INFOSEC UPDATE 2007

Student Workbook

Norwich University

June 19-20, 2007

M. E. Kabay, PhD, CISSP-ISSMP
Program Director, MSIA & CTO
School of Graduate Studies
Norwich University

mkabay@norwich.edu

01 Introduction

Category 01 Introduction

2007-06-12

WELCOME

Welcome to the 2007 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 and finally CyberTrust, 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 provided invaluable assistance in transferring data from NewsScan, NIPC/DHS reports and other sources into the database and also did the first cut of classification and keyword generation. They enormously improved the coverage of the ield and continued their work with me to expand the database to further sources until they graduated in May 2006. It is difficult to estimate the hundreds of hours of time they saved me. Since their departure, I have not found anyone to replace them but am hopeful that a new crop of students will eventually work with me.

Dr Peter Stephenson is working on getting a grant that will allow the IYIR to be put on a stable footing, with a permanent staff member who can relieve me of the basic data-entry and preliminary cataloguing work. I hope that his efforts will work!

I teach the INFOSEC UPDATE course as a two-day workshop for my graduate students in the Master of Science in Information Assurance at Norwich University every June during their graduate week and then periodically during the year at different institutions as the occasion arises.

The complete IYIR reports are posted on my Web site, although there is usually a lag between the time I teach the course and the time the updates are posted. See the page at < http://www2.norwich.edu/mkabay/iyir > for a list of PDF files you can read on screen, search, or print out at will. The database is also available for download in Access 2002 and Access 2000 formats (both raw and compressed into WinZIP archives) for the full period and for the most recent year.

02 Taxonomy of INFOSEC Issues

Category 02 Taxonomy of INFOSEC Issues

2007-06-12

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 in a course; the current taxonomy is listed in the reports and is used throughout this edition of the IYIR report as well as in the INFOSEC UPDATE course based on the IYIR. The current taxonomy is available as a PDF file from the Web site.

Preparations for the June 2007 graduate course involved reorganization of several sections and addition of several new categories.

____

Code Description

01 Introduction
02 Taxonomy of INFOSEC Issues
03 Sources of Information
04 Copyright
05 Using IYIR
06 The INFOSEC UPDATE Course
07 Acknowledgements
08 About the Editor
10 HEADING: 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 (e.g., skimming)
12 Wiretapping, interception (not jamming; not govt/law enforcement)
12.1 Wiretapping
12.2 Interception
12.3 Injection, man-in-the-middle attacks
13 Data diddling, data corruption, embezzlement
13.1 Data diddling
13.2 Data corruption & destruction
13.3 Embezzlement
13.4 Obsolescence
14 Malware (not ActiveX or Java), security hoaxes
14.1 Viruses
14.2 Worms
14.3 Virus/worms & polymorphism
14.4 Trojans
14.5 Rootkits & back doors
14.6 Bots & botnets
14.7 Logic bombs, time bombs
15 Fraud (not embezzlement), extortion, slamming
15.1 Fraud (e.g., advance-fee, con-games)
15.2 Extortion & blackmail
15.3 Slamming
15.4 Stock fraud (e.g., pump 'n' dump, insider trading)
15.5 Click fraud
15.6 Spam
16 INFOWAR, cyberwar, industrial espionage, homeland security, hacktivism
16.1 Industrial espionage
16.2 Industrial information systems sabotage
16.3 Infrastructure vulnerabilities
16.4 Homeland Security preparations, plans, drills, & government actions
16.5 Military perspectives on cyberwar & battlespace
16.6 Hacktivists, terrorists & state-sponsored attackers

16.7 Disinformation, PSYOP, propaganda
17 Penetration, phreaking, PBX subversion, social engineering
17.1 Penetration
17.2 Web vandalism
17.3 Phreaking, PBX subversion, cramming
17.4 Piggybacking, shoulder surfing
17.5 Social engineering
18 Theft/loss of equipment (laptops, ATMs, computers, cables, network components, media, keys)
18.1 Stolen equipment or media
18.2 Lost or missing equipment or media
18.3 Data disposal & remanence (Dumpster® diving, discarded media)
19 Counterfeits, forgery (including commercial software/music piracy)
19.1 Software piracy
19.2 Music piracy
19.3 Movies / TV piracy
19.4 Books / e-books piracy
19.5 Games piracy
19.6 Counterfeit currency, credit-cards, other negotiable tokens
19.7 Counterfeit legal or business documents
19.8 Plagiarism & cheating
19.9 Counterfeit products (hardware, clothing etc.)
1A Criminal hacker scene (conventions, meetings, testimony, biographies, publications)
1A1 Criminal hacker conventions & meetings
1A2 Criminal hacker testimony in court or committees
1A3 Biographical notes on individual criminals (including arrests, trials)
1A4 Criminal hacker publications
1A5 Criminal hacker organizations
1A6 Criminal hacker psychology & methods
1A7 Hacking contests
1B Pornography, Net-harm, cyberstalking, gambling, online auctions & sales
1B1 Adult pornography
1B2 Child pornography
1B3 Pedophilia, kidnapping, Net-adoption fraud
1B4 Stalking & harassment
1B5 Gambling
1B6 Auctions, sales
1B7 Hate groups
1B8 Traffic in women, slavery
1B9 Hoaxes, urban myths
1C Identity, impersonation, spoofing
1C1 Impersonation
1C2 Identity theft
1C3 Pseudonymity
1C4 Anonymity
1C5 Phishing & pharming
1D Law Enforcement & Forensics (technology, organizations, proposals, litigation, rulings, judgements)
1D1 Organizations, cooperation, treaties for law enforcement
1D2 Technology for law enforcement
1D3 Litigation, legal rulings, judgements (not search & seizure, warrants, wiretaps)
1D4 Government funding for law enforcement
20 HEADING: Emerging Vulnerabilities & Defenses
21 Quality assurance failures including design flaws
21.1 General QA failures
21.2 Security product QA failures
21.3 Embedded processors
21.4 SCADA (supervisory control & data acquisition) systems, vehicle controls
21.5 Robots
21.6 Zero-day exploits
21.7 Proof-of-concept code
22 Availability problems
22.1 Denial-of-service (DoS) attacks
22.2 Distributed DoS (DDos) attacks
22.3 DoS countermeasures
22.4 Accidental availability disruptions (e.g., backhoe attacks)
23 Internet tools
23.1 Java

23.2 JavaScript
23.3 ActiveX
23.4 HTML, XML, browsers
23.5 E-mail, instant messaging, chat
23.6 Web-site infrastructure, general Web security issues
23.7 VoIP
23.8 SMS
23.9 Scripting languages (e.g., PERL, CGI scripts, Python, PHP)
23.A Open-source software
23.B Microsoft programs (e.g., Office, Media Player)
23.C Adobe programs (e.g., PDF, Flash, Dreamweaver)
23.D VPNs (Virtual private networks)
24 Operating systems, network operating systems, TCP/IP problems (alerts & improvements)
24.1 Windows 9x/Me/NT/2K/XP/CE
24.2 Windows VISTA
24.3 UNIX flavors
24.4 TCP/IP, HTTP, DNS, IMS (IP Multimedia System)
24.5 LAN OS & protocols (e.g., CSMA/CA, CSMA-CD)
24.6 Wireless (WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax)
24.7 SWDR (Software-defined radio)
24.8 MAC OS & applications (e.g., QuickTime, itTunes)
24.9 Peer-to-peer networking
24.A Secure processors
24.B Robust systems (hw / sw)
25 Computer remote control & disruption
25.1 Remote control, RATs, reprogramming, auto-updates
25.2 Jamming
25.3 RFI, HERF, EMP/T
26 Automated surveillance (IT & real-world)
26.1 Spyware, Web bugs & cookies
26.2 Adware & scumware
26.3 Keystroke loggers
26.4 Cell/mobile phones tracking, eavesdropping & cameras
26.5 Serial numbers
26.6 RFID tags
26.7 Cameras (real-world)
26.8 GPS, GPS tracking & satellite imagery
27 Security tools
27.1 Vulnerability assessment & penetration testing
27.2 Port scans
27.3 Intrusion detection systems
27.4 Firewalls & other perimeter defenses
27.5 Honeypots
27.6 Honeynets
27.7 Anti-malware
27.8 Anti-phishing
27.9 Anti-spyware
27.A Anti-spam
27.B Multifunction packages
28 Health effects of electronic equipment (phones, screens, etc.)
28.1 Radiation
28.2 Toxic materials
28.3 Heat, fires, explosions
28.4 Distraction
29 Sociology of cyberspace
29.1 Addiction, games & violence
29.2 Cyberdating & cybersex
29.3 Digital divide, Internet access
29.4 Online & electronic voting
29.5 Online legal proceedings
29.6 Flash crowds
29.7 Social networks
30 HEADING: Management & Policy
31 The state of information security & technology
31.1 Surveys, studies
31.2 Audits, GAO reports

31.3 Estimates, guesses, predictions, forecasts, recommendations, commentaries
31.4 New technology with potential security vulnerabilities or implications
32 Censorship, indecency laws, 1st amendment (law)
32.1 Censorship in the USA
32.2 Censorship outside the USA
33 Policies, risk analysis, risk management
33.1 Acceptable-use policies
33.2 Spam, spim, spit, splogs, phish, vish & pharms
33.3 Authorization, access controls, audit trails
33.4 Risk analysis & management
33.5 Data encryption policies
33.6 Outsourcing & offshoring
33.7 Facilities security
34 Net filters, monitoring (technologies & applications)
34.1 Net filter (site & content blocking)
34.2 Usage monitoring, audit trails (employees, children)
34.3 Web-site flagging
35 DNS conflicts, trademark violations (Net, Web)
35.1 Cybersquatting & DNS hijacking
35.2 Trademarks vs DNS
35.3 Politics & management of the DNS
36 Responses to intrusion
37 Education in security & ethics
37.1 Elementary & middle school programs & courses
37.2 High school programs & courses
37.3 Undergraduate programs & courses
37.4 Master's programs
37.5 Doctoral programs
37.6 Industry courses
37.7 Conferences & workshops
37.8 Web sites, online courses
37.9 White papers & reports
37.A Books
37.B Public education & awareness
38 Consumer/employee/individual information, profiling & surveillance (non-governmental)
38.1 Consumer/employee/individual profiling & surveillance (non-governmental)
38.2 Legal trade in personal information
38.3 Industry efforts for protection of personal information
38.4 International agreements on data security, individual privacy, Net law
38.5 EU case law, legislation & regulation concerning data security, individual privacy
38.6 US case law, legislation & regulation concerning data security, individual privacy
38.7 Other case law, legislation & regulation concerning data security, individual privacy
38.8 Law enforcement & privacy rights
38.9 Medical information & HIPAA
38.A Data mining & search engines
40 HEADING: Defensive Technology, Law of E-commerce, Intellectual Property
41 Encryption algorithms, products
41.1 New crypto algorithms
41.2 Crypto algorithm weaknesses
41.3 Brute-force attacks & methods (e.g., rainbow tables, supercomputers)
41.4 New crypto products
41.5 Crypto product implementation flaws
41.6 New cryptanalytic methods
42 Steganography
43 New I&A products (tokens, biometrics, passwords, Kerberos) & applications
43.1 Tokens
43.2 Biometrics
43.3 Passwords
43.4 Kerberos
43.5 Single sign-on
43.6 E-mail authentication (e.g., SPF & SenderID)
43.7 IPv6 & Internet2
45 E-commerce security, digital signature, products, digital cash, e-payments
45.1 PKI (Digital signatures / certificates)
45.2 Digital cash, cash cards
45.3 Micropayments

45.4 E-payments; e.g., credit-cards, e-brokers
45.5 Digital-rights management (DRM); e.g., copy protection, digital watermarks
45.6 Smart cards & other e-commerce security measures
45.7 Sales taxes on Internet commerce
45.8 E-commerce laws
45.9 E-shopping carts
48 Evolution of criminal cyberlaw (not cases or sentences)
48.1 Computer-crime laws (US)
48.2 Computer-crime laws (non-US)
48.3 Cryptography laws & regulations (US)
48.4 Cryptography laws & regulations (non-US)
49 Non-commercial surveillance, counter-terrorism programs (law, jurisprudence)
49.1 US-government surveillance
49.2 Non-US-government surveillance
49.3 Anti-terrorist measures (e.g., public-area or school surveillance)
49.4 Airport & Air Transport security
49.5 Rail, Port & Trucking security
49.6 International border security, passports
49.7 National ID cards/documents; REAL ID
49.8 Background checks & security clearances
49.9 Search & seizure & wiretap laws, warrants, court orders
4A Evolution of civil cyberlaw
4A1 Framing, mashups
4A2 Pointing, linking, deep linking, metatext
4A3 Jurisdiction
4A4 Blocking
4A5 Archives
4A6 Defamation (libel, slander, misrepresentation)
4A7 Spam
4A8 Liability
4A9 Net neutrality
4AA Disintermediation
4B Intellectual property law:
4B1 Copyrights
4B2 Patents & trade secrets
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*

2007-06-12

SOURCES

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 to get permission to quote the superb abstracts written by John Gehl and Suzanne Douglas, original editors of EDUPAGE and then of the daily _NewsScan_ (both no longer published). Their work in the weekly _INNOVATION) was also a significant component of the IYIR until they ceased publication at the end of May 2007.

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

The Daily Reports from what was originally NIPC (National Infrastructure Protection Center) and is now the Department of Homeland Security have proven valuable in supplementing the material at hand. In 2006, the reports were renamed the "DHS Daily Open Source Infrastructure Report" or "DHS Daily OSIR."

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.

Additional sources include various news services including Computerworld, CyTRAP, Federal Computer Week, NewsBites, vendor press releases, SearchSecurity, Dan Swanson's newsletters, ZDNet UK Security News, the newsletters of the Electronic Frontier Foundation (EFF) and Electronic Privacy Information Center (EPIC), and the law summaries of the FindLaw project. I also occasionally find useful pieces in ACM news, WindowsSecrets and the New York Times IT section.

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 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 DHS Daily OSIR is available through < http://www.dhs.gov/xinfoshare/programs/editorial_0542.shtm > and is archived in full at < http://www.gov.com/osd/>.

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

04 Copyright

Category 04 Copyright

2007-06-12

COMPILATION COPYRIGHT

As you can see at the bottom of every page of the IYIR report and the INFOSEC UPDATE, I assert copyright over this presentation (only) of the information my research team and 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. I assert copyright purely to prevent scoundrels from SELLING what is supposed to be available FREE.

05 Using IYIR

Category 05 *Using IYIR*

2007-06-12

REFERENCE AND RE-USE OF IYIR MATERIALS

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

2007-06-12

INFOSEC UPDATE COURSE

The INFOSEC UPDATE course is usually 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 500 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 create 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.

During the course, I mark selected abstracts in the book and draw the students' attention to those to stimulate discussion. Usually my problem then becomes stopping the discussion so we can move to a new topic.

07 Acknowledgements

Category 07 Acknowledgements

2007-06-12

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 then later 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.

The editors of EDUPAGE kindly continued the tradition and have allowed me to include occasional abstracts from their publication.

My colleagues at NCSA / ICSA / TruSecure / CyberTrust Corporation were always supportive and encouraging during the years I continued this work until 2000; I especially thank my favorite curmudgeon, David Kennedy, Director of Resarch for CyberTrust, for many years of continuing friendship.

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

My sincere thanks to my Norwich University research assistants, Karthik Raman, Krenar Komoni, Michael Martell, Chris Aldrich, Josh Durdin and Lofton Newton for their work from 2004 through 2006.

The School of Graduate Studies has generously funded the research assistantships that have permitted the project to progress without imposing total exhaustion on me. Many thanks Thanks to Dr Fred Snow, former Dean of Online Graduate Studies and to Dr Bill Clements, current Dean of Graduate Studies, for their support (moral and financial) in building the research team that made this project easier in the 2004-2006 period. I hope to be able to benefit from the SGS funds for the 2007-2008 season if I can find some good research assistants!

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

2007-06-12

BIOGRAPHY

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 the CV link.

I began programming in assembler at age 15 in 1965. In 1976, I received my PhD from Dartmouth College in applied statistics and invertebrate zoology. Joined a compiler team in 1979 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. Have published over 950 technical papers in operations management and security, a 1996 textbook on security, was Technical Editor of the 4th Edition of the _Computer Security Handbook_ (Wiley, 2002) and am working on the 5th edition with Senior Editor Sy Bosworth and new third editor Eric Whyne. Have 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. Returned to academia full time in July 2001 and am Associate Professor of Information Assurance in the Division of Business & Management at Norwich University, Northfield, VT 05663-1035 USA as well as the Director of the Master's Program in Information Assurance (http://www.msia.norwich.edu/) and of the Bachelor's program in IA (http://www.norwich.edu/academics/business/informationassurance.html).

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

11.1 Data leakage

Category 11.1 Data leakage

2006-01-12 RISKS; http://tinyurl.com/qy29o

PEOPLE'S BANK LOSES TAPE WITH PERSONAL DATA ABOUT 90,000 CUSTOMERS

According to John Christoffersen of Associated Press, "A tape containing the Social Security numbers and other confidential data of 90,000 People's Bank customers was lost recently while en route to a credit reporting bureau, state and bank officials said Wednesday [11 Jan 2006]."

As usual, bank employees cheerfully asserted that there was no reason to be concerned by the loss. "People's has no reason to believe the data has been used inappropriately and has received no reports of unauthorized activity, officials said. Customers do not need to close accounts because the information is not sufficient to allow unauthorized access, the bank said."

Category 11.1 Data leakage

2006-05-04 EDUPAGE; http://chronicle.com/daily/2006/05/2006050401t.htm

OHIO UNIVERSITY EXPOSES PERSONAL DATA FOR ALMOST A YEAR

Officials at Ohio University said that a compromised server exposed personal information on about 300,000 individuals for more than a year. William Sams, CIO and associate provost for information technology at the university, said unusually high traffic tipped off IT staff that there was a problem. After investigation, it was determined that hackers had accessed a server that contained an alumni database that included more than 137,000 Social Security numbers as well as data on donations and amounts. The database did not include credit card information. Sams said the data had been exposed since March 2005. The university is working to notify individuals whose data was exposed and to offer them advice about how to minimize the risk of identity theft. Two people in the database have reported misuse of their personal information. Although one was found to be unrelated to the breach at Ohio University, officials are still trying to determine if the other incident is connected.

Category 11.1 Data leakage

2006-08-25 EDUPAGE; CNET http://news.com.com/2100-1029_3-6109883.html

VERIZON MISTAKENLY E-MAILS CUSTOMER DATA

Verizon Wireless mistakenly e-mailed an Excel spreadsheet containing information on more than 5,200 subscribers to about 1,800 customers of the company. The e-mail was supposed to include an electronic order form for a Bluetooth wireless headset as part of a promotional offer. The Excel file did not contain highly sensitive information such as credit card or Social Security numbers, but it did include names, e-mail addresses, and cell phone models and numbers. Even with such relatively benign information, identity thieves have a head start on committing fraud, according to security experts. James Van Dyke, the principal analyst at Javelin Strategy and Research, noted that a skilled con artist could use the information in the spreadsheet to contact someone on the list, posing as a representative of Verizon, and possibly obtain more sensitive information. A spokesperson from Verizon said the company takes seriously its obligation to protect consumer data and has implemented new measures to prevent a recurrence of this kind of incident. The company also encouraged customers to add passwords to their accounts.

11.2 Unauthorized disclosure

Category 11.2 Unauthorized disclosure

2006-07-07 DHS Daily OSIR; Reuters
http://news.com.com/Navy+probes+data+leak+on+100%2C000+sailors%2C+Marines/2100-1009_3-6091936.html?tag=cd.top

NAVY PROBES DATA LEAK ON 100,000 SAILORS, MARINES.

The Navy said on Friday, July 7, that it was trying to determine how personal information on more than 100,000 Navy and Marine Corp aviators and air crew wound up on a publicly available Website for more than six months. In a fresh case of private information on military personnel being compromised, the full names and social security numbers of both active and reserve members appeared on the Naval Safety Center Website last December. Those affected are believed to include any Navy or Marine Corp aviator who has served during the past 20 years. The same information was also disseminated late last year to Navy and Marine Corps commands on 1,083 program disks mailed out as part of the service's Web Enabled Safety Program. The Naval Safety Center removed the information from the Website on Thursday. The Navy said there was no evidence that any of the disseminated data has been used illegally. The service is notifying those affected and setting up a 24-hour call center. Safety center spokesperson Evelyn Odango said the problem appeared to be an errant file.

11.3 Data theft

Category 11.3 Data theft

2006-05-23 EDUPAGE; New York Times (registration req'd)
http://www.nytimes.com/2006/05/24/washington/24identity.html

VA SLOW IN REPORTING DATA THEFT

The theft of personal data on U.S. Veterans has caused an uproar after federal officials learned that the Veterans Affairs (VA) Department did not disclose the incident until two weeks after it happened. A VA employee took a number of computer disks home, against agency policy, and they were stolen from his home. The disks contained names, Social Security numbers, and other information on 26.5 million veterans; little else of value was taken from the employee's home. The theft occurred on May 3, but VA officials did not notify the Department of Justice or the FBI for two weeks and took several days more to notify affected veterans. Officials from the VA said representatives of the Justice Department and the FBI were very upset at the way the VA handled the situation, costing investigators valuable time to try to identify those responsible. Veterans, too, were disgusted with the VA's delay. The Senate will hold a hearing on the incident, and it is not clear what actions the government will take to address the problems.

Category 11.3 Data theft

2006-06-13 DHS Daily OSIR; Associated Press
http://www.forbes.com/entrepreneurs/feeds/ap/2006/06/12/ap2810729.html

NATIONAL NUCLEAR SECURITY ADMINISTRATION COMPUTERS HACKED; INFO ON 1,500 TAKEN.

Last September, a hacker stole a file containing the names and Social Security numbers of 1,500 people working for the Department of Energy's (DOE) National Nuclear Security Administration (NNSA). The data theft occurred in a computer system at a service center belonging to the NNSA in Albuquerque, NM. NNSA Administrator Linton Brooks said that he learned of the security breach late last September, but did not inform Energy Secretary Samuel Bodman about it. NNSA said he assumed DOE's counterintelligence office would have briefed senior DOE officials. Brooks said the file contained names, Social Security numbers, date-of-birth information, a code where the employees worked, and codes showing their security clearances. A majority of the individuals worked for contractors and the list was compiled as part of their security clearance processing, he said. Tom Pyke, DOE's official charged with cyber security, said he learned of the incident only a few days ago. He said the hacker, who obtained the data file, penetrated a number of security safeguards in obtaining access to the system.

Category 11.3 Data theft

2006-06-20 EDUPAGE; Associated Press http://www.siliconvalley.com/mld/siliconvalley/14863904.htm

HACKING AT OHIO UNIVERSITY LEADS TO STAFF SUSPENSIONS

Following a string of computer breaches at Ohio University, school officials have suspended two IT supervisors--the director of communications network services, and the manager of Internet and systems. The university has suffered five separate incidents since March 2005, including a recent episode that may have compromised as many as 173,000 Social Security numbers. About two dozen individuals have reportedly notified the university that they have been the victims of identity theft in the past year. The two members of the IT staff who were suspended will remain on leave through the conclusion of an investigation into the breaches. Roderick McDavis, president of Ohio University, is also expected to ask the trustees for as much as $2 million to fund improvements to the university's computer security.

McDavis apologized to those affected by the breaches, saying, "We hold ourselves fully accountable."

Category *11.3* *Data theft*

2007-03-29 DHS Daily OSIR; Associated Press http://www.chicagotribune.com/business/ats-ap_business10mar29,0,1556914.story?coll=sns-business-headlines

TJX: AT LEAST 45.7 MILLION CARD NUMBERS STOLEN.

