount — although the future could hold more technically savvy terrorists.

# 38.6 US legislation & regulation concerning privacy

*Category 38.6* *US legislation & regulation concerning privacy*

2003-09-27 **speech privacy Do-Not-Call list first amendment telemarketers supreme court FTC**

NewsScan

SPEECH, PRIVACY, AND DO-NOT-CALL: 'I WANT TO BE ALONE'
Privacy and free speech are conflicting values in the current controversy over "Do Not Call" legislation aimed at curtailer commercial telemarketing calls (while continuing to allow calls made for political or philanthropic purposes). David Sobel, general counsel for the Electronic Privacy Information Center, says: "The telemarketers have some First Amendment rights to disseminate information. But the consumer also has some rights to control unwanted information coming into the home." Telemarketers argue that their own free-speech rights are being violated by the FTC's attempt to establish a Do-Not-Call list, and UCLA law professor Eugene Volokh explains: "When it comes to residential privacy, the Supreme Court has suggested that content-based discrimination is illegal. The FTC is setting up content-based discrimination." Some legal experts think the government could legally expand the registry to all telemarketers, with a registry that just says, like Greta Garbo, "I want to be alone." Attorney Bruce Johnson, an expert in First Amendment law, says: "I don't think it's restricting political or religious speech. The registry just says that I don't want to hear from anybody." (San Jose Mercury News 27 Sep 2003)

# 38.7 Other legislation & regulation concerning privacy

*Category 38.7* *Other legislation & regulation concerning privacy*

2003-05-23 **privacy japan personal information databases e-mail**

NewsScan

NEW PRIVACY PROTECTION LAW IN JAPAN
In response to complaints that personal information about consumers is circulating without their permission in databases and e-mail communications, the Japanese parliament has passed legislation that will give individuals the right to obtain information collected about them and will put restrictions on both governmental and corporate entities who maintain such databases. Critics of the new legislation are worrying that Internet operators will be inundated with information requests from individuals, and privacy advocates are saying the legislation will impede freedom of speech. (APOnline/USA Today 23 May 2003)

# 38.8 Law enforcement & privacy

*Category 38.8* *Law enforcement & privacy*

2003-07-07 **FTC personal information Federal Trade Commission cyberspace business privacy policy**

NIPC/DHS

July 07, The Register — FTC calls privacy claims to account. Most online businesses promise they'll protect customer data as if it were their own. Now the government is holding them to it. United States Federal Trade Commission has indicated its intention to actively pursue companies that obtain personal information by promising a level of security, and then not delivering it. Almost every company that does business in cyberspace has a security and privacy policy, typically buried at the bottom of a home page, under "legal notice" or "privacy policy." The FTC concluded that data that is collected under false pretenses is a "deceptive trade practice."

*Category 38.8* *Law enforcement & privacy*

2003-12-23 **online music probe Pressplay MusicNet Roxio EMI digital services**

NewsScan

NO HARM, NO FOUL: U.S. DROPS ONLINE MUSIC PROBE
The U.S. Justice Department has closed its investigation of online music ventures Pressplay and MusicNet because investigators came to the conclusion that the two services have not actually hurt consumers. Pressplay is owned by Roxio Inc., and MusicNet is owned jointly by subsidiaries of Time Warner Inc., Bertelsmann AG and EMI Group Plc. Antitrust chief Hewitt Pate said: "None of the several theories of competitive harm that the Division considered were ultimately supported by the facts. Consumers now have available to them an increasing variety of authorized outlets from which they can purchase digital music, and consumers are using those services in growing numbers." (Reuters/Washington Post 23 Dec 2003)

# 38.9 Surveillance

*Category 38.9* *Surveillance*

2003-01-16 **privacy surveillance law enforcement cameras databases libraries intimidation laws government observation homeland defense terrorism**

NewsScan

ACLU SEES A GROWING 'SURVEILLANCE MONSTER'
In a new report called "Bigger Monster, Weaker Chains," the American Civil Liberties Union says that there is a rapidly growing "American Surveillance Society" brought about by "a combination of lightning-fast technological innovations and the erosion of privacy protections" threatening "to transform Big Brother from an oft-cited but remote threat into a very real part of American life." This "surveillance monster" includes, among other things, cameras monitoring public spaces, proposals for databases filled with personal information on U.S. citizens, and anti-terrorist legislation allowing the government to demand that libraries turn over reading histories of their patrons. Yet the report asserts that these monsters don't even have to be real for them to be terrifying: "It is not just the reality of government surveillance that chills free expression and the freedom that Americans enjoy. The same negative effects come when we are constantly forced to wonder whether we might be under observation." (AP/USA Today 16 Jan 2003)

*Category 38.9* *Surveillance*

2003-01-24 **TIA Total Information Awareness monitoring surveillance law enforcement government privacy**

NewsScan

O BIG BROTHER, WHERE ART THOU? (EVERYWHERE)
In order to monitor the U.S. civilian population in its effort to detect terrorists, the government's Total Information Awareness program will rely almost completely on data collection systems that are already in place — e-mail, online shopping and travel booking, ATM systems, cell phone networks, electronic toll-collection systems and credit card payment terminals. Technologists say that what the government plans to do in data sifting and pattern matching in order to flag aberrant behavior is not very different from programs already in use by private companies. For instance, credit card companies use such systems to spot unusual spending activities that might signal a stolen card. The early version of Total Information Awareness uses a commercial software collaboration program called Groove, which was developed in 2000 by Ray Ozzie, inventor of Lotus Notes. Groove enables analysts at various government agencies to share intelligence data instantly, and links programs that are designed to detect suspicious patterns of behavior. However, some computer scientists question whether such a system can really work. "This wouldn't have been possible without the modern Internet, and even now it's a daunting task," says cryptology expert Dorothy Denning, a professor in the Department of Defense Analysis at the Naval Postgraduate School. Part of the challenge, she says, is knowing what to look for. "Do we really know enough about the precursors to terrorist activity? I don't think we're there yet." (New York Times 23 Dec 2002)

SENATE DELAYS FUNDING FOR PENTAGON SURVEILLANCE PROGRAM
The U.S. Senate voted yesterday to block funding of the Defense Department's Total Information Awareness (TIA) program, which when developed would use "data mining" techniques to scan for patterns in worldwide communications activity and use those patterns to identify terrorist threats. Calling TIA "the most far-reaching government surveillance program in history," Senator Ron Wyden (D-Ore.) said that by blocking R&D funds the Senate thereby "makes it clear that Congress wants to make sure there is no snooping on law-abiding Americans," even if the purpose of the activity is to prevent terrorist attacks against the United States. (Reuters/San Jose Mercury News 24 Jan 2003)

*Category 38.9* *Surveillance*

2003-05-20 **pentagon TIA Terrorist Information Awareness visas driver's license medical records consumer privacy government**

NewsScan

PRIVACY ADVOCATES DOUBT PENTAGON PROMISES ON SPYING
The Pentagon has changed the name of its planned anti-terrorist surveillance systems, but critics say the fundamental program remains the same and would risk violating citizens' privacy if fully implemented. Now renamed the Terrorist Information Awareness program (from Total Information Awareness), the system would broaden government surveillance activities to encompass passport applications, visas, work permits, driver's licenses, car rentals and airline ticket purchases as well as databases including vast amounts of personal information, such as financial, education, medical and housing and identification records. Sen. Ron Wyden (D-Ore.), a major opponent of the TIA, says, "What most Americans don't know is that the laws that protect consumer privacy don't apply when the data gets into government's hands. Lawfully collected information can include anything, medical records, travel, credit card and financial data." Testing of the system is already underway, raising privacy advocates' concerns about "false positives" based on erroneous data. "If TIA is relying on personal information contained in databases to determine whether someone is a suspect, what recourse does that person have whose information has been entered incorrectly?" says a spokeswoman for the Free Congress Foundation, which estimates that an error rate as small as .10% could result in more than 30,000 Americans wrongly being investigated as terrorists. (AP 20 May 2003)

*Category 38.9* *Surveillance*

2003-06-02 **Lifelog Darpa pentagon pattern life behavior habits**

NewsScan

LOOKING FOR MEANINGFUL PATTERNS IN YOUR LIFE? SEE DARPA!
The Pentagon's Defense Advanced Research Projects Agency (DARPA) is taking bids on a new project called LifeLog, which will help someone capture his or her "experience in and interactions with the world" via cameras, microphones, and sensors; the goal is to created advanced software to assist in the analysis of a person's behavior, habits, and routines. Privacy advocates are expressing concern, but DARPA spokesperson Jan Walker says that the "allegation that this technology would create a machine to spy on others and invade people's privacy is way off the mark." LifeLog's software "will be able to find meaningful patterns in the timetable, to infer the user's routines, habits and relations with other people, organizations, places and objects." (AP/USA Today 2 Jun 2003)

*Category 38.9* *Surveillance*

2003-06-29 **privacy black box car data event recorders speed limit**

NewsScan

IS YOUR PRIVACY INVADED BY THE 'BLACK BOX' IN YOUR CAR?
A recent survey found that most people are unaware that many later-model automobiles are equipped with "black box" recording devices (called "data event recorders") which are capable not only of triggering the release of accident airbags but also of recording driving data (such as speed of the car) in the last few seconds before a crash. Such information is increasingly being used as evidence in criminal and civil cases related to the accident, as part of "normal reconstruction" of what happened. But civil libertarians are balking. Defense attorney Bob Weiner calls the black boxes "a tremendous invasion of privacy," and David Sobel, general counsel for the Electronic Privacy Information Center, say: "The real issue is one of notice, and the problem arises from the fact that information is being collected about people's driving behavior without them knowing. If drivers knew about the device, they could at least then begin asking questions." (USA Today 29 Jun 2003)

*Category 38.9* *Surveillance*

2003-07-18 **surveillance privacy airplace security terrorism cameras**

NewsScan

SKY-HIGH SURVEILLANCE HITS AIRLINE INDUSTRY
Southeast Airlines is pioneering an in-flight surveillance program that will use digital videocameras installed through the cabins of its planes to record passengers' activities throughout the flight as a precaution against terrorism and other threats. The charter airline, based in Largo, Fla., says it may use face recognition software to match faces to names and personal records, and plans to store the digital data for up to 10 years. "From a security standpoint, this provides a great advantage to assure that there is a safe environment at all times," says Southeast's VP of planning. The airline says that while such security measures are not required by the FAA, it expects other airlines will adopt similar systems soon. That prediction alarms privacy advocates who especially question the need for retaining the video after the flight is over. "What's the point of keeping track of everyone when nothing happens on the flight?" asks Lee Tien, senior staff attorney for the Electronic Frontier Foundation, who points out that the video system could record conversations between passengers as well as capture the titles of passengers' reading material. (Wired.com 18 Jul 2003)

*Category 38.9* *Surveillance*

2003-07-19 **closed circuit TV camera surveillance privacy spy chip**

NewsScan

SMILE, YOU'RE ON CLOSED CIRCUIT TV
In Cambridge, England, RFID technology will cause a CCTV camera to take a photo of anyone taking a package of Gillette Mach3 razorblades from the shelves of supermarket chain Tesco Ltd.; a second camera then takes a picture at the checkout and security staff then compare the two images. "Customers know that there are CCTV cameras in the store," said a spokesman for Tesco, and says that the purpose of the pilot project is to provide stock information rather than provide security. However, the manager of the Cambridge store says he has shown the police photos of a shoplifter. Civil libertarians says that the so-called "spy chips" are an invasion of consumers' privacy, but manufacturers point out that the chips can be disabled simply by having the data erased at checkout when a consumer leaves the store. (The Guardian (UK) 19 Jul 2003)

*Category 38.9* *Surveillance*

2003-09-29 **surveillance classroom parents children England**

NewsScan

BIG MUMMY AND DADDY ARE WATCHING YOU
Some teachers in England say that Webcams should be installed in every classroom in order to involve parents in their children's education — and let them see whether their children are misbehaving. One advocate said: "Bad behavior in class is a big issue throughout the school system, but teachers have to handle it on their own. If pupils knew their parents could see how they were behaving then they would think twice about disrupting classes." (Evening Standard 29 Jul 2003)

# 41 Cryptanalysis techniques & tools

*Category 41* *Cryptanalysis techniques & tools*

2003-07-22 **crypanalysis password cracking Windows fast**

NewsScan, NIPC/DHS

NEW METHOD CRACKS PASSWORDS IN SECONDS
A senior research assistant at the Swiss Federal Institute of Technology's Cryptography and Security Laboratory has published a paper outlining a way to speed up the process of cracking alphanumeric Windows passwords to only 13.6 seconds on average. The previous average time was 1 minute, 41 seconds. The new method uses massive lookup tables to match encoded passwords to the original text entered by a person, thus reducing the time it takes to break the code. "Windows passwords are not very good," says researcher Phillippe Oechslin. "The problem with Windows passwords is that they do not include any random information." The only requirement for the cracker is a large amount of memory in order to accommodate the lookup tables. The larger the table, the shorter the time it takes to crack the password. Users can protect themselves by adding nonalphanumeric characters to a password, which adds another layer of complexity to the process. Any cracker would then need more time or more memory or both to accomplish the break-in. For more information on Oechslin's method, check out http://lasecwww.epfl.ch/php_code/publications/search.php?ref=Oech03
(Cnet News.com 22 Jul 2003)

[NIPC/DHS:]
July 22, CNET News.com — Cracking Windows passwords in seconds. Swiss researchers from the Cryptography and Security Laboratory of the Swiss Federal Institute of Technology in Lausanne (EPFL) released a paper on Tuesday, July 22, outlining a way to speed the cracking of alphanumeric Microsoft Windows passwords, reducing the time to break such codes to an average of 13.6 seconds from 1 minute 41 seconds. The method involves using large lookup tables to match encoded passwords to the original text entered by a user, thus speeding the calculations required to break the codes. Called a time-memory trade-off, the situation means that an attacker with an abundance of computer memory can reduce the time it takes to break a secret code. Users can protect themselves against the attack by adding non-alphanumeric characters to a password. Philippe Oechslin, one of the researchers, said he hadn't notified Microsoft of the issue before publishing the paper.

*Category 41* *Cryptanalysis techniques & tools*

2003-11-12 **cryptanalysis crack password Kansas auditor IT poor planning**

NIPC/DHS

November 07, Government Computer News — Kansas auditors crack 1,000 passwords. The Kansas Health and Environment Department has serious IT security and disaster recovery problems, the state's legislative auditor has found. The auditors said they used password-cracking software to decipher more than 1,000 of the department's passwords-including several administrative passwords-or 60 percent of the total, in three minutes. The department began fixing the security weaknesses and other problems found in its systems as soon as it learned of them, department secretary Roderick L. Bremby said in response to the report. "The department's anti-virus system was badly flawed, allowing computers to become infected with a large number of different viruses, worms and Trojan horses," said the report. "The department's firewall was poorly configured, creating several large holes in and out," the report said. Auditors found that the department lacked or failed to enforce many basic security policies, such as procedures for incident response, physical security, configuration documentation and former-user account deletion. They also found several major problems with security planning.

# 42 Crypto algorithms (weakness, brute-force attacks, implementation flaws)

*Category 42* *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

2003-04-14 **cryptography history award scientists future trends fundamentals**

ACM; NWF http://www.nwfusion.com/newsletters/sec/2004/0503sec1.html

The famous cryptographers Leonard Adleman, Ronald Rivest, and Adi Shamir - the developers of the RSA encryption code - received the Association for Computing Machinery's 2002 Turing Award "for their seminal contributions to the theory and practical application of public-key cryptography." Their Turing Award lectures, given last June, are available online.

Rivest, Shamir and Adleman implemented public-key cryptography in the 1970s following the landmark work of Whitfield Diffie, Martin Hellman and Ralph Merkle. They then founded RSA Security, which became one of the most respected security companies in the world.

The distinguished scientists' lectures are available online in a variety of formats at:
http://www.acm.org/awards/turing_citations/rivest-shamir-adleman.html

It was exhilarating to listen to these brilliant people speaking to us, and I hope some of you will have an hour to spare to enjoy their lectures.

# 42.2 Brute-force attacks

*Category 42.2* *Brute-force attacks*

2003-01-09 **supercomputers cryptanalysis brute force factoring**

NewsScan

IBM RENTS OUT SUPERCOMPUTING POWER
IBM has launched a new program to rent out processing power on its supercomputers, and has signed up Petroleum Geo-Services, a petrochemical company, as its first customer. PGS has about 1,000 of its own dual-processor Linux computers clustered into a single computing resource, but it's renting another 400 from Big Blue, says a company spokesman. The new service reflects IBM's push toward "utility computing," which enables companies with fluctuating needs for computing power to pay for it as they use it. An e-commerce operation, for instance, may need to beef up its processing power during the busy holiday shopping season, but that demand drops off in January. IBM also expects to find many of its customers in the petrochemical and life sciences industries. (CNet News.com 8 Jan 2003)
http://news.com.com/2100-1001-979780.html

---

*Category 42.2* *Brute-force attacks*

2003-01-28 **parallel processing supercomputer grid computing Unix brute-force decryption encryption cryptography factoring PKC PKI**

NewsScan

GM TO LINK IBM UNIX MACHINES INTO SUPERCOMPUTER
General Motors is buying 10 high-performance Unix computers from IBM and plans to link them together to form one of the world's most powerful supercomputers. GM plans to use the supercomputer to run a range of simulations, from crash tests to noise measurements, and said the new system will quadruple its supercomputing capacity. GM's new system is "a fairly dramatic deployment of technology," says a senior marketing analyst, who notes that using supercomputers to simulate automobile performance is much quicker and cheaper than building prototypes. It will also make it easier for GM to "engage in limited production-run products" for specialty cars. (Wall Street Journal 29 Aug 2002)

TIME MACHINES FOR A NEW CENTURY
Wolfgang Grentzsch of Sun Microsystems thinks that grid computing (which links large numbers of computers into a giant grid-like single system) should be thought of as "time machines," because they will speed up our perception of the world — just as the steam engine and the internal combustion engine speeded up travel and our sense of time. "On the grid, you can do things much, much faster, and you can do things you never were able to do before." Things like virtual tests of new drugs, which could change all the current equations in the nation's health care delivery system. IBM's Dan Powers says that the longer-term vision of grid computing is basically about "the virtualization of information technology." (Reuters/USA Today 29 Aug 2002

GRIDS ARE THE 'JET-AGE' MODEL OF COMPUTING
Grid computing, which links individual computers into a network that harnesses the power of surplus processing cycles and applies them to new tasks, is gaining wider acceptance. Computer scientist Larry Smarr of the University of California at San Diego explains: "Today's Internet could be thought of as a Polynesian model, where you have all these islands, and people use canoes to get from one to another. We're changing that to a jet-age model, where you can get from one city to another traveling at speeds far greater than what you travel at once you get into the city itself." Smarr and colleagues in Illinois are building an "OptIPuter" — a computing grid to connect the University of San Diego with Illinois universities. The OptIPuter project is buying an optical-switching router made by a Texas company called Chiaro Networks. Smarr says: "University researchers can generate some market demand for these products and help get companies like Chiaro through the desert until the commercial economy picks up again." (KRT/San Jose Mercury News 18 Dec 2002)

IBM GRIDS UP FOR BATTLE
Looking at developing new markets that will generate big computer-services business, IBM is launching ten new grid computing initiatives targeted at niche markets where grid technology is being welcomed by early adopters. (Grid computing salvages the unused processing cycles of large numbers of networked computers to allow massing sharing of data storage and computer power.) As part of the initiatives IBM has formed alliances with Toronto-based Platform Computing and New York-based DataSynapse, as well as with Avaki, Entropia, and United Devices. (The Register 28 Jan 2003)
http://www.theregister.co.uk/content/61/29060.html

---

*Category 42.2* *Brute-force attacks*

2003-02-26 **nanotechnology parallel processing cryptanalysis brute-force**

NewsScan

DNA COMPUTING UPDATE
Two years ago Israeli researchers developed an incredibly tiny computer that used DNA and enzymes as its software and hardware (a computer so small that a trillion of the machines could be placed in a single drop of water). Now, the same researchers say they've found a way for molecular machines to do without an external energy source and to perform 50 times faster than the previous version, which is listed in the Guinness Book of Records as the world's smallest biological computing device. (Scientific American 25 Feb 2003)

# 42.3 Crypto product implementation flaws

*Category 42.3* *Crypto product implementation flaws*

2003-02-24 **e-mail code crack Secure Sockets Layer SSL Swiss Federal Institute Technology**

NIPC/DHS

February 20, Reuters — Swiss crack e-mail code, but minimal impact seen. Professor Serge Vaudenay of the Swiss Federal Institute of Technology in Lausanne, Switzerland, found a way to unlock a message encrypted using Secure Socket Layer (SSL) protocol technology, according to a posting on the research institute's Web site. However, U.S. cryptography experts said it was not the version of security that most consumers use to shop online. Rather, it is a version that only affects e-mail, is limited in scope, and not widely used, said Professor Avi Rubin, who is technical director of the Information Security Institute at Maryland's Johns Hopkins University. In addition, an attacker would have to be in control of a network computer located in the middle of the two people communicating over which the messages were flowing, he said. ``It's possible, but it has limited applicability," he said. He said patches are already available to fix the hole, which affects one particular mode of OpenSSL. Like all co-called ``open source" software, OpenSSL is free software created by developers who can modify it at any time. Bruce Schneier, chief technical officer at network monitoring firm Counterpane Internet Security, agreed. Besides the mitigating circumstances which lessen the likelihood that attackers would be successful, Schneier said SSL is irrelevant to security because attackers can more easily get at secret information while it is stored on computers and servers at the sending and receiving ends. ``SSL protects the communications link between you and the Web" server, he said. ``Nobody bothers eavesdropping on the communications while it is in transit."

*Category 42.3* *Crypto product implementation flaws*

2003-07-25 **Windows passwords cryptography salt implementation flaw**

http://www4.gartner.com/DisplayDocument?doc_cd=116510

Gartner analyst Ray Wagner wrote,
"According to news reports published on 23 July 2003, Swiss technology researchers have issued a report that describes how Windows computers protected by alphanumeric passwords can be quickly and easily cracked — in less than 14 seconds — by using precalculated data stored in look-up tables. Such ease of cracking, suggest the researchers, is due to Microsoft not using "salt" (a standard security mechanism applied to encrypted passwords) in its Windows operating system. Other computer operating systems, such as Linux, Mac OS X and Unix, do use salt in their password encoding technologies, which can deter or delay password breaches."