More than two months after first disclosing that hackers accessed customers' financial data from its computers, discount retailer TJX Cos. has revealed that information from at least 45.7 million credit and debit cards was stolen over an 18-month period. In a regulatory filing that gives the first detailed account of the breach initially disclosed in January, the owner of T.J. Maxx, Marshall's and other stores in North America and the United Kingdom also said another 455,000 customers who returned merchandise without receipts had their personal data stolen, including driver's license numbers. TJX spokesperson Sherry Lang said that about 75 percent of the compromised cards either were expired or had data from their magnetic stripes masked, meaning the data was stored as asterisks, rather than numbers. Lang said the extent of the damage may never be known because of the methods used by the intruder. Much of the transaction data was deleted by TJX in the normal course of business between the time of the thefts and the time they were discovered, the filing said, making it impossible to know how many card numbers were obtained.

11.4 Covert channels (e.g., skimming)

Category 11.4 Covert channels (e.g., skimming)

2006-01-04 RISKS

PDF FILES MAY CARRY HIDDEN IMAGES

A colleague recently provided me with a PDF of a presentation he created using Keynote on a Macintosh. I needed to use some photographs from that document in a presentation of my own, so I used pdfimages, a public-domain tool, to extract them. Imagine my surprise when I discovered several images that were not apparent in the original, including logos for Yahoo and MSN, a snapshot of a commercial Web page, and a photograph of some former students.

I have not experimented with random files from the Web, so I don't know what tool is responsible for inserting the inadvertent images in the file, although it seems to be a classic case of using an existing document as a template for a new one. Clearly, however, PDF documents are capable of carrying images that are not visible to the casual user, and thus risk leaking information in the same way as Microsoft Word and Powerpoint.

[Abstract and commentary by Geoff Kuenning]

Category 11.4 Covert channels (e.g., skimming)

2006-08-08 DHS Daily OSIR; Finextra http://finextra.com/fullstory.asp?id=15695

CARD SKIMMERS STEAL FROM COPENHAGEN ATMS.

Three Romanian men have appeared in a Denmark court for creating fake debit cards and stealing cash from ATMs in Copenhagen. The group installed a small skimming device in a credit card reader at a bookshop in Copenhagen, which recorded information from customers' cards. This data was then copied to 'pre-pay' cards which were used at ATMs to steal funds from bank accounts. The gang used the fake debit cards 509 times over three days. In one instance, a suspect was able to withdraw money at the same ATM for nearly two hours.

Category 11.4 Covert channels (e.g., skimming)

2006-11-15 DHS Daily OSIR; Guardian (UK)
http://money.guardian.co.uk/news_/story/0,,1948027,00.html

CASH MACHINES WERE BUGGED WITH MP3S IN SCAM.

A man who used MP3 players to bug cash machines and steal the personal details of unsuspecting bank customers has been jailed for 32 months. The sophisticated technical scam secured data that enabled Maxwell Parsons's accomplices to use cloned credit cards to buy hundreds of thousands of goods in high-street shops. The scheme, put into action before chip and pin cards were introduced, is thought to have been the first of its kind to be used in the UK. Parsons and his team attached MP3 players to the backs of free-standing cash machines in bars, bingo halls, and bowling alleys. The players then recorded customers' data as it was read on their cash cards and transmitted via a telephone line to banks. Technology imported from Ukraine was used to decode the tones from the transactions and turn them into information which could be used to clone new credit cards.

Category 11.4 Covert channels (e.g., skimming)

2007-04-22 DHS Daily OSIR; ABC News
http://abcnews.go.com/WNT/LegalCenter/story?id=3066304&CMP=OTC-RSSFeeds0312

ID THIEVES USE SCANNERS TO 'SKIM' CREDIT CARDS.

Identity thieves have a new tool to steal credit card information -- pocket-sized scanners that allow anyone handling your card to quickly record the personal information stored on it. The Manhattan District Attorney's Office announced Friday, April 20, it has indicted 13 members of an identity theft ring that made more than $3 million worth of illegal purchases. Prosecutors say wait staff in Asian restaurants in Manhattan and along the East Coast were recruited to work as "restaurant skimmers." The skimmers allegedly used small hand-held devices to read and record personal information stored on the card's magnetic strip. The stolen information was then used to make fake cards. There's no way of knowing if a credit card has been skimmed until fraudulent charges are made. The only sure way to protect yourself is to keep your card in sight at all times.

Category *11.4* *Covert channels (e.g., skimming)*

2007-05-09 DHS Daily OSIR; NBC2 (FL) http://www.nbc-2.com/articles/readarticle.asp?articleid=12489&z=3&p=

NEWS GROUP INVESTIGATES CREDIT CARD SKIMMING.

A credit card skimming machine fits inside the palm of your hand and with one swipe can wipe out your bank account. NBC2 investigators in Florida showed how easy it is to purchase a skimmer and how it's used to rip off card holders. The skimmer is a pocket-sized fraud factory that thieves use to steal not only money but also identities. Once the cards are skimmed, all a crook has to do is hook the skimmer up to a computer and it's an instant pay day. The same is true for driver's licenses. When it is scanned, all of the information on the license number pops up. "I've seen cases where driver licenses have credit card info because somebody went behind and erased the data on the driver's license and encoded somebody's credit card information," said Detective Matt Willard. Type the word "skimmer" in a search engine and dozens of Websites come up. One site even sells blank cards and an embossing machine to make them look real. Skimmers sell anywhere from $300 to over $600. Running hotel key cards through skimmers to see if any personal information is stored on them revealed nothing.

Category *11.4* *Covert channels (e.g., skimming)*

2007-05-24 DHS Daily OSIR; Finextra (UK) http://finextra.com/fullstory.asp?id=16961

CARD SKIMMERS LOOT $100,000 FROM WESTPAC ATM USERS.

Australia's Westpac has suspended 900 customer cash cards following the discovery of a skimming device at an ATM in Melbourne. The withdrawals, totaling $100,000, affected approximately 75 customers and have been traced to Toronto in Canada. Westpac is midway through a program to equip all of its ATMs with anti-skimming technology. The "Jitter" system vibrates the card as it enters the ATM and renders the mag-stripe data unreadable. The bank has so far installed the technology at 70 percent of its cash machines nationwide and says incidents of skimming at protected machines has fallen to zero.

12.2 Interception

Category 12.2 Interception

2006-05-23 DHS Daily OSIR; OUT-LAW News http://www.out-law.com/page-6945

WEB CONFERENCING TOOLS CAN EXPOSE DATA.

SecureTest has warned that popular Web conferencing software can be used by hackers to gain direct access to the desktop of any PC on an internal network without detection, provided the hacker can buy the help of a jaded employee. SecureTest reported Monday, May 22, that Web conferencing sidesteps every security barrier an organization may have in place such as PKI, digital signatures, and SSL encryption, and is often not covered by the security policy. The hacker's accomplice need have no technical expertise. Anyone with access to a PC can route information out of the organization undetected. Unlike keylogging or physically downloading data onto a USB key, Web conferencing requires no special equipment or software planting, so it is the type of scam that would succeed where keylogging failed. To carry out a web conferencing attack, the insider logs on to a vendor portal before connecting to a third party conferencing portal. The hacker also connects to the portal, starting the Web conference. The insider allows the hacker to take remote control of his desktop and the hacker can now use the mouse to open files and directories. The discerning hacker can then identify data of interest and extract it.

12.3 Injection

Category 12.3 Injection

2006-10-04 DHS Daily OSIR; Security Focus http://www.securityfocus.com/bid/20308/info

IBM CLIENT SECURITY PASSWORD MANAGER DESIGN ERROR VULNERABILITY.

IBM Client Security Password Manager is prone to a design error that degrades the integrity of client-side Web security. The vulnerability stems from the fact that the Password Manager relies on "Window Title" information as part of the authentication routine it performs on behalf of the user. A malicious Website can establish a Web page that spoofs the same window title that the application expects to map. This will allow authentication to proceed with the hostile site and in turn establish a false sense of security on the part of visitors who use the affected software. Exploiting this issue can help attackers steal user credentials. Other attacks are also possible. Solution: Security Focus is not aware of any vendor-supplied patches for this issue. More information: IBM Client Security:
http://www-307.ibm.com/pc/support/site.wss/document.do?sitestyle=lenovo&lndocid=MIGR-46391
Vendor Home Page: http://www.ibm.com/
Security flaw in IBM Client Security Password Manager: http://www.securityfocus.com/archive/1/447577

Category 12.3 Injection

2007-04-25 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/07/04/25/HNevilwifiaccesspoints_1.html

'EVIL TWIN' WI-FI ACCESS POINTS PROLIFERATE.

Beware of the "evil twin." That's the term for a Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up by a hacker to eavesdrop on wireless communications among Internet surfers. Unfortunately, experts say there is little consumers can do to protect themselves, but enterprises may be in better shape. With the growth in wireless networks, the "evil twin" type of attack is on the rise, said Phil Cracknell, president of the UK branch of the Information Systems Security Association. Such attacks are much easier than others seeking logins or passwords, such as phishing, which involves setting up a fraudulent Website and luring people there, Cracknell said. The growth in the number of Wi-Fi networks poses increasing opportunities for hackers, who can make their networks appear to be legitimate by simply giving their access point a similar name to the Wi-Fi network on the premises.

13.1 Data diddling

Category 13.1 Data diddling

2006-05-10 RISKS

NY CITY POLICE DEPUTY INSPECTOR HACKED POLICE DATABASE

According to the New York Post, a deputy inspector in the NY City Police Department (NYPD) hacked into the NYPD crime statistics database (called the CompStat program) to make his predecessor look bad by inflating old crime statistics and make himself look better by deflating current statistics. Ed Ravin commented in RISKS that "…[T]he Department …. Have stonewalled every outside investigation of this problem, especially the Mayor's Commission to Combat Police Corruption, whose chairman quietly resigned after the NYPD refused to cooperate with the Commission." He added, "The NYPD (and the many police departments worldwide who copy them) have become such slaves of their CompStat system that they spend their effort gaming it rather than doing their jobs and actually reducing crime."

Category 13.1 Data diddling

2006-07-27 EDUPAGE; Chronicle of Higher Education (sub. req'd)
http://chronicle.com/daily/2006/07/2006072702t.htm

STUDENTS HACK PROFESSOR'S ACCOUNT TO CHANGE GRADES

Two California State University at Northridge students have been charged with hacking into a professor's campus network account to change their grades and those of nearly 300 of their classmates. They are also accused of using the professor's credit card to send pizza and magazine subscriptions to the professor's home. Lena Chen and Jennifer Ngan, who confessed to campus police and were subject to the university's disciplinary procedures, now face arraignment on several misdemeanor charges. The two are no longer with the university.

Category 13.1 Data diddling

2006-09-13 DHS Daily OSIR; Associated Press http://abcnews.go.com/US/wireStory?id=2431079

ATM REPROGRAMMED TO DELIVER MORE CASH.

Police are looking for a man who reprogrammed a gas station ATM to give out four times as much money as it should. Surveillance footage shows a man walking into a gas station at 6:17 p.m. EST on August 19, swiping an ATM card, and punching in a series of numbers, breaking the machine's security code. The ATM was reprogrammed to disburse $20 bills but record it was a $5 debit to his account, Virginia Beach Police spokesperson Rene Ball said. He returned a short time later and took out more money. The card was prepaid and can be purchased at several locations, so police are not sure who is behind the theft. No one noticed until nine days later, when a customer told the clerk that the machine was giving out more money than it should.

Category 13.1 Data diddling

2007-05-21 DHS Daily OSIR; Finextra (UK) http://finextra.com/fullstory.asp?id=16944

CYBER SCAMMERS TARGET ACCOUNTS WITH 'ONE CENT DEPOSIT' SCAM.

Online scammers in the U.S. have hit upon a new scam which appears to target validation weaknesses in the private automated clearinghouse system to defraud account holders. Details of the scam have been published by Air Force Link, which tells of an investigation that was launched after a Colorado airman found that his account had been wrongly debited with payments of up to $600. The withdrawals appeared to have been made by an outfit called Equity First. It appears that the scammers had been pinging account numbers until they hit an active account, into which they then deposited a single payment of one cent, and authorized a withdrawal. The automated clearinghouse is used by banks to process large volumes of payroll, credit and debit card transactions, but it also facilitates other types of payments.

13.2 Data corruption & destruction

Category 13.2 Data corruption & destruction

2007-03-20 DHS Daily OSIR; Associated Press
http://www.cnn.com/2007/US/03/20/lost.data.ap/index.html

TECHNICIAN'S ERROR WIPES OUT DATA FOR ALASKA STATE FUND.

While doing routine maintenance work, a computer technician reformatting a disk drive at the Alaska Department of Revenue accidentally deleted applicant information for an oil-funded account and mistakenly reformatted the backup drive, as well. The disk drive contained an account worth $38 billion. The computer foul-up last July would end up costing the department more than $200,000. Nine months worth of information concerning the yearly payout from the Alaska Permanent Fund was gone: some 800,000 electronic images that had been painstakingly scanned into the system months earlier. And the only backup was the paperwork itself--stored in more than 300 cardboard boxes. According to department staff, they now have a proven and regularly tested backup and restore procedure.

14.1 Viruses

Category 14.1 Viruses

2006-02-16 EDUPAGE; http://news.zdnet.com/2100-1009_22-6040681.html

VIRUS WRITERS TURN TO APPLE

A new computer virus that targets the Apple OS X operating system has been identified. Although the malicious code is not sophisticated--it requires users to "download the application and execute the resulting file," according to Apple--and has been labeled a low-level threat by McAfee and Symantec, it may represent the first virus in circulation that attacks users of Apple's operating system. Ray Wagner of Gartner said that the virus is "not really news" except that it is "the first OS X malicious content in the wild that's been noted at this point." The bug spreads primarily by sending itself through Apple's iChat instant messaging program to those on an infected computer's buddy list. Several security firms have updated their threat profiles to include the new virus.

Category 14.1 Viruses

2006-02-27 DHS Daily OSIR; http://www.scmagazine.com/uk/news/article/543503/crossinfect ing-virus-discovered/

CROSS-INFECTING VIRUS DISCOVERED.

The first malware to cross-infect a PC and a Windows wireless pocket device has been discovered, the Mobile Antivirus Researchers Association (MARA) said. The proof-of-concept, file-destroying Trojan automatically spreads from a Win32 desktop to a Windows Mobile Pocket PC. "With the growing use of hand-held devices, this type of virus may become very prevalent in the future. This virus closes the gap between handhelds and desktops," the association said. Jonathan Read of MARA said that previous "crossover" viruses -- "required either Bluetooth on the device and the PC, or the user had to physically transfer the virus on a memory card." But this trojan is the first to use ActiveSync -- a program that synchronizes files and other data between a Windows PC and a Windows Mobile device -- to cross-infect a desktop and hand-held PC. It also is the first crossover malware to infect the PC before attacking the mobile device. Dave Cole, director of Symantec Security Response, said today that he expects hackers to continue to experiment with new platforms, such as mobile devices. He predicts such attacks gradually will become more financially motivated as users increase their reliance on hand-held computers in their daily lives.

Category 14.1 Viruses

2006-03-15 EDUPAGE; http://www.nytimes.com/2006/03/15/technology/15tag.html

RFID SUSCEPTIBLE TO VIRUSES

A group of researchers affiliated with Vrije Universiteit in Amsterdam has discovered a way to spread a computer virus through RFID tags, a scenario most security experts had previously dismissed. The researchers demonstrated that a virus can spread from an infected tag to the scanners and systems that register the tags and to other tags. In an airport, for example, an infected luggage RFID tag can infect airline systems, possibly allowing some luggage to avoid being screened, and can spread to other luggage and other airports. The group called RFID malware "a Pandora's box" of potential problems. Aware of the risks of disclosing a vulnerability, the researchers also offered advice to RFID developers about how to protect their systems. Peter Neumann, computer scientist at research firm SRI International, echoed the researchers' warnings about RFID technology. "It shouldn't surprise you that a system that is designed to be manufactured as cheaply as possible," he said, "is designed with no security constraints whatsoever." Daniel Mullen, president of the Association for Automatic Identification and Mobility, which represents the industry, said companies developing the technology are engaged in an "ongoing dialogue about protecting information on the tag and in the database."

Category 14.1 Viruses

2006-05-30 DHS Daily OSIR;
IDG News Service http://www.infoworld.com/article/06/05/30/78762_HNstaroffice virus_1.html

STAROFFICE HIT BY ITS FIRST VIRUS.

The first virus affecting StarOffice was detected Tuesday, May 30. The virus, named "Stardust," uses macros to attack the office suite from Sun Microsystems. Since the virus has not yet been launched with malicious intent, a teenager hacker may have written it, said Roel Schouwenberg, senior research engineer for Kaspersky Lab. If a user opens a document infected with Stardust, every StarOffice text document, with a ".sxw" extension, or document template, with a ".stw" extension, will be infected. When one of those documents is launched, it opens an adult image hosted on a tripod.com server.

Category *14.1* *Viruses*

2006-08-16 DHS Daily OSIR; TechWorld
http://www.techworld.com/security/news/index.cfm?newsID=6658&pagtype=all

CONSUMER REPORTS GROUP CONDEMNED FOR CREATING 5,500 "TEST" VIRUSES.

A consumer magazine has been condemned for possibly adding to the virus problem by creating a series of "test" viruses just to review anti-virus scanners. In an act that has long been considered technical taboo, U.S.-based consumer affairs organization, ConsumerReports.org, decided to generate 5,500 "test" viruses to run, under lab conditions, against 12 leading anti-virus software products. The organization's own Website describes the methodology used: "To pit the software against novel threats not identified on signature lists, we created 5,500 new virus variants derived from six categories of known viruses, the kind you'd most likely encounter in real life." The organization said it had enlisted the help of Independent Security Evaluators, an external consultancy, to help design the tests and ensure they matched real-world conditions. While the viruses are not expected to pose any threat to companies or individuals, their creation of viruses is still controversial.

Category *14.1* *Viruses*

2007-02-14 DHS Daily OSIR; Sophos
http://www.sophos.com/pressoffice/news/articles/2007/02/fujacks-fix.html

CHINESE POLICE CONSIDER RELEASING HACKER'S PANDA VIRUS FIX.

Sophos has advised computer users to think carefully about how they remedy virus infections, following news that the Chinese police are to release a clean-up program written by the author of the Fujacks worm. According to media reports from China, authorities are planning to issue a fix to the Fujacks worm which turns icons into a picture of a panda burning joss-sticks. Controversially, the utility has been written by Li Jun, the suspect author of the virus. "Hackers and virus writers have shown themselves to be irresponsible and untrustworthy and I certainly wouldn't choose to run their code on my computer," said Graham Cluley, senior technology consultant for Sophos. "Additionally, the Fujacks virus left some infected files unable to run. That hardly suggests that the author took quality assurance seriously when he constructed his malware."

14.2 Worms

Category 14.2 Worms

2006-01-20 DHS Daily OSIR; http://www.techweb.com/showArticle.jhtml?articleID=177102371

NEW WORM CORRUPTS MICROSOFT DOCUMENTS & PDF FILES

A new worm that already accounts for one in every 15 pieces of malicious code carries a "nuclear option" payload that corrupts data in a slew of popular file formats, a security company warned Friday, January 20. The Nyxem.e worm, said Finnish security firm F-Secure, carries code that instructs it to replace data in files with .doc, .xls, .mdb, .mde, .ppt, .pps, .zip, .rar, .pdf, .psd, or .dmp extensions with the useless string "DATA Error [47 0F 94 93 F4 K5]" on the third of the month. This list includes the native document formats for Microsoft Word, Excel, PowerPoint, and Access, as well as for Adobe PhotoShop and Acrobat. Nyxem.e is similar to the VB.bi/Blackmal/MyWife.d worm that climbed the charts earlier last week, added F-Secure. The worm arrives as an attachment to e-mail messages with a variety of subject headlines, many of which tout porn with phrases. It also tries to delete selected security software, and can spread through shared folders as well as by hijacking addresses from infected PCs.

Category 14.2 Worms

2006-01-24 DHS Daily OSIR; http://www.securitypipeline.com/news/177103403

KAMA SUTRA WORM SPOOFS DIGITAL CERTIFICATES.

The Kama Sutra worm can fool Windows into accepting a malicious ActiveX control by spoofing a digital signature, a security company said Tuesday, January 24. Sunnyvale, CA-based Fortinet said the worm -- which also goes by names such as Nyxem.e, MyWife.d, Grew.a, and Blackmal.e -- adds 18 entries to the Windows Registry to slip the ActiveX control by the operating system's defenses. "By creating the following entries, the control is considered 'safe' and digitally signed," said the Fortinet advisory. The ActiveX control, added Fortinet, is used by the worm to automatically run its code each time the PC is turned on and Windows boots. "The threat of worms like this will make them much more dangerous in the future," said Bojan Zdrnja, an analyst for the Internet Storm Center, on the group's site. As of late Monday, January 23, the Kama Sutra worm had infected more than 630,000 systems, said the Internet Storm Center. The worm is considered particularly dangerous because it contains code that triggers an overwrite of all .doc, .xls, .mdb, .mde, .ppt, .pps, .zip, .rar, .pdf, .psd, and .dmp files on the third of each month.

Category 14.2 Worms

2006-01-30 DHS Daily OSIR; http://www.techweb.com/wire/security/177105325

KAMA SUTRA WORM HITS INDIA, PERU HARDEST.

The worm set to overwrite important Microsoft and Adobe documents Friday, February 3, has struck India five times harder than the U.S., and Peru three times harder, a security company claimed. According to Chicago-based LURHQ, the worm -- dubbed Kama Sutra, Blackworm, Blackmal, MyWife, Nyxem, and nearly two-dozen other names -- has infected nearly 80,000 PCs in India. Peru sports almost 55,000 compromised computers. In comparison, the U.S. has about 15,000 machines contaminated with the worm. "Viruses don't always spread uniformly," LURHQ said in its report. "There are many factors at play which are hard to quantitize, such as the initial seeding, social engineering, AV deployment, and random chance. And, as with all statistics, take [these] with a grain of salt." LURHQ tagged the total number of Blackworm-infected computers at around 300,000, even though a Web-based infection counter claims a number in the millions. LURHQ, however, was able to strip out bogus "clicks" on that counter to arrive at is estimate. "An attempt was made by an unknown party to artificially inflate the counter using a set of 279 distributed (presumably compromised) computers," said LURHQ. LURHQ's report: http://www.lurhq.com/blackworm-stats.html

Category 14.2 Worms

2006-02-03 DHS Daily OSIR; http://wireservice.wired.com/wired/story.asp?section=Technology&storyId=1154343

EXPERTS: HYPE MAY HAVE MITIGATED KAMA SUTRA WORM.

Companies and individuals heeded this week's warning about a file-destroying computer worm known as "Kama Sutra," helping minimize its damage Friday, February 3, security experts said. One Italian city shut down its computers as a precaution, but otherwise the worm's trigger date arrived with relatively few reports of problems. Hundreds of thousands of computers were believed to be infected, but security vendors say many companies and individuals had time to clean up their machines following the alarm, carried by scores of media outlets. "The importance of media attention from an awareness and educational standpoint has been a very good thing," said Marc Solomon, director of product management at security vendor management McAfee Inc. "It alerts users to what may have happened and the destruction that could have occurred." David A. Milman, chief executive of the Syracuse, NY-based Rescuecom, said, "the hype was probably what prevented the disaster from happening."

Category 14.2 Worms

2006-02-07 DHS Daily OSIR; http://www.securitypipeline.com/news/179101481

MICROSOFT SAYS KAMA SUTRA WORM OVERBLOWN.

As users and security firms reported little damage done by the Kama Sutra worm, a manager of Microsoft's anti-virus development team warned that overhyping threats could lead to a "cry wolf" syndrome where future alerts aren't taken seriously. "Too much hype in situations that end in false alarms ends up diluting the meaning of warnings for true worldwide threats," wrote Matt Braverman, a program manager with Microsoft's anti-malware team, on the group's blog. In particular, Braverman criticized those who called out warnings based on a Web counter that, though initially reporting the number of Kama Sutra infections accurately, was manipulated later in the process to claim millions of machines had been compromised. Braverman's comments were in sync with earlier positions taken by Microsoft in January on the worm.