# 43.2 Biometrics

*Category 43.2* *Biometrics*

2003-01-09 **biometric iris scanner I&A identification authentication authorization**

NewsScan

RETINAL SCANNING AT U.K. SCHOOL
The Venerable Bede school in London will use advanced eye-recognition software to determine which students are to be billed for their lunches and which may eat for free because they are poor. The school decided to use the technology to protect poor children from being ridiculed by the more well-off children. [As an historical aside, it might be noted that the concern for poor would probably please the school's namesake. Venerable Bede, the 8th century monk best known for his history of ecclesiastical history, said on his deathbed: "I have a few treasures in my box, some pepper and napkins and incense. Run quickly and fetch the priests of our monastery, and I will share among them such little presents as God has given me."] The school's headmaster said that the software will also be used in the library for book check-out and return but added: "This is not a James Bond school for spies... This is not science fiction. This is technology that exists." (USA Today 9 Jan 2003)

*Category 43.2* *Biometrics*

2003-03-10 **biometric I&A identification authentication facial scanning recognition**

NewsScan

FACE SCANNING TECHNOLOGY GOES 3D
A pair of identical whiz-kid twins in Israel have developed a face-scanning system that can even tell them apart. Unlike the two-dimensional scanning technologies now in use in some cities and airports, the 3D system maps the surface of a person's face by scanning it with a series of light patterns and stores the data as a three-dimensional image in a computer. The system uses a mathematical algorithm to measure the distances between a number of sample points on the facial surface, and the distances are then reconfigured as straight lines in a 3D space, creating a new and abstracted image based on precise mathematical calculations. "One of my students calls it sculpting in numbers," says Ron Kimmel, a professor at the Technion Institute in Haifa. "This kind of mapping makes it all invariant, or it is not influenced by our expressions. If we smile a little bit or we change our face a little, it will still be mapped into the same signature, the same kind of surface." Analysts say facial signatures could be embedded in credit cards, building entry permits, or even ATM cards. The facial recognition project began as an assignment in Kimmel's class, where he promised the twins that if they developed a system that could distinguish them, he'd give them a grade of 100. (Reuters 9 Mar 2003)

*Category 43.2* *Biometrics*

2003-07-22 **biometric unready new techonology**

NewsScan

BIOMETRICS TECHNOLOGY: NOT YET READY FOR PRIMETIME
Gartner Research director Anthony Allen told guests at the launch of European Biometrics Forum that while widespread use of biometrics was likely by 2008, the technologies still had some kinks to be ironed out. Biometrics, which includes technologies used for voice, face, iris and fingerprint identification systems, is virtually useless without adequate back security measures and databases, said Allen, and current systems have several fallibilities that must be corrected. For instance, evidence shows that wearing eyeglasses can fool an eyescanner, prosthetic makeup can confuse face scanners, a sore throat can change a voice print and breathing heavily on a fingerprint scanner can make prints unrecognizable. However, newer generations of technology are beginning to rectify some of these shortcomings; the latest fingerprint scanners now incorporate methods of detecting body heat and blood flow and can scan below the surface later, making it more difficult to deceive. (The Register 22 Jul 2003)

*Category 43.2* *Biometrics*

2003-08-24 **biometrics foreign visitors travel visa airplace citizen alien**

NewsScan

BIOMETRIC SCANS FOR U.S. VISITORS
Biometric face and fingerprint scans for travelers will become routine security measures for foreign visitors next year. By October 2004 the 27 countries whose citizens can travel to the U.S. without visas must begin issuing passports with embedded computer chips with the traveler's facial identification. Civil libertarian Marc Rotenberg of the Electronic Privacy Information Center opposes the mandate: "Our government has forced on European governments the obligation to adopt biometric identifiers though most in the U.S. still oppose such systems." But Kelly Shannon of the State Department argues that is not only "more secure for other countries, it's more secure for us. The idea is that it is contingent on reciprocal treatment for United States citizens." And Denis Shagnon of the International Civil Aviation Organization adds: "What was required was a globally interoperable biometric — one biometric that could be used worldwide and can be read worldwide." He regards the biometric techniques as "very user-friendly" and "unobtrusive." (New York Times 24 Aug 2003)

*Category 43.2* *Biometrics*

2003-12-29 **fingerprint terrorist indentify people employment ID biometrics**

NewsScan

'NOT YOUR FATHER'S FINGERPRINT'
The biometrics industry — spurred on by heightened terrorist concerns — has rolled out a variety of new ways to identify people, ranging from retina and iris scans to mapping voice patterns or walking styles, but there's a clear winner among the competing technologies — the old-fashioned fingerprint. "They are looking for proven technology that's stable and familiar," says Joseph J. Atick, CEO of biometric firm Identix. "It's not about technology. It's about lowering your deployment risk." But these aren't your father's fingerprints — today's equipment does away with messy ink in favor of digital records, created by software when fingers are pressed against an electronic pad or sensitive photoplate. And often as not, the fingerprints are then combined with some other form of biometric ID, such as facial recognition. Meanwhile, growing use of passports, drivers' licenses and employment ID cards embedded with ID-data microchips is spawning a new business for data processing giants such as IBM, Unisys and Siemens. "The technology (to integrate ID data with public records) is advancing rapidly. The big growth will be in 2005 and 2006," says a Unisys official. (New York Times 29 Dec 2003)

# 43.4 Kerberos

*Category 43.4* *Kerberos*

2003-03-20 **Kerberos authentication protocol vulnerability leak**

NIPC/DHS

March 17, eWEEK — Details of Kerberos vulnerability leaked. There is a serious weakness in MIT's Kerberos v4 authentication protocol that allows an attacker to impersonate any principal in a given realm. The Kerberos development team at MIT said the contents of an unpublished paper with details of this vulnerability have been leaked on the Internet. Using these details, an attacker familiar with Kerberos could easily exploit the vulnerability. Kerberos v4 tickets-or credentials-do not have a cryptographic hash of the encrypted data, random padding or a random initial vector. As a result, using a chosen plaintext attack, an attacker could fabricate a ticket. An attacker who controls a Kerberos cross-realm key would be able to impersonate any principal in the remote realm to any service in that realm. This attack could lead to a root-level compromise of the Kerberos key distribution center as well as any other hosts that rely on the KDC for authentication. Kerberos, developed at the Massachusetts Institute of Technology, is among the most widely deployed authentication protocols on the Internet. It is implemented in dozens of software applications, as well, including Windows 2000. However, Windows 2000 uses Kerberos v5 and Microsoft officials said that, while they're still researching the issue, they don't believe that operating system is vulnerable. Additional information may be found on the MIT Web site:
http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2003-0 04-krb4.txt

# 44.1 Crypto algorithms

*Category 44.1* *Crypto algorithms*

2003-06-06 **hack-proof communications cryptography bacnk government Quantum research Toshiba Cambridge**

NIPC/DHS

June 06, vnunet.com — 'Hack-proof' cryptography goes quantum. Researchers have developed new technology that could allow companies to implement hack-proof communications in three years. The technology, based on quantum cryptography, was demonstrated by UK-based Toshiba Research Europe last week working over distances of 100km for the first time. Research laboratory group leader Andrew Shields explained that the technology will be applicable for large organizations such as banks and government departments needing highly secure links between local sites. Quantum cryptography allows users on an optical network to guarantee security by encoding each transmitted bit with a single particle of light. Commercial products could be available in less than three years, according to Shields. The Department of Trade and Industry (DTI) in London, England, is partially funding further research into the technology by Toshiba, the University of Cambridge and Imperial College, London.

# 45.5 Watermarks / digital-rights management

*Category 45.5* *Watermarks / digital-rights management*

2003-01-09 **digital rights management copyright copy protection piracy**

NewsScan

REALNETWORKS INCORPORATES DRM TECHNOLOGY
RealNetworks will include its Helix DRM (digital rights management) software in its digital media streaming technology, enabling movie studios and music labels to protect their digital content from copyright violation. Helix DRM is designed to support various digital content standards, including RealAudio, RealVideo, MPEG-4 and MP3. "This breaks the stranglehold that tied a content owner to using a given format if they wanted to use DRM," says Dan Sheehan, VP of media systems at RealNetworks. The move was welcomed by the film and music industries, according to a company statement: "Sony Pictures Digital Entertainment, Starz on Demand and Triggerstreet.com as well as by music label EMI Recorded Music (which includes the EMI, Capitol, Virgin and other record labels) and several Internet media services [will use Helix DRM]." (Reuters 9 Jan 2003)

*Category 45.5* *Watermarks / digital-rights management*

2003-02-20 **copyright intellectual property copy protection**

NewsScan

COPY PROTECTION EFFORTS MISGUIDED, SAYS LESSIG
Lawmakers will be making a big mistake if they bow to Hollywood pressure and enact new copyright-protection legislation based on today's Internet use patterns, says Stanford University professor Lawrence Lessig. Currently, millions of consumers are downloading music to their PCs because slow dialup connections make it impractical to stream content quickly to a variety of devices. "In the future, it will be easier to pay for subscription services than to be an amateur database administrator who moves content from device to device. We're legislating against a background of the Internet's current architecture of content distribution, and this is a fundamental mistake," Lessig told participants at the Digital Rights Management Summit held at Intel headquarters. (AP 20 Feb 2003)
http://apnews.excite.com/article/20030220/D7PA785G0.htm

*Category 45.5* *Watermarks / digital-rights management*

2003-03-21 **digital watermark copyright music rights management**

NewsScan

SUPER DIGITAL WATERMARK IN THE WORKS
SunnComm Technologies is working with Stealth MediaLabs to develop a kind of super-watermark that could be embedded inside digital music files and would be robust enough to withstand digital compression, or being recorded off the radio or rerecorded through an analog connection. The technology, originally developed at the University of Miami, could also be used to embed other information. "The intention was for protecting the security of intellectual property. Adding pictures and liner notes inside a song is kind of a byproduct," says SunnComm COO Bill Whitmore. The technology works by encoding binary data inside the stereo audio signal itself, taking advantage of acoustical properties and human hearing characteristics to make it imperceptible to the listener. Because the signal is embedded in the sound itself, the data is hard to remove without significantly changing the sound of the song. SunnComm plans initially to market the super-watermark technology to record labels, which could use it to detect which recipients of advance discs are putting songs online before the albums' official release dates. "With that anonymity gone, people will be less willing to put advance songs on file-sharing networks," says Whitmore. (CNet News.com 20 Mar 2003)
http://news.com.com/2100-1027-993588.html

*Category 45.5* *Watermarks / digital-rights management*

2003-04-23 **music piracy DRM digital rights management CD ripping protection**

NewsScan

PROTECTION AGAINST CD 'RIPPING'
Macrovision, a company known for helping Hollywood moviemakers prevent their videocassettes and DVDs from being copied, is joining with Microsoft in a project that will allow music companies to make CDs that consumers can copy for themselves but not "rip" them for sharing with others. Because standard CDs are fairly easy to copy, the music industry has seen increasingly declining sales (down 2.5% in 2001 and 8.7% in 2002), and industry analyst Richard Doherty of the Envisioneering Group says fear that such declines will continue has made some music labels "willing to risk consumer playback problems and increased customer wrath." In Europe copy-protected disks have met with strong consumer resistance because some CDs don't play in all playback devices and some get stuck in computers. (USA Today 23 Apr 2003)

*Category 45.5* *Watermarks / digital-rights management*

2003-09-18 **piracy music smart cds antipiracy new generation BMG file-sharing copies**

NewsScan

BMG INTRODUCES 'SMART' CDs
BMG Entertainment is launching a new generation of "smart" CDs aimed at thwarting file-sharing while at the same time allowing CD buyers to make a few copies for themselves and friends. The technology will make its debut next week with the release of "Comin' From Where I'm From" by Anthony Hamilton. Buyers of that CD will be able to burn three copies per computer and will be able to e-mail songs to a limited number of people, each of whom can then listen to the song 10 times before it becomes unavailable. The MediaMax CD-3 antipiracy technology is made by SunnComm Technologies in Phoenix. SunnComm rival Macrovision has also developed protective technology that allows limited copying, and the record labels are watching closely to gauge fans' reactions. Meanwhile, civil liberties advocates say the technology is good in principle, but is still too restrictive. "It is inconsistent with how fair use has always been applied," says Cindy Cohn, legal director for the Electronic Frontier Foundation. (AP/Wall Street Journal 18 Sep 2003)

*Category 45.5* *Watermarks / digital-rights management*

2003-10-03 **digital rights management DRM protect digitial**

NewsScan

DIGITAL RIGHTS MANAGEMENT
In Amsterdam, a film technology group called MPEG LA says it wants to collect all essential patents that can protect digitized music and movies in order to create new content-distribution models over the Internet. The problem is that at present it is often not known which companies own all the relevant patents, and the uncertainty is discouraging film and music publishers from selling their products in new digital ways. MPEG LA hopes that by early in 2004 it will have collected all essential digital rights management (DRM) patents, so that it can begin licensing them later that year. (Reuters/USA Today 3 Oct 2003)

*Category 45.5* *Watermarks / digital-rights management*

2003-10-10 **software protection intellectual property copyright sales boost Fade**

NewsScan

SOFTWARE PROTECTION SCHEME ENDS UP BOOSTING NEW GAME SALES
Companies are using a new software protection system, called Fade, to protect their intellectual property from software thieves. Fade is being introduced by Macrovision, which specializes in digital rights management, and the British games developer Codemasters. What the program does is make unauthorized copies of games slowly degrade, by exploiting the systems for error correction that computers use to cope with CD-ROMs or DVDs that have become scratched. Software protected by Fade contains fragments of "subversive" code designed to seem like scratches, which are then arranged on the disc in a pattern that will be used to prevent copying. Bruce Everiss of Codemasters says, "The beauty of this is that the degrading copy becomes a sales promotion tool. People go out and buy an original version." (New Scientist 10 Oct 2003)

# 45.6 Smart cards and other e-commerce security measures

*Category 45.6* *Smart cards and other e-commerce security measures*

2003-10-22 **Sony smart card cell phone pay FeliCa**

NewsScan

SONY LOOKS FOR WAYS TO GET SMARTER
Sony is working on ways to extend its smart card payment system — dubbed Edy for "euro, dollar, yen" — to cell phones, allowing customers to pay train fares, pick up the restaurant tab and pay for their dry cleaning via their cell phones. A Sony spokesman acknowledged the company's efforts to migrate its FeliCa smart card technology over to the wireless realm but was close-mouthed about the details: "We're looking into the possibility of integrating FeliCa into mobile phones but beyond that we don't wish to comment." Currently, about 2.7 million Edy cards are in circulation. (AP/Los Angeles Times 22 Oct 2003)

*Category 45.6* *Smart cards and other e-commerce security measures*

2003-12-14 **credit cards MasterCard American Express PayPass system store financial data RFID chips**

NewsScan

CREDIT CARDS DO THE WAVE
MasterCard and American Express have been testing "contactless" versions of their credit cards that use an embedded RFID chip rather than a magnetic strip to store financial data. The cards can simply be waved in front of a reader to complete the purchase. "In some instances it's faster than cash. You're eliminating the fumble factor," says a MasterCard VP. The company plans to roll out its PayPass system next year, beginning in fast food joints and other venues where customers tend to be in a hurry. Forrester Research predicts it will take several years for the contactless cards to go mainstream, citing consumers' security concerns and unfamiliarity with the technology as impediments to change. (AP/Wired.com 14 Dec 2003)

# 45.7 Sales taxes on Internet commerce

*Category 45.7* *Sales taxes on Internet commerce*

2003-02-07 **Internet sales taxes Web e-commerce states**

NewsScan

SALES TAXES CREEP ONTO THE WEB
Internet sales traditionally have been exempted from sales taxes, providing the buyer lived in a different state than the e-tailer they purchased from. But a collective push by states to institute Internet sales taxes is gaining momentum, and several big-name retailers — including Marshall Fields, Target and Wal-Mart — are cooperating. The retailers say they're simply streamlining bookkeeping to accommodate situations where customers purchase on the Web and then return or exchange those items at their physical stores. But according to washingtonpost.com, the retailers have ulterior motivations. In return for collecting the taxes, "38 states and the District of Columbia agreed to absolve the retailers for any liability for taxes not previously collected on Internet sales." And while the stakes are high for states — a University of Tennessee report estimated that states could collectively lose more than $45 billion in Internet sales tax revenue in 2006 — there's no groundswell of opposition from consumers. Jupiter Research yesterday released a study that indicates most online shoppers are indifferent to the issue, with most online shoppers unaware that they can shop around on different sites to avoid the extra charge, and some respondents saying they wouldn't choose one retailer over another just because there was no sales tax. (Washington Post 6 Feb 2003)

*Category 45.7* *Sales taxes on Internet commerce*

2003-02-20 **Internet sales taxes interstate e-commerce law**

NewsScan

OREGON SENATOR MOVES AGAINST INTERNET TAXES
Sen. Ron Wyden (D-Ore.) is pushing legislation that would make permanent an existing moratorium on Internet taxes. The current moratorium is set to expire this fall, but Wyden says the pressures on state governments to raise new funds could spark a stampede toward e-commerce sales taxes. "There are thousands of taxing jurisdictions and if all of them, or a significant portion of them, can take a bite out of electronic commerce, I think the consequences would be staggering." (Wall Street Journal 20 Feb 2003)

*Category 45.7* *Sales taxes on Internet commerce*

2003-05-12 **internet sale taxes Amazon.com CFO predicts rates Tom Szkutak**

NewsScan

INTERNET SALES TAXES 'INEVITABLE'
Amazon executives believe that collecting sales taxes on Internet purchases is something that is bound to happen, but not anytime soon. Amazon.com chief financial officer Tom Szkutak said at an investment conference that such a development is "inevitable and it's certainly something we support doing — provided that the process is drastically simplified." The current complexity is due to the fact that there are more than 7,500 taxing jurisdictions across the U.S., with varying tax rates and different administrative rules. (AP/USA Today 12 May 2003)

*Category 45.7* *Sales taxes on Internet commerce*

2003-05-16 **internet tax ban John Snow multiple discriminatory**

NewsScan

GOV'T OFFICIALS ADVOCATE KEEPING NET TAX BAN
Treasury Secretary John Snow and Commerce Secretary Don Evans are urging Congress to extend the current moratorium on Internet taxes that is set to expire in November. "Government must not slow the rollout or usage of Internet services by establishing administrative barriers or imposing new access taxes," said Snow and Evans in a letter to Rep. James Sensenbrenner (R-Wisc.), chairman of the House Judiciary Committee. The ban on "multiple and discriminatory" taxes on Internet access fees and online traffic is separate from the controversial issue of sales taxes on goods and services sold over the Internet, which are currently prohibited under a 1992 Supreme Court decision. Cash-strapped states and other sales tax advocates have sought to link the two issues in an effort to boost support for online sales taxes. (Reuters/CNet 16 May 2003)

*Category 45.7* *Sales taxes on Internet commerce*

2003-09-18 **ban taxes internet access house of representatives bill H.R.49**

NewsScan

HOUSE VOTES FOR PERMANENT BAN ON TAXES FOR INTERNET ACCESS
With bipartisan support, the House of Representatives has passed a bill (H.R. 49) that makes permanent a ban on taxing Internet connections of any kind, including all types of Internet dialup connections and ones made through high-speed DSL or cable access. Rep. Chris Cannon (R-Utah) said: "This bill would broaden access to the Internet, expand consumer choice, promote certainty and growth in the IT sector of our economy and encourage the deployment of broadband services at lower prices." Rep. Gene Green, who was one of several Texas Democrats who opposed the bill, said Texas would lose $45 million a year in tax revenue. "I don't need to remind my colleagues of the fiscal crisis that our states are currently finding ourselves in, including the state of Texas." (AP/San Jose Mercury News 18 Sep 2003)

# 45.8 E-commerce laws

*Category 45.8* *E-commerce laws*

2003-11-07 **FTC Federal Trade Commission MSN messenger microsoft pop-ups security backdoor administrator messages windows**

NewsScan

FTC TAKES AIM AT MESSENGER POP-UPS
The Federal Trade Commission has obtained a temporary restraining order against D Squared Solutions, accusing it of "high-tech extortion" for its annoying marketing campaign, which bombards Microsoft Windows users with pop-up ads touting its $29.95 pop-up blocker software designed to prevent such intrusions. The company set out "to create a problem for consumers and then try to charge them for a solution," said Howard Beales, head of the FTC's consumer protection unit. The FTC is seeking to recoup "hundreds of thousands" of dollars that beleaguered consumers paid to D Squared Solutions for the ad-blocking software. The ads take advantage of a security feature in Microsoft's Windows Messenger service that was originally designed to enable corporate network administrators to send internal messages. These messages are different from the ones imposed on users who visit a Web site, said Beales. "What we are challenging is this 'backdoor' kind of advertising, particularly when it is done in a way and with a frequency that threatens to impair consumers' ability to use their computers." (Los Angeles Times 7 Nov 2003)

# 47 US computer-crime laws

*Category 47* *US computer-crime laws*

2003-01-08 **California law online Internet business computer security breaches notify customers e-commerce**

NIPC/DHS

January 06, Security Focus — California disclosure law has national reach. A new California law requiring companies to notify their customers of computer security breaches applies to any online business that counts Californians as customers, even if the company isn't based in the Golden State. So warned Scott Pink, deputy chair of the American Bar Association's Cybersecurity Task Force, in a conference call Monday organized by an industry trade group, Information Technology Association of America, and attended by approximately 50 representatives of technology companies and law firms. The law, called "SB 1386," is intended to combat identity theft. It was passed last September and will take effect on July 1, 2003. To trigger the law, a breach must expose certain type of information: specifically, customers' names in association with their social security number, driver's license number, or a credit card or bank account number. After such an intrusion, the company must notify the effected customers in "the most expedient time possible and without unreasonable delay." The disclosure only needs to be made to California residents. But as a practical matter, Pink said, online businesses may find it easier to notify everyone impacted by a breach, rather than trying to cherry-pick Californians for special treatment. Companies that ignore the law face potential exposure to class action lawsuits. The law addresses a chronic problem in e-commerce - companies that are hacked are often reluctant to go public for fear of bad publicity or civil liability. But in forcing companies to come clean, the California law takes the opposite approach of the Bush administration's emerging cyber security policies, which encourage secret disclosure to government officials, rather than public warnings.

*Category 47* *US computer-crime laws*

2003-01-16 **criminal hacker sentence term length federal rules**

NIPC/DHS

January 13, Security Focus — Federal government to seek public input on hacker sentencing. Last week the presidential-appointed commission responsible for setting federal sentencing rules formally asked the public's advice on the formula used to sentence hackers and virus writers to prison or probation. The United States Sentencing Commission's (USSC) Federal Sentencing Guidelines set the range of sentences a court can choose from in a given case, based on a point system that sets a starting value for a particular crime, and then adds or subtracts points for specific aggravating or mitigating circumstances. Though they're called "guidelines," the rules are generally binding on judges. Computer crimes currently share sentencing guidelines with larceny, embezzlement and theft, where the most significant sentencing factor is the amount of financial loss inflicted. But in a congressional session that heard much talk about "cyberterrorism," lawmakers became convinced that computer outlaws were more than common thieves. Consequently, one of the provisions in the Homeland Security Act passed last November requires the USSC to review the cyber crime sentencing guidelines to ensure they take into account "the serious nature of such offenses, the growing incidence of such offenses, and the need for an effective deterrent and appropriate punishment to prevent such offenses." The USSC's "Issue for Comment" is available on the Commission's Website: http://www.ussc.gov/. The public comment period ends on February 18th.

*Category 47* *US computer-crime laws*

2003-03-26 **state law legislation S-DMCA encryption VPN e-mail proxy server firewall ISP anonymity identification tracking prosecution**

http://www.freedom-to-tinker.com/archives/000336.html

Prof. Ed Felten < http://www.cs.princeton.edu/~felten/ >of the Secure Internet Programming (SIP) Laboratory at Princeton University posted a warning on his law & technology Web site < http://www.freedom-to-tinker.com/ > about state legislation being called the "Super DMCA" or S-DMCA. These laws are so poorly written that they would make the use of firewalls, proxy servers, and VPNs illegal. The lawmakers, under pressure by the Motion Picture Association of America (MPAA), lack the technical knowledge to understand the implications of the following clauses:

SECTION 6.
(a) A person commits an offense if the person intentionally or knowingly manufactures, assembles, imports into the state, exports out of the state, distributes, advertises, sells, or leases, or offers for sale or lease:
(1) a communication device with an intent to:
(B) conceal from a communication service provider, or from any lawful authority, the existence or place of origin or destination of any communication;

It would appear that an unintended consequence of this legislation would slap criminal penalties on innocent people who set their firewalls at high security levels to preclude responses to pings or other mechanisms for identification of their IP connections. Users connecting to a corporate site via virtual private network to send e-mail could theoretically be in trouble because even the SMTP headers are encrypted on their way to the corporate e-mail server, thus precluding the ISP in the middle from identifying the nature of the traffic or its destination.

The EFFhas taken on the responsibility to keep track of this legislation. Web site is

http://www.eff.org/IP/DMCA/states/

*Category 47* *US computer-crime laws*

2003-04-30 **war driving insecure network wireless Wi-Fi New Hampshire legal**

NIPC/DHS

April 29, Wired — Licensed to war drive in New Hampshire. New Hampshire could become the first in the United States to provide legal protection for people who tap into insecure wireless networks. House Bill 495 defines an operator's failure to secure a wireless network as a form of negligence. According to the proposed amendment, "the owner of a wireless computer network shall be responsible for securing such computer network." What's more, if an alleged intruder can prove he gained access to an insecure wireless network believing it was intended to be open, the defendant may be able to get off the hook using an "affirmative defense" provision of the existing law. As a result, some legal experts contend that New Hampshire's proposed amendment to its computer laws could make it harder to throw the book at criminals who take advantage of insecure wireless systems.

*Category 47* *US computer-crime laws*

2003-05-05 **anti-piracy law overly broad smart cards free satellite cable internet service MPAA Motion Picture Association of America intellectual property VPN**

NewsScan

WILL NEW ANTI-PIRACY LAWS STIFLE INNOVATION?
According to some critics, several of the newly enacted or proposed state laws to outlaw software for downloading movies without paying or unauthorized use of smart cards to get free satellite, cable or Internet service, will not only stifle innovation but might also be interpreted as outlawing such common devices as video recorders and music players. The Motion Picture Association of America (MPAA) says that some state laws are vague on piracy techniques (e.g., smart cards altered to unscramble transmissions). Robin Gross of IP Justice, a civil liberties group focused on intellectual property, says: "These laws are really talking about trying to regulate what somebody can do with the services they have already paid for." Supporters of such legislation see it differently, and insist that people "are seeing demons in these bills, where there are no demons." But critics are adamant, and say they fear the concealment provisions in new legislation could be used to ban security firewalls, encrypted virtual private networks for telecommuters and systems designed to preserve anonymity and protect privacy. (San Jose Mercury News 5 May 2003)

*Category 47* *US computer-crime laws*

2003-06-30 **personal hacking data theft FBI bill law personal data**

NewsScan

BILL WOULD MANDATE NOTIFICATION OF PERSONAL DATA HACKS
Legislation introduced by Sen. Dianne Feinstein (D-Calif.) would require businesses and government agencies to notify consumers when hackers break into corporate computer systems and steal their personal data, such as social security numbers and credit card information. The stipulations of the bill are in direct conflict with efforts by the Bush administration to keep such details hidden from the public, in the hope that hacking victims will notify the FBI and other government agencies when such incidents occur. The FBI director and some top U.S. prosecutors told technology executives recently that they will increasingly work to keep the secret the names of companies that fall victim to major hacking attacks. Consumer groups praised Feinstein's proposed legislation: "It's a really important step forward," said Chris Hoofnagle, deputy counsel at the Electronic Privacy Information Center. "Individuals do not have this right to notice now." (AP/CNN.com 30 Jun 2003)

*Category 47* *US computer-crime laws*

2003-10-23 **Senate Governmental Affairs Committee security P2P bill network systems personal information financial defense law enforcement public health citizens business**

NIPC/DHS

October 23, eSecurity Planet — Senate committee approves P2P security bill. The Senate Governmental Affairs Committee approved a bill mandating federal agencies to develop and implement security plans to protect their network systems from the risks posed by peer-to-peer (P2P) file sharing on Wednesday, October 22. Earlier this month, the U.S. House of Representatives approved the same legislation. Both the House and the Senate have already implemented security measures against P2P security threats through both technical and non-technical means, including firewalls and employee training. The Government Network Security Act of 2003 would give Executive Branch agencies six months to take similar steps. The federal government uses and stores a wide variety of classified and sensitive information, including information vital to national security, defense, law enforcement, economic markets, public health, and the environment. Government computers also contain personal and financial information of U.S. citizens and businesses. Installation of P2P software on government computers can expose this sensitive information to the public. The House Committee on Government Reform issued a staff report in May showing how through a "couple of simple searches" of the most popular P2P programs, personal information such as tax returns, medical records, and confidential legal documents and business files were found.

# 48.2 Non-US computer-crime laws

*Category 48.2 Non-US computer-crime laws*

2003-03-05 **hacktivism criminal hacking laws punishment Europe**

NewsScan

ONLINE VANDAL OR ONLINE ACTIVIST: NO DIFFERENCE IN EU LAWS
New laws enacted by the 15-member European Union requiring member states to make it a crime to illegally access or interfere with an information system are intended to punish vandalism and deter viruses, and those laws give no special dispensation for hackers whose motives are social or political protest rather than pure vandalism. Attorney Leon de Costa in London says that the new code "criminalizes behavior which, until now, has been seen as lawful civil disobedience." (New York Times 5 Mar 2003)

---

*Category 48.2 Non-US computer-crime laws*

2003-12-12 **Peer2Peer P2P Copyright Board of Canada legal Apple iPods MP3**

NewsScan

CANADA RULES P2P DOWNLOADING LEGAL
The Copyright Board of Canada has ruled that downloading copyrighted music from peer-to-peer networks is legal in that country, although uploading files is not. The decision is intended to clarify what had been a somewhat ambiguous area of Canadian law. "As far as computer hard drives are concerned, we say that for the time being, it is still legal," says Claude Majeau, secretary general of the Copyright Board. Meanwhile, the Canadian Recording Industry Association is disputing the ruling: "Our position is that under Canadian law, downloading is also prohibited. This is the opinion of the Copyright Board, but Canadian courts will decide this issue," says a lawyer for the group. The decision has also rankled the U.S. recording industry, which has been aggressively battling music downloading on its own turf. In the same ruling, the Copyright Board imposed a per-unit fee of $15 to $25 on digital music players such as Apple iPods and MP3 players but declined to extend the fee to computer hard drives. The fees are used to compensate musicians and songwriters. (CNet News.com 12 Dec 2003)

---

*Category 48.2 Non-US computer-crime laws*

2003-12-24 **DVD anti-copying Jon Johansen DCMA tougher copyright law enactment Europe Canada Australia Central South America**

NewsScan

COPYRIGHT ACQUITTAL COULD SPUR CHANGES IN LAW
A Norwegian court's recent acquittal of Jon Johansen on charges of writing a software tool that can be used to circumvent DVD anticopying technology may spark a wave of tougher copyright law enactment in Europe, Canada, Australia and Central and South America, where such legislation is proposed. Critics of the U.S. Digital Millennium Copyright Act (DCMA) say the DCMA's tendency to protect content owners at the expense of consumers is flawed and the Norwegian court's action should serve as the basis for further debate over the shortcomings of the U.S. law. "The acquittal is a great development. The whole notion of prohibiting acts of circumvention or circumvention devices when it's not directly tied to infringing conduct is the wrong approach. The point is, there may be lawful reasons why someone would want to circumvent a technology," says intellectual property attorney Jonathan Band. Meanwhile, Hollywood has mounted an aggressive drive to win greater global conformity in copyright law, using the precepts of the DCMA as a bargaining chip with potential trade partners. The European Union has begun implementing such legislation and U.S. negotiators are pushing for similar laws as part of the pending Free Trade Area of the Americas (FTAA) treaty, which would encompass most of North, Central and South America. Meanwhile, foot-dragging on the part of South Korea and Canada has irritated the U.S. entertainment industry: "The (WIPO) treaty was effectively negotiated a decade ago, and for a country like Korea, or Canada, to say now that they need to start examining these issues is crazy," says Neil Turkewitz, executive VP for international issues at the Recording Industry Association of America. (CNet News.com 24 Dec 2003)

---

# 49 Privacy, government surveillance, legislation, agreements

*Category 49* *Privacy, government surveillance, legislation, agreements*

2003-03-31 **PATRIOT II legislation Justice Department encryption punishable**

NewsScan

[U.S.A.P.A.T.R.I.O.T.] II ACT WOULD PUNISH CRIMINALS WHO ENCRYPT
Draft legislation circulating in the Justice Department would impose stiffer prison sentences for scrambling data in commission of a crime — something encryption specialists say would have little effect on fighting terrorism and will only hurt legitimate uses of cryptography. "Why should the fact that you use encryption have anything to do with how guilty you are and what the punishment should be?" asks Stanton McCandlish of the CryptoRights Foundation. "Should we have enhanced penalties because someone wore an overcoat?" The measure, which would add up to five years to a sentence for a first offense and 10 years after that, is backed by police and intelligence agents who worry that encryption will hamper their ability to fight crime. "If you went the extra step to keep us from getting evidence, you should pay an extra price," says a former computer crimes investigator with the New York Police Department. But many question whether such a law would have its intended effect: "You have to be intentional about using encryption, and that's a tricky thing to prove. I do see this provision as largely symbolic rather than effective," says a former National Security Agency counsel. The new proposal is part of legislation dubbed [U.S.A.P.A.T.R.I.O.T. II], a sequel to the 2001 [U.S.A.P.A.T.R.I.O.T.] Act. (AP 31 Mar 2003)

*Category 49* *Privacy, government surveillance, legislation, agreements*

2003-07-14 **privacy terrorism awareness TIA pattern recognition searches**

NewsScan

PRIVACY APPLIANCES TO GUIDE TIA PATTERN-RECOGNITION SEARCHES
Data security expert Teresa Lunt, working at PARC (Palo Alto Research Center), has developed a "privacy appliance" intended to help prevent the Pentagon's Terrorism Information Awareness (TIA) project from inadvertently violating individual rights. Privacy appliances (which filter out personal identifying information) include such built-in protections as an unalterable log of what information is returned and to whom — and the software in such devices would be smart enough to adjust results based on what has previously been released and whether individuals can be identified through inference. Lunt says people have the mistaken idea that TIA would remove data sources from private hands and include them in a government database. But that's not the way it works, and in fact there's nothing new about it; the fact is, marketing companies routinely use data mining techniques to look for customer patterns that would support corporate sales programs, and under TIA those existing techniques would merely be applied to the relatively new problem of identifying and monitoring potential terrorist operations. (AP/San Jose Mercury News 14 Jul 2003)

*Category 49* *Privacy, government surveillance, legislation, agreements*

2003-07-18 **surveillance microchip personal information Mexico**

NewsScan

IMPLANTABLE MICROCHIP STRIKES A CHORD IN MEXICO
Palm Beach, Fla.-based Applied Digital Solutions, maker of the implantable VeriChip, is targeting consumers south of the border, where people see the tiny devices as a possible new way to thwart crime. The microchips, which are available in the U.S. as well, are implanted under the skin and can be used to link to information on identity, blood type and other information housed on a central computer. In Mexico, citizens hope the tiny devices could prove one more weapon in the arsenal needed to combat a rising wave of kidnappings, robberies and other crimes. The Mexican company in charge of distribution says it hopes to implant 10,000 chips in the first year and ensure that 70% of all hospitals contain the technology necessary to read the chips. Company officials say they are working on developing a similar technology that would use satellites to locate people who've been kidnapped, an application that is popular with Mexicans, but has raised privacy concerns in the U.S. (AP 18 Jul 2003)

*Category 49* *Privacy, government surveillance, legislation, agreements*

2003-07-23 **passports 2004 US microchip privacy surveillance**

NewsScan

SMART' PASSPORTS SET FOR 2004 DEBUT
Beginning in October 2004, the U.S. will begin issuing "smart" passports that include an embedded microchip that stores a compressed image of its owner's face. The new digital passports are intended to prevent tampering, but civil liberties groups say such technology could eventually be used to monitor the activities of citizens in unprecedented detail. However, Frank Moss, deputy assistant secretary for Passport Services at the U.S. State Department says such fears are unfounded: "They will include no information other than that on the basic passport information page." Meanwhile, European travelers may also soon be required to carry passports containing both fingerprint and iris scan biometric information, but no date has been set yet for the new passports' introduction. (New Scientist 23 Jul 2003)

*Category 49* *Privacy, government surveillance, legislation, agreements*

2003-08-28 **privacy law Californai information collection**

NewsScan

CALIFORNIA GETS NEW PRIVACY LAW
California has just passed privacy legislation aimed at preventing banks, insurance companies and other institutions from sharing their personal information, and Gov. Gray Davis said: "Most Californians are stunned to learn that financial corporations trade their names for money. That is wrong, and when I sign this bill, that practice will stop." The law will require permission from a customer before financial institutions share any information on that customer with an unaffiliated company or an affiliated firm in a different line of business. (AP/USA Today 28 Aug 2003)

*Category 49* *Privacy, government surveillance, legislation, agreements*

2003-10-19 **intercepting e-mail crime punishment privacy**

NewsScan

INTERCEPTING E-MAIL IS A CRIME
An Arizona woman was sentenced to 60 days of home detention for intercepting at least 215 e-mail messages directed to her husband's ex-wife. Law enforcement officials said Angel Lee fraudulently obtained the ex-wife's user name and password, allowing her to log in and read mail. Ex-wife Duongladde Ramsey said Lee's actions were comparable to breaking into her house and reading her diary, and the judge agreed, saying Lee's penalty is a warning to others who might be tempted to spy on others' e-mail accounts. "Privacy is still a cherished value," said U.S. District Judge Richard P. Matsch. (AP 19 Oct 2003)

# 4A3 Jurisdiction

*Category 4A3* *Jurisdiction*

2003-02-12 **Internet jurisdiction online auctions**

NewsScan

YAHOO EXONERATED IN NAZI MEMORABILIA CASE
A Paris court has thrown out a case brought against Yahoo by French human rights activists who maintained that Yahoo should be held legally responsible for allowing online auctions of Nazi collectibles. French law forbids the display or sale of racist material. The case led to a landmark ruling in France, with a court ordering Yahoo to block Web surfers in France from accessing auctions selling Nazi memorabilia. Yahoo eventually banned sales of Nazi collectibles when it began charging users for auction listings, saying it did not want to profit from such items, but insisted it had nothing to do with the ongoing litigation. Tuesday's decision ends the three-year legal struggle, with the Paris court's decision that Yahoo did not meet the criteria of "justifying war crimes" because its auction listing did not result in "glorifying, praising or at least presenting the crimes in question favorably." (AP 12 Feb 2003)
http://apnews.excite.com/article/20030212/D7P520LO0.htm

*Category 4A3* *Jurisdiction*

2003-04-28 **Internet jurisdiction US supreme court**

NewsScan

SUPREME COURT DODGES QUESTION OF INTERNET JURISDICTION
The U.S. Supreme Court has refused to review a case that might have decided what courts have jurisdiction over cases involving the Internet. The case it rejected was an appeal brought by Healthgrades.com, which rates health care providers, after it had lost a lawsuit to home health care provider Northwest Healthcare Alliance. When Northwest received a poorer rating than it thought it deserved, it sued Healthgrades for defamation, and won. (AP/San Jose Mercury News 28 Apr 2003)

# 4A4 Blocking

*Category 4A4* *Blocking*

2003-03-12 **pop-up advertising blocking software ISP Internet service provider**

NewsScan

EARTHLINK MOVES TO BLOCK POP-UP ADS
EarthLink, in a move to differentiate itself from rival ISPs, says it will offer subscribers free software to block those annoying pop-up ads that clutter the screen. The Pop-Up Blocker software uses technology from FailSafe Technology in Salt Lake City, and by taking the initiative to offer it EarthLink hopes to reinforce its image as an ISP that's more receptive to user needs than many of its competitors. Meanwhile, advertisers are already hard at work on new formats and strategies to outsmart the ad-blockers. And the race continues? (Wall Street Journal 19 Aug 2002)

AOL SMACKS DOWN POP-UP ADS
In an effort to revitalize its online service, AOL is pulling the plug on those annoying pop-up ads that clutter users' screens. Although the company officially stopped selling pop-ups on Tuesday, the ads will continue to appear on the site for several more months, because it must still honor existing advertising contracts, says CEO Jonathan Miller. Also, AOL is reserving the right to run pop-ups on behalf of AOL and other AOL Time Warner divisions. Consumers generally don't like pop-up ads, according to a November 2001 study by Dynamic Logic. In fact, only telemarketing was considered more annoying than pop-ups in that study, which looked at consumer responses to TV commercials, direct mail, and print ads in newspapers and magazines. According to a Nielsen/NetRatings report issued last month, fewer than one in 10 of all companies advertising online use pop-up ads. Meanwhile, Microsoft's MSN service says it will continue to run pop-ups, although with a low frequency, and Yahoo plans to continue using pop-ups on a limited basis, mostly for surveys after a consumer completes a shopping purchase or related to movie ads. (Wall Street Journal 16 Oct 2002)

EARTHLINK DERIDES AOL'S POP-UP ADS
Earthlink has launched a two-week ad campaign in the New York Times and USA Today to try to woo current AOL subscribers who are unhappy with AOL's practice of using pop-ads. One ad asks mockingly, "What can you expect now that AOL only allows pop-up ads from AOL Time Warner businesses?" Another sneers: "It took AOL 8.0 tries to figure out people don't like pop-up ads?" AOL seems to be trying to shrug its rival off, and a spokesman for that company said condescendingly: "It must be frustrating for competitors in the online industry who have lost this wedge issue with customers." (Atlanta Journal-Constitution 1 Nov 2002)

AOL DELIVERS USERS FROM 'POP-UP PURGATORY'
America Online is giving its subscribers some relief from the annoying pop-up ads that seem to be proliferating at an alarming pace across the Web. In response to complaints from users, AOL will automatically install its Web Pop-Up Controls onto the desktops of its 33 million subscribers during the next two weeks. Many AOL users had listed pop-up advertising as one the most annoying features of surfing the Web. "AOL's new Pop-Up Controls will allow our members to explore the Web without being trapped in pop-up purgatory," says an AOL spokesman. The latest move mirrors one made by rival Earthlink several months ago, and comes as the world's largest Internet provider is struggling with stagnant subscriber growth over the past year. (CNet News.com 11 Mar 2003)
http://news.com.com/2100-1024-992142.html

# 4A7 Spam

*Category 4A7 Spam*

2003-02-19 **spam dictionary attack lawsuit ISP Internet service provider**

NewsScan

MICROSOFT STEAMED OVER HOTMAIL SPAM
Microsoft has filed a lawsuit against unnamed bulk mailers who harvested the e-mail addresses of Hotmail users in order to bombard them with junk messages. The spammers allegedly used tools to randomly generate e-mail addresses and then tested them to see which accounts were active. Microsoft argues that this form of dictionary attack violates federal laws, including the Computer Fraud and Abuse Act. (The Register 19 Feb 2003)
http://www.theregister.co.uk/content/6/29382.html

*Category 4A7 Spam*

2003-02-20 **spam laws content filtering**

NewsScan

ANOTHER ANTI-SPAM LAW PROPOSED
At least 26 states already have anti-spam laws on the books, without much to show for them, but California state senator Debra Bowen is trying again, this time by proposing a bill making it a crime to send unsolicited commercial e-mail to accounts in California. Bowen says that spam "is really turning the Internet into a tool of questionable value. I had someone write to me say, 'Spam is turning the Internet into an open sewer, and as the Romans discovered, open sewers are a bad thing.'" However, Jupiter Research analyst Jared Blank says it will take technology rather than legislation to get spam under control. But filtering technology can also be a problem, and the E-mail Service Providers Coalition hopes people will report missing and legitimate e-mail caught in "spam traps." [Good idea. Be sure to do that if you find some befuddled programmer is depriving you of your NewsScan Daily for one silly reason or another, hurting our feelings by confusing us with Spam. Can you BELIEVE that?] (Reuters/USA Today 19 Feb 2003)

*Category 4A7 Spam*

2003-02-21 **spam legislation laws task force ISP Internet service providers**

NewsScan

AOL PREPARES FOR NEW BATTLE AGAINST SPAM
America Online has told its 27 million U.S. customers that it is forming an anti-spam task force and will seek tougher legislation to stop unsolicited junk e-mail. . . . (San Jose Mercury News 21 Feb 2003)

THE AOL APPROACH TO SPAM
America Online, which says it blocks an average of 28 junk e-mail messages per account per day, trashed a billion (presumably unsolicited) messages in a two-day period this week, without letting them arrive at customers' in-boxes. AOL spokesman Nicholas Graham asserts that only "an extremely small fraction" of the messages trapped in AOL's spam filters are legitimate communications. . . . (AP/San Jose Mercury News 6 Mar 2003)

*Category 4A7 Spam*

2003-02-25 **spam marketing proposed legislation penalties**

NewsScan

DIRECT MARKETERS JOIN FIGHT AGAINST SPAM
An unlikely ally has joined the battle against unsolicited commercial e-mail — the Direct Marketing Association announced it is now backing the push for federal legislation to restrict spam. The DMA previously had urged self-regulation, but now says the spam problem has gotten totally out of hand: "The volume is so great that we have to have some sort of government intervention," says DMA senior VP Jerry Cerasale. The group says that legitimate marketers should still be allowed to use e-mail, but plans to suggest that marketers who violate consumers' requests to be removed from mailing lists should pay stiff penalties of $11,000 per incident (per unsolicited message). Spam now comprises 41% of all e-mail, according to Brightmail, and accounts for $4 billion a year in lost productivity, according to a Ferris Research study. (Wall Street Journal 25 Feb 2003)

*Category 4A7 Spam*

2003-03-30 **e-mail bomb Intel free speech private poperty lawsuit**

NewsScan

INTEL VS. HAMIDI: FREE SPEECH CASE OR PRIVATE PROPERTY CASE?
The California Supreme Court will soon be reviewing a lawsuit first brought five years by chipmaker Intel against a terminated employee whom it charges violated its private property rights by bombarding its e-mail system with messages to Intel employees. The ex-employee, Ken Hamidi, has portrayed the dispute as a freedom of speech case, whereas Intel says the issue is not about the content of Hamidi's messages but about the fact that he used Intel's own systems without its permission. Intel says, "For us, it's not a First Amendment issue and never has been. Ken has been very persistent and creative in exercising his right to speak out. But our view is that, in exercising his rights to free speech, he needs to protect the property fights of Intel, including our e-mail system." On the other hand, Stanford law professor Jennifer Granick argues that there was no violation of Intel's property rights because there was no actual damage to Intel property: "There is no harm to Intel's servers — it's the communication of the message that Intel considers the harm. That's not the kind of harm the courts should be in the business of protecting people from. It undermines the nature of the Internet as a place to exercise free speech rights."(San Jose Mercury News 30 Mar 2003)

*Category 4A7 Spam*

2003-04-15 **spam lawsuits AOL America Online**

NewsScan

AOL SUES SPAMMERS
AOL has filed five federal lawsuits against alleged distributors of mass junk-mail, seeking damages of more than $10 million plus an end to the messages. The case comes in response to about 8 million individual spam complaints registered by AOL subscribers, most of whom used a "Spam Report" feature introduced on the Web site last fall. Most of the defendants are referred to as "John Doe," meaning that AOL could not determine their true identities, but the suits also name Michael Levesque of Issaquah, Wash., and George A. Moore Jr. of Linthicum, Md., both of whom had listed false phone numbers in their domain name registrations. By filing the lawsuits, AOL gains additional authority to subpoena Internet service providers and others trying to track down the other spammers. Meanwhile, AOL has also begun targeting spammers who use residential broadband services such as Comcast and RoadRunner, which is owned by AOL Time Warner. (AP 15 Apr 2003)

*Category 4A7 Spam*

2003-04-17 **spam Australia Internet harm**

NewsScan

SPAM WARS: THE BATTLE FOR AUSTRALIA
Another spam story. Richard Alston, Australia's minister for communications and information technology, says that Internet spam "is now completely out of hand" — "no longer a nuisance but costly, disruptive and a threat to IT systems." He therefore will propose to that country's federal parliament legislation that would ban unsolicited commercial Internet messages and impose substantial fines on Australian spammers. Estimates of lost time and productivity are $960 per employee bombarded with e-mail messages offering black market drugs, pornography, Nigerian money laundering schemes, and other such unwelcome material. (The Age, Australia, 17 Apr 2003)

*Category 4A7 Spam*

2003-04-18 **spam pornography lawsuit FTC**

NewsScan

FTC ACCUSES MAN OF PORNOGRAPHIC SPAMMING
There is no federal law banning governing spam, so the Federal Trade Communications is invoking laws against business fraud to file a lawsuit against Brian Westby of Missouri, whom it charges with netting $1 million from his Internet pornographic e-mail campaigns using fake subjects such as "What is wrong?" and "Fwd: You may want to reboot your computer." The FTC says that more than a third of the 120,000 pieces of pornographic spam it receives each day from displeased spam recipients is accounted for Westby's activities. (Washington Post 18 Apr 2003)

*Category* *4A7* *Spam*

2003-04-26 **spam fight against bounty legislation**

NewsScan

A BOUNTY ON THE HEADS OF SPAMMERS
Congresswoman Zoe Lofgren plans to introduce legislation drafted by Stanford law professor Larry Lessig that would require unsolicited commercial e-mails ("spam") to be identified as advertising and would put a bounty on anyone who breaks that law, by offering rewards of thousands of dollars or more to the person who is first to provide the government with proof and the identity of offending spammers. Lessig is so confident his war on spam will be effective that he's promising to quit his Stanford job if the bill becomes law and "does not substantially reduce the level of spam." (San Jose Mercury News 26 Apr 2003)

*Category* *4A7* *Spam*

2003-04-30 **spam anti-spam law Virginia jail term e-mail**

NIPC/DHS

VIRGINIA'S NEW LAW THREATENS SPAMMERS WITH JAIL TERMS
Under a new law enacted in Virginia, individuals who use deception to send high-volumes of unsolicited commercial e-mail will be declared felons and liable to one- to five-year prison terms. Virginia Governor Mark R. Warner says, "Many spammers see the current system that imposes civil fines as just a cost of doing business. We hope we will see some high-profile prosecutions. If someone faces a jail sentence and a major forfeiture of assets, it will serve as a deterrent." The new law, which outlaws practices such as forging the return address line of an e-mail message or sending spam surreptitiously, would apply to anyone who sent high volumes of spam to or from anyone in Virginia. (New York Times 30 Apr 2003)

*Category* *4A7* *Spam*

2003-05-03 **spam out of control law unsolicited e-mail FTC Orson Swindle**

NewsScan

SPAM OUT OF CONTROL — BUT LAW IS NOT THE ANSWER
Eileen Harrington, the director of the Federal Trade Commission's marketing practices, that the problem of spam (bulk unsolicited e-mail) is "worse than we imagined. There is consensus that the problem has reached a tipping point. If there are not immediate improvements implemented across the board by technologists, service providers and perhaps lawmakers, e-mail is at risk of being run into the ground." Legislators at both federal and state levels have been busy enacting or proposing new laws, but FTC Commissioner Orson Swindle remains skeptical: "New laws that are unenforceable for myriad reasons or that are overtaken by the advances of technology have the potential to do more harm than good. No single law, no single new technology, no new initiative, no new meetings are going to solve this problem alone." And John Patrick, chairman of the industry-supported Global Internet Project, agrees, saying that the only solution to spam is to block it with new technology. (AP/Atlanta Journal-Constitution 3 May 2003)

*Category* *4A7* *Spam*

2003-05-07 **earthlink buffalo NY spammer spamage accounts 825 million messages award**

NewsScan

EARTHLINK AWARDED $16M IN SPAMAGES
A federal judge awarded Earthlink $16.4 million in damages and instituted a permanent injunction against a Buffalo, NY, man identified as the ringleader of a group that used Earthlink's network to send 825 million spam messages over the past year. Earthlink said Howard Carmack and his cronies used Internet accounts opened with stolen identities and credit cards to send junk e-mail. The ruling is the latest in a series of legal actions taken by ISPs against bulk spammers. Last year Earthlink won $25 million in damages in a suit against another bulk e-mailer, Kahn C. Smith of Tennessee, but it hasn't collected the award. The company also has several other lawsuits pending. Meanwhile, last December, America Online won a $6.9 million judgment against a now-defunct Illinois company that specialized in p*rnographic spam. Over the last few years, AOL has won 25 spam-related lawsuits against more than 100 companies and individuals, says a company spokesman. (AP 7 May 2003)

*Category 4A7* *Spam*

2003-05-13 **spam legislation law proposal farce opt-out lobbyists industry ISPs direct mail retailers divisions subsidiaries**

WP http://www.washingtonpost.com/ac2/wp-dyn/A47350-2003May12?language=printer

W.J. "Billy" Tauzin (R-LA), head of the House Energy and Commerce Committee, and F. James Sensenbrenner Jr. (R-WI), chairman of the Judiciary Committee sponsored an effort to define federal legislation to protect spammers in response to heavy lobbying by the direct mail industry, ISPs, and retailers. Writing in the Washington Post, Jonathan Krim reported, "According to participants in at least three meetings in recent weeks, e-mail marketers prevailed in adding provisions that would supersede tougher state anti-spam laws, would prohibit consumers from suing spammers and would give companies the right to send e-mail to anyone who has done business with them in the past three years." The bill would support opt-out provisions to allow one-time spamming. In addition, every "line of business" or subsidiary could send junk e-mail and require a separate opt-out instruction from recipients.