Category 14.2 Worms

2006-03-29 DHS Daily OSIR; http://www.eweek.com/article2/0,1895,1944133,00.asp

LATEST BAGLE WORM HAS STEALTH CAPABILITIES

Malicious hackers have fitted rootkit features into the newest mutants of the Bagle worm, adding a stealthy new danger to an already virulent threat. According to virus hunters at F-Secure, of Helsinki, Finland, the latest Bagle.GE variant loads a kernel-mode driver to hide the processes and registry keys of itself and other Bagle-related malware from security scanners. The use of offensive rootkits in existing virus threats signals an aggressive push by attackers to get around existing anti-virus software and maintain a persistent and undetectable presence on infected machines. The Bagle threat started as a simple e-mail executable in 2004 but has grown and evolved over the years to become one of the most active threats against PC users. Security researchers estimate that the numerous Bagle variants have infected more computers than any other virus group.

Category 14.2 Worms

2006-05-22 DHS Daily OSIR; IDG News Service http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9000660

YAHOO MESSAGING WORM INSTALLS BOGUS BROWSER

Malware writers have created a new worm that installs a new browser, plays screeching music and dumps a graphic on the victim's desktop. It starts with a link to a so-called “Safety Browser” apparently sent by a friend in Yahoo Inc.'s instant messaging program. Instant messaging security company FaceTime Communications Inc. described the malware, which it called "yhoo32.explr", as "insidious" in a security advisory Friday, May 19. The bug also hijacks Internet Explorer's homepage, directing users to the Safety Browser's Website.

Category 14.2 Worms

2006-06-30 DHS Daily OSIR; IDG News Service http://www.infoworld.com/article/06/06/30/HNwormmsantipiracy_1.html

WORM APPEARS AS MICROSOFT ANTIPIRACY PROGRAM.

Security analysts have detected a new piece of malware that appears to run as a Microsoft program used to detect unlicensed versions of its operating system. The malware has been classified as a worm and spreads through AOL's Instant Messenger program, said Graham Cluley, senior technology consultant for Sophos. Sophos is calling it W32.Cuebot-K, a new variation in the Cuebot family of malware. After it's installed, the worm immediately tries to connect to two Websites, a sign it may try to download other bad programs on the machine.

Category 14.2 Worms

2006-09-26 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2164996/experts-warn-worm-presents

KASPERSKY LAB WARNS OF 'SEVERE RISK' E-MAIL WORM.

IT security experts have issued a "severe risk" threat warning after detecting a virulent new worm spreading in the wild. Kaspersky Lab warned that Win32.Warezov.at uses its own SMTP engine to send itself to e-mail addresses harvested from the Windows address books on infected machines. The worm runs when the user clicks on the attached file, a portable executable of around 117KB, packed using UPack. The worm copies itself to disk and modifies the registry to ensure that it loads automatically on start up. For further detail: http://www.viruslist.com/en/viruses/encyclopedia?virusid=135921

Category 14.2 Worms

2006-11-20 DHS Daily OSIR; PC Adviser (UK) http://www.pcadvisor.co.uk/news/index.cfm?newsid=7652

SECOND LIFE WORM CAUSES UNREST.

Online gamers were locked out of Second Life Sunday, November 19, after a self-replicating worm planted spinning golden rings throughout the virtual world. The rings caused game servers to slow down, and forced Second Life's creator -- Linden Lab -- to prevent people from logging on. The game was reopened within 25 minutes. Over 1.5 million people have registered to use Second Life, and Linden Lab claims the population is growing by 38 percent every month.

Category 14.2 Worms

2007-02-28 DHS Daily OSIR; Register (UK) http://www.theregister.co.uk/2007/02/28/warezov_skype_im_worm/

WAREZOV WORM FIENDS TARGET SKYPE.

The authors of the prolific Warezov worm are targeting users of Skype. Instead of arriving via an e-mail attachment, the latest variant of the worm spreads using a bogus Skype chat message asking users to click on a link, which points to a hacker-controlled Website hosting malicious codes. The plausibility of the attack is increased because infected messages likely come from a target's list of known contacts, though the abrupt dialogue it generates might trigger a few alarm bells. Some older Warezov variants used other Instant Messaging clients in a similar fashion, but this variant (Warezov-LY) is the first to use Skype, anti-virus firm F-secure reports.

Category 14.2 Worms

2007-03-01 DHS Daily OSIR; Sophos http://www.sophos.com/pressoffice/news/articles/2007/03/toptenfeb07.html

MALWARE ADOPTS DISGUISES IN ATTEMPT TO DUPE IT DEFENSES.

Sophos has revealed the most prevalent malware threats and e-mail hoaxes causing problems for computer users around the world during February 2007. The figures, compiled by Sophos' global network of monitoring stations, show that the HckPk family has had the greatest impact on computer users this month, accounting for more than half of malware seen during February. Hackers are increasingly using encryption and packer tools -- such as those belonging to the HckPk family -- to camouflage their malicious code. January's hardest-hitting worm, Dorf, plus the prevalent Dref mass-mailing worms are just two examples of the malware currently being hidden within HckPk programs. Sophos has also found that cybercriminals are constantly modifying their HckPk disguises in an attempt to bypass IT defenses.

Category 14.2 Worms

2007-04-02 DHS Daily OSIR; InformationWeek
http://www.informationweek.com/news/showArticle.jhtml?ArticleID=198701817

THE NETSKY FAMILY OF WORMS HAD THE BIGGEST IMPACT ON THE INTERNET IN MARCH.

While new malware threats littered the Internet last month, it was a three-year-old worm that caused the most trouble. The Netsky family of worms had the biggest impact in March, according to Sophos. The worms, which first appeared in March of 2004, accounted for one-third of all malware in circulation for the entire month. Overall, Sophos detected 8,835 new threats in March, bringing the total protected against to 231,548. Analysts also found that 0.18% or one in 555 e-mails, was infected with malware, a number that has dropped dramatically over the past year or two. According to Sophos analysts, these numbers indicate that while malware spread via e-mail is still causing trouble, the vectors used to distribute threats are changing. Hackers are continuing their move away from mass-mailing worms in favor of using spam messages with links pointing to infected Web pages. "Since December 2006, we have seen some remarkable changes in the countries hosting the most malware," said Theriault. "China has taken the lead from the United States, but more dramatically, the United Kingdom, which hosted less than 1% in December is now responsible for more than 5%."

Category 14.2 Worms

2007-05-04 DHS Daily OSIR; Government Technology
http://www.govtech.net/magazine/story.php?id=105336

USB WORM TARGETS REMOVABLE MEMORY STICKS TO INFILTRATE BUSINESS.

A warning has been released about a family of worms that spreads by copying itself onto removable drives such as USB memory sticks, and then automatically runs when the device is next connected to a computer. The W32/SillyFD-AA worm hunts for removable drives such as floppy disks and USB memory sticks, and then creates a hidden file called autorun.inf to ensure a copy of the worm is run the next time it is connected to a Windows PC. It also changes the title of Internet Explorer windows to append the phrase "Hacked by 1BYTE." "With USB keys becoming so cheap they are increasingly being given away at tradeshows and in direct mailshots. Marketing people are prepared to use them as 'throwaways' with the aim of securing sales leads," said Graham Cluley, senior technology consultant for Sophos. "Computer owners should tread very carefully when plugging an unknown device into their PC, however, as it could have malicious code planted on it. With a significant rise in financially motivated malware it could be an obvious backdoor into a company for criminals bent on targeting a specific business with their malicious code."

14.3 Virus/worms & polymorphism

Category 14.3 Virus/worms & polymorphism

2006-02-03 EDUPAGE; http://news.com.com/2100-7349_3-6034706.html

EXPECTED DAMAGE FROM KAMA SUTRA WORM DOESN'T MATERIALIZE

The latest high-profile worm making the rounds on the Internet has so far failed to unleash the damage that some had predicted. The Kama Sutra worm, also known as Nyxem.E, MyWife, and Blackworm, was scheduled to attack infected computers on Friday and begin deleting files and causing other headaches for users. However, Paul Ducklin, head of technology at Sophos Asia-Pacific, said there have been no reports of problems so far. Ducklin attributed the lack of consequence to effective efforts by businesses to identify the worm and keep computers from becoming infected. Allan Bell, marketing director for McAfee, echoed Ducklin's remarks. "No local outbreaks reported," he said, "and very few reports of infections." F-Secure's Mikko Hypponen noted, however, that home users are typically much less aware of security threats and therefore much more widely affected by such worms. "The full scope of the problem won't come to light until during the weekend or early next week," he said, when home users turn on their computers.

14.4 Trojans

Category 14.4 Trojans

2006-01-23 DHS Daily OSIR; http://www.businessweek.com/technology/content/jan2006/tc20060123_003410.htm

TARGETED TROJANS ON THE RISE.

It was a stealth cyberattack: Last November 18, an e-mail with a nefarious purpose was dispatched from an Internet address in the Tianjin province of China. The targets: individual employees of the U.S. and European military and pharmaceutical, petrochemical, and legal companies, according to e-mail security firm MessageLabs. Attached was an apparently innocuous Microsoft Word document with a news story from CNN. And it was designed to look like it came from a trustworthy source. In this case, the Trojan was a particularly insidious variety known as a targeted Trojan because it was directed at a specific recipient -- intended to infect the computer networks of American companies. When opened, the Word document could have become a ticking time bomb. Buried inside was special code that would allow hackers to take remote control of each employee's PC. Then, working from inside the corporate networks, the hackers could steal corporate secrets or use the compromised computers to send spam and viruses. According to computer-security experts, spam, phishing e-mails, viruses, and worms will grow more slick and secretive in 2006.

Category 14.4 Trojans

2006-01-23 DHS Daily OSIR; http://www.techworld.com/security/news/index.cfm?NewsID=5219

FOUR NEW TROJANS ON THE LOOSE.

Four new Trojans are on the loose, three aimed at mobile phones and a fourth at PCs, anti-virus companies have warned. The mobile phone worms are disguised as legitimate applications and spread via Bluetooth or multimedia messages and affect phones running Symbian. The computer worm spreads via e-mail and purports to offer pornography. The phone worms -- Bootton.E, Pbstealer.D and Sendtool.A -- have a low infection rate at the moment. The first was spotted last week by F-Secure and Symantec and is perhaps the most potentially crippling of the three to those infected. It restarts the mobile but also releases corrupted components that cause a reboot to fail, leaving the device unusable. Fortunately, the phone worms are unlikely to spread very far. Unlike worms on computers, the Trojan horses hitting cell phones spread as attachments that require users to download them. The PC worm, Nyxem, however, is spreading rapidly and carries a potentially destructive set of instructions. Also nicknamed the Kama Sutra worm, it is programmed to overwrite all of the files on computers it infects on Friday, February 3, said Mikko Hypponen, chief research officer at F-Secure Corp. So far, there's no indication where Nyxem originated.

Category 14.4 Trojans

2006-03-01 DHS Daily OSIR; http://www.securitypipeline.com/news/181401932

MYSTERY OVER PC-TO-MOBILE TROJAN ANNOYS RESEARCHERS.

Anti-virus researchers complained Wednesday, March 1, that a group claiming to have proof of the first PC-to-mobile Trojan hasn't shared the sample, a normal practice among security investigators. Monday, February 27, the Mobile Antivirus Researchers Association (MARA), which bills itself as a non-commercial collection of mobile malware researchers, said it had anonymously received malicious code it dubbed "Crossover." The sample, said MARA, could cross-infect a Windows Mobile Pocket PC from a desktop PC running Windows. According to MARA, the first-of-its-kind Trojan spreads to the mobile device via Microsoft's ActiveSync, then erases all files in the My Documents directory of the Windows CE- or Windows Mobile-based gizmo. But unlike the usual practice where virus researchers share samples, MARA's not willing to let others see the code, no-strings-attached, say some commercial researchers. They're left without a way to confirm Crossover's existence or MARA's claims, or update their own signatures to defend against the attacker.

Category 14.4 Trojans

2006-03-08 DHS Daily OSIR; http://www.informationweek.com/news/showArticle.jhtml?articleID=181502074

SECURITY RESEARCHERS TERMINATE SITES SELLING TROJANS.

Several Websites selling made-to-order Trojan horses to hackers have been shut down, thanks to the cooperation between U.S.-based RSA Security and Spain's Panda Software. The two companies collaborated in the effort to identify, locate, and shutter five sites: three were marketing la carte Trojans and two were sites where the buyers could monitor the infections the malware caused.

Category *14.4* *Trojans*

2006-05-15 DHS Daily OSIR; Computerworld Today (Australia)
http://www2.csoonline.com/blog_view.html?CID=21091

SOCIAL ENGINEERING REPLACES GUNS IN BANK HEISTS

Australia's banking industry is under threat due to a heavy reliance on Single Socket Layer (SSL) encryption that hackers are increasingly finding their way around. There are no "stick-em-up" dramatics in today's million-dollar bank heists, but it simply involves the use of SSL-evading Trojans and refined phishing techniques. Australia's Computer Emergency Response Team (AusCert) says its research proves attacks are on the rise. AusCert general manager Graham Ingram said a false sense of security surrounds SSL encryption. This reliance on Internet browser encryption means banking sessions can be hijacked by Trojans and key-logging programs, especially if users engage in lax security protocols and don't use current anti-virus signatures. The bottom line is that social engineering tricks are circumventing Internet banking encryption. Neal Wise, director of security firm Assurance, said SSL does serve a good purpose but leaves users prone to a "man in the middle"-type attack.

Category *14.4* *Trojans*

2006-05-16 DHS Daily OSIR; TechWeb News http://www.techweb.com/wire/187203724

CYBER-CROOKS TARGET ONLINE GAMERS

Online criminals are targeting gamers with viruses written to steal virtual assets that can be sold to other players, security firm Panda Software said Tuesday, May 16. Cyber-crooks are going after login details needed to install and access online games. Trojans sent through e-mail and chat rooms are the most common forms of malware used in the thefts. Online gaming is a growing multi-billion-dollar business worldwide that offers lots of opportunities for cyber-crooks. Gamers are willing to pay for virtual assets, such as weapons and powers, in order to reach high levels in a game and increase their reputations.

Category *14.4* *Trojans*

2006-07-05 DHS Daily OSIR; TechWeb http://www.darkreading.com/document.asp?doc_id=98493

NEW TROJAN CAN CHANGE IP ADDRESSES.

A new Trojan is on the loose that enables attackers to reroute users to phony Websites -- even when the user types the URL out manually. The Trojan, dubbed DNSChanger.eg, corrupts the process of translating a domain name into an IP address, according to security researchers at security software vendor MicroWorld Technologies, which discovered the vulnerability. The exploit has "high risk potential," the researchers say. When a user types in a URL, the smart Trojan changes the "NameServer" registry key value to a fraudulent IP address. Phishers can design the fraudulent page to look very much like the pages of the site they are defrauding -- such as a bank or retailer -- and fool the user into typing in their account information. "Phishing usually requires you to be lured through emails that lead you to impostor Websites, but this requires nothing of that sort," says Govind Rammurthy of MicroWorld Technologies.

Category *14.4* *Trojans*

2006-07-25 DHS Daily OSIR; Tech World
http://www.techworld.com/security/news/index.cfm?newsID=6507&pagtype=samechan

REPORT: CRYPTO MALWARE CLOSE TO BEING UNCRACKABLE.

File-encrypting Trojans are becoming so complex that the security companies could soon be powerless to reverse their effects, Kaspersky Lab has said in a new report, entitled Malware Evolution: April – June 2006, Hidden Wars. Commonly termed "ransomware," Trojans that encrypt data files on a user's PC before demanding a payment in return for supplying the key to unlock the files, have come from nowhere in recent months to become a measurable problem. Aleks Gostev of Kaspersky Lab raised the alarming possibility that victims could at some point in the near future have their files encrypted in such a way that the security industry would not be able to issue a fix. If this comes to pass -- and Kaspersky's claims that the day is not far off are plausible -- it will mark an important moment for the whole software security industry. To view the report: http://www.viruslist.com/analysis?pubid=191951869

Category *14.4* *Trojans*

2006-10-13 DHS Daily OSIR; CNET News
http://news.com.com/The+future+of+malware+Trojan+horses/2100-7349_3-6125453.html

THE FUTURE OF MALWARE: TROJAN HORSES.

Some of the most dangerous cyberattacks are the least visible ones. Widespread worms, viruses or Trojan horses spammed to millions of mailboxes are typically not a grave concern anymore, security experts said at the Virus Bulletin conference Thursday, October 12. Instead, especially for organizations, targeted Trojan horses have become the nightmare scenario, they said. The stealthy attacks install keystroke-logging or screen-scraping software, and they are used for industrial espionage and other financially motivated crimes, experts said. Cybercrooks send messages to one or a few addresses at a targeted organization and attempt to trick their victim into opening the infected attachment -- typically, a Microsoft Office file that exploits a yet-to-be-patched vulnerability to drop the malicious payload. Security technology can stop common attacks, but targeted attacks fly under the radar. That's because traditional products, which scan e-mail at the network gateway or on the desktop, can't recognize the threat. Alarm bells will ring if a new attack targets thousands of people or more, but not if just a handful of e-mails laden with a new Trojan horse is sent.

Category *14.4* *Trojans*

2006-11-13 DHS Daily OSIR; Information Week
http://www.informationweek.com/story/showArticle.jhtml?ArticleID=193700286

MOBILE DEVICES PROVIDE MORE OPPORTUNITIES FOR MISCHIEF AND THEFT.

Smartphones and similar devices increasingly are being used by business professionals to store information, tap into customer accounts, and exchange data with the office. The expanded use of mobile devices has caught the interest of criminals and malicious hackers, and several proof-of-concept mobile viruses have emerged in recent months. The growth of Microsoft Windows Mobile 5.0 in the device market also creates new security concerns. Windows Mobile 5.0, released to manufacturers in May, offers more and easier ways to exchange information with back-end servers than previous versions, and it's the first Windows operating system to appear on popular Palm devices. Trojan.Wesber, a proof-of-concept virus for Windows Mobile discovered in September, sends messages from a mobile device via the Short Message Service wireless protocol without the device user's consent, similar to the Redbrowser Trojan reported earlier this year. MSIL.Cxover.A, discovered in March, searches for a device connected to a wireless network, then attempts to establish an ActiveSync connection to the device. If successful, the worm copies itself as a file and disconnects the ActiveSync connection. While there haven't been any public reports of data breaches or other incidents resulting from these viruses, they demonstrate hacker interest in mobile devices.

Category *14.4* *Trojans*

2006-11-27 DHS Daily OSIR; Computerworld
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=274599&intsrc=news_ts_head

DEPARTMENT OF DEFENSE REPORT TO DETAIL DANGERS OF FOREIGN SOFTWARE.

A U.S. Department of Defense (DoD) task force early next year plans to warn the Pentagon of a growing threat to national security from adversaries who could insert malicious code in software developed overseas. The Defense Science Board (DSB), a military/civilian think tank within the DoD, will issue a report that calls for a variety of prevention and detection measures but stops short of recommending that all software procured by the military be written in the U.S., said the head of the task force that has been studying the so-called foreign influence issue. The possibility that programmers might hide Trojan horses, trapdoors and other malware inside the code they write is hardly a new concern. But the DSB will say in its report that three forces the greater complexity of systems, their increased connectivity and the globalization of the software industry have combined to make the malware threat increasingly acute for the DOD. Robert Lucky, the chairman of the DSB task force, said this month that all the code the DoD procures is at risk, from business software to so-called mission software that supports war-fighting efforts.

Category *14.4* *Trojans*

2007-03-15 DHS Daily OSIR; Websense
http://www.websense.com/securitylabs/alerts/alert.php?AlertID=752

LARGE CHINESE SITES HOSTING TROJAN EXPLOITS.

There are reports of new malicious Websites, designed to install Trojan horse and Password Stealing malicious code. The Websites are hosted in China and attempt to exploit several Microsoft vulnerabilities to download and install a Trojan downloader without end-user interaction. Among the sites are a popular Chinese book store hosted on Myrice. All sites appear to have been compromised.

Category 14.4 Trojans

2007-04-16 DHS Daily OSIR; ComputerWorld
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9016685&intsrc=hm_list

CLEAR EVIDENCE OF A TWO-PHASE ATTACK PLAN, SAY RESEARCHERS.

The group behind last week's massive Storm Trojan spam blast set up Windows users with a one-two punch by switching tactics in mid-run, making the second stage's subject headings more believable, researchers said Monday, April 16. "There was a very distinct transition point" between the two stages, said Adam Swidler, senior manager of solutions marketing at Postini Inc. "It was a concerted effort to trick users." The huge wave of worm-infected spam e-mails sent out starting early Thursday had receded by about 2 a.m. Pacific Time Friday. "It petered out around then, and spam went back to its average daily and hourly rates," said Swidler. Although most of the attention was paid to the attack's second phase -- when spammed messages arrived with subject headings such as "Worm Alert!" and "Virus Activity Detected!" -- the assault began with less alarming mail marked "Our Love Nest," "A Token of My Love" and other romantic phrases. The switch, speculated Swidler, was by design.

14.5 Rootkits & back doors

Category 14.5 Rootkits & back doors

2006-01-11 DHS Daily OSIR; http://www.betanews.com/article/Symantec_Found_Using_Rootkit_Feature/1137029426

SYMANTEC FOUND USING ROOTKIT FEATURE [NO, IT'S NOT A ROOTKIT]

Symantec is cleaning up a feature in Norton SystemWorks that uses a rootkit-like technique to hide a system folder from Windows. The technology works similar to Sony BMG's controversial rootkit DRM in the way it masks files and makes them invisible to the operating system. The Norton Protected Recycle Bin feature adds a directory called Nprotect, which stores temporary copies of files that users delete. The idea was to supplement the standard Windows Recycle Bin and enable users to recover files they removed accidentally. However, hiding a directory from Windows can open the door to vulnerabilities, as the Sony DRM rootkit debacle exposed. Malware authors were able to write viruses and worms that hid in the cloaked directory, effectively preventing scanning software from discovering their existence on a PC. Users of Norton SystemWorks can download the patch now through LiveUpdate. The rootkit-like activity was discovered by Mark Russinovich of Sysinternals, who first released details on the Sony XCP software.

[MK notes: this article illustrates an improper use of the word "rootkit." It has never meant "stealth" alone. It is specifically used to denote software that allows an attacker to return to a compromised system and regain root privileges.]

Category 14.5 Rootkits & back doors

2006-01-26 DHS Daily OSIR; http://www.securityfocus.com/news/11372

RESEARCHERS: ROOTKITS HEADED FOR BIOS.

Insider attacks and industrial espionage could become stealthier by hiding malicious code in the core system functions available in a motherboard's flash memory, researchers said on Wednesday, January 25, at the Black Hat Federal Conference. A collection of functions for power management, known as the Advanced Configuration and Power Interface (ACPI), has its own high-level interpreted language that could be used to code a rootkit and store key attack functions in the Basic Input/Output System (BIOS) in flash memory, according to John Heasman, principal security consultant for UK-based Next-Generation Security Software. The researcher tested basic features, such as elevating privileges and reading physical memory, using malicious procedures that replaced legitimate functions stored in flash memory. "Rootkits are becoming more of a threat in general -- BIOS is just the next step," Heasman said during a presentation at the conference. "While this is not a threat now, it is a warning to people to look out." The worries come as security professionals are increasingly worried about rootkits. While some attacks have attempted to affect a computer's flash memory, the ability to use the high-level programming language available for creating ACPI functions has opened up the attack to far more programmers.

Category 14.5 Rootkits & back doors

2006-02-17 DHS Daily OSIR; http://www.infoworld.com/article/06/02/17/75492_HNrootkitregulation_1.html

SONY ROOTKIT MAY LEAD TO REGULATION; DHS WORRIED ABOUT POTENTIAL VULNERABILITIES.