*Category 4A7* *Spam*

2003-05-14 **buffalo spammer identity theft forgery criminal possession howard cormack earthlink accounts**

NewsScan

'BUFFALO SPAMMER' COULD GET UP TO SEVEN YEARS
Howard Carmack, the so-called "Buffalo Spammer," has become the first person in New York state to be charged under the state's identity theft laws. If convicted, he could be sentenced to 2-1/2 to 7 years in prison for identity theft, forgery, criminal possession of forgery devices (in the form of software used to create phony return addresses), and falsifying business records. According to the indictment, Carmack "stole the identities of innocent New Yorkers to spam millions of consumers throughout New York and the nation." He is charged with using 343 stolen identities to send his unsolicited bulk mailings through Earthlink accounts. An Earthlink executive said the main impact of the arrest would be to demonstrate to others the "very high cost of doing business" in spam. (New York Newsday 14 May 2003)

*Category 4A7* *Spam*

2003-05-23 **spam fraudulent e-mail headers spoofing lawsuits racketeering RICO law legislation**

Macworld http://maccentral.macworld.com/news/2003/05/23/antispam/

Sen. Bill Nelson (D-FL) introduced an antispam bill that would apply the Federal Racketeer Influenced and Corrupt Organizations Act (RICO) to spammers using fraudulent e-mail headers as well as allowing civil lawsuits for damages against spammers.

*Category 4A7* *Spam*

2003-05-27 **federal law legislation private lawsuits opt-out industry lobbyists direct marketing**

PCWorld http://www.pcworld.com/resource/printable/article/0,aid,110881,00.asp

By the end of May 2003, there was a great deal of activity in the US Congress concerning Federal legislation to control spam. Antispam activists severely criticized the majority of the measures and even the concept of using laws as a defense against spam on the following grounds:

* The very definition of spam remains ambiguous;
* Most bills would explicitly supersede more severe state antispam laws, reducing pressure on spammers;
* Many of the laws preclude civil litigation for damages against spammers;
* Most of the laws are based on opting out of spam, allowing potentially huge numbers of unwanted e-mail messages to be sent to victims;
* The laws would essentially legalize spam and place the burden of stopping it on the recipients;
* Offshore spammers would be unaffected by any legislation;
* Litigation against criminal spammers using false identification would remain difficult.

*Category 4A7* *Spam*

2003-06-11 **FTC fight spam Federal Trade Commission ICPEA FBI criminal databases foreign servers overseas**

NewsScan

June 11, CNET News.com — FTC seeks broad powers to fight spam. The Federal Trade Commission (FTC) Wednesday asked Congress for sweeping new powers that would let it cooperate closely with governments abroad and prosecute domestic and overseas spammers more readily. The International Consumer Protection Enforcement Act (ICPEA), a 13-page proposal drafted by the FTC, would turn the agency's investigators into virtual spam cops, granting them the power to serve secret requests for subscriber information on Internet service providers, peruse FBI criminal databases and swap sensitive information with foreign law enforcement agencies. "A recent study by the commission found that 66 percent of spam contained obvious indicia of falsity," the FTC's five commissioners said in a joint statement to Congress released Wednesday. "Moreover, a significant portion of spam is likely to be routed through foreign servers."

*Category 4A7* *Spam*

2003-06-11 **FTC Spam fight new powers U.S. Federal Trade Commision**

NewsScan

FTC ASKS FOR NEW POWERS TO FIGHT SPAM
U.S. Federal Trade Commission Chairman Timothy Muris is asking Congress to broaden the FTC's authority to investigate and prosecute spammers. The request follows congressional hearings on the subject and an FTC study concluding that two-thirds of spam is fraudulent or misleading. Meanwhile, several bills to fight spam have been introduced in Congress, the frontrunner of which is sponsored by Rep. W.J. Tauzin (R-La.), chairman of the House Energy and Commerce Committee. Tauzin's proposed legislation would require e-mail marketers to reveal their true e-mail addresses, honor consumer requests to be removed from mailing lists, and require that p*ornographic spam be labeled as such. The bill would authorize ISPs, state attorneys general and federal law-enforcement officials to track down suspected spammers and would allow fines up to $1.5 million and jail time up to two years for guilty parties. Consumer groups have criticized the Tauzin bill, saying it would override tougher state laws and is full of loopholes. (Wall Street Journal 11 Jun 2003)

*Category 4A7* *Spam*

2003-06-17 **spam civil lawsuit litigation harvesting addresses deceptive subject lines pornography children**

http://www.microsoft.com/presspass/features/2003/jun03/06-17SpamEnforcement.asp

In May and June of 2003, Microsoft launched an assault again spammers by filing 13 civil suits in US and two in the UK. The lawsuits included complaints about deceptive subject lines and harvesting e-mail addresses. Tim Cranton, a senior attorney at Microsoft, said in an interview, "We're focusing our efforts on the type of spam that troubles our customers the most: consumer deception and unsolicited pornography. Deceptive spam includes e-mail that uses misleading information — either about who sent the e-mail or what the e-mail is regarding — to trick the recipient into opening the mail because they think it's something that it isn't. These often come in the form of get-rich-quick schemes, adult services or purported health offerings. An FTC study found that an estimated 66 percent of spam has some type of false information, so this is a huge problem that must be addressed. Another significant customer concern is unwanted, sexually explicit material that may reach children or that is otherwise offensive to recipients who did not request to receive such material."

*Category 4A7* *Spam*

2003-06-18 **microsoft sues spammers msn hotmail**

NewsScan

MICROSOFT SUES 15 SPAMMERS
Estimating that more than 80% of the 2.5 billion e-mail messages sent each day to customers of its free Hotmail service are the work of spammers, Microsoft has filed lawsuits against 15 groups of individuals and corporations it claims are major spammers. Like many Internet companies, Microsoft is also looking for technological solutions to the problem of spam. It has already introduced anti-spam software filters on its MSN Internet access service, and plans to include similar software at the next release of its Outlook e-mail software. (New York Times 18 Jun 2003)

*Category 4A7* *Spam*

2003-06-20 **against spammers legislate bill law false e-mail headers subject lines**

NewsScan

SENATE TRIES AGAIN TO LEGISLATE AGAINST SPAMMERS
The Senate Commerce Committee has unanimously approved a bill that would make it illegal for any person or company to use fraudulent or deceptive return e-mail address, false e-mail headers, or false and misleading subject lines. The bill, if passed into law, will also require that all e-mail marketing messages label those messages as advertisements, provide the sender's physical address, and offer a way for recipients to decline to receive any further messages from the marketer who sent them. (New York Times 20 Jun 2003)

*Category 4A7* *Spam*

2003-07-01 **anti-spam bill law legislations Consumer Union**

NewsScan

FEDERAL ANTI-SPAM BILLS WON'T DO THE TRICK
The legal counsel of the Consumers Union, which publishes Consumer Reports, has told a U.S. House subcommittee that the anti-spam legislation Congress is considering is insufficient, because it places too much burden on consumers: "Thus far, the bills proposed, including H.R. 2214, have an 'opt-out' as part of their core solution. In other words, an Internet service provider must first pass on the spam to consumers, consumers must then read the spam, and then they can exercise their right to stop receiving messages from that particular sender... This puts too much burden on consumers to block spam and makes it too difficult to hold spammers legally accountable for their inappropriate interference with consumers' e-mail." (TechWeb 9 Jul 2003)

*Category 4A7* *Spam*

2003-07-18 **spam legislaltion anti-spam laws Congress e-mail**

NewsScan

WHY ARE SPAMMERS BACKING SPAM-CONTROL LAWS?
Bigtime spam-mongers and junk-mail proponents like the Direct Marketing Association are backing proposed antispam legislation, while consumer and public-interest groups, almost without exception, oppose the bills. What's going on? "It's a sign of who benefits from these bills and who doesn't," says a spokesman for the Coalition Against Unsolicited Commercial Email. "When you see some of the biggest spammers in the country backing legislation that is allegedly antispam, you really need to wonder about what these bills actually do." The answer is that rather than banning all unsolicited e-mail outright, as many consumer groups wish, they legitimize spam, as long as the perpetrators adhere to certain rules, such as using accurate subject lines and valid return addresses, and allowing recipients to opt out of future mailings. Two bills are currently making their way through Congress and a variant of thereof is expected to pass overwhelmingly and be signed into law later this year. (Wall Street Journal 18 Jul 2003)

*Category 4A7* *Spam*

2003-07-23 **anit-spam legislation support lawsuits FTC**

NewsScan

CONSUMERS SUPPORT LEGISLATION ANTI-SPAM LEGISLATION
A recent poll conducted by ePrivacy Group confirms a tidal wave of consumer sentiment against spam: 74% of respondents said they support a "do not e-mail" list and 59% said spammers should be punished. Of those who supported punishment, 80% said they favored consumer lawsuits against spammers. The news comes as no big surprise, but bolsters current efforts in Congress to pass legislation restricting unsolicited commercial e-mail. There are two bills currently moving through the legislative process: one introduced by Sen. Charles Schumer (D-N.Y.), which advocates creating a "do not e-mail" list and allows consumer lawsuits, and another sponsored by Sens. Conrad Burns (R-Mont.) and Ron Wyden (D-Ore.), which would direct the Federal Trade Commission to investigate the feasibility of a "do not e-mail" list. (Wall Street Journal 23 Jul 2003)

*Category 4A7* *Spam*

2003-07-23 **spam law legislation opt-in do-not-spam list FTC**

NWF http://www.nwfusion.com/cgi-bin/mailto/x.cgi

Sen. Charles Schumer (D-NY) supported his introduction of the Stop Pornography and Abusive Marketing (SPAM) Act by releasing results of a survey of 1,093 U.S. Internet users polled by the ePrivacy Group. Respondents

* supported a national do-not-spam list (74% ),

* agreed that unwanted e-mail should be banned or limited by law (79% ), and

* said spammers should be punished (59%).

Critics of the do-not-spam list, including FTC staffers, worried that the list would simply become a source of e-mail addresses for spammers to abuse. Many doubted that spammers would pay any attention to such restrictions.

---

*Category 4A7* *Spam*

2003-07-23 **anit-spam legislation Australia new law**

NewsScan

GOOD LUCK: AUSTRALIA CONSIDERS NEW LAW TO BAN SPAM
Australia's federal government plans to introduce legislation to end unsolicited commercial email by banning the "sending of commercial electronic messages without the prior consent of end-users unless there is an existing customer-business relationship"; imposing a range of penalties for breaking this law including fines, infringement notices and the ability to seek injunctions; requiring all commercial electronic messages to include a working opt-out mechanism and the sender's accurate contact details; banning the use of e-mail address harvesting software; and cooperating with overseas organizations to develop international guidelines and mechanisms to battle spam. The legislation would be enforced by the Australian Communications Authority (ACA). Jodie Sangster of the Australian Direct Marketing Association (ADMA) urges caution: "This is an issue where if they get it wrong could have a huge impact on business, particularly small businesses. For that reason, it's in the government's interest to make sure they fully consult and take into account the businesses it's going to impact on." (ZDNet 23 Jul 2003)

---

*Category 4A7* *Spam*

2003-08-26 **spam Amazon lawsuit sue e-mail unsolicited**

NewsScan

AMAZON SUES SPAMMERS
Amazon.com has filed federal lawsuits against 11 e-mail marketers it accuses of faking their e-mail addresses to appear as though the messages were sent by Amazon (a practice that is known as "spoofing" and is linked with spam abuses). The research firm IDC predicts that half of all external corporate e-mail — more than 2 trillion messages this year — will be spam. (USA Today 26 Aug 2003)

---

*Category 4A7* *Spam*

2003-08-27 **spam Earthlink lawsuit sue e-mail unsolicited**

NewsScan

EARTHLINK SUES SPAMMERS
EarthLink, the third largest U.S. Internet service provider, has sued 100 spammers located mostly in Alabama and Canada, alleging they used stolen credit cards, identity theft and banking fraud to pay for Internet accounts used to send out more than 250 million junk e-mails. The spammers eluded detection for about six months by creating bogus accounts and leasing phone lines that would automatically connect to EarthLink, even if the bogus users were kicked off. "Our investigation has been ongoing for a number of months, and this is a very tech-savvy spam ring which has made this a particularly challenging investigation," says Karen Cashion, lead counsel for EarthLink's lawsuit. The spam messages included ads for herbal impotence treatments, mortgage loans and fake company Web sites used for "phishing" personal and financial information from unsuspecting victims. EarthLink says it is still working to identify each spammer (the lawsuit lists the Alabama culprits as John Does 1-25), but plans to contact law enforcement officials once it can finger individuals. (AP 27 Aug 2003)

---

*Category* *4A7* *Spam*

2003-09-18 **spam UK criminal offense stephen timms law EU legislation unsolicited junk e-mail**

NewsScan

UK MAKES SPAM A CRIMINAL OFFENSE
A new law introduced by U.K. Communications Minister Stephen Timms means spammers could face fines of £5,000 in a magistrates court or an unlimited penalty from a jury. "These regulations will help combat the global nuisance of unsolicited e-mails and texts by enshrining in law rights that give consumers more say over who can use their personal details," says Timms. The law, which takes effect December 11, follows similar steps taken by the Italian government, which recently imposed fines of up to 90,000 euros and a maximum sentence of three years in prison for sending spam. Meanwhile, EU legislation banning unsolicited junk e-mail will be enforced beginning on October 31, but officials say it may have little effect because most spam originates in the U.S. and Asia, and thus will be out of its reach. (BBC News 18 Sep 2003)

*Category* *4A7* *Spam*

2003-09-24 **spamming california anti-spam law marketing companies**

NewsScan

CALIFORNIA SPAMMIN'
California's new anti-spam law may face the same fate as a similar law in Utah earlier this year. Kevin Johnson of the e-mail marketing company Digital Impact warns: "Hard-core spam will still come through, but legitimate companies will be more hesitant to send e-mail"; he also warns that when companies try to determine whether e-mail recipients live in California, spammers and advertisers may be forced to learn more about consumers, thereby reducing privacy. E-mail marketer Trevor Hughes suggests that the only answer is national legislation to harmonize spam laws in more than 30 states. (USA Today 24 Sep 2003)

*Category* *4A7* *Spam*

2003-10-04 **anti spam legislation e-mail**

NewsScan

SENATORS INTRODUCE ANTI-SPAM BILL
Senators Conrad Burns (R-Mont.) and Ron Wyden (D-Ore.) have introduced legislation that seeks to cut down on junk e-mail by requiring Internet marketers to provide legitimate return addresses on their e-mail and to honor consumers' requests to be taken off e-mail distribution lists. "This bill will help to keep legitimate Internet traffic and e-commerce flowing by going after those unscrupulous individuals who use e-mail in annoying and misleading ways," said Wyden in a statement. The bill would not allow individuals to sue spammers directly, but would require that state attorneys general sue on their behalf. The Federal Trade Commission could also fine violators, and ISPs could block spammers from their networks. The average U.S. Internet user received more than 2,200 spam messages last year, according to Jupiter Research, and the UK government said last month that spam now accounts for 40% of global e-mail traffic. A similar bill sponsored by Burns and Wyden cleared the Commerce Committee last year, but was not taken up for a vote in the Senate. "Now it's time to move forward. This legislation has been on hold for too long," says Burns. (Reuters 10 Apr 2003)

*Category* *4A7* *Spam*

2003-10-23 **spam OK Senate litigation laws**

NewsScan

SENATE VOTES TO CAN SPAM
The U.S. Senate has unanimously approved the "Can Spam" bill, sponsored by Sens. Conrad Burns (R-Mont.) and Ron Wyden (D-Ore.), which would ban the sleaziest techniques used by spammers to spew out millions of junk e-mail messages each day. Under the provisions of the bill, senders of unsolicited e-mail would be prohibited from disguising their purpose by using a fake return address or misleading subject line, and would no longer be allowed to harvest e-mail addresses off the Web to bulk up their lists. In addition, junk e-mail would be required to include a legitimate "opt out" function that recipients could use to get off lists. A provision proposed by Sen. Charles Schumer (D-N.Y.) authorizes the Federal Trade Commission to establish a "do-not-spam" list, similar to the recently implemented "do-not-call" list that blocks telemarketing calls. "Kingpin spammers who send out e-mail by the millions are threatening to drown the Internet in a sea of trash, and the American people want it stopped," said Wyden, who urged foreign countries to adopt similar measures. (AP 23 Oct 2003)

*Category* *4A7* *Spam*

2003-10-28 **spam privacy opt-out Web**

NYT http://www.nytimes.com/2003/10/28/technology/28SPAM.html?th

The CAN-SPAM antispam bill passed by the Senate may do little to stop legitimate companies from sending so-called white-collar spam.

*Category* *4A7* *Spam*

2003-11-26 **Can Spam Act Anti-Spam Bill House Senate President Bush filters**

NewsScan

ANTI-SPAM BILL PASSES IN HOUSE, SENATE
The Senate passed a bill to curb junk commercial e-mail by voice vote on Tuesday, and the House passed a similar measure on Saturday by a vote of 392 to 5. President Bush is expected to sign the legislation (known as the "Can Spam" Act) once the two bills are reconciled. Many are skeptical. California state Democrat senator Debra Bowen says, "The bill doesn't can spam, it legalizes it. It's full of loopholes. It's difficult to enforce. It's weaker than many state laws." And telecom attorney Charlie Kennedy advised: "The best line of defense for consumers are the antispam filters which are available commercially." (New York Times 26 Nov 2003)

---

*Category* *4A7* *Spam*

2003-12-09 **congress anti-spam bill five years prison commercial e-mail identity**

NewsScan

CONGRESS PASSES ANTI-SPAM BILL
Congress has passed anti-spam legislation that would supplant tougher anti-spam laws already passed in some states. The bill encourages the Federal Trade Commission to create a do-not-spam list of e-mail addresses and includes penalties for spammers of up to five years in prison. The legislation would prohibit senders of unsolicited commercial e-mail from disguising their identities by using a false return address or misleading subject line, and would require them to let recipients say they do not want future mass mailings. (Los Angeles Times 9 Dec 2003)

---

*Category* *4A7* *Spam*

2003-12-10 **anit-spam legislation reply-to FTC**

NewsScan

December 09, Associated Press — New anti-spam legislation compels consumers to hit 'reply' to e-mails. As the deluge of unsolicited pitches worsened during the Internet's growth, experts have cautioned computer users against doing what comes naturally: Reply to unwanted e-mails to demand an end to them. The reason? Unscrupulous spammers deem each such demand a verification that someone actually received their e-mails—and promptly sent dozens more to the same address. But the "can spam" legislation that Congress approved Monday requires unsolicited e-mails to include a mechanism so recipients could indicate they did not want future mass mailings. The legislation also will prohibit senders of unsolicited commercial e-mail from disguising their identity by using a false return address or misleading subject line, and it will prohibit senders from harvesting addresses off Websites. President Bush has indicated he intends to sign the measure into law. Indeed, the White House revamped its own e-mail system this summer over a flood of so-called spam. The anti-spam bill encourages the Federal Trade Commission to create a do-not-spam list of e-mail addresses and includes penalties for spammers of up to five years in prison in rare circumstances.

---

*Category* *4A7* *Spam*

2003-12-12 **anti-spam law virginia unsolicited mass e-mailing Internet History Eraser Pornographic Sites**

NewsScan

FIRST INDICTMENTS UNDER VIRGINIA ANTI-SPAM LAW
The state of Virginia has lodged criminal indictments against two people charged with making unsolicited mass e-mailings; it's the first case to be brought under a new antispam law in that state. Prosecutors say that in a one-month period last summer more than 100,000 AOL subscribers clicked a "report spam" button to complain about messages sent by the two defendants. The e-mail messages, sent with fake return addresses, contained information about stock-picking methods, mortgages and "Internet history eraser" software for deleting evidence that a user had visited pornographic sites. (New York Times 12 Dec 2003)

---

*Category* *4A7* *Spam*

2003-12-16 **anti-spam law George W. Bush e-mail marketing CAN-SPAM bill**

NewsScan

BUSH SIGNS NATIONAL ANTI-SPAM LAW
A new law signed by President Bush will attempt to rid the Internet of unsolicited commercial e-mail ("spam") — though many technology experts believe it will not be impossible for legislation passed by a single country to eliminate spam, because it is a global problem. However, supporters of the legislation say it gives state and federal law authorities the tools needed to track down and prosecute the largest and best-organized spammers. Democrat Senator Ron Wyden of Oregon, a coauthor of the CAN-SPAM bill, explains: "Our message is the fight has just begun and enforcement has got to be tough, tough, tough." (Washington Post 16 Dec 2003)

*Category* *4A7* *Spam*

2003-12-18 **spammers civil suits Scott Richter's OptInRealBig e-mail marketing**

NewsScan

CIVIL SUITS AGAINST SPAMMERS
New York State and Microsoft are filing civil lawsuits suits against prominent e-mail marketing operations, including Scott Richter's OptInRealBig. The lawsuits will attempt to hold responsible not just those accused of actually sending spam but also those who financially benefit from it. Richter, who has stoutly and publicly defended his marketing practices, says he's unconcerned about the lawsuits: "Messing with us is a big mistake. The more press I get, even bad press, the bigger we get." (New York Times 18 Dec 2003)

*Category* *4A7* *Spam*

2003-12-19 **spammers new york Eliot Spitzer bankruptcy Synergy6 Delta Seven OptInRealBig**

NewsScan

NEW YORK, MICROSOFT TARGET SPAMMERS
New York Attorney General Eliot Spitzer has filed a civil lawsuit against three top spam firms, threatening to seek penalties so large it would drive the companies out of business: "We will drive them into bankruptcy. Therefore, others will not come into the marketplace because they will see there is no viable business model here." The companies under fire are OptInRealBig, of Westminster, Co.; Synergy6, a New York marketing firm; and Delta Seven, a Dallas mailing company whose co-owner has already filed for bankruptcy protection. In addition to spewing spam, prosecutors have accused Delta Seven of obscuring the messages' origin by breaking into computers owned by others — including an elementary school in Korea and the Kuwaiti ministry of finance — to send the mail. Meanwhile, Microsoft has jumped on the anti-spam bandwagon with its own suit filed in Washington State seeking $18.8 million in damages caused by overloading its Hotmail service with junk e-mail. "Any money that is left over after the attorney general's suit, we will happily go after," says Microsoft general counsel Bradford L. Smith. (New York Times 19 Dec 2003)

*Category* *4A7* *Spam*

2003-12-28 **spam politicians legislators unsolicited non-commercial e-mail exemption CAN-SPAM**

http://www.nytimes.com/2003/12/28/politics/28EMAI.html?th=&pagewanted=print&position=

While they were passing the CAN-SPAM Act, members of Congress sent out hundreds of thousands of junk e-mail messages to constituents, buying e-mail addresses from spam-suppliers, and exempted their own junk e-mail from coverage by the CAN-SPAM Act, which applies to commercial junk but not to political junk.

# 4A8 Liability

*Category 4A8* *Liability*

2003-02-06 **legal liability worm damage operating system vulnerability class-action lawsuit**

NewsScan

KOREAN GROUP SAYS MICROSOFT LIABLE FOR SLAMMER DAMAGE
With support from more than 3,000 broadband subscribers, a South Korean group called the PSPD (People's Solidarity for Participatory Democracy) may file a product-liability class-action suit against Microsoft, alleging the company didn't "perform its duty to the fullest" to prevent the extensive damage caused in South Korea by the Slammer worm that exploited known vulnerabilities in Microsoft SQL 2000 servers. Slammer is also known as the Sapphire worm and SQLExp.(Cnet News.com 6 Feb 2003)
http://news.com.com/2100-1001-983578.html

*Category 4A8* *Liability*

2003-08-29 **liability due diligence worm Slammer telco lawsuit**

Maine Today; http://business.mainetoday.com/yourbusiness/030829yourbiz.shtml

When the SQL Slammer worm hit the Verizon ISP in Maine in January 2003, the company shut down access to some of its Internet services as part of its emergency response. Unfortunately, the shut down also triggered penalties for violating its performance standards as regulated by the
Maine Public Utilities Commission (PUC). The judgment hinged on Verizon's failure to apply critical patches that would have prevented the infection

In August, the PUC rejected horizons request for a waiver of penalties for its failure to meet its contractual performance standards and put the company at risk of paying more than $40,000 in rebates to its customers in Maine. Frank Jaffe and Jon Stanley, writing in _Maine Today_, commented, "This decision is one of the first anywhere in the world to define a legal duty requiring the prevention of damage and losses from new types of 'foreseeable' computer security incidents. This same logic could be applied to preventing losses from viruses, or most configuration or programming errors that lead to Web site or system security problems."

In a similar case, the Guess company was fined $11,000 in federal proceedings because the Slammer infection reduced security measures on its web site and compromised customer data.

In both cases, concluded the writers, much of the damage resulted from inadequate preparation for computer incident response.

*Category 4A8* *Liability*

2003-10-07 **Microsoft lawsuit security flaws software criminal network vandal**

NewsScan

MICROSOFT SUED FOR DAMAGES CAUSED BY SECURITY FLAWS
Film producer Marcy Levitas Hamilton, whose Social Security number was stolen by network vandals, has filed a lawsuit aimed at holding Microsoft responsible for damage stemming from security flaws in its software. The suit is designed to form the basis of a class action, and alleges that the majority of cyberattacks trace back to vulnerabilities in Microsoft software. Internet security and privacy consultant Richard M. Smith sasy: "This is the first time Microsoft has had its feet held to the fire on security issues." Hamilton's lawsuit notes that after the vandals stole her Social Security number, her bank accounts were accessed and frozen, and her attorney says: "They completely cannibalized her life." Microsoft executive Sean Sundwall responds: "This complaint misses the point. The problems caused by viruses and other security attacks are the result of criminal acts." (USA Today 7 Oct 2003)

# 4B1 Copyrights

*Category 4B1* *Copyrights*

2003-01-08 **copyright laws international variations**

NewsScan

EU COPYRIGHT LAWS SPAWN 'FREE-SWAPPING ZONE' FOR OLDIES
European and Canadian copyright protections for audio recordings last just 50 years, compared with 95 years in the U.S., a disparity that has spawned a boomlet in legitimate sales of golden oldies from 1950s artists, ranging from Miles Davis to Elvis Presley. The expiration of music copyrights overseas just adds one more piece to an antipiracy puzzle that is growing increasingly complex. "There are some implications for enforcement, creating an additional wrinkle," says Neil Turkewitz, executive VP for international affairs at the Recording Industry Association of America. "But it doesn't affect the legality of a U.S. user accessing a foreign hard drive and downloading a file." Record industry officials say they are keeping an eye out for the emergence of Web sites that offer archives of material that is in the public domain in a foreign country but still illegal to trade freely in the U.S. If a Web-based service comes online, it may be possible to block access to the site from the U.S. by going through ISPs, says Turkewitz. Trying to shut down peer-to-peer services would be more difficult, however, he acknowledges. That's part of the reason that the RIAA has been pressuring European policy-makers to extend their copyright protections to match those of the U.S., but so far those efforts have met with little success. (CNet News.com 7 Jan 2003)
http://news.com.com/2100-1023-979532.html

---

*Category 4B1* *Copyrights*

2003-01-14 **intellectual property copyright digital rights technology negotiation**

NewsScan

TECH FIRMS, HOLLYWOOD HEADED TO NEGOTIATING TABLE
About 20 lobbyists representing technology and entertainment companies are headed for a closed-door meeting today to try to hammer out some of their differences in the long-running squabble over digital copyright. Companies and trade associations represented at the meeting will include: Microsoft, Verizon, the Business Software Alliance, AOL Time Warner, the Motion Picture Association of America and the Fox Entertainment Group. "We're pleased that so many people who are important players in this debate are willing to sit down with us to discuss the consumer perspective on digital copyright," says Alan Davidson, deputy director of the Center for Democracy and Technology, which is sponsoring the series of meetings. "We don't know what the outcome will be, but we're hopeful that we can make progress in representing what has been an underrepresented voice — consumers." Political tension between the two groups has increased significantly in the last year, which has resulted in an impasse. (CNet News.com 21 Nov 2002)

MUSIC, TECH GROUPS REACH COMPROMISE ON COPYRIGHT ISSUES
The Recording Industry Association of America, the Business Software Alliance and the Computer Systems Policy Project have hammered out a compromise agreement that they say will protect copyrights on music and movies without the need for further government intervention. The pact is intended to head off efforts by Congress to legislate the inclusion of government-approved copy restriction technology in all new "digital media devices." This latest agreement, described by participants as a "landmark consensus," politically isolates the powerful Motion Picture Association of America, which was noticeably absent from the negotiations. MPAA has aggressively advocated new government requirements for built-in locking controls on new devices, such as DVD players. (AP 14 Jan 2003)

---

*Category 4B1* *Copyrights*

2003-01-23 **copyright law intellectual property fair use**

NewsScan

COPYRIGHT LAW IS A TWO-WAY STREET
Robin Gross, head of the new watchdog group IP Justice and former Electronic Frontier Foundation attorney, says copyright holders are taking unfair advantage of new technologies to restrict use of their content: "Sure, (digital technology) makes it easier for people to copy and share works, but digital technology also makes it easier for copyright holders to restrict what people can do with their works. So it's not fair to say that this technology is very harmful to these industries because it's actually providing them with more power than they've ever had before to control what people can do with their works. That point is often overlooked — that they're controlling it to the point that they're taking away from the public side of the copyright bargain. So while it's not fair for consumers to copy and distribute copyright works in a fashion that doesn't compensate the creators, it's also not fair for the creators to use digital technology to take away the rights of the public. For example, making sure these works fall into the public domain at some point, or making sure that consumers are able to exercise their fair-use rights. It's simply not fair for the copyright holders to take all of the rights and have none of the responsibilities associated with copyright law." (CNet News.com 23 Jan 2003)
http://news.com.com/2008-1082-981663.html

---

*Category 4B1* *Copyrights*

2003-01-24 **copyright intellectual property organization lobby battle**

NewsScan

HIGH-TECH GROUP BATTLES HOLLYWOOD ON COPYRIGHT ISSUES
The Alliance for Digital Progress (ADP) — a new Washington, D.C.-based lobbying group whose members include Microsoft, Dell, Motorola and the Information Technology Association of America (ITAA) — will fight Hollywood's positions on access to digital music, movies, and books, and the entertainment industry's efforts to require anti-copying technology in digital entertainment devices. ITAA president Harris N. Miller says sarcastically that Hollywood leaders "would have organized to burn down Gutenberg's printing press, if they were alive during that period of rapid change and innovation." (AP/USA Today 24 Jan 2003)

*Category 4B1* *Copyrights*

2003-02-03 **copyright intellectual property sanitizing censorship bowdlerizing video TV television lawsuits**

NewsScan

HOLLYWOOD THREATENED BY CONTENT-CLEANSING SOFTWARE
The entertainment industry is taking aim at new technology that has spawned a growing business dedicated to cleaning up movies and TV programs. On one side are a chain of video rental stores and a number of software companies that cater to an audience sick of gratuitous sex, violence and foul language in today's Hollywood offerings. On the other are film studios and the Directors Guild of America (DGA). The two groups are at legal loggerheads over software, such as MovieMask and ClearPlay, which filter out objectionable content, either by skipping certain frames entirely, or by substituting new dialogue, or in some cases by clothing naked actors or turning steel swords into light sabers. Last August, the owner of a Colorado "CleanFlicks" video store, which rents sanitized video tapes, fired the first volley by suing the DGA and asking a federal judge to declare the editing practices protected under federal copyright law. The following month, DGA filed a countersuit against CleanFlicks as well as the software companies that do the editing. Eight Hollywood studios have now joined DGA's fight, alleging that the companies violated trademark law when they rent or sell an altered movie in the original packaging. Meanwhile, moviemakers warn that the same software used to sanitize content could also be used to spice up G-rated fare. "It's a double-edged sword," says Jack Valenti, head of the Motion Picture Association of America. "If there are people who want to do it for benign reasons, that's one thing. But they can take 'Spider-Man' and make it into a pornographic movie, and that's a problem." A hearing on the CleanFlicks case is scheduled for Feb. 14. (AP 3 Feb 2003)
http://apnews.excite.com/article/20030203/D7OV77582.htm

*Category 4B1* *Copyrights*

2003-02-21 **copyright intellectual property music P2P peer-to-peer swapping piracy international court ruling**

NewsScan

MUSIC INDUSTRY THREATENED BY DUTCH RULING
A court ruling in the Netherlands last March appears to provide legal protection for businesses that enable peer-to-peer services, where users can swap copyrighted songs and movies for free. The Dutch decision is being appealed, but the ruling demonstrates the breadth of the challenge facing music companies and other owners of copyrighted works as more P2P providers move their operations overseas. Still, record-label officials maintain that the Netherlands ruling was an aberration that will be reversed in the appeals process, noting that courts in South Korea and Japan have ruled against P2P services in copyright cases. "We intend to enforce our rights not just in the United States, but worldwide," says Cary Sherman, president of the Recording Industry Association of America. Meanwhile, when U.S. courts side with the music industry, as in last month's federal ruling against Sharman Networks, which is based in Vanuatu and offers Kazaa file-swapping software, the question of enforcement looms large. "How are they going to enforce" the judgment, questions one of Sharman's lawyers. And even in the Netherlands case, a U.S. judgment isn't automatically enforced, says Tim Kuik, director of Brein, a Dutch foundation that deals with copyright enforcement, but would probably have to go through a separate Dutch court proceeding. (Wall Street Journal 21 Feb 2003)

*Category 4B1* *Copyrights*

2003-03-11 **intellectual property copyright copying consumer rights bill proposed legislation**

NewsScan

BILL AIMED TO PROTECT CONSUMERS' DIGITAL MEDIA RIGHTS
New legislation called the "Digital Choice and Freedom Act" is being introduced in Congress by Zoe Lofgren (D-Calif.) to ensure that consumers may legally copy CDs, DVDs, and other digital works for their personal use, just as they do now with TV shows and audio tapes. Paula Samuelson, a law professor at University of California-Berkeley's Boalt Hall, says: "Lofgren's bill aims to restore what Congress thought it was doing [when it passed the 1998 Digital Millennium Copyright Act] — preserving fair use for people who have lawful rights to use stuff. The Lofgren bill offers meaningful protections for a number of ordinary activities by consumers that should be lawful under copyright law but about which the law is presently ambiguous." (San Jose Mercury News 1 Oct 2002)

LEGISLATION TO ESTABLISH DIGITAL COPYING RIGHTS
Rep. Zoe Lofgren (D, CA) is reintroducing legislation called the Balance Act, intended to give people the right to make back-up copies of copyrighted digital works for use on other devices (such as car CD players) and to protect consumers who break technological locks in order to view DVD movies on their computers. Lofgren says, "Most people — at least, most adults — don't expect to get content as a freebie. But when people pay good money to buy something and then can't use it in the way they've become accustomed to, it makes them mad." The Motion Picture Association of America (MPAA) and the Business Software Alliance (BSA) strongly oppose the proposed legislation, which is thought to have just a long-shot chance of being passed. Arguing that such legislation "would provide safe harbor for pirates," Jack Valenti of the MPAA said, "As drafted, this legislation essentially legalizes hacking." (San Jose Mercury News 11 Mar 2003)

*Category 4B1* *Copyrights*

2003-03-27 **copyright Internet download peer-to-peer P2P issues PDF**

NewsScan

WHEN IS A FREE DOWNLOAD NOT?
It seemed like a good idea at the time — author Glen Fleishman reasoned that by offering his book, "Real World Adobe GoLive 6," as a free download, he might be able to kickstart sales, which were languishing. Rather than taking the time to download the 922 pages of the PDF file, maybe readers would decide to buy a hard copy on Amazon or elsewhere. It turns out that instead of the few hundred downloads that Fleishman was anticipating, the book was downloaded 10,000 times in just 36 hours, racking up a bandwidth bill of $15,000 (Fleishman's provider, Level 3, charges incrementally for bandwidth used). "It's a financial catastrophe. I'm a working stiff with a mortgage… I never suspected the penalty would be so high for giving something away… It's like living in Singapore and getting 15 years in jail for chewing gum… I was aware I would be charged a fortune for high bandwidth. But I never suspected we would have topped a few hundred downloads." Fleishman could have made use of file-sharing networks like Kazaa or Gnutella, which require users to bear the cost, says sci-fi author Cory Doctorow, who recently released his first novel, "Down and Out in the Magic Kingdom," as a free download. Alternatively, Fleishman could have released the book under an open Creative Commons license, which would have allowed it to be posted to the Internet Archive and other open content Web sites, says Doctorow. "It doesn't make any sense to be the sole point of distribution for a file like this. It highlights the design flaw in the client-server Internet. The more popular a file becomes, the more of a penalty people pay to get it. I think the lesson is 'Use P2P networks.'" (Wired.com 27 Mar 2003)

*Category 4B1* *Copyrights*

2003-03-27 **music webcasting copyright issues reform held**

NewsScan

PANEL PUTS WEBCAST ROYALTIES REFORM ON HOLD
A House subcommittee has indefinitely postponed deliberation of a new bill, titled the Copyright Royalty and Distribution Act, which calls for the Library of Congress to hire a full-time judge to settle disputes over "reasonable" copyright royalty fees for webcasts. The measure, sponsored by Reps. Lamar Smith (R-Texas) and Howard Berman (D-Calif.), had been expected to receive a favorable reception at today's hearing. Fees for streaming music via the Internet have been a bone of contention since the enactment of a 1998 copyright law in which Congress required webcasters to pay record labels and artists a royalty fee for playing their music online. Under the Smith and Berman bill, the appointed judge would be required to consider a "fair income" for the copyright holder and could adjust rates for inflation. (CNet News.com 27 Mar 2003)

*Category 4B1* *Copyrights*

2003-05-14 **dvd copying court District Court 321 studios Digital Millennium Copyright Act's anti-circumvention**

NewsScan

BATTLE OVER DVD-COPYING HEADS TO COURT
U.S. District Court Judge Susan Ilston in San Francisco will be overseeing a case that analysts say will have important ramifications not only for software developers and the movie industry, but also for consumers who want to make back-ups of the DVDs they buy. Seven major movie studios have filed suit against software startup 321 Studios, seeking to prohibit it from shipping its DVD X-Copy and DVD Copy Plus software programs. The lawsuit invokes the 1998 Digital Millennium Copyright Act's "anti-circumvention" provision, which bans the sale of products that can "get around" copyright protection measures. Legal experts say this case is of particular interest because Judge Ilston is being asked to clarify whether the law prevents all circumvention, or whether there are cases in which circumvention is legal. "That's a big open issue that this will help define," says an intellectual property lawyer, who adds, "This is one of the first tough cases" to address this issue. Courts in the past have allowed copyright exemptions for personal use, such as using a VCR to record a TV show for later viewing, but up until now those exemptions have not extended to digital media. "The court is going to have to come up with a new, nuanced interpretation of the statute," says 321 attorney Daralyn Durie. "What's at stake here is the ability to engage in fair use in a digital environment." (CNet News.com 14 May 2003)

---

*Category 4B1* *Copyrights*

2003-06-10 **copyright TV digital lawtechnology electronics**

NewsScan

LEGISLATOR URGES FAIR USE RIGHTS FOR DIGITAL TV
U.S. Rep. Lamar Smith (R-Texas), chairman of the House subcommittee overseeing copyright law, urged the Federal Communications Commission to ensure that future regulations involving digital TV do not "have an adverse effect on how consumers may legitimately use lawfully acquired entertainment products." Smith voiced his firm opposition to legislation introduced last year that would require consumer electronics makers to implant mandatory copy-protection technology in PCs and other devices. "I am skeptical of government mandates on the technology industry… Until evidence shows otherwise, I believe existing copyright law is adequate," said Smith. He also urged greater cooperation on the part of colleges and universities in disciplining perpetrators of peer-to-peer music piracy, noting that research shows 16% of files available on Kazaa are located on their networks. "It's unlikely that this amount of file-sharing activity is in furtherance of class assignments," he said. (CNet News.com 10 Jun 2003)

---

*Category 4B1* *Copyrights*

2003-06-18 **machines copyright destroying computers music**

NewsScan

MACHINES OF COPYRIGHT VIOLATORS MAY NEED TO BE ZAPPED
Senator Orrin Hatch (R, UT) — who, besides being Chairman of the Senate Judiciary Committee, is a composer whose royalties were $18,000 last year from songs he's written — says that maybe people who keep abusing copyright laws should get their computers destroyed. That kind of action "may be the only way you can teach somebody about copyrights. If we can find some way to do this without destroying their machines, we'd be interested in hearing about that. If that's the only way, then I'm all for destroying their machines... There's no excuse for anyone violating copyright laws." (AP/San Jose Mercury News 18 Jun 2003)

---

*Category 4B1* *Copyrights*

2003-07-09 **Google search engine caching copyright intellectual property concern**

NewsScan

GOOGLE CACHING FEATURE SPARKS COPYRIGHT CONCERNS
A caching feature on the Google search site sometimes enables users to call up snapshots of archived Web pages that for whatever reason are either restricted or no longer available at the original source, such as newspaper articles that require user registration to access or those that "expire" after a certain number of days. The feature has raised the ire of some publishers. "We are working with Google to fix that problem — we're going to close it so when you click on a link it will take you to a registration page," says a New York Times Digital spokeswoman. "We have established these archived links and want to maintain consistency across all these access points." Google says its caching feature benefits Web surfers trying to access a site that's experiencing technical difficulties, but some copyright experts say they expect the issue will end up in court: "Many of us copyright lawyers have been waiting for this issue to come up: Google is making copies of all the Web sites they index and they're not asking permission. From a strict copyright standpoint, it violates copyright," says Electronic Frontier Foundation attorney Fred Lohman. Most search engines make a statistical record of a Web page when they "spider" it, or use "robots" to scan the page's content for meaning or context, but Google goes one step beyond by snapping a digital picture of pages and making them available to users. The picture exists on Google's site until the next time it crawls that particular page, whether it's a few days or six weeks or more. Web sites can block the caching feature, but some publishers are reluctant to do so because they fear losing favor in the company's powerful search rankings, even though Google has assured them the "no cache" tags do not affect search results. (CNet News.com 9 Jul 2003)

*Category 4B1* *Copyrights*

2003-07-22 **intellectual property copyright infringement theft AOL**

NewsScan

HARLAN ELLISON, CUDGEL IN HAND AGAINST COPYRIGHT THIEVES
Well-known science fiction writer Harlan Ellison is suing America Online for copyright infringement because it didn't respond quickly enough to delete from its Web site a fan's posting of some of Ellison's stories, without permission, on an AOL online forum. America Online says it removed the stories as soon as it was aware of them. Ellison has always been a fierce protector of copyright protections, and now says: "People like AOL have turned this nation and its kids into a nation of thieves, who have no more notion of what's right than the man on the moon. I really see myself as standing there on the g-d- barricade, with a cudgel in my hand.... We are up against inimical forces. We are up against city hall." Ellison's lawsuit, to be heard by the Ninth U.S. Circuit Court of Appeals, is being supported by a number of major software firms and record labels. (Wall Street Journal 22 Jul 2003)

*Category 4B1* *Copyrights*

2003-07-24 **download movies legal Disney intellectual property**

NewsScan

MOVIELINK AND DISNEY SIGN MOVIE DOWNLOAD DEAL
Dozens of Disney films are going to be made available for downloading from the Internet through a licensing deal just reached between Disney and online movie service Movielink. With this new agreement in place, Movielink will have access to film titles from all the major studios except Twentieth Century Fox, and will have a library of about 400 digitized films. Movies from Walt Disney Pictures, Touchstone, Miramax and Dimension will be available through the service, and among the first releases will be "Gangs of New York," "The Recruit" and "The Jungle Book 2." Disney will set the retail price for the movie downloads (typically ranging between $2.95 and $4.99), and the downloaded movies will be viewable either on a PC or on a TV connected to a computer. (AP/USA Today 24 Jul 2003)

*Category 4B1* *Copyrights*

2003-07-31 **copyright intellectual property RIAA Pacific Bell DMCA privacy constitution**

NewsScan

SBC'S PAC BELL JOINS LEGAL BATTLE AGAINST RIAA
SBC Communications' Pacific Bell Internet Services unit has filed a complaint against the Recording Industry Association of America, alleging that many of the subpoenas recently served against online music swappers were done so improperly. Pac Bell contends that more than 200 subpoenas seeking file-sharers' e-mail addresses were issued from the wrong jurisdiction, and also states that the RIAA's demand for information on multiple file-sharers cannot be grouped under one subpoena. An SBC spokesman added that the RIAA's use of a provision in the Digital Millennium Copyright Act to force ISPs to reveal information on their subscribers interferes with customer privacy: "The action taken by SBC Internet Services is intended to protect the privacy of our customers. Misapplication of DMCA subpoena power raises serious constitutional questions that need to be decided by the courts, not by private companies who operate without duty of due diligence or judicial oversight." (AP 31 Jul 2003)

*Category 4B1* *Copyrights*

2003-08-28 **intellectual property copyright RIAA webcaster lawsuit**

NewsScan

WEBCASTER ALLIANCE THREATENS RIAA WITH ANTITRUST SUIT
Angry over a new music royalty rate structure it says may force nine out ten small Internet radio stations to shut down, the 300-member Webcaster Alliance of small stations is threatening an antitrust lawsuit against the Recording Industry Association of America. The Librarian of Congress worked out a compromise fee-structure last year between the music industry and Internet radio station operators, but small stations continue to argue that they're being asked to pay too much for the right to play music. The RIAA has not yet commented officially on the newly threatened lawsuit, but a spokesman says: "We have worked diligently to negotiate fair agreements that offer a broad and flexible array of rates and terms to large, small, and non-commercial webcasters." (Washington Post 9 Jul 2003)

WEBCASTERS SUE RIAA
Webcaster Alliance, an organization of 400 music broadcasters, has filed a federal lawsuit charging that the major music labels and the Recording Industry Association of America (RIAA) are monopolists who violated federal antitrust laws when they went about setting music royalty rates for the Internet. The webcasters seek an injunction to prevent the major labels from enforcing their intellectual property rights and collecting royalty payments. The RIAA calls the suit a publicity stunt without merit." (AP/USA Today 28 Aug 2003)

---

*Category 4B1* *Copyrights*

2003-09-03 **apple itunes consumer reselling music files cds digital copyrights pre-owned digital tune**

NewsScan

'PRE-OWNED' DIGITAL TUNE HITS AUCTION BLOCK
George Hotelling is pushing the envelope in digital music with his attempt to auction off a song that he purchased on Apple's iTunes Music Store. Hotelling says he's not concerned about recouping his 99-cent investment in Devin Vasquez's rendition of "Double-Dutch Bus," but he's interested in probing the murky legal ground surrounding digital copyrights. "I'd just like to know that if I buy something, whether it's physical or intellectual property, that I'll have my right of 'First Sale,'" says Hotelling. The terms of service contract that accompanies iTunes songs doesn't say much about the rules that guide resale of songs but does stipulate that the songs are only for "personal, noncommercial use." One nagging question concerns the lack of legal guidelines governing the rights of an owner of a second-hand digital song, says Fred von Lohmann, senior staff attorney at the Electronic Frontier Foundation. "If you were to win that auction and get that song, you have no relationship with Apple. You didn't agree to the terms of service. What governs that song after you've repurchased it?" (CNet News.com 3 Sep 2003)

---

*Category 4B1* *Copyrights*

2003-09-08 **pop-ups ads copyright violation gator whenu.com screen savers web surfing habits**

NewsScan

JUDGE SAYS POP-UP ADS DON'T VIOLATE COPYRIGHTS
A federal judge in Virginia has ruled that pop-up ads for rival companies' products that obscure the original Web site's offerings do not violate trademark or copyright laws, potentially giving a green light to more aggressive online advertising tactics. The pop-ups — distributed mainly by Gator and WhenU.com — often divert online shoppers to competitors' offers, an action that infuriates Web site operators. According to Judge Gerald Bruce Lee's reasoning, however, consumers have accepted these ads when they agree to download Gator's and WhenU's free programs, such as screen savers or games, which piggyback on software that tracks users' Web surfing habits and then delivers ads based on their apparent interests. In the case brought by U-Haul International, Lee ruled that when WhenU's software delivers a competitor's ad to a Web surfer perusing U-Haul's Web site, it doesn't "copy or use U-Haul's trademark or copyright material" and therefore can't be accused of infringing on them. "Computer users, like this trial judge, may wonder what we have done to warrant the seizure of our computer screens by pop-up advertisements for secret Web cameras, insurance, travel values and fad diets," the judge wrote. But he argued that people "invited" those ads when they downloaded the free software, and that "(u)ltimately, it is the computer user who controls how windows are displayed on the computer desktop." The legal battle isn't over however — U-Haul lawyers are contemplating an appeal, and similar suits have been filed by several Web-site operators, including Hertz Corp. (Wall Street Journal 8 Sep 2003

---

*Category 4B1* *Copyrights*

2003-09-10 **RIAA file sharing music 12-year-old lawsuits against song-sharing**

NewsScan

FILE-SHARING COMPANIES PAY FOR GIRL'S MUSIC SETTLEMENT
A coalition of companies that run Internet song-sharing services have offered to pay the $2,000 settlement a mother agreed to pay the Recording Industry Association of America (RIAA) after it lodged lawsuits against her 12-year-old daughter (and 260 other defendants) for music copyright infringement. Wayne Rosso, president of the Internet file-sharing service Grokster charges: "These people give Joe Stalin a good name." And the group's executive director, Adam Eisgrau, adds: "We don't condone copyright infringement, but it's time for the RIAA's winged monkeys to fly back to the castle and leave the Munchkins alone." Before it filed the lawsuits, the RIAA was dismissive of predictions that "the recording industry's aggressive legal strategy might result in a consumer backlash." (Washington Post 10 Sep 2003)

*Category 4B1* *Copyrights*

2003-09-26 **California RIAA Gray Davis governor film music theft business loss money piracy**

NewsScan

NEW CALIFORNIA LEGISLATION FRIENDLY TO ENTERTAINMENT INDUSTRY
California Gov. Gray Davis says he will sign new legislation that is friendly to the entertainment industry and aimed at stopping the theft of film and music. Cary Sherman, president of the Recording Industry Association of America (RIAA), is pleased with the legislation: "The piracy problem is severe and we're seeing it in terms of layoffs. We are really grateful for anything that can be done to deal with this problem... Thousands of people in the recording industry have lost their jobs, artists are having trouble being signed ... retailers are going out of business." (AP/San Jose Mercury News 26 Sep 2003)