A U.S. Department of Homeland Security (DHS) official warned Thursday, February 17, that if software distributors continue to sell products with dangerous rootkit software, as Sony BMG Music Entertainment recently did, legislation or regulation could follow. "We need to think about how that situation could have been avoided in the first place," said Jonathan Frenkel, director of law enforcement policy with the DHS Border and Transportation Security Directorate, who was speaking at the RSA Conference 2006 in San Jose, CA. Last year, Sony began distributing XCP software in some of its products. This digital rights management software, which used rootkit cloaking techniques normally employed by hackers, was later found to be a security risk, and Sony was forced to recall millions of its CDs. While Sony's software was distributed without malicious intent, DHS is worried that a similar situation could occur again, this time with more serious consequences. "It's a potential vulnerability that's of strong concern to the department," Frenkel said. Though DHS has no ability to implement the kind of regulation that Frenkel mentioned, the organization is attempting to increase industry awareness of the rootkit problem.

Category 14.5 Rootkits & back doors

2006-03-13 DHS Daily OSIR; http://www.theregister.co.uk/2006/03/13/virtual_rootkit/

VIRTUAL ROOTKITS CREATE STEALTH RISK.

Security researchers have uncovered new techniques to hide the presence of malware on infected systems. By hiding rootkit software in virtual machine environments, hackers have the potential to avoid detection by security software, experts at Microsoft Research and the University of Michigan warn. Existing anti-rootkit tools commonly rely on comparing file system and API discrepancies to check for the presence of rootkits, a technique that wouldn't be able to unearth virtual machine malware.

Category 14.5 Rootkits & back doors

2006-07-14 DHS Daily OSIR; TechWorld
http://www.techworld.com/security/news/index.cfm?newsID=6453&pagtype=all

INVISIBLE ROOTKIT HERALDS TROUBLE AHEAD.

Security researchers have discovered a new type of rootkit they believe will greatly increase the difficulty of detecting and removing malicious code. The rootkit in question, called Backdoor.Rustock.A by Symantec and Mailbot.AZ by F-Secure, uses advanced techniques to avoid detection by most rootkit detectors. The rootkit is "unique given the techniques it uses," Symantec's Elia Florio wrote in a recent analysis. "It can be considered the first-born of the next generation of rootkits." To read more of Florio's analysis:
http://www.symantec.com/enterprise/security_response/weblog/2006/06/raising_the_bar_rustocka_advan.html

Category 14.5 Rootkits & back doors

2007-02-28 DHS Daily OSIR; CNET News
http://news.com.com/PC+hardware+can+pose+rootkit+threat/2100-7349_3-6162924.html

PC HARDWARE CAN POSE ROOTKIT THREAT.

PC hardware components can provide a way for hackers to sneak malicious code onto a computer, a security researcher warned Wednesday, February 28. Every component in a PC, such as graphics cards, DVD drives and batteries, has some memory space for the software that runs it, called firmware. Miscreants could use this space to hide malicious code that would load the next time the PC boots, John Heasman, research director at NGS Software, said in a presentation at this week's Black Hat event. "This is an important area and people should be concerned about this," Heasman said. "Software security is getting better, yet we run increasingly complicated hardware. Unless we address hardware security, we're leaving an interesting avenue for attack." Malicious code delivered via the memory on hardware components poses a rootkit threat since it will run on the PC before the operating system loads, Heasman said. This likely will hide it from security software and other protection mechanisms, he added. Such low-level malicious code is known as a rootkit.

14.6 Bots & botnets

Category 14.6 Bots & botnets

2006-01-20 DHS Daily OSIR; http://www.techworld.com/security/news/index.cfm?NewsID=5205&Page=1&pagePos=4&inkc=0

HACKER COMPUTER NETWORKS GETTING HARDER TO FIND.

Hacked computer networks, or botnets, are becoming increasingly difficult to trace as hackers develop new means to hide them, says security experts. Botnets are used to send spam, propagate viruses, and carry out denial of service attacks. Extortion schemes are frequently backed by botnets, and hackers are also renting the use of armadas of computers for illegal purposes through Web advertisements, said Kevin Hogan, senior manager for Symantec Security Response. Three or four years ago, it was easier to connect to botnets and estimate the size of one by noting the number of IP addresses on the network, he said. As legislation emerged cracking down on spammers, those who ran botnets started pursuing more clandestine ways to continue their operations. Rather than deter hardcore spammers, it drove them further underground, said Mark Sunner of MessageLabs. Botnets have an ebb and flow similar to biological behavior, Sunner said. Viruses on an infected computer may download new variants in an attempt to evade anti-virus sweeps. Law enforcement authorities have become more adept at tracking down botnet admins. However, the admins have countered by sticking to smaller groups of around 20,000 machines that are less likely to be detected as quickly, Sunner said.

Category 14.6 Bots & botnets

2006-02-08 EDUPAGE; http://www.techworld.com/security/news/index.cfm?NewsID=5326&inkc=0

MCAFEE TACKLES BOTS

McAfee has introduced a new tool designed to defend against bots. Most distributed denial-of-service (DDoS) attacks are carried out by networks of computers running automated programs, or bots, that are controlled centrally. So-called botnets typically consist of thousands of computers hijacked by a hacker who can use them to launch DDoS attacks. Most attacks involve bots sending thousands of incomplete packets to the targeted server, which may be overwhelmed by the traffic. Defending against such attacks is difficult because it is not easy to distinguish legitimate traffic from DDoS traffic, and system administrators do not want to inadvertently block legitimate server requests. McAfee said that its new system, called Advanced Botnet Protection, is able to identify traffic that consists of incomplete packets, allowing network operators to separate malicious botnet traffic and avoid DDoS attacks.

Category 14.6 Bots & botnets

2006-03-02 DHS Daily OSIR; http://www.eweek.com/article2/0,1895,1933210,00.asp

HUNT INTENSIFIES FOR BOTNET COMMAND AND CONTROLS.

A group of high-profile security researchers, which includes international representatives from anti-virus vendors, ISPs, educational institutions and dynamic DNS providers, is ramping up efforts to find and disable the command and control infrastructure that powers millions of zombie drone machines, or bots, hijacked by malicious hackers. The idea is to open up a new reporting mechanism for ISPs and IT administrators to report botnet activity, especially the command and control system that remotely sends instructions to botnets. "If that command-and-control is disabled, all the machines in that botnet become useless to the botmaster. It's an important part of dealing with this problem," said Gadi Evron, a botnet hunter who serves in Israel's Ministry of Finance. Over the last year, the group has done its work quietly on closed, invite-only mailing lists. Now, Evron has launched a public, open mailing list to enlist the general public to help report botnet command and control servers. The new mailing list will serve as a place to discuss detection techniques, report botnets, pass information to the relevant private groups and automatically notify the relevant ISPs of command and control sightings.

Category 14.6 Bots & botnets

2006-03-16 DHS Daily OSIR; http://www.finextra.com/fullpr.asp?id=8488

FACETIME IDENTIFIES NEW IM BOTNET THREAT.

Research experts at FaceTime Security Labs identified and reported a new threat Thursday, March 16, affecting instant messaging applications. Acting on an anonymous tip, researchers have uncovered two botnet networks that collectively represent up to 150,000 compromised computers, one of which is being used as a vehicle to fraudulently scan desktop and back-end systems to obtain credit card numbers, bank accounts, and personal information, including log-ins and passwords. The operators could potentially launch these scans from any computer on the botnet to mask their actual location. With this new threat, FaceTime has identified more than 40 unique files -- many designed to take advantage of social engineering techniques, stored passwords, auto-complete data and vulnerable payment systems.

Category 14.6 Bots & botnets

2006-04-05 DHS Daily OSIR; http://www.gcn.com/online/vol1_no1/40334-1.html

TRENDS IN BOTNETS: SMALLER, SMARTER.

Some recent statistics on e-mail traffic provide more evidence of the trend toward smarter, more targeted online attacks. Botnets -- networks of compromised computers taken over by spammers and hackers -- are getting smaller. Rather than hundreds of thousands of zombie computers spitting out unwanted e-mail and malicious code, they now consist of tens of thousands. "They stay under the radar for longer," said MessageLabs chief technology officer Mark Sunner. "The return is still equal, if not greater, because the attacks are more targeted." Sunner said he expects continued refinement in attacks to be the distinguishing trend this year for spammers, hackers and purveyors of malicious code.

Category 14.6 Bots & botnets

2006-05-15 DHS Daily OSIR; Register (UK)
http://www.theregister.co.uk/2006/05/15/google_adword_scam/

BOTNET IMPLICATED IN CLICK FRAUD SCAM

Botnets are being used for Google Adword click fraud, according to security watchers. The SANS Institute has uncovered evidence that networks of compromised PCs are being used to click on banner ads, generating revenue for unscrupulous publishers. Pay-per-click schemes such as Google Adsense have programs to detect fraudulent clicks and suspend publishers implicated in click fraud. In an effort to disguise bogus visits, these publishers have begun hiring botnets to slip under the radar of fraud detection programs.

The SANS Institute findings: http://isc.sans.org/diary.php?storyid=1334

Category 14.6 Bots & botnets

2006-06-15 DHS Daily OSIR; CNET News http://news.com.com/2102-7349_3-6084317.html

ONLINE THREATS OUTPACING LAW CRACKDOWNS.

Authorities are cracking down on phishing and botnets, but the threats are advancing, representatives from the U.S. Department of Justice (DOJ) and the U.S. Air Force Office of Special Investigations said at the Computer Security Institute's NetSec event. Jonathan Rusch of DOJ said almost 17,500 phishing Websites were reported to the Anti-Phishing Working Group in April. Increasingly, phishers use Trojan horses that pack backdoors, screen grabbers, or keystroke loggers to capture log-in names, passwords, and other information, he said. In April, there were 180 unique examples of such malicious code. Wendi Whitmore of the Air Force Office of Special Investigations, said "Botnets are one of the greatest facilitators of cybercrime these days. Really the cybercrime arena is wrapped around botnets." Meanwhile, bot masters are getting smarter about hiding. Today, most botnets are controlled using Internet Relay Chat, or IRC, servers, and channels. Soon that could become instant messaging, peer-to-peer technology, or protocols used by Internet phone services such as Skype or Vonage, Whitmore said. Whitmore expects cybercrooks to maintain smaller botnets with the hope of staying under the radar.

Category 14.6 Bots & botnets

2006-09-07 DHS Daily OSIR; Register (UK) http://www.theregister.co.uk/2006/09/07/wiki_exploit/

HACKERS ARE EXPLOITING VULNERABILITIES IN WIKI SOFTWARE.

Software bugs in Pmwiki and Tikiwiki software applications are being actively used to create botnets, the SANS Institute's Internet Storm Center reports. The Pmwiki exploit can only be exploited where the "Register_globals" attribute is enabled. However, the Tikiwiki exploit can be exploited regardless of this setting. As well as loading an IRC bot that connects to different channels to access to Undernet IRC servers, attackers are also loading a variety of other exploits and attack tools on the compromised machines. Alongside Perl flood scripts, useful for launching denial-of-service attacks, exploits for both 2.4 and 2.6 Linux kernels are also being loaded onto vulnerable machines.

Category 14.6 Bots & botnets

2006-09-19 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/06/09/19/HNnewaimworm_1.html

NEW AIM WORM MAY PROVE DIFFICULT TO FIGHT.

A sophisticated computer worm spreading via AOL Instant Messenger (AIM) is setting up a botnet that may be difficult to combat, security researchers said. The worm, known as W32.pipeline, propagates when AIM users click on a Web link that appears to have been sent to them by someone on their buddy list. If the recipient clicks on the link, an executable file that looks like a JPEG will download into a Windows folder, according to researchers at security company FaceTime Communications Inc. The file can then execute a number of different attacks. It can open up the e-mail port on the PC and send out spam messages. It can also install a variant of the "hacker defender" rootkit. One of the most dangerous aspects of the worm is that it can also connect to remote file upload sites. Once a computer is infected, the program will propagate using the same instant messaging method.

Category 14.6 Bots & botnets

2006-10-12 DHS Daily OSIR; Security Focus http://www.securityfocus.com/brief/328

SPYING ON BOT NETS BECOMING HARDER.

The workings of bot nets will become more difficult to divine in the future, because the people who control the networks are moving away from using Internet Relay Chat rooms to link the compromised computers together, a security researcher told attendees at the Virus Bulletin 2006 conference. José Nazario, a senior security researcher for Arbor Networks, spent more than six months delving into the chat rooms typically used by bot herders as the central command posts for their compromised networks. The research, which was part of a project dubbed "Bladerunner," used a mock bot that Nazario and an intern at Arbor coded using Python. The researchers found that the command and control channels are increasingly becoming encrypted and are increasing moving away from chat rooms to Web servers.

Category 14.6 Bots & botnets

2006-10-24 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2036439,00.asp

MICROSOFT: TROJAN, BOT INFECTIONS HIGH; ROOTKITS LOW.

New statistics from Microsoft's anti-malware engineering team have confirmed fears that backdoor Trojans and bots present a "significant" threat to Windows users. However, according to data culled from the software maker's security tools, stealth rootkit infections are on the decrease, perhaps due to the addition of anti-rootkit capabilities in security applications. The latest malware infection data, released at the RSA Europe conference in Nice, France, covers the first half of 2006. During that period, Microsoft found more than 43,000 new variants of bots and backdoor Trojans that control millions of hijacked Windows machines in for-profit botnets. Of the 4 million computers cleaned by the company's malicious software removal tool (MSRT), about 50 percent contained at least one backdoor Trojan. While this is a high percentage, Microsoft notes that this is a decrease from the second half of 2005. During that period, the MSRT data showed 68 percent of machines cleaned by the tool contained a backdoor Trojan. Despite increased industry interest in Windows rootkits in 2005, Microsoft found a surprising 50 percent reduction in the attacks, which employ stealthy tricks to maintain an undetectable presence on infected computers. "This is a potential trend that will bear watching," the report said.

Category 14.6 Bots & botnets

2007-01-07 DHS Daily OSIR; New York Times
http://www.nytimes.com/2007/01/07/technology/07net.html

ATTACK OF THE ZOMBIE COMPUTERS IS GROWING THREAT.

With growing sophistication, botnets are being blamed for the huge spike in spam that bedeviled the Internet in recent months, as well as fraud and data theft. Security researchers have been concerned about botnets for some time because they automate and amplify the effects of viruses and other malicious programs. What is new is the vastly escalating scale of the problem -- and the precision with which some of the programs can scan computers for specific information to drain money from online bank accounts and stock brokerages. Although there is a wide range of estimates of the overall infection rate, the scale and the power of the botnet programs have clearly become immense. In recent years, botnet attacks have increasingly become endemic, forcing increasingly stringent security responses. “It represents a threat but it’s one that is hard to explain,” said David J. Farber, a Carnegie Mellon computer scientist who was an Internet pioneer. “It’s an insidious threat, and what worries me is that the scope of the problem is still not clear to most people.”

Category 14.6 Bots & botnets

2007-02-08 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2092435,00.asp

BOTNET STALKERS SHARE TAKEDOWN TACTICS AT RSA.

A pair of security researchers speaking at the ongoing RSA Conference Wednesday, February 7, demonstrated their techniques for catching botnet operators who use secret legions of infected computers to distribute malware programs and violent political propaganda. The botnet experts, both of whom are employed by anti-malware software maker FaceTime Communications, detailed how they identified and pursued individuals believed to be responsible for running a pair of sophisticated botnet schemes, which have been subsequently shut down or significantly scaled back. Addressing a packed room of conference attendees, Chris Boyd and Wayne Porter offered a rare inside glimpse into the world of botnet herders, which the researchers entered by hanging out on the shady online bulletin boards and chat relays where the schemers meet to share the tricks of the trade and their malware programs. By luring the prolific scammers to offer details about their work, and spying on the criminals, the researchers claim to have pieced together the identities of several of the unsavory individuals and helped take down their networks of subverted machines.

Category 14.6 Bots & botnets

2007-03-07 DHS Daily OSIR; SC Magazine http://scmagazine.com/us/news/article/642351/irc-bot-growing -threat-enterprise-networks/

IRC BOT A GROWING THREAT TO ENTERPRISE NETWORKS.

A new Internet relay chat (IRC) bot is building an even larger zombie family that could pose a significant threat to enterprise networks, security researchers said Wednesday, March 7. The Nirbot family is based on relatively new code and spreads after receiving instructions from the botmaster inside an IRC channel, said Jose Nazario, of Arbor Networks. The bot attempts to exploit patched vulnerabilities in Symantec anti-virus programs and the Microsoft server service function. More dangerous for enterprises, though, is that the bot preys on password weaknesses in Windows file-sharing networks, researchers said. Once launched, the bot joins the IRC server and can download arbitrary code, unleash DDoS attacks or launch an HTTP or FTP server to browse an infected PC for sensitive files, he said.

Category 14.6 Bots & botnets

2007-03-19 DHS Daily OSIR; Government Computer News http://www.gcn.com/online/vol1_no1/43339-1.html

HACKERS BECOME MORE PROFESSIONAL.

An analysis of Internet-based threats by Symantec Corp. shows that hacking continued its two-year trend toward criminalization in the last half of 2006, with data theft fueling a thriving underground economy. The United States has the highest number of command and control computers driving these bot networks, with 40 percent late last year, and the U.S. government is a primary source of data breaches. Agencies accounted for 25 percent of reported exposures of personal data. The number of infected computers used in malicious botnets increased by 29 percent in the last half of 2006 to just more than six million, but the number of command and control servers dropped by 25 percent. Symantec speculates that this is because the networks are consolidating. These fewer but larger networks also are becoming more interoperable, using suites of malicious code that can cooperate with each other. An initial compromise can be followed up with a variety of malicious tools that allow the user to exploit a computer, making the networks more dangerous and more valuable.

Category 14.6 Bots & botnets

2007-04-12 DHS Daily OSIR; InformationWeek http://www.informationweek.com/software/showArticle.jhtml

GOOGLE DISSECTS A CLICKBOT, AND DISCUSSES THE COST OF CLICK FRAUD.

Over the past year, Google has been reaching out to the media and the public to allay fears that click fraud represents a serious threat to its business. Its executives have repeatedly said the problem is under control and not significant for Google. On Tuesday, April 11, Google published "The Anatomy of Clickbot.A," an analysis of malicious software used to commit click fraud. Despite Google CEO Eric Schmidt's past insistence that click fraud is "immaterial," the paper argues that more needs to be done to protect search engines and computers in general against botnet attacks. "We believe that it is important to disclose the details of how such botnets work to help the security community, in general, build better defenses," the paper states, adding that Google identified and invalidated all the clicks originating from the Clickbot.A botnet in question. The particular Clickbot.A botnet described in the paper consisted of 100,000 machines when analyzed in June 2006. The Clickbot.A software was designed to conduct "a low-noise click fraud attack against syndicated search engines."
Anatomy of Clickbot.A: http://www.usenix.org/events/hotbots07/tech/full_papers/daswani/daswani.pdf

Category 14.6 Bots & botnets

2007-05-02 DHS Daily OSIR; Internetnews.com
http://www.internetnews.com/security/article.php/3675331

BOTNET EXPEDITION REVEALS CORPORATE WEAKNESSES.

It has long been assumed that corporate computers are relatively free of bots, pieces of malicious code hidden on a computer without the owner's knowledge to perform spamming or other undesirable activities. Support Intelligence (SI), a network security company in San Francisco, has been running what it called "30 Days of Bots," featuring corporate networks infected with spam-churning bots. It began analyzing data in February, monitoring 10,000 domains that plow data into a trap much like a fishnet, except the intelligence in the data is designed to determine what information to keep by looking for spam. Forrester Research security analyst Natalie Lambert said in an e-mail to internetnews.com: "Enterprises do not have the necessary protections in place to mitigate today's threat landscape. Enterprises need full-suite solutions that include anti-malware, personal firewalls and some sort of behavior detection." SI CEO Rick Wesson said the worst offenders are ISPs, followed by university networks. But beneath the ISPs, SI began finding corporate IP addresses in its fishing.

14.7 Logic bombs, time bombs

Category 14.7 Logic bombs, time bombs

2006-06-09 DHS Daily OSIR; Fine Extra (UK) http://www.finextra.com/fullstory.asp?id=15420

DISGRUNTLED UBS IT WORKER ACCUSED OF UNLEASHING LOGIC BOMB ON BANK NETWORK.

A U.S. court has heard how a former IT worker for UBS allegedly unleashed a "logic bomb" computer virus on the bank's network because he was unhappy with his bonus payment. But not only has Roger Duronio, 60, of New Jersey been charged with using the logic bomb to cause more than $3 million in damage to the computer network at UBS's stockbroking unit Paine Webber, he has also been charged with securities fraud for his failed plan to drive down the company's stock with activation of the logic bomb. Duronio resigned from the company on February 22, 2002, and on March 4, 2002, his program activated and began deleting files on over 1000 of UBS PaineWebber's computers. Around 17,000 UBS traders across the U.S. were unable to trade shares for more than a day because of the damage.

15.1 Fraud (e.g., advance-fee, con-games)

Category 15.1 Fraud (e.g., advance-fee, con-games)

2006-01-18 EDUPAGE; http://www.nytimes.com/2006/01/18/technology/18data.html

ONLINE BROKER TO COVER FRAUD LOSSES

Online stock broker E*Trade has announced a "zero liability" policy in which it will cover all losses resulting from online fraud. Although some other online brokerage firms said they have absorbed some or all of the costs of fraud in past incidents, E*Trade becomes the first to establish such a policy. Losses due to fraud in the online brokerage industry remain relatively small and are a fraction of losses to credit card fraud, but the number of data breaches is rising. Moreover, when people are victimized through brokerage fraud, they are harmed "to the tune of hundreds of thousands of dollars," according to Gerri Walsh, acting director of the Securities and Exchange Commission's Office of Investor Education. Officials at E*Trade said they expect other brokers will follow suit and implement similar policies, bringing the entire industry to a level similar to that of credit card companies. A federal law passed in the 1970s requires issuers of credit cards to limit customer liability to $50, but most issuers cover all losses.

Category 15.1 Fraud (e.g., advance-fee, con-games)

2006-03-02 DHS Daily OSIR; http://www.wired.com/news/technology/0,70320-0.html?tw=rss.technology

FCC PROBES CALLER-ID FAKERS.

Last week the Federal Communications Commission (FCC) opened an investigation into the caller-ID spoofing sites -- services that began popping up late 2004, and have since become a useful tool for private investigators, pranksters and more than a few fraud artists. A seven-page demand from the FCC's enforcement bureau sent to one such service, called TeleSpoof, says the commission is investigating whether the site is violating the federal Communications Act by failing to send accurate "originating calling party telephone number information" on interstate calls. A copy was also sent to VoIP service provider NuFone. The FCC is demanding business records from both companies, as well as the name of every customer that has used TeleSpoof, the date they used it and the number of phone calls they made.

Category 15.1 Fraud (e.g., advance-fee, con-games)

2006-05-29 DHS Daily OSIR;
BusinessWeek http://www.businessweek.com/magazine/content/06_22/b3986093.htm

UKRAINIAN CYBERCRIMINAL RELEASED BECAUSE OF POLITICIANS' CHARACTER REFERENCES

Dimitry Ivanovich Golubov was arrested last July for his involvement in credit card fraud and U.S. law enforcement officials hailed it as a big break in their fight against cybercrime. Subsequently, in January 2006, the U.S. Attorney's office charged Golubov with a number of cybercrimes, including credit card fraud. U.S. Postal Inspection Service senior investigator Gregory S. Crabb, who worked with Ukrainian authorities on their case, says Golubov and others controlled the numbers, names, and security codes attached to credit cards. Low-level criminals would use that to load up fake cards and withdraw cash from automated teller machines or buy merchandise. But last December, Golubov's story took a bizarre twist. Two Ukrainian politicians vouched for Golubov's character in court, and the judge released Golubov. "Chat from the carding community" indicates Golubov may be back in business, says Crabb. His story portrays a picture of organized gangs of young, mostly Eastern European hackers who are growing more brazen about doing business on the Web. They meet in underground forums with names like DarkMarket.org and theftservices.com to trade tips and data and coordinate scams that span the globe.

Category 15.1 Fraud (e.g., advance-fee, con-games)

2006-07-06 DHS Daily OSIR; Plain Talk (SD) http://www.plaintalk.net/stories/07062006/localnews_20060706 021.shtml

FOILED SCAMS TOP $1 MILLION FOR FIRST NATIONAL BANK.

First National Bank South Dakota has helped stop $1,130,397.23 in fraud for its customers so far in 2006. The counterfeit and fraud checks were received by bank customers and either turned in or caught by the alert staff at the bank. The bank's security officer, Lee Gass, said "What we've stopped at the bank so far this year comes from Nigerian scams, Internet sales schemes, fake lottery winnings,' and various other types of fraud..." To keep staff on alert, Gass regularly notifies all staff of reported fraud throughout the U.S. Almost on a daily basis, he relays alerts to the staff about counterfeit bank checks, cashiers checks, and other false monetary exchanges. There can be as many as six of these alerts a day, and some of these strike very close to home.

Category 15.1 Fraud (e.g., advance-fee, con-games)

2006-08-13 DHS Daily OSIR; Associated Press http://www.washingtonpost.com/wp-dyn/content/article/2006/08/13/AR2006081300302.html

RELIGION-RELATED FRAUD GETTING WORSE.

Randall W. Harding donated part of his wealth to the Crossroads Christian Church in Corona, CA. In his business dealings, he named his investment firm JTL, or "Just the Lord." Pastors and churchgoers entrusted their money to him. By the time Harding was unmasked as a fraud, he and his partners had stolen more than $50 million from their clients, and Crossroads became yet another cautionary tale in what investigators say is a worsening problem plaguing the nation's churches. Billions of dollars have been stolen in religion-related fraud in recent years, according to the North American Securities Administrators Association. Typically, a con artist will target the pastor first, by making a generous donation and appealing to the minister's desire to expand the church or its programs, according to Joseph Borg, director of the Alabama Securities Commission, who played a role in breaking up the Greater Ministries scam.

Category 15.1 Fraud (e.g., advance-fee, con-games)

2006-09-01 DHS Daily OSIR; DM News (NY) http://www.dmnews.com/cms/dm-news/legal-privacy/38117.html

FTC BUSTS USPS JOB SCAM.

An operation accused of selling worthless prep materials for U.S. Postal Service (USPS) jobs that didn’t exist will pay $105,000 to settle Federal Trade Commission (FTC) charges that the scam violated federal law. The FTC charged that the operation misrepresented an affiliation with the USPS, the availability of postal jobs, and that a passing score on a postal entrance exam guaranteed applicants a job. The FTC alleged that the defendants -- Jeffrey Charles Lord and his company, Job Resources Inc. -- ran classified ads across the nation in employment guides and newspapers. The ads led consumers to believe that the defendants were hiring for postal jobs and were connected with, or endorsed by, the USPS, the FTC alleged. Consumers were charged a “registration fee” of $108.80.

Category 15.1 Fraud (e.g., advance-fee, con-games)

2006-10-25 http://www.finextra.com/fullstory.asp?id=16073

CUSTOMERS STEAL FROM MALFUNCTIONING ATM

In Bristol, England, hundreds of people [who presumably perceived themselves as honest] lined up to steal money fromn a malfunctioning automatic teller machine (ATM) that was dispensing twice the amount of cash requested. Bank officials noted that they had records of everyone who withdrew the "free" money. [MK adds: anyone without the funds to cover the extra withdrawal would likely be charged with criminal fraud.]

Category 15.1 Fraud (e.g., advance-fee, con-games)

2006-11-08 DHS Daily OSIR; This Day (Africa) http://www.thisdayonline.com/nview.php?id=62683

CYBERCRIME GROUP WARNS BANKS AGAINST HACKERS.

Coordinator of the Nigerian Cybercrime Working Group, Basil Udotai, has disclosed that the consolidation of banks has made them vulnerable to on-line crimes. Udotai said the increase in the capital base of banks had enlisted them among the big financial houses in the world, making targets of high level on-line hackers. Udotai said the hackers invest a lot of money to buy communication equipment for high level crimes and only big banks attract their interest. Aome of the banks had already brought complaints of Website cloning by unknown persons and the risks would keep increasing as their investments continue to grow. He stressed the need for all banks to build a "virtual center" where they would be sharing information from time to time instead of hoarding facts for fear of competition. The center for sharing information must be based on a framework of "readiness, responsiveness, and resilience "and the benchmarking of global best practices in checking hackers. Access banks, UBA, Diamond bank, and Skye bank agreed to endorse a synergy known as FinCERT Nigeria project to take pro-active measures against hackers.

Category 15.1 Fraud (e.g., advance-fee, con-games)

2007-01-10 DHS Daily OSIR; Cleveland Plain Dealer http://www.cleveland.com/printer/printer.ssf?/base/news/116843010895130.xml&coll=2

THE LATEST ONLINE SCAM: PUPPIES.

The "puppy scam," is one of the newest tricks among Internet scam artists, said Sue McConnell of the Better Business Bureau of Cleveland. Victims are lured to Websites offering rare dog breeds at affordable prices. Photos and text are often stolen from Websites of legitimate breeders, McConnell said. The puppy purchaser is told to wire payment in advance, and the seller continues soliciting money until the buyer gives up. By then, however, the money is irretrievable. The cases are often reported to the FBI or Internet crime investigators, McConnell said. But most of these scam artists typically operate overseas, and the anonymity of the Internet makes these cases nearly impossible to solve, she said. Blogs and message boards are filled with posts from victims, alerting others to variations of the puppy scam. TerrificPets.com, which matches prospective buyers with breeders, keeps a running list of suspected scammers who have tried to use the site.

Category 15.1 Fraud (e.g., advance-fee, con-games)

2007-01-25 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2173418/official-accused-paying-419

U.S. OFFICIAL ACCUSED OF PAYING 419 SCAMMER $1.2 MILLION.

A former treasurer of Alcona County in Michigan has been arrested after allegedly investing more than $1.2 million of county funds in Nigerian fraud scams. Sophos said that Thomas Katona, who was treasurer of Alcona County for 13 years, has been charged with forgery and multiple counts of embezzlement. It is reported that county treasury employees became suspicious of Katona's dealings after local bank officials informed them that he had directed several unauthorized transfers to overseas accounts during late 2006, including to beneficiaries linked with Nigerian 419 scams. It was then uncovered that he had made further payments using his personal savings, and had previously been advised by bank officials that he was investing money in fraudulent schemes.

15.2 Extortion & blackmail

Category 15.2 Extortion & blackmail

2006-01-18 DHS Daily OSIR; http://news.ft.com/cms/s/cd05a42c-87c6-11da-8762-0000779e234 0.html

HACKERS BLACKMAIL WEBSITE

The FBI is investigating the hijacking of a Website that hosts micro-advertisements by hackers who demanded a ransom to restore the site. Alex Tew of Britain was sent a demand for US$50,000 by e-mail by a hacker, believed to be Russian. When he refused, the Website crashed. Tew first received a threat on January 7 from a body calling itself The Dark Group, demanding $5,000. He thought the blackmail was a hoax and took little notice. However, on Wednesday, January 18, when Tew reached his goal of earning $1 million, the hackers intensified their attack and hijacked the Website.

Category 15.2 Extortion & blackmail

2006-03-13 DHS Daily OSIR; http://www.eweek.com/article2/0%2C1895%2C1937408%2C00.asp

CRYZIP TROJAN ENCRYPTS FILES, DEMANDS RANSOM.

Virus hunters have discovered a new Trojan that encrypts files on an infected computer and then demands $300 in ransom for a decryption password. The Trojan, identified as Cryzip, uses a commercial zip library to store the victim's documents inside a password-protected zip file and leaves step-by-step instructions on how to pay the ransom to retrieve the files. It is not yet clear how the Trojan is being distributed, but security researchers say it was part of a small e-mail spam run that successfully evaded anti-virus scanners by staying below the radar. While this type of attack, known as "ransomware," is not entirely new, it points to an increasing level of sophistication among online thieves who use social engineering tactics to trick victims into installing malware, said Shane Coursen, senior technical consultant at Moscow-based anti-virus vendor Kaspersky Lab.

Category 15.2 Extortion & blackmail

2006-07-24 DHS Daily OSIR; ZDNet News http://news.zdnet.com/2100-1009_22-6097741.html

BEWARE OF RANSOMWARE, FIRM WARNS.

Smaller companies should back up their data if they want to avoid being held to ransom by hackers, a security company has warned. Hackers are using sophisticated ransomware, which is malicious code, to hijack a company's user files, encrypt them and then demand payment in exchange for the decryption key, Kaspersky Labs said on Monday, July 24. The security specialist said that the encryption algorithms used by cybercriminals are becoming increasingly complicated, foxing antivirus companies. "Within a corporation, the IT department normally backs up files. The danger is where attacks are launched at smaller businesses (without IT departments) and individuals," said David Emm, senior technology consultant at Kaspersky UK.

Category 15.2 Extortion & blackmail

2006-11-16 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2168823/police-nab-spanish-webcam-spies

SPANISH POLICE NAB WEBCAM BLACKMAILERS.

Four suspected cyber-criminals have been arrested in Spain in connection with a series of online crimes including malware creation, blackmail, data theft, and credit card fraud. According to Spanish newspaper reports, two 17 year-olds were arrested Wednesday, November 15, in Alicante charged with creating a Trojan horse which allowed them to take control of Webcams at local educational institutions. The hackers allegedly spied on students and recorded compromising images which were then used to blackmail the victims. Two adults were also arrested in Madrid in connection with the original inquiry, accused of using the teenaged malware authors to obtain confidential data in order to commit credit card fraud. Using fake credit card details, the two individuals allegedly made purchases amounting to more than €60,000. The investigation, codenamed 'Praxis', has been ongoing since a Spanish computer science organization fell victim to a hack attack in August 2005.

Category 15.2 Extortion & blackmail

2007-01-15 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2172503/ftc-prunes-site-pay-pop-ads

U.S. WATCHDOG CRACKS DOWN ON PAY-UP POP-UPS.

The Federal Trade Commission (FTC) has reached a short-term agreement with a video download site accused of bombarding users with pop-ups and demanding money to make them go away. Digital Enterprises Inc has entered into an interim agreement with the FTC to limit its pop-up software and to inform users what the software will do beforehand. The deal will apply to three Digital Enterprises video sites: Movieland.com, Moviepass.tv and Popcorn.net. The original FTC complaint accused Movieland.com of flooding users' systems with pop-up windows which played minute-long audio files and demanded that users pay a $29.95 fee to stop the notices from appearing. Pop-ups could not be closed or minimized and the software was "difficult or impossible" to remove. The agreement allows all three sites to continue to install the pop-up software, but limits their frequency to one per hour, five times a day, and no longer than 40 seconds in length.

Category 15.2 Extortion & blackmail

2007-02-07 DHS Daily OSIR; Kaspersky Labs, he said. CNET News http://news.com.com/Antivirus+expert+Ransomware+on+the+rise/2100-7355_3-6157092.html

ANTIVIRUS EXPERT: 'RANSOMWARE' ON THE RISE.

Online criminals are turning away from threatening companies with massive cyberattacks in favor of encrypting a victim's data and then demanding money to decrypt it, an antivirus expert has claimed. Eugene Kaspersky, head of antivirus research at Russia's Kaspersky Labs, told the RSA Conference Tuesday, February 6, that the use of so-called "ransomware Trojans" is a key trend for 2007. This malicious software infects a PC, encrypts some data and then displays an alert telling the victim to send money to get the decryption key needed to access their data again. Such malicious software isn't new. Early examples include Cryzip, discovered in March 2006, and GPCode, discovered in May 2005. Cryzip and GPCode didn't cause massive damage, but Kaspersky believes cybercriminals will refine their use of ransomware Trojans this year. The final version of GPCode used a 660-bit encryption key, which should have taken a single powerful PC around 30 years to crack but was actually broken quickly by

Category 15.2 Extortion & blackmail

2007-04-24 DHS Daily OSIR; Computerworld http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9017723

A NEW WAVE OF EXTORTION E-MAILS CIRCULATE THE INTERNET.

A new wave of extortion e-mails that threaten recipients with bodily harm and death if they do not pay thousands of dollars to the sender is circulating on the Internet, according to security vendor SecureWorks Inc. The e-mails are sent directly to the victims from valid e-mail accounts instead of the usual spam relays and bot proxies -- an apparent attempt to make them seem authentic. The accounts are set up by scammers purporting to be assassins hired by third parties to harm the recipients. The sender offers to spare the recipient from harm in return for thousands of dollars. About 1,000 of the e-mails have been spotted over the past few days, and they appear to be targeted largely at higher-income professionals such as doctors, lawyers and business owners, according to Don Jackson, a researcher at SecureWorks. The numbers could be higher because many people don't report the e-mails, he said. A similar run of e-mails in December and January prompted the FBI to issue an alert about the scam and urge recipients to simply ignore the messages. The e-mails were sent using popular e-mail services such Gmail, Yahoo and Hotmail by people believed to be outside the U.S., Jackson said.

Category 15.2 Extortion & blackmail

2007-04-27 DHS Daily OSIR; SecurityFocus http://www.securityfocus.com/brief/491

NO PAY OFF IN EXTORTION ATTACKS?

Denial-of-service attacks against online service providers have declined, suggesting that extortion attacks don't pay, a security engineer at Symantec stated in the company's blog on Thursday, April 26. The brief analysis attempts to explain a 15 percent decline in attacks noted by the company's bi-annual Internet Security Threat Report. Symantec witnessed a drop, from 6,110 denial-of-service (DoS) attacks in the first half of 2006 to 5,213 attacks in the latter half of 2006. "The thing is that DoS attacks are loud and risky," Yazan Gable, security response engineer for Symantec, stated in the blog post. "Whenever a bot-network owner carries out a denial of service attack they run the risk of losing some of their bots." Bot masters are increasingly focusing on spamming and stealing financial account data. Researchers have discovered a number of underground e-commerce servers on the Internet that attempt to sell credit-card and financial information. Security firm SecureWorks found that prices varied from about $30 for the log-on credential for a small e-commerce company to $250 for the account information for a major financial institution. Gable noted that, while denial-of-service attacks have decreased in the last six months of 2006, spam levels have jumped.

15.4 Stock fraud (e.g., pump 'n' dump, insider trading)

Category 15.4 Stock fraud (e.g., pump 'n' dump, insider trading)

2006-08-25 DHS Daily OSIR; BBC http://news.bbc.co.uk/2/hi/technology/5284618.stm

SPAMMERS MANIPULATE STOCK MARKETS.

Spam messages that tout stocks and shares can have real effects on the markets, a study suggests. E-mails typically promote penny shares in the hope of convincing people to buy into a company to raise its price. People who respond to the "pump and dump" scam can lose eight percent of their investment in two days. Conversely, the spammers who buy low-priced stock before sending the e-mails, typically see a return of between 4.9 percent and 6 percent when they sell. The study recently published on the Social Science Research Network say their conclusions prove the hypothesis that spammers "buy low and spam high". The researchers say that approximately 730 million spam e-mails are sent every week, 15 percent of which tout stocks. Other estimates of spam volumes are far higher. The study, by Professor Laura Frieder of Purdue University and Professor Jonathan Zittrain from Oxford University's Internet Institute, analyzed more than 75,000 unsolicited e-mails.

Category 15.4 Stock fraud (e.g., pump 'n' dump, insider trading)

2006-08-29 DHS Daily OSIR; Finextra (UK) http://www.finextra.com/fullstory.asp?id=15778

CANADIAN PHISHERS IN PUMP-AND-DUMP PROBE.

Canadian regulators are investigating a rash of phishing frauds at online brokerages in which raiders used the funds from looted accounts to artificially inflate the price of penny stocks. The Investment Dealers Association of Canada has warned brokerages to be on the alert for suspect account activity after a number of member firms reported the scams, in which customer accounts were liquidated and the funds used to place orders for specific securities listed on the OTC Bulletin Board and the Nasdaq pink sheets. A number of customers of BMOInvestorLine were hit by the crooks, while TD Waterhouse is also investigating a rash of similar incidents.

Category 15.4 Stock fraud (e.g., pump 'n' dump, insider trading)

2006-09-04 DHS Daily OSIR; Sophos
http://www.sophos.com/pressoffice/news/articles/2006/09/stockpromo.html

NEW TWIST AS SPAMMERS OFFER TO HELP COMPANIES CHEAT THE STOCK MARKET.

SophosLabs has identified a new tactic being used by spammers involved in lucrative "pump-and-dump" stock spam campaigns. These criminals are now targeting companies offering to boost their stock prices in return for payment. Pump-and-dump scams are e-mail campaigns which encourage people to invest in a particular company's stock, in order to quickly inflate its value and enable the spammers to make a fast profit. It is thought that these scams take place unbeknown to the company involved. Now, in a new twist seen in an e-mail campaign, scammers are telling companies that they can boost their own stock prices by up to 250 percent within two to three weeks, and are even offering a one day free trial. The e-mails also claim that the scammers will offer advice on future share price movements to investors, for a 30 percent share of the income.

Category 15.4 Stock fraud (e.g., pump 'n' dump, insider trading)

2006-11-16 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2060235,00.asp

'PUMP-AND-DUMP' SPAM SURGE LINKED TO RUSSIAN BOT HERDERS.

The recent surge in e-mail spam hawking penny stocks is the handiwork of Russian hackers running a botnet powered by tens of thousands of hijacked computers. Internet security researchers and law enforcement authorities have traced the operation to a well-organized hacking gang controlling a 70,000-strong peer-to-peer botnet seeded with the SpamThru Trojan. According to Joe Stewart, senior security researcher at SecureWorks, the gang functions with a level of sophistication rarely seen in the hacking underworld. For starters, the Trojan comes with its own anti-virus scanner that removes competing malware files from the hijacked machine. Once a Windows machine is infected, it becomes a peer in a peer-to-peer botnet controlled by a central server. If the control server is disabled by botnet hunters, the spammer simply has to control a single peer to retain control of all the bots and send instructions on the location of a new control server. The bots are segmented into different server ports, determined by the variant of the Trojan installed, and further segmented into peer groups of no more than 512 bots. This allows the hackers to keep the overhead involved in exchanging information about other peers to a minimum, Stewart explained.

Category 15.4 Stock fraud (e.g., pump 'n' dump, insider trading)

2007-03-09 DHS Daily OSIR; Computerworld http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=standards_and_legal_issues&articleId=9012699&taxonomyId=146

SEC FREEZES $3M MADE IN HACKER STOCK SCAM.

A federal judge, acting on behalf of the Securities and Exchange Commission (SEC), has frozen $3 million belonging to an Eastern European cybercrime gang that allegedly hacked into seven U.S. brokerage firms, then used stolen funds to mount a stock manipulation scheme. According to a complaint filed by the SEC Tuesday, March 7, the gang's 20 members live in Russia, Latvia, Lithuania and the British Virgin Islands. The frozen assets, which include at least $733,000 in profits from the scam, are in a Latvian bank. After buying lightly-traded "penny" stocks, the criminals hacked into accounts at a number of online brokerage houses, including Charles Schwab, E*Trade, Merrill Lynch, TD Ameritrade, Vanguard and others. Securities in those accounts were sold and the proceeds used to buy thousands--and in one case, millions -- of the same shares. That, said the SEC, artificially drove up the price. "Then, at the height of the price surge, the defendants sold in their own accounts their previously-purchased shares of the same stocks at the inflated prices," the complaint read. The scheme went on for at least a year and cost the brokerages about $2 million in losses before ending in December.
SEC complaint: http://www.sec.gov/litigation/complaints/2007/comp20030.pdf

Category 15.4 Stock fraud (e.g., pump 'n' dump, insider trading)

2007-03-29 DHS Daily OSIR; VNUnet http://www.vnunet.com/vnunet/news/2186770/euro-investors-hit-large-scale

PUMP-AND-DUMP SCAM TARGETS GERMAN INVESTORS.

European investors were warned to be on their guard against pump-and-dump stock scams following the discovery of a large-scale spam campaign designed to manipulate the share price of a company listed on the German stock exchange. IT security firm Sophos said that, unlike previous pump-and-dump scams, the new campaign tries to influence the share price of a company listed outside the U.S. The scam tries to encourage German investors to buy shares in U.S.-based energy company Stonebridge Resources Exploration Ltd, which announced its listing on the Frankfurt Stock Exchange on March 1 under the ticker symbol S3C. "This is the first time we have seen a widespread spam campaign trying to influence a stock market based outside the U.S.," said Graham Cluley, senior technology consultant at Sophos.

15.5 Click fraud

Category 15.5 Click fraud

2006-01-11 INNOVATION (Wired Jan 2006)
<http://www.wired.com/wired/archive/14.01/fraud_pr.html>

CLICK FRAUD COULD RUIN THE INTERNET

Pay-per-click is the fastest growing segment of all advertising, according to the Interactive Advertising Bureau. The business model, which is used by search engine sites, requires advertisers to pay for keywords related to their product or service. When a user types in the keyword, an ad is displayed, and if the user clicks on it, the advertiser pays the search engine site $10 or whatever the negotiated rate is. The arrangement has proven a boon to Google and Yahoo, which earned billions of dollars last year in keyword advertising revenue, but the model's viability is now threatened by "click fraud," which occurs when a competitor illicitly manipulates the ad. "If we get clicked fraudulently, it uses up our ad budget," says one victim, who found that 40% of the clicks he was paying for came from a single address belonging to a rival business. And because most advertisers set limits on how much they will spend, fraudulent clicking "literally pushes us off the page." Meanwhile, with the introduction of automated zombie networks and India-based click farms, the amount of click fraud is estimated at anywhere between 10% and 50% and rising, and marketing consultant Joseph Holcomb calls it "a billion-dollar mess" that "has the potential of destroying the entire industry."

Category 15.5 Click fraud

2006-10-09 DHS Daily OSIR; San Francisco Chronicle http://www.azstarnet.com/business/150195

ONLINE SCAM CLICKS FOR SCAMMERS.

Louise, a disabled housewife, plays a small part in a ring of online scammers. She spends her days at home in Ohio entering queries in obscure search engines and then clicking on the ads -- over and over again. Louise's illicit clicks cost advertisers untold amounts of money. Armies of average citizens have been lured into similar fraud rings to earn money from home. Their work is known as click fraud, a problem that has bedeviled Internet giants Google and Yahoo in recent years. Shuman Ghosemajumder of Google dismissed the idea that the mom-and-pop scammers are having much success bilking his company and its advertisers. The techniques they use, he said, are unsophisticated and present little challenge to his company's automated fraud filters. Louise said she works with 20 recruiters. They send her up to 600 e-mails daily that include links to the search engines that she is supposed to visit and use.

Category 15.5 Click fraud

2006-12-11 EDUPAGE; New York Times (registration req'd)
http://www.nytimes.com/2006/12/11/technology/11push.html

POP-UPS USED TO PAD VIEWERSHIP NUMBERS

Some online companies are using pop-ups to inflate the statistics of how many Web surfers visited their site. In that scenario, a company pops up content, rather than an advertisement, to users who have not necessarily asked to see such content. The company behind the pop-up counts that instance as a page view, however, giving it an edge in the growing battle for sheer numbers of views. Nielsen/NetRatings recently discounted such "push traffic" from its usage numbers for financial site Entrepreneur.com, slashing the number of unique visitors from 7.6 million in April to just 2 million. Benjamin Edelman, a doctoral student at Harvard University, has set up a computer with many forms of adware and uses it to track, among other things, which companies use pop-ups to pad their usage numbers. According to Edelman's data, sites including Concierge.com, ForbesAutos.com, and Heavy.com all appear to use push technology. The issue is at the heart of advertising rates, which are often based on how many unique viewers visit a site.