*Category 4B1* *Copyrights*

2003-10-03 **file-sharing copyright infringement peer-to-peer fines reduced**

NewsScan

SENATOR SEEKS TO REDUCE FILE-SHARING FINES
Senator Norm Coleman (R-Minn.) says the penalties currently on the books for downloading copyrighted music are too stiff and he will sponsor legislation to reduce them. "I can tell you that $150,000 per song is not reasonable, and that's technically what you can put in front of somebody. That forces people to settle when they may want to fight, but they're thinking, 'goodness, gracious, what am I going to face?'" Coleman says he will also push for changes in the 1998 Digital Millennium Copyright Act that would restrict the recording industry's subpoena power, instituting a judicial review process which currently is unnecessary. Coleman's recommendations come as a followup to a high-profile congressional hearing on the subject that included representatives of the recording and file-sharing industries as well as rappers LL Cool J and Chuck D. (AP 3 Oct 2003)

*Category 4B1* *Copyrights*

2003-10-07 **intellectual property copyrights digital DRM CD copy-protection disable Princeton**

NewsScan

DISABLING CD LOCK IS EASY AS PRESSING THE SHIFT KEY
A Princeton University student has posted instructions for disabling the copy-protection "lock" incorporated into the latest CD released by soul artist Anthony Hamilton on the BMG label. The anti-copying software, developed by SunnComm Technologies, is automatically loaded onto a Windows PC whenever the Hamilton CD is played in its CD drive, but graduate student John Halderman found that he could prevent the software from being loaded simply by holding down the shift key for awhile. The discovery was confirmed by BMG and SunnComm, but they downplayed its significance. "This is something we were aware of," said a BMG spokesman. "Copy management is intended as a speed bump, intended to thwart the casual listener from mass burning and uploading. We made a conscious decision to err on the side of playability and flexibility." SunnComm's technology is one of the most flexible on the market, and includes "pre-ripped" versions of songs on the CD, which buyers are free to transfer to a computer, burn to a CD several times, or transfer to a variety of portable devices. The Anthony Hamilton CD is the first release to come with these "second session" tracks designed for use on a computer, but holding down the shift key prevents access to that feature. (CNet News.com 7 Oct 2003)

*Category 4B1* *Copyrights*

2003-10-24 **Amazon search inside book feature intellectual property book page**

NewsScan

AMAZON'S NEW 'SEARCH INSIDE THE BOOK' FEATURE
Amazon.com has announced a new feature called "Search Inside the Book" that is making the text of 120,000 books (more than 33 million pages) fully searchable at no charge. The feature makes it possible to scan a database for the word or phrase entered by a visitor to Amazon's site for each relevant portion of a searchable book. The pages that are found can be read onscreen and printed but not copied or downloaded. University of Washington computer scientist Oren Etzioni says: "It's an impressive feat — a bold concept, coupled with nice execution and clear business thinking. This really shows Amazon is a technology company, not innovating just with things like free shipping but putting something out there that's brand new."(Seattle Post-Intelligencer 24 Oct 2003)

*Category 4B1* *Copyrights*

2003-10-27 **MIT LAMP analog transmission music library**

NewsScan

EXTENDING THE MUSIC LIBRARY
Two students at MIT have developed an electronic music library that allows anyone on campus to access 3,500 CDs. Called the Library Access to Music Project (LAMP), the system lets a student go to its Web site to select a CD and have it delivered through the campus closed-circuit cable TV to the student's dorm room or other campus site. One of the students who conceived of LAMP explains: "We had a library in school that closed at 7 p.m. The school had this great music in the library, but you couldn't get there. I was thinking, how could we get students better access to this library?" In 2001, the two creators of LAMP received a grant from iCampus, a Microsoft-backed alliance with MIT. (San Jose Mercury News 27 Oct 2003)

*Category 4B1* *Copyrights*

2003-10-27 **MIT file-swap copyright infringement workaround analog transmission music**

NewsScan

STUDENTS CREATE A FILE-SWAP WORK-AROUND
Two students at MIT have discovered a way to give their fellow attendees free dorm-room access to a library of 3,500 CDs without breaking copyright laws. Keith Winstein and Josh Mandel developed software that routes the tunes over the school's cable TV network, making it an analog transmission. Unlike digital copies swapped over the Internet, analog transmissions are not exact copies, which makes the likelihood of prosecution much more remote since most universities already have licenses to "perform" analog music. "I think it's fascinating. As a copyright lawyer, I think they've managed to thread the needle," says Electronic Frontier Foundation legal counsel Fred Von Lohmann. "They've basically managed to cut the record labels out of the equation altogether." The students managed to circumvent the Recording Industry Association of America completely by purchasing MP3 versions of the CDs from Seattle-based Loudeye under license from the National Music Publishers Association. "The students get access to a broad array of music, and the copyright owners get paid. This is where we should all be heading. I hope the record industry takes not and realizes this is a whole lot more promising than suing people," says Von Lohmann. (AP 27 Oct 2003)

*Category 4B1* *Copyrights*

2003-10-30 **copyright law Library Congress DMCA Digital Millenium Copyright Act**

NewsScan

COPYRIGHT LAW EXEMPTIONS NIXED
The Librarian of Congress has rejected requests for exemptions to a provision in the 1998 Digital Millennium Copyright Act that forbids "circumventing" the electronic locks on copyrighted works, including making backup copies and other personal uses of digital movies, games and music owned by consumers. However, exemptions were granted for software programs and video games locked to obsolete media or equipment, and cases of electronic books whose digital rights management software would prevent them from being translated into audio or other formats for the visually impaired. (Los Angeles Times 30 Oct 2003)

*Category 4B1* *Copyrights*

2003-10-31 **amazon book inside search security property rights copying abuse user**

NewsScan

AMAZON TURNS OVER A NEW LEAF ON BOOK SEARCHES
Amazon says its new "Search Inside the Book" feature does not allow users to print pages from within books, allaying authors' fears that unscrupulous readers might use it to print out recipes, hotel recommendations or other such reference material. Amazon VP Steve Kessel refused to confirm that Amazon had changed the feature to prevent such abuses, citing security concerns, but acknowledged that 15 authors had requested their books to be removed from the Search the Book database. Up until Friday, according to Authors Guild executive director Paul Aiken, the Search Inside the Book tool allows users to search the complete text of a book for words or phrases and print out pages where the phrases appeared. That feature appears to be disabled, said Aiken, who praised the feature but said "we just think it needs a little work." (AP 31 Oct 2003)

*Category 4B1* *Copyrights*

2003-11-04 **anti-piracy digital broadcast flag stop copying hard drive internet information**

NewsScan

DIGITAL ANTI-PIRACY MEASURE
In a 5-0 vote, the Federal Communications Commission has approved a requirement that some personal computers and other consumer electronic devices be equipped with technology to help block Internet piracy of digital entertainment. The movie industry is happy with the FCC's decision, but consumer advocates are worrying that the move will force people to buy new equipment, will result in new regulation of how computers are designed, and will hinder the copying of programming that's not entitled to industry protection (e.g., shows no longer covered by copyright). Under the new rules, a piece of digital code known as a "broadcast flag" could be embedded into a piece of program content, which then could only be copied by a digital recording device equipped with technology that recognizes the flag. A computer could not copy the file to its hard drive or send it over the Internet. (Washington Post 4 Nov 2003)

*Category 4B1* *Copyrights*

2003-12-23 **unix battle linus torvalds linux code SCO Darl McBride Novell**

NewsScan

UNIX COPYRIGHT BATTLE HEATS UP
Novell has thrown a monkey wrench into SCO Group's plan to extract hundreds of millions of dollars in licensing fees and damages from IBM and other companies using the Linux operating system, which SCO says violates its copyright and license because it includes some Unix code. In the past few months, Novell has quietly registered for the copyrights on many of the Unix versions claimed by SCO, which says it acquired them through a transfer from Novell back in 1995. SCO has reacted with outrage, calling Novell's recent move a backdoor attempt to reclaim code that is rightfully SCO's. "We see this as a fraudulent attempt by Novell to get something they don't have," says SCO president and chief executive Darl C. McBride, who added that Novell's actions were probably prompted by IBM, the lead Linux seller in the corporate market. "It's not just Novell. It's an attack by IBM." Meanwhile, Novell executives maintain they have full ownership of the copyrights in question: "Novell believes it owns the copyrights in Unix, and has applied for and received copyright registrations pertaining to Unix consistent with that position. SCO has been well aware that Novell continues to assert ownership of the Unix copyrights," said the company in a statement. (New York Times 23 Dec 2003)

*Category 4B1* *Copyrights*

2003-12-24 **SCO Linus Torvalds Linux intellectual property rights code unix**

NewsScan

SCO OR LINUS? WHO'S RIGHT?
The Utah-based SCO Group, which owns the rights to the Unix operating system, claims that Linux creator Linus Torvalds violated its intellectual property rights. To buttress its case, SCO provided the court a list of Linux files that "have been copied verbatim from our copyrighted Unix code and contributed to Linux." But Torvalds, who created the kernel of Linux while still a student in Finland, said in a message to a reporter that he wrote the code in those files all by himself and now feels "a bit ashamed" because some of the program macros he wrote are "so horribly ugly that I wouldn't admit to writing them if it wasn't because somebody else claimed to have done so ;). I can show, and SCO should have been able to see, that the list they show clearly shows original work, not copied." But SCO chief executive Darl C. McBride insists: "As a social revolutionary, Linus Torvalds is a genius. But at the speed the Linux project has gone forward something gets lost along the way in terms of care with intellectual property." (New York Times 24 Dec 2003)

# 4B2 Patents

*Category 4B2* *Patents*

2003-01-23 **patent Web frame interface licensing**

NewsScan

SBC CLAIMS PATENT ON WEB INTERFACE
SBC Communications is enforcing its patents on what it claims is any use of frame-like user interfaces in Web sites. According to SBC's interpretation of its "Structured Document Browser" patents, hundreds of thousands of Web sites, including that of the U.S. Patent and Trademark Office, could be infringing on the telecom's intellectual property. "SBC Intellectual Property currently is working with several commercial Web site owners regarding patent licensing agreements related to specific techniques for enabling consistent navigation features from different pages of a Web site," SBC announced in a statement yesterday. At issue are Web sites that use an interface that remains on-screen while a user navigates the site. SBC so far has contacted only a few sites with requests for licensing fees, with suggested amounts ranging between $527 and $16.6 million per year, depending on the annual revenue of the company and what kind of license they sign up for. (The Register 23 Jan 2003)
http://www.theregister.co.uk/content/6/28985.html

---

*Category 4B2* *Patents*

2003-02-06 **patent law streaming audio Web**

NewsScan

STREAMING PATENT HAS NET RADIO SITES STEAMED
A company that says it owns patents on the process of transmitting compressed audio or video online is flexing its muscle, demanding fees from a host of Internet multimedia companies. Acacia Media Technologies says its patents may even cover pay-per-view movies on cable TV and in hotel rooms. And while Acacia's move has outraged Internet entrepreneurs, many of them are reluctantly forking over the fees. "We did research on the claims and found that they were pretty clear — somewhat broad, but specific enough to cover us," says Zack Zalon, general manager of the Radio Free Virgin Web site. "We realized that they were tight enough that a license would be substantially less expensive in the long run than litigation." Meanwhile, the trend toward companies exercising ownership over what generally are viewed as overly broad patents has drawn the ire of many experts, but analysts admit it's a strategy that's likely to increase in popularity. "With the economy the way it is, you see a lot more people trying to leverage their intellectual property. It's one of the few ways left that people can actually make money," says Rich Belgard, an independent patent consultant. (CNet News.com 6 Feb 2003)
http://news.com.com/2100-1023-983552.html

---

*Category 4B2* *Patents*

2003-02-20 **patent dispute lawsuit I&A identification authentication PKC public key cryptosystem PKI infrastructure**

NewsScan

PATENT DISPUTE ON AUTHENTICATION SOFTWARE
Inventor and retired electronics engineer Leon Stambler is suing VeriSign, RSA Security, and other companies for allegedly violating his patents on software used in electronic transactions to let one party be certain of another's true identity. Although Internet security experts generally believe that the inventor's patents merely imitate work previously done by Stanford and MIT cryptographers during the 1970s and 1980s, intellectual property lawyers predict that the retired engineer's effort may very well be successful. Attorney Jack Russo says: "Patent litigation is fairly expensive and you will see people settle for what seems to be large sums." (New York Times 20 Feb 2003)

---

*Category 4B2 Patents*

2003-02-25 **patent law overly broad software**

NewsScan

U.S. PATENT SYSTEM IS BROKEN, SAYS LESSIG
Stanford law professor Lawrence Lessig has warned Europeans not to follow the same path toward software patent protection as the U.S., saying "The system in America is broken — to the great detriment of software developers generally — and there is no reason to believe the Europeans could do any better." Critiquing the last 10 years' tendency toward granting overly broad patents, he notes that software developers — those whom patents ostensibly would protect — are actually some of the most vocal critics of the current system. "Developing software is [now] like crossing a minefield," says Richard Stallman, the originator of the free software movement that has developed the GNU/Linux operating system. "With each design decision, you might step on a patent that will blow up your project." Lessig says that Europeans should take pains to avoid a similar quagmire: "American software developers will continue to choke on software patents, especially as more and more get enforced in massively expensive litigation? Until software patents prove themselves safe and effective, Europe could gain a great deal by sparing its developers the same drug. Rather than copying a failed American policy, the Europeans could be exploring alternatives to patents that might provide protection without sinking the intended beneficiaries. No doctor would approve an untested drug for his or her patient. Nor should Europe inflict such a remedy on its already weakened software industry." (Financial Times 20 Feb 2003)

*Category 4B2 Patents*

2003-04-10 **video on demand patent infringement lawsuit movie studios**

NewsScan

MOVIELINK SLAPPED WITH PATENT INFRINGEMENT LAWSUIT
Movielink, a joint venture involving five Hollywood studios, has been sued for patent infringement by USA Video Technology in a case that could have an impact on other future video-on-demand endeavors. The USA Video lawsuit alleges that Movielink, which sells digital copies of films for downloading from the Internet, violates a patent called "Store and Forward System" that was awarded in July 1992. The patent broadly covers a method for Internet users to request and receive "a digitized video program for storage and viewing," according to the complaint. The plaintiff's attorney says the resolution of the case could affect many other VOD offerings. "This case is ripe now because the content is available and the legal landscape permits (an online movie rental service)," says Erik B. Cherdak, plaintiff attorney for the case. "The reality is this case has far-reaching effects on whether the corner video store will remain as a going concern in the future." Movielink, which launched last November, is a partnership of MGM, Paramount Pictures, Warner Brothers, Sony Pictures Entertainment and Universal Pictures. (CNet News.com 10 Apr 2003)

*Category 4B2 Patents*

2003-04-24 **intellectual property rights eBay patent violation defense**

NewsScan

EBAY DEFENDS ITSELF AGAINST PATENT-VIOLATION CHARGES
Online auction eBay is involved now in patent litigation involving in claims by MercExchange LLC that eBay stole from MercExchange founder Thomas G. Woolston his ideas for the programs and processes now used by eBay in the auctions it conducts on the Internet. Attorneys for eBay say the patent-violation charges are baseless. The judge presiding over the trial (estimated to last about three weeks) cautioned the two sides in the dispute: "It's going to be your responsibility to make sure this is something the average person can understand." (AP/San Jose Mercury News 24 Apr 2003)

*Category 4B2 Patents*

2003-04-27 **trade secret law violation University Chicago student**

NewsScan

STUDENT CONFESSES TO VIOLATION OF TRADE SECRET LAW
University of Chicago student Igor Serebreyany is pleading guilty to charges of putting secret documents about DirecTV's anti-piracy technology on the Internet, in violation of the federal Economic Espionage Act of 1996, which prohibits anyone from disclosing trade secrets for economic benefit. He theoretically faces penalties of up to 10 years in prison and a $250,000 fine, but has negotiated a deal under which his prison sentence would be no more than one year. The documents described details about the design and architecture of DirectTV cards. (AP/ContraCostaTimes 27 Apr 2003)

*Category 4B2* *Patents*

2003-05-14 **SCO intellectual property infringement linux unix open software**

NewsScan

LINUX USERS WARNED OF INTELLECTUAL PROPERTY INFRINGEMENT
The SCO Group, which acquired control of Unix intellectual property from Novell after it bought the rights from AT&T back in 1992, has sent letters to Linux customers warning that commercial users may face legal liability for using Linux with a license from SCO. If SCO's tactic is successful, it could undermine one of the basic tenets of the open software movement, of which Linux has been the most successful example. Linux is a Unix derivative first developed in the 1990s, and has won a loyal following because of its low cost, reliability and ability to run on inexpensive computer hardware. Linux developer Linus Torvalds says he has not heard what parts of Linux might be infringing: "I'd dearly love to hear exactly *what* they think is infringing, but they haven't told anybody. Oh well. They seem to be more interested in FUD [fear, uncertainty and doubt] than anything else." The latest move follows a $1-billion lawsuit filed by SCO in March against IBM, alleging IBM took parts of the Unix code and transferred them to Linux. IBM dismissed the lawsuit as unfounded. (AP 14 May 2003)

---

*Category 4B2* *Patents*

2003-05-19 **Unix license Microsoft SCO Group part of code duplicative Darl McBride**

NewsScan

MICROSOFT SCOOPS UP UNIX LICENSE FROM SCO
Microsoft is buying the rights to SCO Group's Unix technology for an undisclosed amount, in a move that will bolster SCO's controversial campaign to demand royalties from users of the Linux operating software, which SCO claims infringes on its Unix patents. Linux supporters have demanded that SCO identify which parts of the code are duplicative, but SCO says that doing that would allow programmers to cover up their transgressions by rewriting the software. "That's like saying, 'show us the fingerprints on the gun so you can rub them off,'" says SCO CEO Darl McBride. Microsoft, which competes fiercely with both Linux and Unix, at the same time has been a long-time backer of SCO and some in the Linux community have speculated the software giant is secretly bankrolling SCO's litigation to reduce the Linux threat. A Microsoft spokeswoman denied that rumor. (Wall Street Journal 19 May 2003)

---

*Category 4B2* *Patents*

2003-05-21 **patent W3C World Wide Web Consortium Patent Policy Working Group Daniel Weitzner**

NewsScan

W3C ADOPTS POLICY ON PATENTS
The World Wide Web Consortium (W3C) has approved a policy on patents that requires all those who participate in the development of a W3C recommendation must license essential claims on a royalty-free basis. It also requires W3C members to make disclosures on patents they own and requests that anyone else who sees technical drafts share their knowledge of patents which may be essential. At the same time, the policy suggests a process for handling unexpected patent claims that are inconsistent with the terms of the W3C Patent Policy. In that instance, the W3C will convene a Patent Advisory Group, which may then recommend: a legal analysis of the patent, the removal of the patented feature, or cessation of work in that area altogether. The W3C's efforts to create a patent policy have been contentious since it first released its Patent Policy Framework Draft in 2001, says Daniel Weitzner, chair of the Patent Policy Working Group, who cautioned technology companies against trying to exploit the patent exception process. "Anyone who thinks that's going to be an easy way to squeeze fees out of Web standards I think is mistaken," says Weitzner. (Internet News 21 May 2003)

---

*Category 4B2* *Patents*

2003-05-28 **software group linux SCO threatned proof of intellectual property rights**

NewsScan

GERMAN SOFTWARE GROUP THREATENS SCO OVER LINUX
German software alliance Linuxtag, which backs the Linux operating system, has issued an ultimatum to SCO Group: prove your claims that Linux infringes on your Unix technology patents by May 30 or we'll see you in court. "SCO is massively unsettling our members and the companies that are potential exhibitors at the fair with those claims," says a Linuxtag spokesman. "It they don't stop that, or present proof for the intellectual property rights they are claiming, we are going to apply for a preliminary injunction at the court on Friday." SCO's German unit says it's received Linuxtag's motion and is considering whether to respond before SCO's case against IBM, a major Linux promoter, goes to court. Some of Germany's largest companies, including Siemens AG, the Deutsche Bundesbahn and Volkswagen, have received letter from SCO notifying them their use of Linux may be in violation of its rights. (Reuters 28 May 2003)

---

*Category 4B2* *Patents*

2003-05-28 **ebay patent MercExchange Buy it Now section half.com purchase auctions**

NewsScan

EBAY LOSES PATENT-INFRINGEMENT LAWSUIT
A federal jury in Virginia has concluded that online auction eBay and its Half.com unit intentionally infringed on patents belonging to MercExchange. MercExchange is also seeking an injunction prohibiting eBay from continuing its current "Buy it now" program, which allows eBay customers to make fixed-priced purchases rather than participating in auctions. EBay is asking the judge to reverse the $35-million judgment against it, whereas MercExchange is saying that the judgment should be tripled, because the jury's verdict was that the patent infringement was deliberate rather than accidental. (Bloomberg/New York Times 28 May 2003)

*Category 4B2* *Patents*

2003-08-25 **intellectual propery copyright DVD copy-protection California**

NewsScan

FREE SPEECH TRUMPED BY TRADE SECRETS
The California Supreme Court has ruled Monday that courts may block Internet users from posting computer code that could be used to illegally copy DVD movies if the code revealed legitimate trade secrets online. Justice Janice Rogers Brown, in reversing a lower court ruling on a 7-0 vote, said the California Supreme Court's action "does not violate the free speech clauses of the United States and California constitutions." Companies such as Boeing, Ford and AOL Time Warner filed briefs urging the justices to side with the plaintiff, which had argued that trade secret protections trump First Amendment speech protections. (AP/San Jose Mercury News 25 Aug 2003)

*Category 4B2* *Patents*

2003-10-29 **patent Microsoft W3C Tim Berners-Lee**

NewsScan

BERNERS-LEE SIDES WITH MICROSOFT IN PATENT CASE
The World Wide Web Consortium (W3C) has come out on Microsoft's side in a patent-infringement lawsuit the company has on appeal. A lower court awarded $521 million to a researcher who holds a patent the Web consortium contends is based on "prior art" that was not considered when the patent was granted (nor was it considered in the Microsoft trial). W3C director Tim Berners-Lee has asked that the U.S. the patent office begin a review of the patent "to prevent substantial economic and technical damage to the operation of the World Wide Web."(New York Times 29 Oct 2003)

*Category 4B2* *Patents*

2003-11-12 **patent office University Califronia web pages tim berners-lee microsoft interactive programs internet explorer**

NewsScan

PATENT OFFICE RECONSIDERS CONTROVERSIAL NET PATENT
The U.S. Patent and Trademark Office is taking the unusual step of reconsidering a patent awarded to three University of California researchers in 1998. Patent No. 5,838,906 covers technology used to build small interactive programs into Web pages, potentially affecting everything from banner ads to interactive customer service. The patent's validity was invoked by Eolas Technologies (which was founded by one of the inventors and has licensed the patent exclusively) in its lawsuit against Microsoft. That legal action resulted in a $520 million jury award in favor of Eolas and prompted Microsoft to pledge a redesign of its Internet Explorer browser to avoid further infringement, a move that Web creator Tim Berners-Lee says could "render millions of Web pages and many products of independent software developers incompatible." Deputy patent commissioner Stephen G. Kunin cited "a substantial outcry from a widespread segment of the affected industry" in his decision to reexamine the patent and noted that patent examiners may not have adequately considered "prior art" in their investigations. (AP 12 Nov 2003)

*Category 4B2 Patents*

2003-11-24 **system for managing intellectual property alain rossmann**

NewsScan

NEW SYSTEM FOR MANAGING INTELLECTUAL PROPERTY
French-born Silicon Valley entrepreneur Alain Rossmann is creating his fifth high-tech start-up, PSS Systems, to develop a product that will help companies keep their documents compliant with government and industry regulations. Rossman's past start-ups have included Phone.com (now Openwave Systems), C-Cube Microsystems, Radius, and EO; the first three went public and the fourth was sold to AT&T. The new PSS system will allow a company to manage its intellectual property by tracking even those documents that are used for R&D outsourcing. It will also help government agencies collaborate in the fight against terrorism. (San Jose Mercury News 24 Nov 2003)

*Category 4B2 Patents*

2003-12-04 **patent intellectual property agreements cooperation**

NYT
http://www.nytimes.com/2003/12/04/technology/04soft.html?th=&pagewanted=print&position=

In December 2003, Microsoft announced "that it would adopt a more liberal policy for licensing its intellectual property, opening the doors to its storehouse of patents and copyrights to outsiders." [Steve Lohr, New York Times]. The reporter continued with an analysis suggesting that Microsoft could be trying to demonstrate a better attitude to regulators in the United States and Europe who are investigating monopolistic practices of the enormous company.