15.6 Spam

Category 15.6 Spam

2006-09-18 DHS Daily OSIR; IDG News Service
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9003411&intsrc=news_ts_head

SPAMMERS MAKING MONEY FROM FREE WEB-HOST SERVICES.

Spammers have found a way to mine free Web-hosting services for cash. Online scammers have long used free hosting services such as Yahoo Geocities or Tripod as a way to get around e-mail filters that might otherwise recognize their spam Websites. But now some enterprising spammers have begun selling each other these free Web pages, according to security vendor McAfee Inc. For $25 per week a spammer will sell 50 Web-hosting accounts that can be used to redirect Web traffic to sites that normally would be flagged. "These 'link providers' create and maintain thousands of free hosting accounts on behalf of the spammers," wrote McAfee's Nick Kelly in a recent posting to McAfee's Avert Labs blog. "They know that the bigger hosts are unlikely to get blacklisted because they have so many legitimate users," he added. McAfee blog: http://www.avertlabs.com/research/blog/?p=88

Category 15.6 Spam

2007-01-09 DHS Daily OSIR; Register (UK)
http://www.channelregister.co.uk/2007/01/09/scam_decline/

MYSTERY DROP IN FRAUD AND SPAM.

Spam levels suddenly dropped 30 percent last week, according to SoftScan, which attributes the let-up to a "broken" botnet. SoftScan believes the most likely explanation is that hackers have temporarily lost control of a significant network of compromised machines. It seems unlikely that new computers at Christmas had much to do with affecting the number of compromised machines. Alternatively the drop in spam might be a result of the recent earthquake in Asia disrupting spamming activity from that region, but this theory fails to explain a gradual (rather than more sudden) drop off in spam levels this month. Early Warning reports that fraud surprisingly fell last month, even though Christmas witnessed a rise in e-commerce sales. "This is really an unexpected and encouraging first in Internet fraud statistics. As e-commerce goes on rising, we are used to corresponding increases in [scammers]' activities to capitalize on it," said Andrew Goodwill of Early Warning. "As the number and value of sales has risen so sharply, fraud -- as a proportion -- is definitely down. The reason for this drop is I believe the increased awareness of Internet merchants ... and ... measures [they have] in place to detect the fraudulent attempts."

Category 15.6 Spam

2007-01-12 DHS Daily OSIR; SecurityFocus http://www.securityfocus.com/print/news/11435

SPAMMERS GET BULLISH ON STOCKS.

A year ago, stock spam made up only about five percent of all spam e-mail messages, according to MessageLabs. Now, stock spam is on a trajectory to become the biggest category in unsolicited e-mail marketing, with 35 percent or more of spam touting a stock. Symantec has also noted the trend, finding that the monthly fraction of spam dedicated to stocks varies between 20 percent and 40 percent. The increasing popularity of stock-touting spam is also notable because the total amount of spam -- driven by botnet activity -- is on the rise. While a Christmas drop in the number of compromised PCs appears to have led to a general drop in spam volume, the number of PCs coopted by botnets for use in spamming operations continues to increase. Stock spammers are becoming more savvy about the practice. "The spam in the early day -- by which I mean the late 1990s -- use to contain blatant falsehoods," said John Reed Stark of the Securities and Exchange Commission. "It was very easy to prove the false statements. Now, the spammers aren't as bold in their projections and use disclosures to attempt to appear legitimate."

Category 15.6 Spam

2007-02-12 DHS Daily OSIR; ComputerWorld
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=279934&intsrc=hm_ts_head

SPAM, VIRUSES, BOTNETS: CAN THE INTERNET BE SAVED?

Advances in IT over the decades have come mostly in small increments. That kind of evolutionary approach has served users well, boosting speeds, capacities and application capabilities by many orders of magnitude. But such incremental improvements are no longer sufficient to keep the Internet viable, according to a growing number of researchers. In fact, they say, the Internet is at the tipping point of overwhelming abuse and complexity. The most sanguine of observers say that even if the Internet is able to avoid some kind of digital Armageddon brought on by spammers, hackers, phishers and cyberterrorists, it nevertheless will drown in a flood of mobile gadgets, interactive multimedia applications and Internet-enabled devices. And it isn't just a problem of security and reliability, says Nick McKeown, a computer scientist at Stanford University; the Internet is getting crushed by complexity. He points out that the original Internet design was based on the idea that users were immobile and connected to the Net by wires.

Category 15.6 Spam

2007-04-19 DHS Daily OSIR; IDG News Service
http://news.yahoo.com/s/infoworld/20070419/tc_infoworld/87849;_ylt=AgdXD_ihKXtAYBBKpR0f5XMjtBAF

SPAMMERS, HACKERS SEIZE ON VIRGINIA TECH SHOOTINGS.

Spammers and hackers are using the slayings at Virginia Tech as a gory lure to infect computers with malicious software, security experts noted Thursday, April 19. While the video made by gunman Cho Seung-hui prior to the killing of 33 people on Monday was widely posted on news Websites and YouTube.com, spam e-mails were intercepted Wednesday night purporting to link to the footage on a Brazilian Website, said Graham Cluley, senior technology consultant, at security vendor Sophos. If clicked, the link caused a computer to automatically download a malicious screensaver, called TERROR_EM_VIRGINIA.scr by Sophos, which installs a Trojan horse program that collects banking details, Cluley said. It's unclear yet what banks the Trojan is engineered to exploit, Cluley said. The e-mails are unlikely to mean much to English speakers since they're written in Portuguese, Cluley said. But hackers have repeatedly used breaking news events to try to trick users into opening malicious programs.

Category 15.6 Spam

2007-05-01 DHS Daily OSIR; Sophos http://www.sophos.com/pressoffice/news/articles/2007/05/postcard.html

ELECTRONIC POSTCARD ARRIVES WITH A WEB STING IN ITS TAIL.

Sophos has warned computer users to be wary of unsolicited e-mails and defend their Web gateways, following a spam campaign that poses as an electronic postcard, but is really an attempt to lure the unwary into being infected by a Web-based Trojan horse. E-mails seen by experts at SophosLabs have the subject line "You have received a postcard!". Users who follow the Web link are taken to a downloadable executable file (postcard.exe). The file is designed to allow remote hackers to gain access to the infected Windows computer.

16.1 Industrial espionage. insider threats

Category 16.1 Industrial espionage. insider threats

2006-06-02 DHS Daily OSIR;
Federal Computer Week http://www.fcw.com/article94741-06-02-06-Web

DISA SEEKS INPUT ON INSIDER THREAT TOOLS.

The Defense Information Systems Agency (DISA) wants industry input on tools that could counter insider threats to Department of Defense (DoD) information systems. DISA said traditional efforts to secure networks focus on outside hreats, but insiders pose an equally damaging threat and they can access DoD networks without detection by the security systems. DISA, in a request for information (RFI) released Thursday, June 1, said it's looking for an insider threat focused observation tool that could be deployed on selected host DoD machines to aggressively gather and analyze data on inside threats. The due date for RFI responses is Wednesday, July 5.

Category 16.1 Industrial espionage. insider threats

2006-07-06 DHS Daily OSIR; Washington Post http://www.washingtonpost.com/wp-dyn/content/article/2006/07 /05/AR2006070501489_pf.html

CONSULTANT BREACHED FBI'S COMPUTERS.

A government consultant, using computer programs easily found on the Internet, managed to crack the FBI's classified computer system and gain the passwords of 38,000 employees, including that of FBI Director Robert S. Mueller III. The break-ins, which occurred four times in 2004, gave the consultant access to records in the Witness Protection Program and details on counterespionage activity, according to documents filed in U.S. District Court in Washington. As a direct result, the bureau said it was forced to temporarily shut down its network and commit thousands of man-hours and millions of dollars to ensure no sensitive information was lost or misused. The government does not allege that the consultant, Joseph Thomas Colon, intended to harm national security. But prosecutors said Colon's "curiosity hacks" nonetheless exposed sensitive information. Colon, an employee of BAE Systems who was assigned to the FBI field office in Springfield, IL, said in court filings that he used the passwords and other information to bypass bureaucratic obstacles and better help the FBI install its new computer system. And he said agents in the Springfield office approved his actions.

Category 16.1 Industrial espionage. insider threats

2006-09-11 DHS Daily OSIR; New York Times
http://www.nytimes.com/2006/09/11/technology/11hewlett.html?hp&ex=1157947200&en=6a513dcc71002d5c&ei=5094&partner=homepage

PRETEXTING: AN INDUSTRY BASED ON A SIMPLE MASQUERADE.

People who obtain calling records often use a technique known as pretexting -- using a pretext, like masquerading as a customer, to get a company to disclose information. Their shady subculture has been getting renewed attention since the revelation last week that a subcontractor for an investigative firm working for Hewlett-Packard used pretexting to obtain the call records of company board members and reporters. It is hard to quantify the size of the telephone pretexting economy, but in recent years it has turned into a small industry. Pretexters often use techniques similar to those employed by identity thieves to obtain not only telephone records but also other private data. The Federal Trade Commission, some state legislatures and telephone companies have all tried to shut the industry down, with mixed success so far. Many Websites that sold calling records have disappeared, but experts say many pretexters remain in business. "Part of the problem is that there is still no law at the federal level making it clear that the activity is illegal," said Marc Rotenberg, executive director of the Electronic Privacy Information Center.

Category *16.1* *Industrial espionage. insider threats*

2007-01-16 DHS Daily OSIR;

PRESIDENT SIGNS PRETEXTING BILL INTO LAW.

It's official: "pretexting" to buy, sell or obtain personal phone records -- except when conducted by law enforcement or intelligence agencies -- is now a federal crime that could yield prison time. President Bush on Friday, January 12, affixed his signature to the Telephone Records and Privacy Protection Act of 2006. The measure threatens up to 10 years behind bars to anyone who pretends to be someone else, or otherwise employs fraudulent tactics, to persuade phone companies to hand over what is supposed to be confidential data about customers' calling habits.
CNET News http://news.com.com/President+signs+pretexting+bill+into+law/2100-10283-6150572.html

Category *16.1* *Industrial espionage. insider threats*

2007-01-18 DHS Daily OSIR; Associated Press http://www.washingtonpost.com/wp-dyn/content/article/2007/01/18/AR2007011801152.html

U.S. RETRACTS CANADA SPY COINS CLAIM.

Reversing itself, the Department of Defense (DoD) says an espionage report it produced that warned about Canadian coins with tiny radio frequency transmitters was not true. The Defense Security Service said it never could substantiate its own published claims about the mysterious coins. The service had contended since late June that such coins were found planted on U.S. contractors with classified security clearances on at least three separate occasions between October 2005 and January 2006 as the contractors traveled through Canada. Intelligence and technology experts were flabbergasted over the initial report, which suggested such transmitters could be used to surreptitiously track the movements of people carrying the coins. Robert Moroz, who organizes an annual technology conference in Canada, said one vendor in 2005 attached coin-sized transmitters to casino chips as part of a proof-of-concept demonstration. Moroz also cited previous industry proposals -- later abandoned -- to build such transmitters into the euro. But he was skeptical about DoD's claims even before the Pentagon said its own report was false.

Category *16.1* *Industrial espionage. insider threats*

2007-03-06 DHS Daily OSIR; Los Angeles Times http://www.latimes.com/business/la-fi-spying7mar07,0,3688427.story

WAL-MART FIRES EMPLOYEE FOR ELECTRONIC SNOOPING.

Wal-Mart Stores Inc. said Monday, March 5, it had fired an employee for recording phone calls between its public-relations staff and a newspaper reporter and for intercepting text messages. Wal-Mart said the employee was acting alone. It was the latest incident involving snooping on reporters by employees of companies they cover. In this case, the retailer said an unnamed computer-systems technician was not authorized by the company to seek or obtain the information. The company also said it fired one manager and disciplined another for "failure to carry out their management duties." Wal-Mart said that between September 2006 and January 2007, the technician recorded calls with Michael Barbaro, who writes about Wal-Mart for The New York Times. Over the previous year, The Times was printing stories of the company's personnel policies, based on leaked employee memos. The company said the same employee also intercepted text messages using equipment that searched for key words in messages sent within a several-mile radius of Wal-Mart's Bentonville, AR, headquarters.

Category *16.1* *Industrial espionage. insider threats*

2007-04-02 DHS Daily OSIR; CNET News http://news.com.com/FCC+imposes+rules+to+prevent+pretexting/2100-1037_3-6172705.html

FCC IMPOSES RULES DESIGNED TO PREVENT PRETEXTING.

The Federal Communications Commission (FCC) hopes to prevent data burglaries with a set of new regulations for phone companies aimed at preventing the fraudulent practice called "pretexting." On Monday, April 2, the FCC issued an order designed to strengthen its current privacy rules by requiring telephone and wireless operators to adopt additional safeguards to protect personal telephone records from being disclosed to unauthorized people. The new regulations come as lawmakers have already outlawed the practice of "pretexting," which encompasses any technique used to fraudulently obtain personal information. Congress is now looking to impose stricter regulations on phone companies to protect customer data. Specifically, the FCC order prohibits carriers from releasing--either over the phone or online--sensitive personal data, such as call detail records, unless the customer provides a password. It also requires operators to notify customers immediately when changes are made to their accounts. And it requires providers to notify their customers in the event of a breach of confidentiality.

Category 16.1 Industrial espionage. insider threats

2007-04-11 DHS Daily OSIR; Associated Press http://www.azstarnet.com/allheadlines/177833

AGENT SAYS CHINESE-BORN ENGINEER ADMITTED PASSING SECRETS.

A Navy investigator testified Tuesday, April 10, that a Chinese-born engineer initially denied passing U.S. defense technology secrets to China with the help of his younger brother but then admitted the allegations several days later. Gunnar Newquist, a special agent with the Naval Criminal Investigative Service, played an hour of excerpts from a 4 1/2-hour, secretly videotaped interview done after the arrest of defendant Chi Mak in which he repeatedly denied passing sensitive military information to China. Newquist said Mak made his confession two days later during an untaped interview. Mak, a naturalized U.S. citizen who worked for an Anaheim-based naval defense contractor, has pleaded not guilty to charges of conspiracy to export defense material to China, failure to register as a foreign agent, attempted and actual export of defenseArticles and making false statements. His wife, brother and other relatives also have been indicted. Mak, 66, was arrested on Oct. 28, 2005, after his brother and sister-in-law were stopped at Los Angeles International Airport as they tried to board a flight to Hong Kong and Guangzhou, China. FBI agents found encrypted disks containing copies of documents on a submarine propulsion system hidden in their luggage, according to court papers.

Category 16.1 Industrial espionage. insider threats

2007-04-22 DHS Daily OSIR; Associated Press
http://www.knoxnews.com/kns/national/article/0,1406,KNS_350_5498078,00.html

EX-NUCLEAR PLANT ENGINEER ALLEGEDLY TOOK DATA TO IRAN.

A former engineer at the nation's largest nuclear power plant has been charged with taking computer access codes and software to Iran and using it to download details of plant control rooms and reactors, authorities said. The FBI said there's no indication the plant employee had any terrorist connections. Mohammad Alavi, who worked at the triple-reactor Palo Verde power plant west of Phoenix, was arrested April 9 at Los Angeles International Airport when he arrived on a flight from Iran. According to court records, the software is used only for training plant employees but allowed users access to details on the Palo Verde control rooms and the plant layout. In October, authorities alleged, the software was used to download training materials from Tehran, using a Palo Verde user identification. The FBI said there was no evidence to suggest the software access was linked to the Iranian government.

16.2 Industrial information systems sabotage

Category 16.2 Industrial information systems sabotage

2006-06-28 DHS Daily OSIR; GovExec http://govexec.com/story_page.cfm?articleid=34443

NAVY CONTRACTOR ARRESTED FOR ALLEGED COMPUTER SYSTEM SABOTAGE.

A Navy contractor was arrested Monday, June 26, in connection with planting malicious code on a government computer system. Richard Sylvestre owned and worked for Ares Systems International. SAIC Corp. recently won a contract to provide a third network administrator at the center, the filing said, beating Ares, which also had submitted a bid to fill the position. According to the complaint, two network computers at the center went offline unexpectedly on May 21. Both Ares contractors were away on travel and the SAIC systems administrator found the computers had been programmed with malicious code that deleted critical operating system files at a specified time after his departure. Further investigation revealed similar code on three other computers, including a network server, although that code had not yet executed. . . .

Jenny Mandel, writing in _Government Executive_, added "Later, investigators used computer records and interviews to trace the malicious code back to Sylvestre, who had apparently programmed them to run at a future date shortly before his departure. Sylvestre's colleague at Ares said his boss had made what appeared to be a joke that he should set up a program to operate while the two were away that would make the SAIC contractor "look bad."

When confronted, Sylvestre admitted that he had set up the code for that reason, though he denied any intention to cause a collision by any vessels relying on the system for data on underwater obstacles, according to the filing.

Sylvestre is charged with knowingly damaging a protected computer and causing losses that would have exceeded $5,000 in one year. A trial date has not yet been set, but a Justice Department statement said he faces a maximum of 10 years in prison, a fine of up to $250,000 and a period of post-release supervision if found guilty."

Category 16.2 Industrial information systems sabotage

2006-08-09 DHS Daily OSIR; Tech Web http://www.darkreading.com/document.asp?doc_id=100932

ABUSE OF INSIDER SECURITY PRIVILEGES OFTEN GOES UNMONITORED.

As the keepers of the keys, IT and security staff have the best chance to access sensitive corporate data without being detected. Of course, some functions require security staffers to access, even read, sensitive documents as part of everyday system surveillance, an audit, or an investigation of suspected policy violations. However, when an IT staffer is unhappy or disgruntled, the abuse of security privileges can escalate to a much more threatening level. In fact, 86 percent of "insider" computer sabotage -- malicious system attacks that don't involve fraud or information theft -- is perpetrated by employees in technical positions, according to a study published last year by the U.S. Secret Service's National Threat Assessment Center and the Carnegie Mellon Software Engineering Institute's CERT Program. It's difficult to quantify the online behavior of IT people, principally because they are capable of excluding themselves from most efforts to analyze online activity. In most cases, though, the abuse of security privileges leads to more snooping than sabotage. Even in those cases, however, it's a good idea to have the ability to monitor IT staffers' behavior.

Category 16.2 Industrial information systems sabotage

2006-08-25 http://www.cybercrime.gov/araboSent.htm

CONSPIRACY TO ORDER DESTRUCTIVE COMPUTER ATTACKS ON COMPETITORS

NEWARK, N.J. -- A Michigan man was sentenced today to 30 months in prison for conspiring to conduct highly destructive computer attacks on competitors of his online sportswear business, including a web-based New Jersey company, U.S. Attorney Christopher J. Christie announced.

U.S. District Judge Joseph E. Irenas also ordered Jason Salah Arabo, 19, of Southfield, Michigan, to make restitution of $504,495 to his victims -- the websites he targeted as well as an Internet hosting company.

Arabo pleaded guilty today before Judge Irenas on April 12, to a one-count Information charging him with conspiracy to cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer.

In pleading guilty, Arabo acknowledged that in 2004, he ran two web-based companies, www.customleader.com and www.jerseydomain.com, that sold sports apparel, including reproductions of sports uniforms, popularly known as "retro" or "throwback" jerseys.

"Arabo's 30-month prison sentence reflects the very serious and damaging nature of the computer attacks he orchestrated," said Christie. "This case went far beyond a teenager using his computer for online pranks. We will continue to investigate and aggressively prosecute the misuse of computers to commit crime."

According to Assistant U.S. Attorney Eric H. Jaso, who prosecuted the case, Arabo admitted that in online "instant message" conversations he met a New Jersey resident, Jasmine Singh, who communicated using the online name "Pherk." Arabo learned that Singh had covertly infected some two thousand personal computers with programs that enabled him to remotely control them. Singh demonstrated to Arabo online that he could command these computers to conduct attacks, known as distributed denial of service, or "DDOS" attacks, on computer servers and disable websites supported by those servers. Arabo admitted that he asked Singh to take down the websites and online sales operations of certain of his competitors. Arabo promised to compensate Singh for the attacks with merchandise, including designer sneakers.

In August 2005 Singh, who was 16 at the time of the attacks, pleaded guilty as an adult to two counts of computer theft in New Jersey State Superior court. He has since been sentenced to five years in prison and ordered to pay $35,000 in restitution for damage caused by the attacks.

Arabo admitted that, starting in July 2004, he identified competitors' websites to Singh that he wanted taken down. One of these was Jersey-Joe.com, a New Jersey-based online business that, like Arabo's online businesses, sold "throwback" jerseys and other merchandise. Arabo believed that once his competitors' websites were disabled, his online business would improve. Arabo continued requesting these attacks until early December 2004, pressing Singh to disable the competitors' websites for as long as possible. Arabo sent Singh designer sneakers and other merchandise for conducting successful attacks. The attacks stopped in December 2004 when FBI agents and New Jersey State Police investigators conducted a search of Singh's Edison, New Jersey home and seized his computer.

Arabo was originally charged by criminal complaint on March 18, 2005. According to that complaint, the computer attacks were conducted by Singh from his home computer. Singh secretly infected thousands of computers with copies of a computer program known as a "bot" (short for "robot"). As described in the complaint, a "bot" can have legitimate functions, but can also be used to gain unauthorized access to and control over computers that they infect, and can thus cause the infected computers to attack other computers. "Bots" used for such illicit purposes are frequently disguised as MP3 music files or photographs that unsuspecting computer users download from public Internet sites. Having downloaded an infected file, a computer user is usually unaware of the presence of a "bot" on his or her computer.

In this case, according to the complaint, the infected computers included those of students on at least two college campuses in Massachusetts and Pennsylvania. Singh remotely ordered hundreds of the implanted "bots" to attack computer servers that supported Arabo's competitors' websites. The "bots" caused the infected computers to access the targeted website all at once, overloading the website's hosting computer server and causing it to "crash."

The complaint alleged that the attacks caused widespread harm and disruption to Internet and computer services far beyond the online businesses that Arabo targeted. According to the complaint, the Internet service providers that hosted the targeted websites also provided website hosting and other Internet services to a number of unrelated businesses which as a result were also harmed by the attacks.

The complaint alleged that the attacks affected businesses as far away as Europe, and caused disruption to the operations of major online retail businesses, banks, and companies that provide communications, data backup, and information services to the medical and pharmaceutical industries. The attacks disrupted crucial services to these companies that included Internet access, corporate websites, email, data storage and disaster-recovery systems. The complaint did not include an estimate of the financial losses attributable to the attacks.

Category 16.2 Industrial information systems sabotage

2006-08-25 DHS Daily OSIR; Associated Press
http://www.siliconvalley.com/mld/siliconvalley/news/editoria l/15363417.htm

ONLINE RETAILER SENTENCED FOR ARRANGING COMPUTER ATTACKS ON RIVALS.

A 19-year-old Michigan man who ran an Internet business selling retro sports jerseys was sentenced Friday, August 25, to 30 months in federal prison for recruiting a New Jersey teen to carry out computer attacks against competitors. Jason Salah Arabo was also ordered to pay $504,495 to his victims, which included operators of competing Websites, as well as an Internet hosting company. Arabo said he used online instant message conversations to recruit Jasmine Singh of Edison, NJ, who was 16 at the time, to electronically bombard other throwback jersey Websites.

16.3 Infrastructure vulnerabilities

Category 16.3 Infrastructure vulnerabilities

2006-02-15 DHS Daily OSIR; http://www.techweb.com/wire/security/180202527

CHERTOFF SAYS IT WEAKNESSES HURT KATRINA RESPONSE.

Department of Homeland Security Secretary Michael Chertoff took responsibility for the poor response to Hurricane Katrina Wednesday, February 15, but he also blamed the department's inability to conduct surveillance, communicate efficiently, track shipments, and handle Web traffic. Testifying before the U.S. Senate Committee on Homeland Security and Governmental Affairs, Chertoff said the Department of Homeland Security and the Federal Emergency Management Agency need interoperability, hardened communications, a tracking system for shipments, improved surveillance resources, upgraded software and better hardware. Without hardened communications equipment, leaders could not obtain the information they need to make proper decisions during disasters, Chertoff said. Improvements are underway, but the department has to come up with agreements for supply chain management and real-time monitoring, Chertoff said. Chertoff's remarks: http://www.dhs.gov/dhspublic/interapp/testimony/testimony_00 46.xml

Category 16.3 Infrastructure vulnerabilities

2006-02-15 DHS Daily OSIR; http://www.pcworld.com/news/article/0,aid,124741,00.asp#

FBI DIRECTOR: CYBER THREATS FLUID AND FAR REACHING.

Hacker hunters need to develop new techniques to take on the latest generation of sophisticated and well-organized cyber criminals, FBI Director Robert Mueller told attendees of the RSA Conference 2006 on Wednesday, February 15. In particular, Mueller said in a keynote address, the FBI must work with corporations and international law enforcement to help combat online criminal acts that are seldom reported. "Increasingly our cyber threats originate outside of the United States," he said. "The once-clear divisions of jurisdiction and responsibility between agencies [and nations]...have been rendered obsolete by the fluid and far-reaching nature of today's threats." The FBI now has more flexibility to work with international law enforcement and is helping build relationships with those foreign agencies by putting operatives "on the ground" in countries that may be hotbeds for cybercrime, according to Steven Martinez, the deputy assistant director for the FBI's Cyber Division, who spoke after Mueller.

Category 16.3 Infrastructure vulnerabilities

2006-05-11 DHS Daily OSIR; TechWeb
http://www.informationweek.com/news/showArticle.jhtml?articl
eID=187202331&subSection=All+Stories

EMERGENCY RESPONDERS CAN'T COMMUNICATE, DHS WARNS

The federal government has given more than $2.1 billion to states for interoperable communications since 2003, but many emergency responders still cannot communicate with each other, Department of Homeland Security Secretary Michael Chertoff warned at a conference in Washington. Chertoff said that a task force of first responders, not representatives from telecommunications companies, would form within two months and begin identifying requirements. "And I want to be very clear about this. It is not up to industry to come to us and tell us what we need. It is up to us to define the requirements that we need for our first responders and then tell industry, here's the solution you've got to come up with," he said. The Department of Homeland Security will set functional requirements and performance standards for the next generation of communications equipment after gaining input from emergency responders. It will also use scorecards to measure performance of departments.

Category 16.3 Infrastructure vulnerabilities

2006-06-10 DHS Daily OSIR; Washington Post http://www.washingtonpost.com/wp-dyn/content/article/2006/0609/AR2006060901769.html

DC AREA'S SECURITY PROPOSAL SCORED POORLY.

The Department of Homeland Security sharply cut the Washington region's anti-terrorism funding in part because its grant application was among the weakest nationwide -- with one proposal scoring so low that money cannot be drawn without federal permission, officials said. The region's spending proposals were less innovative and less likely to produce sustained, high-impact results than those submitted by other cities, DHS officials said. The application ranked in the bottom 25 percent of those submitted by urban areas from across the country. George W. Foresman, DHS undersecretary for preparedness, said the region's ranking indicates that its proposals were less likely to produce tangible, sustainable improvements than some other applicants' ideas. The Washington region still got the fourth-highest grant--$46 million, behind New York, Los Angeles and Chicago. But local officials had expected an increase from the $77 million they received last year. One reason it is difficult to justify more money for the capital region is that it already has federal forces helping to protect it, including the military, Foresman said. Also, the area has already received hundreds of millions of dollars in DHS anti-terrorism money in recent years, he said.

Category 16.3 Infrastructure vulnerabilities

2006-06-14 DHS Daily OSIR; Associated Press http://www.local6.com/news/9366455/detail.html

HACKER REPLACES FLORIDA'S EMERGENCY SITE DURING TROPICAL STORM.

Internet users logging onto Florida's public disaster Website Tuesday, June 13, 2006 for an update on Tropical Storm Alberto instead got an imposter page after a hacker broke into the site. Technicians quickly pulled the imposter page from the Floridadisaster.org Website and relocated the site to another server system.

Category 16.3 Infrastructure vulnerabilities

2006-06-23 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,1980979,00.asp

NET DISASTER COULD PARALYZE ECONOMY, STUDY WARNS.

America's Internet and cyber infrastructure have become such a critical backbone for the exchange of information, that any major disruption could have significant economic and security repercussions. The report, issued on Friday, June 23, by the Business Roundtable, a group comprised of chief executives of 160 of the country's largest companies, calls on the federal government to set up response plans and establish clear lines of responsibility.

[MK has added the following section for discussion in the IYIR seminar.]

* * *

The report was entitled "Essential Steps to Strengthen America's Cyber Terrorism Preparedness: New Priorities and Commitments from Business Roundtable's Security Task Force." The panel's recommendations were as follows (quoted in their entirety with reformatting for ASCII representation and added numbering from pages 11-15):

1 The private sector must undertake most of the responsibility for fixing weaknesses in key Internet assets.
Business executives are dependent on a patchwork of public- and private-response programs to restore Internet infrastructure services. In many cases, these programs are not fully coordinated via a central organization. Immediate- and long-term commitments to change the current reality should include the following steps:
1.1 Establish a single point of contact and responsibility for government interaction. Executives must appoint a single management professional (or corporate office) to coordinate Internet restoration in the company and with responsible government officials. In many cases, government decision makers must navigate across various corporate offices, undermining efficient restoration activities. This appointee should be responsible for quickly learning existing government protocols and programs. CEOs must clearly define expectations, roles and responsibilities in the event of a widespread Internet disruption. Companies must also provide ample resources so that managers can coordinate within the company, across the private sector and with the government.
1.2 Set strategic needs and direction. In addition to creating a single manager responsible for coordinating Internet restoration within the company, corporate executives must also develop a strategic plan that accounts for the movement of goods and services, corporate wide priorities for Internet services, and restoration of corporate communications.
1.3 Consolidate early warning and response organizations. The private sector has created institutions to respond to communications disruptions. However, the gap analysis for this initiative concludes that there is confusion about multiple organizations with overlapping responsibilities. In addition, some of these organizations are founded on trust models, where actions during emergencies are not required or part of an industry wide agreement. The private sector must change this by limiting the number of authorized institutions, shoring up membership of resulting institutions, and crafting agreements so that response activities can occur in a predictable and disciplined manner.
1.4 Ultimately, networking early warning and response efforts must also occur in a seamless manner. Thus, even if industry leaders choose to rely on more than one organization for early warning and response services, we must find ways to fabricate a single, consolidated reconstitution process. This process must account for a wide range of strategic needs (e.g., roles and responsibilities in the event of a national outage) and operational challenges (e.g., how to communicate with the right people at the right time). Dependability and clarity can occur across different industry centers through business rules, finely honed memoranda of agreement or mutual aid agreements.
1.5 Irrespective of the format, our industry-populated centers must undertake full and transparent responsibility for fulfilling national goals for reconstituting the Internet.
1.6 Agree on an information-sharing mechanism. Industry must consolidate into a single information-sharing framework for early detection, response and reconstitution of the Internet. Currently, there are information-sharing programs for different ISACs, for the HSIN tool deployed by the federal government and for other ad hoc organizations that are based in academia or the not-for-profit community. Industry leaders, individually or via entities such as the NCC-Communications ISAC, must work to consolidate these protocols and present a formalized process to the government for formal recognition.

2 The federal government should complete response plans by defining key terms and responsible parties.
Clearly, the federal government must continue to prioritize threats from weapons of mass destruction, such as biological or nuclear weapons, as well as catastrophic natural disasters. However, the government's policies should fully and completely address reconstitution of the Internet given the catastrophic damage that could result from an Internet attack. Establishing clarity, responsibility and accountability would not undermine other priority programs. Specifically, the federal government's strategy should incorporate the following:
2.1 Communicate the government's policy for reconstitution of the Internet. The gap analysis suggests that the federal government has no clearly defined policy for reconstituting the Internet in the event of a massive disruption. Such a policy should:
2.1.1 Determine the role and responsibility of DHS in supporting reconstitution activities.
2.1.2 Detail as much as possible the role and responsibility for US-CERT as the office in DHS responsible for cyber security.
2.1.3 Ensure that US-CERT has statutory and regulatory authority to implement its responsibilities, as well as sufficient funding.
2.1.4 Specify how DHS principals will use the Homeland Security Operations Center, if at all, to coordinate complex cyber-reconstitution actions — even where restoration is occurring as the result of a natural disaster or accident and not an attack.

2.1.5 Explain the role of regulators, such as the Federal Communications Commission (FCC) or sector-specific agencies (such as those in the financial services sector). In particular, the administration needs to explain how the FCC will operate once a critical warning occurs and in the aftermath of an event, and how the FCC coordinates with DHS and other entities. Since Hurricane Katrina, the FCC has created the Public Safety and Homeland Security Bureau, which is charged with helping to manage a massive Internet disruption. There is no guidance, however, on how the FCC's evolving responsibilities duplicates DHS' mission and operations.
2.1.6 Explain the role and responsibility of the Federal Emergency Management Agency (FEMA) and how it will operate during a cyber event of national significance. If a disaster declaration is approved, there is no clarity about how the emergency support functions (ESFs) — other than the communications ESF — operate to support reconstitution following a cyber event. Similarly, DHS should clarify the roles and responsibilities for the White House prior to and in the aftermath of a disruption. For example, if a disruption is global, how will roles and responsibilities differ for the Homeland Security Council and National Security Council? DHS should explain the roles and responsibilities of other entities, including the State Department, Department of Defense and others with global responsibilities to manage global incidents.
2.2 Fix the NRP's Cyber Annex. The administration should review the NRP and immediately make changes that reflect the administration's policy. At a minimum, the administration should define key assumptions and statements directly in the NRP, which includes the Cyber Annex. For example, the administration states that it has the authority to declare a cyber emergency and will consult with industry leaders. The administration should set forth the factors for declaring such an emergency and the details of what aspect of the industry DHS will consult. It should define the roles and responsibilities of various government entities — such as the NCSD, NCS, FCC and the White House's Office of Science and Technology Policy (OSTP).
2.3 Develop a national economic recovery system. The gap analysis suggests that the sole use of the NRP for cyber events might not be the most prudent course of action. The NRP has worked successfully at times for natural disasters and terrorist attacks. However, more than any other critical infrastructure, Internet disruptions can raise serious market concerns, undermine the delivery of critical business services and harm the economy. The Roundtable recommends developing a separate planning mechanism that allows final decision makers to balance the priorities of first responders with those of more sophisticated market issues.

3 The private sector and the government should cooperate to create joint public and private programs and institutions.
The Roundtable's gap analysis identified strategic gaps that require joint collaboration across the critical infrastructure sectors, with government and partners in academia. These coordinated efforts would seek to accomplish the following:
3.1 Improve the ability to warn globally about Internet attacks. Government, industry and academia must come to terms with the lack of clarity surrounding early warning mechanisms and services. The Roundtable recommends that the administration direct appropriate entities to prepare documentation to clarify roles and responsibilities for early warning systems. The Roundtable also recommends that DHS' chief financial officer and business office commit to funding US-CERT (or some other entity) to provide these and other services. At this time, neither DHS nor US-CERT has set forth, in clear and unmistakable language, how the federal government will identify trip wires and share such findings with appropriate industry stakeholders. Nor are such services amply funded within DHS.
3.2 Increase the ability to respond quickly. The initial 24 hours after a major cyber disruption is identified may determine the success of protective actions as well as reconstitution. As the nation consolidates and authorizes institutions to manage reconstitution, efforts must immediately focus on how best to coordinate the initial actions once a threat is identified. Also, the Roundtable recommends that the stakeholders immediately clarify who is responsible, whether in industry or government.
3.3 Create a panel of subject matter experts. The Roundtable recommends that Congress, the administration, industry and academia immediately resolve the lack of formally recognized subject matter experts that can help restore Internet services in the event of a massive disruption. Both public and private sectors point to available expertise to serve as subject matter experts, such as the National Infrastructure Coordinating Center (NICC) in DHS. Other groups, such as the NCC-Communications ISAC and IT-ISAC, also offer expertise. However, there is no single, agreed-upon center of such support, with business rules and relevant agreements on how experts will be called on to provide support. Congress must also authorize and appropriate funds for support — whether in the form of NET Guard or some other format.
3.4 Exercise, train and develop processes from lessons learned. The Roundtable recommends that DHS and industry institutions create formal processes to exercise and train for Internet-reconstitution emergencies. At this time, there are no formal programs; DHS is in the process of creating a large-scale cyber exercise, but we will need several exercises that focus on various goals and objectives. Lessons learned for each is required as is a governance process to ensure that lessons are integrated into formal programs and procedures, whether in government or industry.
3.5 Develop a joint program to shore up market confidence. The public and private sectors must have a single plan for shoring up the financial markets and public trust and confidence following an event. Lessons learned from Hurricane Katrina suggest that political and business leaders must consider, in advance, how they intend to respond prior to and in the aftermath of a major cyber disruption.
3.6 Provide effective oversight and strategic direction. To date, Congress has not outlined its oversight role with regard to Internet reconstitution. The Roundtable recommends that Congress work more closely with the administration and industry to develop a strategic agenda. The Roundtable also believes that there are long-term funding needs that must be met. In many cases, the funding required is not substantial. For example, funding for communications capabilities, such as the ACN, HSIN and the Critical Infrastructure Warning Information Network (CWIN) should be consolidated into a single, reliable capability essential to meet cyber-reconstitution goals. However, these programs overlap, have had to fight for resources internally at DHS and are not receiving the attention required given the importance of the Internet. Congress must carve out an oversight and legislative agenda to meet these short-term needs as well as other long-term challenges.

* * *

The full report: http://www.businessroundtable.org/pdf/20060622002CyberReconFinal6106.pdf

Category 16.3 Infrastructure vulnerabilities

2006-07-18 DHS Daily OSIR; Washington Post http://www.washingtonpost.com/wp-dyn/content/article/2006/07 /17/AR2006071701170.html

TO AGENCY INSIDERS, CYBER THEFTS AND SLOW RESPONSE ARE NO SURPRISE.

To government officials responsible for information security and to outside experts, intrusions into government Websites is no surprise. Over the past several years, some agencies have received failing grades on a congressional report card for their information-security practices. The overall grade for federal agencies in 2005 was D-plus. Officials and experts say that the frequency of the recent security incidents is not unusual, and that much more work needs to be done in the federal government to implement effective cybersecurity policies. In fiscal 2005, major federal agencies reported about 3,600 incidents that were serious enough to warrant alerting the government's cybersecurity center at the Department of Homeland Security, including 304 instances of unauthorized access and 1,806 cases of malicious computer code, according to a yearly Office of Management and Budget report. But that does not present a full picture. Despite requirements to do so, agencies are "not consistently reporting incidents of emerging cybersecurity threats," government auditors said last year.

Category 16.3 Infrastructure vulnerabilities

2006-07-26 DHS Daily OSIR; Associated Press http://www.contracostatimes.com/mld/cctimes/business/15129656.htm

TXU TO HIRE GUARDS, DEFEND COPPER FROM THEFT.

More people are risking their lives to steal copper, prompting TXU Electricity Delivery to hire off-duty police officers and security personnel to protect the wire at some of its substations. TXU Electricity Delivery, which is based in Dallas, TX, said Wednesday, July 26, it also will replace stolen copper with a less valuable metal, install lighting, update security systems at facilities, and partner with local law enforcement to catch metal thieves. TXU lost $633,000 last year to copper theft, not including the cost of the accompanying power outages, said TXU spokesperson Carol Peters. Jim Owen of the Edison Electric Institute, said he has heard from many members worried about increasing metal thefts. "Different companies are handling this in different ways, and some have been more agressive than others," Owen said. Peters said copper theft can also endanger substation workers if important safety equipment is purloined. Peters said the company has occasionally employed security since 1989 when copper thefts were an intermittent problem, but TXU is now seeing an unprecedented rate of theft, she said.

Category 16.3 Infrastructure vulnerabilities

2006-08-02 DHS Daily OSIR; Associated Press http://wcbstv.com/topstories/local_story_214104503.html

INDIAN POINT SIRENS DISABLED FOR SIX HOURS.

The emergency sirens that are designed to alert nearby residents of an emergency at the Indian Point nuclear power plants were out of service for more than six hours Wednesday morning, August 2, because of a computer malfunction. The sirens, which have a history of operating problems and will be replaced by next year, were out from 12:06 a.m. to 6:35 a.m., EDT, said Jim Steets, spokesperson for Indian Point owner Entergy Nuclear Northeast. He said the malfunction was unrelated to heat and power problems currently plaguing the area. He said a computer program that continuously monitors the sirens malfunctioned. Had an emergency during the outage, a backup plan involving trucks with loudspeakers would have been implemented.

Category 16.3 Infrastructure vulnerabilities

2006-08-04 DHS Daily OSIR; Associated Press http://www.billingsgazette.net/articles/2006/08/04/news/wyoming/50-backup.txt

BACKUPS TO 911 BEING REVIEWED.

While the Public Service Commission investigates an outage that left much of Wyoming without 911 service for hours Tuesday, August 2, some in law enforcement are questioning the effectiveness of backup systems. Michael Dunne, a spokesperson for Qwest Communications, said the backup plan worked as calls were routed to city lines. But not everyone in law enforcement agreed, noting that some communities were without their 911 service for three to seven hours. In many areas, law enforcement contacted local media, hoping to spread the word that 911 service was down and to tell people they could contact emergency services through other means. But even that caused complications. Dispatchers are trained to take 911 calls before other calls, but with everything coming in on the same lines, there was no way to distinguish one call from another. Dispatchers also had to get callers' phone numbers and locations -- information the 911 system provides automatically -- over the phone.

Category 16.3 Infrastructure vulnerabilities

2006-08-14 DHS Daily OSIR; WCAV TV (VA)
http://www.charlottesvillenewsplex.tv/news/headlines/3553512.html

VIRGINIA CSX HIT BY COPPER THIEVES.

With copper worth nearly $4 per pound criminals can make a pretty penny selling it and they are going to great lengths to get it. “Copper is bringing in a lot of money right now. It’s over $3 a pound,” said Patrick Sheridan of the Louisa County (VA) Sheriff’s Department. That's why Louisa County sheriff's department says thieves have been stealing it at alarming rates from these CSX utility poles along the railroad tracks. CSX reports stolen copper wire in Louisa, Cismont, and in Scottsville. The railroad is losing thousands in personal property so when operators saw someone suspicious on the tracks Wednesday, August 9, they called the sheriff. “We hid in the woods and while hiding in the woods we were able to watch him pull down the copper wire from the poles, cut it down, roll it into small rolls and set it on the tracks,” said Sheridan.

Category 16.3 Infrastructure vulnerabilities

2006-08-19 DHS Daily OSIR; Associated Press http://www.kotv.com/news/?109641

COPPER THEFT LEADS TO SECOND POWER OUTAGE.

Utility officials blamed a blackout that left several thousand households in Oklahoma City, OK, without power on the theft of copper from a substation. The Friday, August 18, outage marked the second time in two weeks that thieves broke into Oklahoma Gas and Electric Co. (OG&E) substations to steal copper, which is selling for near-record high prices. The latest outage apparently was caused by a stolen copper wire used to ground the substation equipment, OG&E spokesperson Brian Alford said. The theft is believed to have occurred late Thursday night or early Friday morning even though the power outage began about 3:30 Friday afternoon. The outage follows just eight days after someone broke into an OG&E power substation in Moore to steal copper from a transformer. That attempt shut off electricity for about 5,500 customers. Oklahoma Corporation Commissioner Denise Bode said, "This is critical infrastructure...When you're shutting down a substation or knocking out a transmission line, you have an impact on a segment of the economy and the infrastructure that's being supplied." The commission is working with the state Department of Homeland Security, the Oklahoma Sheriff's Association, and other groups to curtail thefts.

Category 16.3 Infrastructure vulnerabilities

2006-09-20 DHS Daily OSIR; Journal News (NY)
http://www.thejournalnews.com/apps/pbcs.dll/article?AID=/200
60920/NEWS02/609200374/1023/NEWS07

COMPUTER MALFUNCTION DOWNS INDIAN POINT SIREN SYSTEM.

A computer malfunction knocked 156 emergency sirens offline in a 10-mile radius around the Indian Point nuclear power plants in Buchanan, NY, for about an hour Tuesday, September 19. The siren system's computer malfunctioned after a routine maintenance check at 12:08 p.m. EDT said Larry Gottlieb, a spokesperson for Entergy, the plants' owner. Technicians rebooted the system and had it operating by 1:10 p.m., and the Nuclear Regulatory Commission, local emergency planning personnel, and government officials were notified. Gottlieb said the system, which is on schedule to be completely replaced by January, now runs with two computers that were designed to back each other up, but do not function independently during maintenance. Gottlieb added that in the event of an emergency and a complete failure of the siren system, the plant has several backup plans, beginning with a fleet of vehicles with mounted speakers to alert residents to tune in to radios or televisions where more detailed information would be made available. On September 13, the company tested all 156 sirens, ten of which failed to properly activate. The new system being installed may also involve high-speed automated telephone calling to residents' homes as a backup.

16.4 Homeland Security preparations, plans, drills, & government actions

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2006-01-11 EDUPAGE; http://www.internetnews.com/security/article.php/3576886

DHS GRANT FUNDS OPEN SOURCE RESEARCH

The Department of Homeland Security (DHS) has awarded a $1.24 million, three-year contract to improve the quality of open source software. Given the growing reliance on open source technologies for infrastructure that underpins national security, DHS expects to see real benefits from the grant. The award will be split among Stanford University, Symantec, and Coverity, a firm that specializes in code analysis. Rob Rachwald, senior director of marketing at Coverity, said, "The DHS in many ways is obviously brokering this and they are the main beneficiary." For the grant, Coverity will identify security flaws and risks; Stanford will offer academic analysis of trends and provide opinions about the relative security of various technologies; and Symantec will provide consulting on how governmental agencies can incorporate open source products in a secure fashion into their own applications.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2006-01-24 DHS Daily OSIR; http://www.washingtontechnology.com/news/1_1/homeland/27812-1.html

DHS VOWS TO PROTECT INFO ON NATIONAL DATABASE.

The Department of Homeland Security (DHS) has stepped up assurances that it will maintain the confidentiality of critical infrastructure information submitted to the National Asset Database, according to the newly revised draft National Infrastructure Protection Plan (NIPP) Base Plan version 2.0. DHS will evaluate all requests to view the database and will grant access only to select DHS employees and others on a “tightly controlled, need-to-know” basis, the revised plan states. The new language is set forth in the 234-page NIPP distributed by DHS this week. The plan was delivered by e-mail via NIPP@dhs.gov. The plan establishes a work and time frame for assessing vulnerabilities and risks and coordinating protections for 17 critical infrastructure sectors, including IT and telecommunications. Cybersecurity is treated as a cross-sector responsibility. DHS’ assurances about database access appear to address concerns raised by IT executives and others over protecting confidentiality of the information they might submit on specific vulnerabilities within their sectors. One fear raised by IT industry members is that disclosing weak spots in their own networks may result in leaks that can be exploited by competitors.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2006-01-30 DHS Daily OSIR; http://www.washingtontechnology.com/news/1_1/daily_news/2787 7-1.html

DHS, AGENCIES PLAN JOINT CYBER STORM EXERCISE.