# 4B3 Reverse engineering

*Category 4B3* *Reverse engineering*

2003-01-06 **reverse engineering copyright infringement copy protection DVD**

NewsScan

SUPREME COURT BACKS OFF ON DVD DESCRAMBLING CODE
The U.S. Supreme Court has rescinded an emergency stay barring defendant Matthew Pavlovich from distributing DeCSS, a software utility that descrambles the digital lock on most DVDs to prevent copying them. Pavlovich is now free to distribute the code, but could be sued again if he decides to do so. "The entertainment companies need to stop pretending that DeCSS is a secret," says Cindy Cohn, legal director for the Electronic Frontier Foundation, which is assisting Pavlovich. "Justice O'Connor correctly saw that there was no need for emergency relief to keep DeCSS a secret. It doesn't pass the giggle test." The rescission is just the latest twist in a case that has been winding its way through the courts since 1999, when the DVD Copy Control Association — a coalition of movie studios and consumer electronics makers — filed a lawsuit against scores of people, alleging violations of California's trade secret laws. (CNet News.com 3 Jan 2003)
http://news.com.com/2100-1023-979197.html

---

*Category 4B3* *Reverse engineering*

2003-04-09 **digital copyright act defended ACLU Harvard student reverse engineer**

NewsScan

JUDGE DISMISSES CHALLENGE TO DIGITAL COPYRIGHT ACT
U.S. District Judge Richard Stearns has dismissed a lawsuit by the American Civil Liberties Union on behalf of a Harvard student who sought proprietary information from software company N2H2 so that he could reverse-engineer its software filtering product. The student and the ACLU had argued that software filters violate constitutional free speech protections because such filters unintentionally block far more than just pornography, and thereby deny people access to information to which they have a right. But Judge Stearns ruled that "there is no plausible protected constitutional interest that Edelman can assert that outweighs N2H2's right to protect its copyrighted material from an invasive and destructive trespass." (AP/USA Today 9 Apr 2003)

---

*Category 4B3* *Reverse engineering*

2003-04-16 **Digital Millenium Copyright Act Super DMCA privacy anonymizing restrictions bill law legislation offshore**

NIPC/DHS

April 14, SecurityFocus — 'Super-DMCA' fears suppress security research. University of Michigan graduate student Niels Provos who is noted for his research into steganography and honeypots — techniques for concealing messages and detecting hackers, respectively — says he's been forced to move his research papers and software offshore and prohibit U.S. residents from accessing it, in response to a controversial new state law. At issue are the so-called "Super-DMCA" (Digital Millennium Copyright Act) bills under consideration in seven states, which have already become law in six others. The state measures appear to target those who would steal pay-per-view cable television shows or defraud broadband providers. The Michigan law, which took effect on March 31st, typifies the legislation: Among other things, residents of the Great Lakes State can no longer knowingly "assemble, develop, manufacture, possess, deliver, offer to deliver, or advertise" any device or software that conceals "the existence or place of origin or destination of any telecommunications service." It's also a crime to provide written instructions on creating such a device or program. Violators face up to four years in prison. Taken literally, the law would target businesses like Anonymizer.com and Hushmail — both services cater to privacy-conscious Internet users determined to conceal their place of origin from marketers, or to communicate anonymously. Critics say it would also ban firewalls and NAT boxes, dealing a blow to Internet security.

---

*Category 4B3* *Reverse engineering*

2003-05-13 **DMCA copy protection Digital Millennim Copyright Act ACM Association Computing Machinery hackers ckrack security systems patents copyright**

NIPC/DHS

May 13, SecurityFocus — Security research exemption to DMCA considered. Computer security researchers would be allowed to hack through copy protection schemes under a proposed exception to the Digital Millennium Copyright Act (DMCA) being debated in official hearings this week. The DMCA's anti-circumvention provision generally makes it unlawful for anyone to "circumvent a technological measure that effectively controls access" to DVD movies, digital music, electronic books, computer programs, or any other copyrighted work. However, the Association for Computing Machinery (ACM) would like an exemption permitting white hat hackers to crack copy protection schemes "that fail to permit access to recognize shortcomings in security systems, to defend patents and copyrights, to discover and fix dangerous bugs in code, or to conduct forms of desired educational activities."

*Category 4B3* *Reverse engineering*

2003-09-16 **dmca verizon provacy information personal music piracy indentity**

NewsScan

CHALLENGE TO DMCA; 'TOO SOON TO CHANGE THE LAW' SAYS HATCH
Verizon is challenging the constitutionality of the subpoenas forcing Verizon to turn over names and addresses for at least four Internet subscribers. The Digital Millennium Copyright Act of 1998 permits music companies and others to force Internet providers to turn over the names of suspected pirates upon subpoena from any U.S. District Court clerk's office (and a judge's signature is not required). Sen. Orrin Hatch (R-Utah), chairman of the Senate Judiciary Committee, has said that it's too early to consider changing the 1998 law. "These issues have not ripened enough. I don't think we can yet determine if these subpoenas are being used responsibly to identify alleged infringers... As we start to hear more voices protesting the impact of these subpoenas, there may be more of a chance to reconsider their impact." (AP/San Jose Mercury News 16 Sep 2003)

# 4C1 Paradigms, security standards

*Category 4C1* *Paradigms, security standards*

2003-01-31 **worm vulnerability analysis homeland defense infrastructure protection network vulnerabilities management**

NewsScan

SAFE & SOUND IN THE CYBER AGE: INTERNET GRAND SLAM
Could your company survive without the Internet? This is not a rhetorical question. In the wake of last weekend's "Slammer" attack, corporations may have to contemplate getting by without the Internet. That sounds like hyperbole until realize how much trouble was caused by just 376 bytes of worm code. The basic facts have been widely reported. Late last Friday, or early Saturday in Asia, a worm was released onto the Internet targeting a vulnerability in Microsoft Corp's SQL Server 2000. Activity generated by the worm's probing for systems to infect brought Internet traffic to its knees, at least in parts of Asia. Weekend Web surfers in North America experienced everything from momentary delays to complete lack of access. American Express customers couldn't check their accounts online. Web operations were paralyzed for two days at Countrywide, the country's biggest residential mortgage provider. The Atlanta Journal-Constitution couldn't print Sunday's first edition on time. Some 911 emergency services were forced to revert to manual dispatching. On top of that, some weekend shoppers found their Bank of America cash cards couldn't produce "cash back" at supermarkets. For some, even plain old cash at ATM machines was unavailable.

A lot of technical staff at companies that rely on SQL Server and related code spent the weekend at work, removing the worm from infected systems and patching them to prevent reinfection. Even so, some employees couldn't get to their data on Monday morning, including some employees at Microsoft itself. An internal memo, issued over the weekend and leaked to the press on Tuesday, made it clear that Microsoft had failed to apply to many of its own systems the very patches it had urged customers to install to avoid this problem in the first place.

Unfortunately, all the talk about Microsoft and SQL Server has tended to obscure two of the scariest parts of the story:
1. Our society is a lot more dependent on the Internet and "immature" systems than anyone has so far been prepared to admit.
2. The Internet exists at the whim of those who know how to destroy it.
In this column and the next we will address these points in the above order, starting with the issue of dependency.

Over the last few months, Bank of America has spent millions of dollars on a television advertising campaign touting the ubiquity of its ATM machines. Imagine that you just switched your account to Bank of America because of those ads, only to find that access to your money is denied, by 376 bytes of rogue computer code released onto the Internet. In our admittedly unscientific sampling of consumer opinion at the coffee shop we found universal disbelief that such a thing could happen. Sadly, it comes as no surprise to us. As security experts, we have made it our business to know a lot about network infrastructure (after all, that's where a lot of data is most vulnerable). People who know more than we do about that infrastructure have been warning us for years about excessive inter-dependencies, lack of redundancy, single points of failure, and so on (they have also pointed out that 90% of all military communications are handled by commercial carriers, but that's another column). There have also been plenty of warnings about excessive reliance on immature code, i.e. software which is not deployed through a production process that includes thorough pre-production testing and a proper maintenance cycle (companies that had installed the patches for SQL Server before the weekend were not infected, although they may still have been affected by the traffic overload which the worm created). Now the public has very concrete proof that the experts were right.

Now we know we cannot rely on our bank to provide 24/7 access to our money. Hopefully, companies will now set about beefing up their networks, providing redundant channels and managing their code (funded by some of the huge costs savings they reaped by shifting data and voice from private lines to the Internet). Fortunately, the advice of network experts can also help the consumer. Redundancy is the best strategy to avoid being denied access to your cash by an ATM system failure. Just make sure you have debit card accounts at more than one bank!

In the next column we will explain why we think the Internet exists at the whim of those who know how to destroy it.

[Chey Cobb, the author of "Network Security for Dummies," is an independent consultant (www.cheycobb.com) and a former senior technical security advisor to the NRO. Her email address, chey@patriot.net, is heavily spam-filtered... Stephen Cobb, the author of "Privacy for Business: Web Sites and Email," is Senior VP of Research and Education for ePrivacy Group (www.eprivacygroup.com). He can be reached at scobb@cobb.com.]

*Category 4C1* *Paradigms, security standards*

2003-03-03 **Department of Defense DoD security policy release update information assurance controls standards**

NIPC/DHS

February 27, Government Computer News — DoD releases second half of security policy. Directive 8500.2, an information assurance policy that sets specific controls and standards for how users should secure Department of Defense (DoD) networks, was released by the Pentagon on Thursday. While 8500.1, which was released last October, supplied a framework for DoD to follow to protect its information systems, 8500.2 tells users how to secure their networks, said Robert F. Lentz, director of information assurance for the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence. The 8500.2 policy instructs Defense agency leaders to provide security training to all military and civilian personnel, including contractors, that meets an employee's job level of responsibility for working with DoD information systems. The policy establishes information assurance (IA) managers and officers to ensure that DoD systems meet IA specifications. According to 8500.2, information transmitted on Defense networks is shared across the Global Information Grid and is becoming more vulnerable to attacks and denial of service. The vulnerabilities stem from "increased reliance on commercial information technology and services; increased complexity and risk propagation through interconnection; the extremely rapid pace of technological change; a distributed and nonstandard management structure; and the relatively low cost of entry for adversaries."

*Category 4C1* *Paradigms, security standards*

2003-03-26 **security specifications standards base requirements**

NIPC/DHS

March 24, eWEEK — Security specs in the works. The CEO Cybersecurity Task Force by the end of this year will release a set of network security best practices for enterprises to adopt as a minimum standard. The task force plans to challenge executives to have their companies meet these base-line requirements by a certain date, which has yet to be determined. The hope is that peer pressure and a walk-before-you-run approach will entice laggard enterprises into shoring up their security. The task force, formed last week, is a subset of TechNet-a national organization of technology industry CEOs, somewhat akin to a lobbying group, that works with legislators to help shape policy. In addition to developing the base-line security guidelines, the task force plans to work with government security officials to develop an efficient, workable plan for public and private information sharing of attack and threat data. This is a hot topic both in Washington and in Silicon Valley, where corporate IT staffs see little to gain by divulging such sensitive data.

*Category 4C1* *Paradigms, security standards*

2003-04-09 **cyber terrorism cyberspace attack Australia risk threat open door**

NIPC/DHS

April 08, Next — Australia leaves the hack door open to cyber sabotage. Australia's critical information infrastructure is at risk because of the Federal Government's focus on physical infrastructure and terrorism, the head of Australia's Computer Emergency Response Team (AusCERT) says. AusCERT general manager Graham Ingram says that Malaysia, South Korea and Japan are spending enormous amounts of money on protecting information infrastructure - things such as government, banking, public utility, telecommunications and emergency networks. In Australia, many of these assets are in private hands. AusCERT has been contracted by the Federal Government to provide a free service to the general public and business about new threats to networked computer systems as part of the Trusted Information Sharing Network (TISN). TISN is a voluntary forum for owners of critical infrastructure to exchange information on security issues announced last November. But Kate Lundy, IT spokeswoman for Australia's Labor Party, says laws are needed to force the private sector to comply with minimum standards of protection for critical information infrastructure.

*Category 4C1* *Paradigms, security standards*

2003-04-09 **corporate security single entity holistic**

NIPC/DHS

April 07, Computerworld — Handle corporate security as single entity, users say. Companies can improve their ability to detect and respond to both cyber and physical threats by tying their IT security to other aspects of corporate security. But the cultural and business-process changes involved in implementing such a holistic view of security can be daunting for most corporations, users said here last week at a conference organized by ASIS International, an organization of security professionals. Lew Wagner of the MD Anderson Cancer Center at the University of Texas in Houston, said coordinating IT security functions with areas such as physical protection, facilities management, human resources and legal and audit functions has helped enhance overall threat-detection and incident-response capabilities at the hospital. A holistic view of enterprise security can help plug gaps that might otherwise be missed, said James Litchko, of Litchko & Associates Inc., a security consultancy in Kensington, MD. For instance, the majority of IT-related security threats still stem from procedural and process flaws-such as failure to secure access to crucial systems, inadequate backups and lack of auditing-rather than from technology glitches, Litchko said.

*Category 4C1* *Paradigms, security standards*

2003-04-18 **Federal Information Processing Standard FIPS crypto cryptography international Canada Britain UK**

NIPC/DHS

April 15, Government Computer News — FIPS-140 gains international acceptance. The Federal Information Processing Standard for cryptographic modules, FIPS-140, has become the de facto international standard for cryptography, with 300 products validated by independent laboratories. It is moving toward becoming an official international standard as well. In October, the International Standards Organization began considering a proposal to make FIPS-140-2 an international standard, and Britain in November accepted it as the standard for protecting personal information submitted to the government. The National Institute of Standards and Technology (NIST) and its Canadian equivalent, the Communications Security Establishment, jointly run the validation program, which certifies product compliance with FIPS-140-2. "I have heard that many states are recognizing FIPS-140," said Ray Snouffer, manager of NIST's Security Management and Testing Group. The standard is also required by many private-sector organizations, including banks in Europe and U.S. companies such as Visa International Service Association and Boeing Co. But the United Kingdom is the first country other than the United States to adopt the standard.

*Category 4C1* *Paradigms, security standards*

2003-04-28 **Peter Neuman software testing quality assurance manufacturer reponsibility**

NewsScan

SOFTWARE MAKERS DON'T DO ENOUGH TESTING, SAYS NEUMANN
Peter Neumann, principal scientist at SRI International's Computer Science Laboratory in Menlo Park, California, says that most software is released without undergoing a sufficient amount of testing, and adds: "The idea that we depend on something that's inherently untrustworthy is very frightening." Last year a study commissioned by the National Institute of Standards and Technology found that software errors cost the U.S. economy about $59.5 billion a year, or 0.6% of the country's entire GDP. Should software makers be held responsible for shoddy code? Barbara Simmons, former president of the Association for Computing Machinery, thinks they certainly should: "Software is being treated in a way that no other consumer products are. We all know that you can't produce 100% bug-free software. But to go to the other extreme and say that software makers should have no liability whatsoever strikes me as absurd." (AP/USA Today 28 Apr 2003)

*Category 4C1* *Paradigms, security standards*

2003-05-16 **NIST National Institute Standards Technology FISMA FIPS security risk categorize national confidentiality integrity availability information**

NIPC/DHS

May 16, Federal Computer Week — NIST releases draft security standard. The National Institute of Standards and Technology's (NIST) Computer Security Division Friday released the draft of a new Federal Information Processing Standard, FIPS 199, which dictates how agencies should categorize their systems based on the security risk faced by each. The standard is the first step in several requirements generated by NIST under the Federal Information Security Management Act (FISMA) of 2002, all aimed at setting minimum security requirements for all government systems not related to national security. The draft outlines three categories of risk, which are based on the potential impact of a breach in three areas: the confidentiality, integrity and availability of the information in the system. Comments on the draft are due within 90 days. The draft is available on the NIST Website:
http://csrc.nist.gov/publications/drafts.html

*Category 4C1* *Paradigms, security standards*

2003-07-25 **cybersecurity DoD COTs monoculture vulnerability**

NewsScan

CYBERSECURITY AT THE DEFENSE DEPARTMENT
Purdue University computer science professor Eugene Spafford says there is too much reliance in the Defense Department on off-the-shelf commercial software: "Most of those products are not written to be used in an environment where there is a significant threat. We have attacks being committed by hackers, by anarchists, by criminals, probably by foreign intelligence services. The products have not been designed to be reliable or robust under those kinds of circumstances." There's also a "near mono-culture" resulting from the use of common products across many different DOD systems: "When a new attack is found that has affected any one of these products, it seeps through the entire network. Operators of systems may be in the position of applying three to five security critical patches per week for every system under their control. That really is unacceptable for us to be in a state of high readiness." Microsoft chief security strategist Scott Charney offers an perspective on the issue: "Reasonable minds are debating whether a homogeneous environment or a heterogeneous environment is better for decreasing risk. The advantage of a homogeneous environment, or more of a mono-culture, is it's much easier to manage. You train your people in a particular system, and they manage that system, they know all the security settings, you run tools to make sure they lock it down." (IDG News/Infoworld 25 Jul 2003)

*Category 4C1* *Paradigms, security standards*

2003-11-04 **NIST security control proposal standards federal information systems FIPS**

NIPC/DHS

November 03, Federal Computer Week — NIST releases security controls proposal. The National Institute for Standards and Technology (NIST) released the first draft of a publication describing mandated security controls for federal information systems on Monday, November 3. NIST officials want agencies to experiment with the initial public draft, "Special Publication 800-53: Recommended Security Controls for Federal Information Systems." It outlines electronic and physical controls for systems categorized under three levels of potential impacts, such as what would happen if someone steals information from a federal system and modifies the data or disrupts a government service. NIST's Computer Security Division plans to use agencies' comments from the initial draft and an open workshop in March to develop final security controls that would become the new "FIPS 200: Minimum Security Controls for Federal Information Systems." FIPS 200 is required under the Federal Information Security Management Act of 2002. NIST expects to publish FIPS 200 in the fall of 2005, when its controls will become mandatory for all federal agencies.

*Category 4C1* *Paradigms, security standards*

2003-11-06 **microsoft virus writers reward anti-virus money program information arrest**

NewsScan

MICROSOFT PUTS A PRICE ON THE HEADS OF VIRUS WRITERS
Microsoft is using an old-fashioned tactic to fight new-fangled viruses — it's created a $5-million Anti-Virus Reward Program and is offering $250,000 bounties for information leading to the arrest and conviction of the people behind last summer's Blaster worm and Sobig virus. Together, those attacks are blamed for $2 billion in losses by businesses and consumers, according to consulting firm Computer Economics Inc. Security experts are split on whether the new initiative will prove successful, but Microsoft senior security strategist Philip Reitinger says, "What we hope to accomplish is to give people an incentive to do the right thing." (Los Angeles Times 6 Nov 2003)

*Category 4C1* *Paradigms, security standards*

2003-11-18 **NIST security guidelines posted draft federal information systems protection**

NIPC/DHS

November 14, Government Computer News — NIST posts security control guidelines for comment. The National Institute of Standards and Technology (NIST) released an initial public draft of recommended security controls for federal information systems Thursday, November 13. The guidelines for mandatory controls are expected to go into effect in two years. The Special Publication 800-53 was drafted under the Federal Information Security Management Act. SP 800-53 is one of seven NIST publications to be completed over the next two years as a security framework. Federal Information Processing Standard Publication 200, "Minimum Security Controls for Federal Information Systems," will replace SP800-53 in late 2005 and will be mandatory for government systems not involved in national security. Controls include management, operational and technical safeguards and countermeasures that ensure the confidentiality, integrity and availability of government systems. The current 238-page report is preliminary and covers only guidelines for low and moderate security baselines. NIST's Computer Security Division will accept comments on the initial draft of SP 800-53 until January 31, 2004. The draft is available online: http://csrc.nist.gov/publications/drafts.html

*Category 4C1* *Paradigms, security standards*

2003-11-25 **worms msblast slammer code red carnegie mellon software information systems security**

NewsScan

NEW STUDY TARGETS IT MONOCULTURE
The National Science Foundation is funding two universities — Carnegie Mellon and the University of New Mexico — to investigate ways to diversify software and information systems in an effort to fend off cyberattacks. "We are looking at computers the way a physician would look at genetically related patients, each susceptible to the same disorder," says Carnegie Mellon engineering professor Mike Reiter. "In a more diverse population, one member may fall victim to a pathogen or disorder while another might not have the same vulnerability." The $750,000 grant comes in response to massive digital epidemics caused by the Code Red, Slammer and MSBlast worms, which disabled hundreds of thousands of computers over the past year. The researchers hope to create an application that could generate diversity in key aspects of software programs without hampering their utility. The result could prove a boon for Microsoft by helping it to break up its monoculture without losing market share. (CNet News.com 25 Nov 2003)

*Category 4C1 Paradigms, security standards*

2003-12-24 **NIST security guidance standards FISMA FIPS**

NIPC/DHS

December 22, Federal Computer Week — NIST releases security level guidance. The National Institute of Standards and Technology (NIST) released a draft of the last piece of guidance for agencies to determine the proper level of security on information systems last week. The "Special Publication 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories" provides the middle step for guidance and standards required under the Federal Information Security Management Act (FISMA) of 2002. NIST's categories of security impact are based on draft Federal Information Processing Standard (FIPS) 199, which the division released in September. The goal of the guidance is to have agencies assign impact levels without considering potential security controls and countermeasures, but in October, NIST released another draft guide outlining minimum-security controls for each category. NIST also released a draft interagency report on smart card technology development and adoption within agencies. The draft report is in response to a January General Accounting Office report that recommended that NIST play a greater role in smart card implementation governmentwide. Additional information is available on the NIST Website:
http://csrc.nist.gov/publications/drafts.html

# 4C2 Risk management methodology & tools

*Category 4C2* *Risk management methodology & tools*

2003-01-15 **Microsoft expands security rating system vulnerabilities listing**

NIPC/DHS

January 13, Info World — Microsoft adds category to security rating system. After customers complained that they couldn't identify the most serious security vulnerabilities, Microsoft has added a fourth category to its vulnerability rating system. But critics feel that the extra tier adds even more complexity to an administrator's job. Under the new system, fewer bulletins get the "critical" stamp. Only vulnerabilities that could be exploited to allow malicious Internet worms to spread without user action are now rated critical. Many issues that were previously rated critical are now "important," a new category in the rating system. These "important" vulnerabilities could still expose user data or threaten system resources, but they might not receive the urgent attention from administrators that they deserve. A two-tiered system would let administrators quickly decide whether they need to drop all tasks at hand and apply a patch, or whether the risk is small enough that they can wait and include it in a weekly patch cycle.

*Category 4C2* *Risk management methodology & tools*

2003-01-16 **network sharing attack data countermeasure hacking**

NIPC/DHS

January 13, eWeek — Sharing attack data could thwart hackers. Two Harvard University security researchers have developed a model showing that enterprises that share their sensitive data about network attacks and security breaches are less attractive targets and, hence, less likely to be attacked. The reason is that attackers who spend time, and in some cases money, finding and exploiting vulnerabilities in common applications will not want information about their attacks shared, as it would reduce their chances of compromising other potential targets. The paper, to be presented later this month at the Financial Cryptography conference in Gosier, Guadeloupe, supports the U.S. government's contentions about the importance of sharing attack data. The next draft of the National Strategy to Secure Cyberspace, due early this year, is expected to include language encouraging CIOs to forward more information to the government. Security specialists and CIOs worry that sharing sensitive data with anyone will expose them to embarrassment and potential lawsuits from customers. The government's interest in attack data is partially due to the creation of the Department of Homeland Security which will be responsible for early warning and analysis.

*Category 4C2* *Risk management methodology & tools*

2003-01-29 **hacking insurance risk mitigation**

NewsScan

HACKER INSURANCE
The latest cyber attack (last weekend's SQL Slammer virus, which infected thousands of computer servers throughout the world) has given a new boost to "network risk insurance" (AKA "hacker insurance"), which is expected to grow from the $100 million industry it is now to a $2.5 billion industry by 2005. Bruce Schneier, the chief technology officer for Internet security at Counterpane, thinks that insurance is every bit as important as prevention: "I believe that within a few years hacking insurance will be ubiquitous. The notion that you must rely on prevention is just as stupid as building a brick wall around your house. That notion is just wrong." But getting "hacker insurance" is not as easy as one might think, because insurers typically require a third-party assessment of the insurance applicant's security system, which might cost as much as $50,000. (Reuters/USA Today 28 Jan 2003)

*Category 4C2* *Risk management methodology & tools*

2003-02-07 **probabalistic risk management software mathematics statistics**

NIPC/DHS

February 06, New York Times — Assessing the odds of catastrophe. A rapidly evolving set of conceptual and computing tools allow mathematicians, engineers and insurance executives to assess the risk of low-probability, high-consequence events. The field, known as probabilistic risk assessment, helps companies and government agencies decide whether they are prepared to take the chances involved. And now some of the techniques are being used to analyze the chances of terrorist attack. Developed four decades ago, the idea behind probabilistic risk assessment is that mathematics can help determine the chances of a particular outcome (a power system failure, or a hurricane that destroys thousands of homes) based on what is known or estimated about the smaller variables that lead to those outcomes. Jim Goodnight of SAS, a maker of statistical software, said that with faster processors, more advanced software and a huge availability of memory - whether on big mainframe computers or on lashed-together PC systems - "the ability to do the incredibly difficult modeling is becoming more reachable every day." Probabilistic models, of course, are only as useful as the assumptions fed into them. Moreover, they are best used when a system or piece of equipment is being designed. The most daunting challenge, however, may be modeling minds. In describing the challenge of modeling terrorism, Hemant H. Shah of RMS, a risk-modeling firm, said, "Hurricanes do not make an effort to strike your weak points. In the case of terrorism you're dealing with a question of intent. You're modeling an adversary in the context of conflict."

*Category 4C2* *Risk management methodology & tools*

2003-04-17 **coporate IT security disclosure secure cyberspace**

NIPC/DHS

April 14, eWEEK — Feds mull IT disclosure. Momentum is building in Washington to require all public companies to annually report the performance of their IT security initiatives, not just the financial services and health care industries that face scrutiny now. The Bush administration considered requiring companies to report on network security during the crafting of the National Strategy to Secure Cyberspace. But the idea was unpopular in many enterprises and did not make the final plan, released in February. Last week, former presidential adviser for cyberspace Richard Clarke, who spearheaded the strategy, urged Congress to act quickly to legislate such obligations. Enterprises object to the suggestion of broad reporting requirements, but some see a certified audit process reflected in annual Securities and Exchange Commission filings as beneficial. Possible requirements include disclosing measures taken to secure systems, identifying IT security auditors and detailing breaches.

*Category 4C2* *Risk management methodology & tools*

2003-05-07 **report attacks failure e-commerce serious damage businesses cyber police NHTCU Len Hynds Infosecurity**

NIPC/DHS

May 07, vnunet.com — UK ecommerce hit by failure to report attacks. Consumer and corporate trust in ecommerce will be seriously damaged if businesses do not report electronic crimes, says the UK's online police force. The National Hi Tech Crime Unit (NHTCU) is trying to convince companies to report cyber attacks. Only 56 per cent of larger companies report electronic crime to the police, and the figure is believed to be even lower among smaller organizations. "It's vitally important that people trust their technology," Len Hynds, head of the NHTCU, told delegates at last week's Infosecurity conference in London.

*Category 4C2* *Risk management methodology & tools*

2003-11-05 **data sharing disaster recovery business continuity planning Homeland Security**

NIPC/DHS

November 04, GCN.com — Data sharing needs to begin before first response, officials say. For the National Guard Bureau, the ability to share data for disaster planning and first response has been hampered by a constant stream of hacker intrusions on its unclassified networks over the past two years. “We’re getting hacked all over the place. I actually see it getting worse, and it’s making it harder and harder for us to share information,” said Maureen Lischke, CIO for the National Guard Bureau. She and other government officials spoke about data sharing to support homeland security at an Industry Advisory Council event in Washington. Although cultural barriers represent the biggest hurdle, federal groups also need to think about sharing information before a major atrocity occurs, not after, said David Boyd, the Homeland Security Department’s deputy director of R&D and director of the Safecom program to provide wireless communications to federal, state and local first responders. There’s very little of such pre-disaster data sharing occurring now, beyond of the tactical warfighting level, said John Paczkowski, director of operations and emergency management for the Port Authority of New York and New Jersey. An open architecture is necessary to maintain some fundamental level of interoperability, Paczkowski said.

*Category 4C2* *Risk management methodology & tools*

2003-11-25 **Veterans Affair department security program**

NIPC/DHS

November 24, Federal Computer Week — VA has new security program. The Department of Veterans Affairs (VA) started a proactive vulnerability management program to provide improved cybersecurity at more than 250 facilities nationwide. The new strategy will provide more frequent security assessments, reducing risks and ensuring compliance with privacy regulations and internal security standards, officials said. Potential vulnerabilities can more easily be identified and reported to the VA's central incident response center for centralized management. In addition, the new service will allow individual facilities to quickly respond to security bulletins released by the response center.

# 4C3 Certification of site security, privacy protection

*Category 4C3* *Certification of site security, privacy protection*

2003-08-13 **NIST IT security metrics National Institute Standards Technology policy Self-Assessment Guide Systems 800-26 800-55**

NIPC/DHS

August 13, Government Computer News — NIST releases guidelines for IT security metrics. The National Institute of Standards and Technology (NIST) has released its final version of guidelines for developing metrics to help ensure agencies meet IT security requirements. Metrics-measurable standards-monitor the effectiveness of goals and objectives established for IT security. They measure the implementation of security policy, the results of security services and the impact of security events on an agency's mission. The publication uses the critical elements, and security controls and techniques laid out in an earlier NIST publication, 800-26, Security Self-Assessment Guide for IT Systems. NIST Special Publication 800-55, Security Metrics Guide for IT Systems is available online
http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf

*Category 4C3* *Certification of site security, privacy protection*

2003-11-20 **Congress cyber security cyberspace report FISMA**

NIPC/DHS

November 19, Government Computer News — Congress plans report cards on cybersecurity. On the heels of Office of Management and Budget efforts over the past year to boost cybersecurity, lawmakers are set to weigh in on agency progress. The House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census next month will issue a cybersecurity report card detailing agency progress in meeting the requirements of the Federal Information Security Management Act (FISMA). The subcommittee has been working to focus the legislative and executive branches on the importance of cybersecurity with a variety of hearings over the past year. Subcommittee staff director Bob Dix, speaking Wednesday, November 19, at the Enterprise Architecture 2003 Conference in Washington D.C. said the subcommittee also plans to explore whether the federal procurement process can be used to improve software security. "If we use the purchasing power of the federal government to insist that developers provide more secure products, that will benefit all users in both the public and private sectors," he said.

# 4C5 Academic / Industry / Vendor / Govt efforts

*Category 4C5 Academic / Industry / Vendor / Govt efforts*

2003-01-10 **report INFOSEC standards US federal government infrastructure protection**

NIPC / DHS

January 09, Federal Computer News — Council offers vision for infosec standards. President Bush's private-sector infrastructure protection advisory council agreed January 8 that the federal government should encourage the development and use of open standards in the market instead of dictating specific standards. But federal officials should also use the government's significant buying power to push for interoperability in those market standards and solutions that will raise the baseline of security across all sectors. The National Infrastructure Advisory Council's report will go to the president later this month along with a revised National Strategy to Secure Cyberspace, said Richard Clarke, chairman of the President's Critical Infrastructure Protection Board. The recommendations fall in line with the approach taken by the Bush administration in its draft cybersecurity strategy, which the White House released in September 2002 for comment. Revisions proposed by Clarke's office include setting specific priorities, such as taking a closer look at the Common Criteria security product certification program. Later this month, the council plans to meet again to look at other infrastructure protection issues, including the international migration to Version 6 of the Internet Protocol and developing a systematic vulnerability assessment program for private-sector infrastructure.

---

*Category 4C5 Academic / Industry / Vendor / Govt efforts*

2003-01-16 **Microsoft international governments access secret code security testing Russia NATO**

NIPC / DHS

January 15, New York Times — Microsoft to give governments access to code. Microsoft announced today that it will allow most governments to study the programming code of its Windows systems. Under the program, 97 percent of the code to Windows desktop, Windows server and Windows CE hand-held software will be available to governments online for inspection and testing. To view the other 3 percent - the most sensitive technology - government representatives must come to Microsoft headquarters in Redmond, WA. Governments will also be allowed to plug their security features instead of Microsoft's technology into Windows. More than two dozen countries are encouraging agencies to use "open source" software - developed by programmers who distribute the code without charge and donate their labor to debug and modify the software cooperatively. The best-known of the open source projects is GNU Linux, an operating system that Microsoft regards as the leading competitive threat to Windows. One appeal of Linux is that developers have complete access to the underlying source code, whereas Microsoft has kept some Windows technology secret. Microsoft expects that perhaps 60 foreign governments and international agencies will eventually join its government security program. The first to join were Russia and the North Atlantic Treaty Organization, and the company is negotiating with 20 other groups.

---

*Category 4C5 Academic / Industry / Vendor / Govt efforts*

2003-02-03 **cyber security agenda research development**

NIPC / DHS

January 31, Federal Computer Week — Cybersecurity RD agenda unveiled. The Institute for Information Infrastructure Protection (I3P) has unveiled its 2003 Cyber Security Research and Development Agenda, which identifies critical areas that require significant research and development to help secure the nation's information infrastructure. The agenda, announced January 30, outlines eight crucial RDgaps that are not being sufficiently addressed by ongoing government, private-sector or academic research: 1) Enterprise security management; 2) Trust among distributed autonomous parties; 3) Discovery and analysis of security properties and vulnerabilities; 4) Secure system and network response and recovery; 5) Traceback, identification and forensics; 6) Wireless security; 7) Metrics and models; 8) Law, policy and economics. The I3P, a consortium of 23 leading cybersecurity research institutions from academia, national labs and nonprofit organizations, is funded by the Commerce Department and the National Institute of Standards and Technology. The agenda will help the White House's Office of Science and Technology Policy better coordinate RDefforts across government agencies, said Susan Hays, deputy associate director for technology at the office. I3P received input, gathered over nine months in 2002, from more than 900 experts and security professionals from the private sector, academia and government, said Michael Vatis, chairman of I3P.

---

*Category 4C5* *Academic/Industry/Vendor/Govt efforts*

2003-03-18 **best security practice report Telecom NRIC FCC infrastructure**

NIPC/DHS

March 14, Government Computer News — Telecom advisory group finishes work on best security practices. The Network Reliability and Interoperability Council (NRIC) completed work Friday on a set of best practices to ensure the security and availability of the nation's communications infrastructure. During its quarterly meeting, industry working groups chartered by the Federal Communications Commission (FCC) presented 162 recommendations for steps to be taken by network operators, manufacturers and service providers to help with service restoration in the event of man-made or natural disruptions. The recommendations will be voted on by the entire council by March 28. NRIC was created as an industry advisory committee in 1992, and received its most recent charter from FCC chairman Michael Powell in January 2002. NRIC VI focuses on homeland security and was charged with coming up with a set of voluntary best practices for network security and survivability. Approval of recommendations made Friday would complete the first phase of the council's current work. The second phase is education and outreach to encourage use of the best practices. Practices recommended for adoption Friday focus on restoring service after attacks on or damage to physical or cyber links.

*Category 4C5* *Academic/Industry/Vendor/Govt efforts*

2003-04-11 **Microsoft source code partner access shared debug test secure**

NIPC/DHS

April 10, New York Times — Microsoft to allow partners to alter some source code. Microsoft announced Wednesday that it would allow its industry partners to modify and then redistribute the underlying programming code used in cellphones, hand-held computers, television set-top boxes and other small devices. The new policy does not apply to Microsoft's mainstay products in personal computer desktop software and data-serving software that runs computer networks. According to analysts, the move shows that even Microsoft must respond, at least in markets it does not dominate, to the changed attitudes and practices in the software industry prompted by the rise of "open source" software - software developed by programmers who distribute the code without charge and then cooperatively debug, modify and add improvements to the software. Microsoft does not embrace the open source formula as a way of doing business. But the company is selectively borrowing some of the open source practices for the way it develops software. It is doing so mainly in response to the growing popularity of the best-known open source project, the GNU Linux operating system, a competitor to Microsoft's Windows. Microsoft rivals like IBM and Oracle are promoting Linux. Microsoft calls its approach the Shared Source Initiative, which it began nearly two years ago.

*Category 4C5* *Academic/Industry/Vendor/Govt efforts*

2003-04-16 **Open Security Exhange group Computer Associates security standards specifications implementation**

NIPC/DHS

April 14, eWEEK — Companies form Open Security Exchange. Computer Associates International Inc. (CA) and several other companies announced Monday the formation of a group that is working to define and implement open specifications and best practices for integrating information security and physical security. The group plans to submit the specifications to an industry standards body, but has yet to decide which one it will approach with the idea. The Open Security Exchange grew out of CA's own efforts to integrate the management of network and physical security within large enterprises. The announcement of the group's formation came at the RSA Conference in San Francisco. Among the specific problems that the new group plans to address initially are audit and forensics, authentication, and centralized provisioning. Whether competitors and large companies from disparate industries can work together to make the idea work remains to be seen. The group's specification is available on its Web site, which is
http://opensecurityexchange.com.

*Category 4C5* *Academic/Industry/Vendor/Govt efforts*

2003-04-17 **e-government legislation bureaucracy services IT**

NewsScan

E-GOV
In implementing the E-Government Act of 2002, the Bush Administration is creating an Office of Electronic Government within the White House. A main mission of the E-Gov office will be to make it easier for citizens to apply for government services and to obtain information from federal agencies; other goals will be to reduce bureaucratic redundancies by providing better coordination and oversight of money being spent by federal agencies on information technology. (San Jose Mercury News 17 Apr 2003)

*Category 4C5* *Academic/Industry/Vendor/Govt efforts*

2003-04-17 **industry vendor TechNet alliance security standards specifications**

NIPC/DHS

April 15, CNET News.com — Alliance takes security call to boardroom. TechNet, a lobbying group of more than 150 information technology companies, said Tuesday that it would work with the Internet Security Alliance and the four large accounting firms to create guidelines and best practices that they say executives need in order to secure their companies. The accounting firms are KPMG, PricewaterhouseCoopers, Deloitte & Touche and Earnst & Young. The starting point will be a top-10 list of security steps for executives that the Internet Security Alliance has already created. "We wanted to aim at the top because we believe that at the top, with boardroom involvement and (policy) trickling down, we can get the best results," said John Shaughnessy of the Internet Security Alliance. President George W. Bush in February 2003 said the United States government would not regulate technology companies, but rather would promote cooperation between the industry and the government to secure infrastructure. The groups plan to release the guidelines and then to set a date by which its membership should comply with the security steps.

*Category 4C5* *Academic/Industry/Vendor/Govt efforts*

2003-04-22 **Indiana Purdue University cybersecurity center information assurance security research studies**

NIPC/DHS

April 18, Associated Press — Law professor will head university's cybersecurity center. Indiana University (IU) law professor Fred Cate will be the inaugural director of the Center for Applied Cybersecurity Research which will research computer and Internet security issues. Cate, an expert on privacy and information law, said the center will encourage university partnerships with businesses and with federal and state government agencies. IU created the center with $125,000 from a private donor and a matching amount from its own funds, said Michael McRobbie, IU's vice president for information technology and chief information officer. He said the center will be based both in Bloomington and at Indiana University-Purdue University at Indianapolis. It will bring together university staff with computer-security duties - from information technology, legal, audit and police departments - with faculty performing research related to cybersecurity, he said.

*Category 4C5* *Academic/Industry/Vendor/Govt efforts*

2003-04-23 **cyber risk e-crime cyber sabotage Australia companies share information protect infrastructure**

NIPC/DHS

April 22, The Australian — Austrialian business called on to fight cyber risks. Australian companies are being asked to share information freely in order to defeat threats ranging from cyber-sabotage to e-crime. "If just one part of the economy is attacked, the repercussions are likely to be felt by all sectors and all businesses," Attorney-General Daryl Williams told business representatives at the launch of the Trusted Information Sharing Network (TISN) in Melbourne this month. Businesses often view infrastructure protection as a government problem, according to Tom Patterson of Deloitte & Touche Security. "If you look at what runs the economy, it's not your government, it's your companies. Every company has an obligation to protect its business not only for its stakeholders and its shareholders but also for the economy as a whole," he says. The government hopes TISN will become a forum for open exchange of information about system attacks and vulnerabilities, as well as protection of key sites from cyber-sabotage. A Critical Infrastructure Advisory Council will be set up to oversee efforts in various industry sectors as well as developing strategies for business continuity and consequence management.

*Category 4C5* *Academic/Industry/Vendor/Govt efforts*

2003-07-25 **Microsoft integrated security Windows Office R&D**

NewsScan

MICROSOFT PROMISES 'INTEGRATED INNOVATION'
Microsoft plans to increase its R&D spending this year by perhaps 8%, to a total of $6.9 billion, and to expand its work force by 4,000 to 5,000 positions during the current fiscal year. Disputing recent pronouncements by others, Microsoft co-founder and chairman Bill Gates says that that the computer industry is far from being in decline or in a state of rapid consolidation: "The debate about what came out of the boom and what these information technology investments mean has really gotten fairly extreme. Obviously we put our money where our beliefs are in saying we disagree with all of this." And Microsoft's business strategy at this point in time? "Integrated innovation" that will give the company's Windows and Office software customers a continuous stream of features and service. Gates says, "It shouldn't be necessary for people to buy additional products for their secure infrastructures." (New York Times 25 Jul 2003)

*Category 4C5* *Academic/Industry/Vendor/Govt efforts*

2003-10-22 **Carnegie Mellon lab cyber-security engineering technologies new CERT Internet Explorer CyLab education research**

NIPC/DHS

October 22, eWEEK — Carnegie Mellon lab tackles cyber-security. Security, engineering and public policy experts at Carnegie Mellon University are joining together to form a new lab at the school dedicated to researching and developing new security technologies. The new organization, known as the Carnegie Mellon CyLab, will include representatives from the school's engineering, computer science and public policy departments, as well as personnel from the CERT Coordination Center. The group will seek to promote collaboration between the government and the private sector. CyLab's charter will differ significantly from that of CERT, which is charged with analyzing and responding to security threats and attacks. A quasi-public organization, CERT is partially funded by the federal government. CyLab will also receive public money, but will concentrate on finding long-term solutions to pervasive security problems instead of looking at how to mitigate the latest attack on Internet Explorer, as CERT does. The group's mission is essentially threefold: education; research and development; and response and prediction. In addition to offering bachelor's, master's and doctorate degrees in security-related disciplines, CyLab will also work to educate home users on the inherent dangers of the Internet and the steps they can take to combat those issues.

*Category 4C5* *Academic/Industry/Vendor/Govt efforts*

2003-10-24 **Iowa State University fight hackers ISEAGE Internet laboratory**

NewsScan

SECURITY PROJECT AT IOWA STATE
Iowa State University researchers are creating a laboratory to fight computer hackers. The project, which is being funded by a $500,000 grant from the U.S. Justice Department, will allow ISU to develop what it calls Internet-Scale Event and Attack Generation Environment (or ISEAGE, pronounced ice age), which is designed to allow realistic tests of security defenses. Computer scientist Doug Jacobson explains: "Since we can't take over the real Internet, we've decided to recreate our own Internet laboratory. We will be able to carry out computer attacks exactly as they happen in the real world." (AP/USA Today 24 Oct 2003)

*Category 4C5* *Academic/Industry/Vendor/Govt efforts*

2003-11-14 **technology security alliance chief security officer importance Internet**

NIPC/DHS

November 12, Washington Post — Tech security chiefs form alliance. Nearly a dozen top technology luminaries are lending their star power to a new think-tank that will look for ways to elevate the status of chief security officers in the private sector, a move that they say will go a long way toward improving Internet security. The Global Council of Chief Security Officers was formed by former White House cybersecurity adviser Howard Schmidt. The council will consult with technology vendors and industry groups to help design more secure products for the next generation of the Internet, Schmidt said. MCI's Vint Cerf said that the council should also encourage more compatibility between different and competing technologies. Failure to do so, especially as the Internet grows into even more of a commercial medium, could prove damaging to online networks. The council will hold its first meeting in San Jose in January and a CSO summit in San Francisco the following month. U.S. CERT, a new partnership between the Department of Homeland Security and the CERT Coordination Center—a government funded security watchdog group at Carnegie Mellon University in Pittsburgh—will oversee the council's day-to-day activities. The council is on the Web at:
http://www.csocouncil.org

*Category 4C5* *Academic/Industry/Vendor/Govt efforts*

2003-11-19 **cyber security summit US CERT education strategy secure cyberspace**

NIPC/DHS

November 17, US-CERT — US-CERT announces the National Cyber Security Summit. The National Cyber Security Summit, to be held December 3 in Santa Clara, CA, is the first of a series of invitational events focusing on Internet security. Invited delegates to this one-day summit may serve on one of the five cross-sectoral task forces, which will be responsible for recommending solutions to the challenges posed in the President's National Strategy to Secure Cyberspace. The five task forces, which will be sponsored by the private sector, are: Awareness for Home Users and Small Businesses, Cyber Security Early Warning, Best Practices and Standards: Corporate Governance, Best Practices and Standards: Technical Standards and Common Criteria, and Security Across the Software Development Life Cycle: Secure Software.

*Category 4C5* *Academic/Industry/Vendor/Govt efforts*

2003-12-04 **government official security summit Department Homeland Security DHS cooperation public private sector**

NIPC/DHS

December 02, CNET News.com — Government officials join security summit. Silicon Valley executives are slated to meet on Wednesday , December 4, with top bureaucrats from the Department of Homeland Security (DHS) to hammer out ways that the private sector can work with government to enhance national security and avoid creating regulations. The National Cyber Security Summit will bring together top executives at security and technology companies with policy-makers. Corporate leaders are expected to announce several new task forces and initiatives aimed at making information security a boardroom issue. The gathering comes nine months after the Bush administration unveiled its plan to secure the Internet through cooperation instead of regulation. It also comes just in time to stiffen opposition to a bill that would require companies to reveal the results of a security audit in their financial reports. The meeting, which will be held at the Santa Clara Marriott, will try to convince government officials that security-savvy organizations can teach industry executives to consider information security at the boardroom level. The meeting will establish at least three task forces, including the Corporate Governance Task Force, the CEO Cyber Security Task Force, and the Technical Standards and Common Criteria Task Force.

*Category 4C5* *Academic/Industry/Vendor/Govt efforts*

2003-12-05 **industry security tools software release cyber summit GISRA FISMA**

NIPC/DHS

December 04, — Industry groups release security tools. A pair of information technology industry groups unveiled security assessment tools at this week's National Cyber Security Summit in Santa Clara, CA. TechNet, an association of chief executive officers (CEO) and other senior executives, unveiled its Corporate Information Security Evaluation tool, which takes CEOs, chief information officers, and chief security officers through 88 points on risk management, people, processes, and technology. The Information Technology Association of America, in partnership with the Marshall School of Business at the University of Southern California, announced its Cyber Security Assessment, which will build on information provided by the TechNet evaluation. The key is performing both assessments regularly and measuring progress at every step, said Harris Miller, president of ITAA. Both tools drew from the government's recent experience with self-assessments under the Government Information Security Reform Act (GISRA) of 2000 and the Federal Information Security Management Act (FISMA) of 2002, said Art Coviello, co-chairman of TechNet's Cyber Security CEO Task Force. There, the focus also was on repeated measurements to identify shortcomings and demonstrate improvement or regression, he said.

*Category 4C5* *Academic/Industry/Vendor/Govt efforts*

2003-12-16 **National Science Foundation NSF program secure computer network**

NIPC/DHS

December 15, Government Technology — NSF announces $30 million program. To promote research into more dependable, accountable and secure computer and network systems, the National Science Foundation (NSF) has issued a solicitation for the Cyber Trust program, which expects to fund up to $30 million in awards. The Cyber Trust program will support up to three research center-level efforts as well as single-investigator and team awards, subject to NSF's merit-review process and the availability of funds. The Cyber Trust program is seeking innovative proposals in three broad areas: fundamental research, multi-disciplinary research, and education and workforce development. Fundamental research is needed to advance the state of the art in knowledge and technology about trustworthy computing. This covers such areas as security and privacy models and metrics, evaluation and certification methods, denial-of-service prevention, long-lived data archiving methods, privacy protection, and network and application forensics. Multi-disciplinary research is needed to improve understanding of the social, legal, ethical and economic trade-offs that affect the design and operation of trusted information systems. Additional information is available online:
http://www.nsf.gov/pubs/2004/nsf04524/nsf04524.htm

# 4D Funny / miscellaneous

*Category 4D* *Funny / miscellaneous*

2003-03-24 **Microsoft security advertisement withdrawn South Africa software vulnerable**

NIPC/DHS

ADVERTISING AUTHORITY TELLS MICROSOFT: 'NOT SO FAST THERE'
South Africa's Advertising Standards Association has forced Microsoft to withdraw a magazine ad suggesting that Microsoft's software is now so secure that it has almost made hacking as extinct as the dodo, the wooly mammoth, and the sabre-tooth tiger. A freelance journalist had called attention to the ad and claimed it was untrue because Microsoft software has been shown to have many vulnerabilities. (VNUnet 24 Mar 2003)

*Category 4D* *Funny / miscellaneous*

2003-07-29 **Pentagon DARPA INFOWAR betting assisinations contracts Middle East**

NewsScan

PENTAGON'S ONLINE TRADING MARKET PLAN DRAWS FIRE
The U.S. Defense Department's Defense Advanced Research Projects Agency (DARPA) has plans to set up an online Policy Analysis Market that will allow traders to bet on the likelihood of future terrorist attacks and political assassinations in the Middle East. The bizarre scheme has drawn fire from Senators Ron Wyden (D-Ore.) and Byron Dorgan (D-N.D.). "The idea of a federal betting parlor on atrocities and terrorism is ridiculous and it's grotesque," said Wyden, while Dorgan described the plan as "useless, offensive and unbelievably stupid. How would you feel if you were the King of Jordan and you learned that the U.S. Defense Department was taking bets on your being overthrown within a year?" However, the Pentagon defended the initiative, comparing it to commodity futures markets. "Research indicates that markets are extremely efficient, effective and timely aggregators of dispersed and even hidden information. Futures markets have proven themselves to be good at predicting such things as election results; they are often better than expert opinions." The market would allow traders to deposit money in an account and then use it to buy and sell contracts. If a particular event comes to pass, the bettors who wagered correctly would win the money of those who guessed wrong. (BBC News 29 Jul 2003)

*Category 4D* *Funny / miscellaneous*

2003-09-04 **virus names sophos anna kournikova VBSWGJ**

NewsScan

WHAT'S IN A VIRUS NAME?
Did you ever wonder who's responsible for all those quirky virus names making the news headlines from time to time? There are macho names, like Blaster, Chernobyl and Slammer; cute ones like Birthday, Smile and Teddy Bear; steamy ones like DeepThroat, Hooker and NakedWife; and nonsense names like Klez, Nimda and Yaha. Then, of course there are those names that seem to refer to the virus creator, like Brat, Faker and Slacker. "Sometimes it's obvious what to call a new virus because it's similar to a previous virus, or contains a message inside its code," says Chris Beltoff, security analyst with Sophos. "Other times analysts have to seek inspiration — I remember there was one which was named after the meal a virus analyst had just had." There *are* some rules: researchers are not supposed to name viruses after businesses, brand-name products or celebrities. That's why the Anna Kournikova virus is officially know as VBSWG.J. But sometimes analysts just have to scan those memory banks to come up with something appropriate. Researcher George Smith recalls naming one particularly shoddy virus "Heevahava" after a childhood memory: "I grew up in Pennsylvania Dutch country and a heevahava was the farmhand given the job of holding the bull's pizzle during the collection of semen. Locally, heevahava was used as an insult meaning 'dolt' or 'idiot.'" (Wired.com 4 Sep 2003)