The Department of Homeland Security (DHS) will test how well it works with other federal agencies and private IT companies to protect cybersecurity in a national exercise from February 6-10. The Information Technology Information-Sharing and Analysis Center will take part in the exercise, known as “Cyber Storm,” with DHS to test its draft concept of operations for responding to cybersecurity incidents. Participating in Cyber Storm are Cisco Systems Inc., Citadel Security Software Inc., Computer Associates International Inc., Computer Sciences Corp., Intel Corp., Microsoft Corp., Symantec Corp., and VeriSign Inc., the center announced on its Website. Cyber Storm also will involve government agencies. According to Donald Purdy, acting director of DHS’ National Cyber Security Division, the division established the Government Forum of Incident Response and Security Teams (GFIRST) to facilitate interagency information sharing and cooperation for readiness and response. The teams, comprising government computer experts, are responsible for IT security at government agencies. In addition to the GFIRST teams, the agency has worked with the Defense and Justice departments to form the National Cyber Response Coordination Group to provide an organized federal response to cybersecurity breaches.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2006-02-16 EDUPAGE; http://www.fcw.com/article92354-02-16-06-Web

FBI DIRECTOR CALLS FOR MORE PARTNERSHIPS

Speaking at the RSA Conference this week, FBI Director Robert Mueller called for more partnerships among law enforcement agencies, the private sector, and colleges and universities. Mueller characterized cyberspace as a "largely unprotected frontier with seemingly limitless opportunity," noting that much of that opportunity is exploited by criminals. He said the changing landscape of technology infrastructure makes traditional jurisdictional boundaries obsolete. The FBI now includes a division created in 2002 that focuses exclusively on cybersecurity, and each of the bureau's 56 field offices includes a squad that deals with computer crimes. The FBI has a number of existing programs coordinated with private-sector organizations, but those partnerships need to expand, Mueller said.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2006-05-16 DHS Daily OSIR; WZRB-TV (LA) http://www.2theadvocate.com/news/2807481.html

PANEL APPROVES EMERGENCY COMMUNICATION BILL

On Monday, May 15, a Louisiana state House committee approved a plan that would rely on text messages, e-mails and message boards to keep the public informed during emergencies, but it can't be put into place before June 1. During Hurricanes Katrina and Rita, many cell phone towers lost power or were damaged by wind, and the ones left standing were so overloaded that text messages became one of the best ways to communicate. That's why lawmakers want to allow the state to send residents messages with the latest emergency information.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2006-06-20 DHS Daily OSIR; Government Health IT http://govhealthit.com/article94971-06-20-06-Web

OASIS ADOPTS INFO SHARING STANDARD FOR EMERGENCY RESPONDERS.

Emergency responders in the field now have a data-sharing standard that provides role-based information sharing in a crisis. The Organization for the Advancement of Structured Information Standards (OASIS), a nonprofit, international consortium, has approved the Emergency Data Exchange Language Distribution Element (EDXL-DE) Version 1.0 as an OASIS standard. EDXL-DE facilitates emergency information sharing and data exchange across local, regional, tribal, national and international organizations in the public and private sectors, OASIS officials said. The Department of Homeland Security (DHS) has collaborated since 2004 with private-sector members of the Emergency Interoperability Consortium (EIC), a public/private partnership, to create EDXL, OASIS officials said. DHS and the EIC created the requirement for the standard and OASIS developed the actual standard, according to Elysa Jones, chairwoman of the OASIS Emergency Management Technical Committee.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2006-06-21 DHS Daily OSIR; KSBI-TV 52 (OK) http://www.ksbitv.com/technology/3066781.html

SOLDIERS, FIRST RESPONDERS TEST NETWORK SKILLS.

Exercise Grecian Firebolt, June 10-23, has been testing the connections between military and civilian response agencies in case disaster strikes. The annual exercise also lets soldiers throughout the United States prove their ability to set up voice, data and video services to units operating from Massachusetts to California. This year, the Federal Emergency Management Agency (FEMA) is using Grecian Firebolt 2006 to test its network and how it communicates with the Army's. "Grecian Firebolt provides an excellent venue for testing equipment interoperability between FEMA and Army communications systems; sharing tactics, techniques, and procedures; contingency planning; design of communications infrastructure; and building habitual interagency relationships," said Maj. Gen. Donna Dacier, commander of the 311th Theater Signal Command.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2006-06-27 DHS Daily OSIR; Washington Post http://www.washingtonpost.com/wp-dyn/content/article/2006/06/26/AR2006062601304.html

BUSH ORDERS UPDATE OF EMERGENCY ALERT SYSTEM.

President Bush Monday, June 26, ordered Department of Homeland Security Secretary Michael Chertoff to overhaul the nation's hodgepodge of public warning systems, acknowledging a critical weakness unaddressed since the 2001 terrorist attacks and exposed again last year by Hurricane Katrina. The Emergency Alert System, best known for weather bulletins and Amber Alerts for missing children, should be upgraded to explore communicating by cell phones, personal digital assistants and text pagers targeted to geographic areas or specific groups, U.S. officials said. In a 30-paragraph executive order issued by the White House without comment, Bush assigned Chertoff to implement a freshly stated U.S. policy "to ensure that under all conditions the President can communicate with the American people," including in cases of war, terrorist attack, natural disaster or other public danger. The move follows mounting criticism that the nation's alert systems are outmoded relics of the Cold War.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2006-07-06 DHS Daily OSIR; Department of Homeland Security http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0942.xml

DHS ANNOUNCES GRANTS TO SECURE THE NATION'S CRITICAL INFRASTRUCTURE.

The U.S. Department of Homeland Security (DHS) announced on Thursday, July 6, that nearly $400 million in Fiscal Year 2006 grants will be made available to strengthen the nation's ability to prevent, protect against, respond to and recover from terrorist attacks, major disasters and other emergencies that could impact this country's critical infrastructure. The funding will be dispersed through the DHS Office of Grants and Training's Infrastructure Protection Program. "The Infrastructure Protection Program provides the means to move forward in developing sustainable, risk-based critical infrastructure security initiatives for man-made and natural threats that could potentially have devastating impacts on the economy and communities throughout the nation," said DHS Under Secretary for Preparedness George Foresman. The infrastructure grants will be divided among seven programs that constitute major critical infrastructure sectors ranging from transportation modes to the nation's ports. Allocation totals have been determined for five of the programs: Transit Security Grant Program (intracity rail, bus, and ferry systems), Buffer Zone Protection Program, Chemical Sector Buffer Zone Protection Grant Program, Intercity Passenger Rail Security Grant Program, and the Trucking Security Program. For information on allocations and eligible applicants visit the Office of Grants and Training: http://www.ojp.usdoj.gov/odp/grants_programs.htm

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2006-07-11 DHS Daily OSIR; Government Executive http://www.govexec.com/story_page.cfm?articleid=34523

OPM: IN PANDEMIC, HOMES COULD BECOME 'SAFE HAVENS' FOR WORK.

In the case of a pandemic flu outbreak, federal agencies could find ways to encourage employees barred from leaving their houses to work from home, despite the lack of legal authority to mandate telework, according to new guidelines from the Office of Personnel Management (OPM). The 76-page OPM document released Monday, July 10 is the second of three guides prepared in response to President Bush's request for a plan to keep federal agencies operating during emergency situations such as an outbreak of pandemic flu. The document, drawing on existing laws and regulations, states that neither agency heads nor OPM can mandate telework. By ordering an evacuation and authorizing pay for evacuated employees, however, agencies can declare the employees' homes "safe havens," and require them to "perform any work necessary" from their homes during the evacuation period, the document states. If employees refuse to work from home in such a situation, they could be required to use annual leave and could be furloughed or disciplined, the guidelines state. Future guidance is expected to address the administration of evacuation payments during pandemic influenza. OPM guidelines, "Human Capital Planning for Pandemic Influenza": http://www.govexec.com/pdfs/HandbookOPM2ndJuly72006.pdf

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2006-07-19 DHS Daily OSIR; Associated Press http://www.nytimes.com/aponline/technology/AP-Cybersecurity-Protection.html

AGENCIES TO TEACH CYBERSECURITY PROTECTION.

Federal scientists who study how hackers try to break into computer-based controls for nuclear reactors and other automated industrial systems are passing the secrets on to the private operators of such facilities. The U.S. Department of Energy and U.S. Department of Homeland Security will sponsor free classes in protecting remote controls of critical infrastructure during an international cybersecurity summit in Las Vegas September 28-30. Researchers from the Idaho National Laboratory will demonstrate cybersecurity attacks on Supervisory Control and Data Acquisition, or SCADA, networks that regulate electrical-supply systems and other automated industrial controls of potential terrorist targets, such as railroads, chemical plants and hydroelectric dams.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2006-08-11 DHS Daily OSIR; Navy Compass http://www.navycompass.com/news/newsview.asp?c=192164

LOCAL ORGANIZATIONS DISCUSS HOW THE MILITARY CAN ASSIST IN A DISASTER.

Various San Diego County officials came together in El Cajon, CA, on Thursday, August 3, to discuss how the military could assist in the event of a natural disaster. The meeting allowed major San Diego emergency preparedness organizations and two major military commands within the region to discuss policies and procedures on how to request use of military assets in an emergency. Commander, Navy Region Southwest Rear Admiral Len Hering, said Katrina was an example of how local and state agencies did not know enough about how to energize the federal government system in an emergency. San Diego Chief for the California Department of Forestry Charles Manner said he had an idea of how the process went for requesting military assistance in a local or state emergency and that the biggest thing he was concerned about was knowing exactly what military assets are available at the time of a disaster. San Diego County Office of Emergency Services Coordinator Debra Keeney said, "This was a really good beginning to a conversation that we need to continue to have. We can't afford to not have an open line of communication and response."

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2006-09-05 DHS Daily OSIR; Contra Costa Time (CA) http://www.contracostatimes.com/mld/cctimes/news/15441796.htm

DISASTER PLAN IS KEY FOR SCHOOLS.

The San Ramon Valley, CA, school district is becoming a partner in regional disaster preparedness, which advocates say is crucial because thousands of students are likely to be stuck at their schools after a major earthquake. Administrators and teachers will receive training in such skills as basic fire-fighting, triage and wound treatment and how to manage a disaster team. Planners say the school district's involvement is important because, on a given day, 20 percent of the San Ramon Valley population is at a district facility: 22,000 students, 2,500 employees occupying 32 buildings. The district encompasses a wide swath from Alamo to San Ramon, including several new schools in Dougherty Valley. The district has evaluated supply inventories on campuses, for which they have 40-foot containers; they plan to train administrators; and the goal is for each individual school to have an emergency operations plan.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2006-09-25 DHS Daily OSIR; Associated Press http://www.cnn.com/2006/EDUCATION/09/25/schools.warnings.ap/

HAZARD-WARNING RADIOS PROVIDED TO PUBLIC SCHOOLS.

The government plans to supply hazard-warning radios to all 97,000 public schools in the United States. The National Weather Service, part of the National Oceanic and Atmospheric Administration (NOAA), operates more than 950 short-range radio stations and has encouraged schools, businesses, and homeowners to buy warning radios that are activated with a broadcast signal that automatically turns a radio on and announces a potential hazard. The Department of Homeland Security will provide $5 million to make sure these radios are in every public school, NOAA Administrator Conrad Lautenbacher said. Originally conceived as a means to deliver weather warnings, the system now covers all hazards -- for example, terrorism, abducted children, and derailed trains carrying toxic materials.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2006-09-29 DHS Daily OSIR; Montgomery Advertiser (AL)
http://www.accessmontgomery.com/apps/pbcs.dll/article?AID=/20060929/NEWS02/609290328/1009

ALABAMA'S RESPONSE SYSTEM: A MODEL FOR OTHER STATES.

Alabama's Homeland Security response system is so good that other states are sending representatives to see how they can improve their operations, a state official said Thursday, September 28. Joe Davis, assistant director of the Alabama Office of Homeland Security, said a communications system that links hundreds of state agencies and local departments to speed response to crisis situations is a big factor. Davis said in the past, only 350 of the state's 850 departments had access to each other because of equipment disparities. He said a $12 million communications upgrade has "greatly improved" the system. "We've developed a world-class communications system that puts law enforcement and emergency response teams in touch with each other immediately," Davis said.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2006-10-23 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article96546-10-20-06-Web

DHS TO BOOST USE OF SECURE DATA-SHARING NET.

The Department of Homeland Security (DHS) is pushing to strengthen the deployment of the Homeland Security Information Network (HSIN). The department recently established a HSIN advisory committee to provide independent advice from representatives of state, local and tribal governments, as well as from the private sector, about what users specifically need from HSIN, which could go a long way toward answering complaints about the network. There were high expectations when the initiative was first proposed several years ago. The network was seen as a vital means for quickly sharing information about security threats among all levels of government. DHS Secretary Michael Chertoff, speaking at the recent International Association of Chiefs of Police annual conference in Boston, reiterated the need for real-time data sharing. “We are going to build upon some of our early initial efforts...by creating a national network of intelligence fusion centers to support state and local decision-makers, chiefs of police, and state and local intelligence officials,” he said. A part of that will entail use of a new homeland secure data network. Charlie Allen, DHS’ chief intelligence officer, said there are plans for providing HSIN, which was initially designed as an unclassified network, with a classified component.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2006-10-27 DHS Daily OSIR; Government Computer News
http://www.gcn.com/online/vol1_no1/42432-1.html

CHERTOFF LAYS OUT PLAN FOR FUSION CENTERS.

As the United States faces threats from weapons of mass destruction, as well as high-consequence international and homegrown plots, the Department of Homeland Security (DHS) is working with state, local, federal and international law enforcement to defend the country from terrorism. DHS Secretary Michael Chertoff said stopping domestic terrorism threats is best done through shared intelligence, starting at the local level. To ensure that this coordination and collaboration happens, DHS will establish fusion centers, stocked with experts, and will work to grant clearance of classified information more quickly. Both initiatives are part of the department’s effort to take its relationships with major city police chiefs and information sharing to the next level. The fusion centers will be made up of intelligence personnel from the federal intelligence community, subject matter experts and intelligence analysts and operators of local police departments. The goal is to “become more deeply embedded in one another’s day-to-day intelligence analysis and operational activity,” Chertoff said. DHS plans to have 20 fusion centers by the end of the fiscal year and up to 35 fusion centers by the end of the next fiscal year.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2006-11-13 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article96761-11-13-06-Print

DEPARTMENT OF DEFENSE TESTS WIRELESS TECHNOLOGY FOR FIRST RESPONDERS.

The Joint Task Force-Civil Support (JTF-CS) and Joint Forces Command (JFCOM) are testing wireless technology needed to assist first responders and civilian agencies during a chemical, biological, radiological or nuclear attack. As part of U.S. Northern Command, JTF-CS is designated to be the first military team on the ground in such a crisis. The unit must integrate its efforts with first responders and civilian agencies. Lives depend on its ability to deploy and set up operations quickly. JTF-CS officials say wireless networks are the solution. Currently, tactical units on the front lines cannot set up wireless local area networks quickly and securely. But now JTF-CS and JFCOM say they hope to fill that need with a program called Wireless for the Warfighter (W4W). That program provides a wireless extension for computer and phone lines that can be set up within minutes rather than hours. In addition to cutting the time needed to set up a network, W4W pushes network access to individual warfighters and reduces the command’s footprint on the ground by eliminating cabling and related equipment, said Patty Critzer, deputy director of computer systems at JTF-CS.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2007-01-09 DHS Daily OSIR; Department of Homeland Security
http://www.dhs.gov/xnews/releases/pr_1168366069190.shtm

DHS ANNOUNCES $445 MILLION TO SECURE CRITICAL INFRASTRUCTURE.

The Department of Homeland Security (DHS) released on Tuesday, January 9, fiscal year 2007 grant guidance and application kits for five grant programs that will total roughly $445 million in funding for state, local and private industry infrastructure protection initiatives. These five programs comprise the Infrastructure Protection Program (IPP), which to date have provided more than $1.5 billion in grants to strengthen security at critical facilities ranging from chemical plants to mass transit systems and seaports. "We're investing resources where risk is greatest and where the funds will have the most significant impact," said Homeland Security Secretary Michael Chertoff In addition to other grants, Amtrak will receive $8 million under the Transit Security Grants Program to enhance intercity passenger rail security initiatives and to coordinate efforts with local and regional transit systems. In addition to other grants, for the first time, Transit Security Grants will provide award recipients the flexibility to decide where they can better focus their resources. In the past, these awards were allocated in specific amounts for rail and separate amounts for bus. Transit Security Grants will further fund enhanced security for 19 ferry systems in 14 regions

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2007-02-01 DHS Daily OSIR; Beacon News (IL)
http://www.suburbanchicagonews.com/beaconnews/news/238528,2_1_AU01_CODERED_S1.article

NEW EMERGENCY CALL SYSTEM CAPABLE OF DIALING UP 60,000 RESIDENTS PER HOUR.

Kane County in Illinois is implementing an emergency telephone notification system that calls the public with a pre-recorded message providing vital information during an emergency. "The CodeRED system will give county officials a new tool to help disseminate emergency information during any emergency or disaster," said Don Bryant, director of the Kane County Office of Emergency Management. Bryant said emergency management officials can record the message, then call up to 60,000 listed telephone numbers per hour. It is similar to a reverse 911 system, he said. Anyone with an unlisted phone number or cell phone must register on the emergency management office's Website, www.kcoem.org and enter their information on the CodeRED Residential and Business Data Collection page. He said the information will be kept secure and confidential. The Office of Emergency Management will use the system to relay information about boil orders, local Amber Alerts or to provide information after a natural or man-made disaster, Bryant said. Officials use a map to pinpoint where calls should be made, he said. Additional information about CodeRED: http://www.kcoem.org/CodeRED/CodeRED.htm

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2007-02-01 DHS Daily OSIR; National Defense
http://www.nationaldefensemagazine.org/issues/2007/Febuary/Fusioncenters.htm

FUSION CENTERS AIM TO CONNECT FEDERAL, STATE, LOCAL AGENCIES.

The Maryland Coordination and Analysis Center (MCAC) is one of about 20 state, local or regional "intelligence fusion centers" that has received Department of Homeland Security (DHS) funding. The concept calls for states, regions or cities to gather representatives from all their law enforcement agencies under one roof, along with intelligence analysts and representatives from federal agencies. Charles Allen, DHS intelligence officer, said if there is pertinent information, the department will find a way to quickly push it down to the appropriate officials, regardless of whether they have a fusion center. For top secret documents, DHS, Justice and the Defense Department are forming a federal coordinating group at the National Counterterrorism Center to find ways to vet source material for local officials. Allen is also leading efforts to install the classified homeland security data network terminals at fusion centers, or other state and local law enforcement offices. Among the systems MCAC is using is the Defense Department's secret Internet protocol router network (SIPRNET), DHS' homeland security information network (HSIN) and the Justice Department's Guardian system. The HSIN allows the center to link to other state and local fusion centers. MCAC Website: http://www.mcac-md.gov/ Maryland Governor's Office of Homeland Security: http://www.gov.state.md.us/gohs/gohs_initiatives.html

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2007-02-04 DHS Daily OSIR; Washington Post http://www.washingtonpost.com/wp-dyn/content/article/2007/02/03/AR2007020301120.html

CDC PRACTICES FOR INFLUENZA PANDEMIC.

The Centers for Disease Control and Prevention (CDC) held a pandemic "war game" in Atlanta, GA, last week but aborted it at midnight Wednesday, January 31, halfway through its planned 24-hour run. The reason was concern about public safety. The CDC did not want a hundred of its most valuable employees rushing on Thursday morning, February 1, over ice-slick roads to a mock disaster. A real pandemic, which is considered inevitable, won't be stopped by weather. In fact, it probably won't be stopped by anything. But public health experts believe it could be made less disastrous with practice and preparation. The federal government is hard at work trying to ready the country for a global outbreak of a new, highly transmissible strain of influenza -- a pandemic. The drill will pick up in April with an exercise in which pandemic flu has spread to many states. In a final round in May, the virus gets to Atlanta and takes out 40 percent of the CDC's workforce.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2007-02-08 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article97613-02-08-07-Web

DHS TO TEST COMMUNICATIONS STRATEGY IN EXERCISE.

As part of an exercise involving a simulated terrorism attack, the Department of Homeland Security (DHS) wants to gauge the extent to which the public would trust information DHS releases electronically. Like its predecessors, the fourth Top Officials (TopOff) exercise is intended to test the nation's readiness to deal with a large-scale terrorist attacks. This time, the exercise will test the department's public communications strategy. The idea is to give the public information that is as complete and timely as possible about the events surrounding the attacks and what actions they should take to protect themselves. DHS will provide that information in two formats: a live video feed and a Website. The live feed will resemble a newscast, according to DHS, featuring interviews with public officials and other experts, while the Website will function more like a newspaper.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2007-02-09 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2093175,00.asp

CYBER-SECURITY CZAR CALLS ON IT INDUSTRY FOR HELP.

Addressing a crowded room of attendees at the ongoing RSA Security Conference on Thursday, February 8, Greg Garcia, assistant secretary for cyber-security and telecommunications at the Department of Homeland Security, said that he and his team are already hard at work creating policies that aim to better protect critical infrastructure. Over the first four months on the job, Garcia said, he has focused primarily on establishing a game plan for his office's future projects and working to establish inroads with members of the IT and communications industries to encourage private companies' contribution to those efforts. While the federal government is aggressively looking for ways to create stronger protections for the nation's IP backbone, the process will not be able to move forward quickly unless businesses and academic institutions that control the nation's largest networks are willing to pitch in, he said. The cyber-security chief said that his initial priorities revolve around work to breed cooperation between federal agencies to develop common security policies for defending networks and to help the private sector strengthen national preparedness and incident-response plans.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2007-02-12 DHS Daily OSIR; IDG News Service http://www.infoworld.com/article/07/02/12/HNcyberstorm2_1.html

U.S. GOVERNMENT READYING MASSIVE CYBERSECURITY TEST.

The Department of Homeland Security (DHS) is planning a large-scale test of the nation's response to a cyberattack to be held in early 2008. The test will be a follow-up to the February 2006 Cyber Storm test, which was billed as the largest-ever U.S. government online attack simulation. Cyber Storm 2 will be conducted in March 2008, said Gregory Garcia, assistant secretary for cyber security and telecommunications with DHS, speaking at the RSA Conference in San Francisco last week. Like the first Cyber Storm, this exercise will evaluate the ability of the public and private sector to provide a coordinated response to a large-scale cyber event, he said. The second Cyber Storm test, which is in the planning stages right now, will include a greater number of participants than its predecessor. In particular, the number of international participants will be increased.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2007-03-02 DHS Daily OSIR; ComputerWorld
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9012132&source=rss_topic85

FEDS HOPE TO BOOST BUSINESS ROLE IN SLOWING CYBERATTACKS.

As reports of cybersecurity incidents grow, Department of Homeland Security (DHS) officials plan to improve their ability to work on the problem face to face with private-sector experts. The DHS plans to co-locate private-sector employees from the communications and IT industries with government workers at the U.S. Computer Emergency Readiness Team (US-CERT) facility, said Gregory Garcia, assistant secretary of cybersecurity and telecommunications at DHS. The teams will work jointly on improving US-CERT's information hub for cybersecurity, Garcia said. The agency didn't specify a starting date for the program but said it will begin soon. US-CERT is a four-year-old DHS-run joint effort of the public and private sectors to protect the nation's Internet infrastructure. "It's through this co-location that we are going to build a strong trust relationship, an information-sharing relationship," said Garcia.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2007-03-02 DHS Daily OSIR; Department of Homeland Security
http://www.dhs.gov/xnews/releases/pr_1172866131042.shtm

HOMELAND SECURITY TESTS FIRST RESPONDER CREDENTIAL CAPABILITIES.

The Department of Homeland Security Office of National Capital Region Coordination and the Department of Defense Pentagon Force Protection Agency joined public and private sector participants February 15 in a demonstration to validate the functionality of the First Responder Authentication Credential. The demonstration, known as Winter Storm, was a multi-jurisdictional test to verify the integration and interoperability of credential system attributes such as qualifications, authorizations, certifications, and privileges. More than 50 organizations, in over 20 locations across the United States, including the National Capital Region, actively participated in Winter Storm. Participants and observers viewed details on a commercially available mapping program that gave local, regional, and nationwide emergency operation centers real-time situational awareness of first responders.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2007-03-19 DHS Daily OSIR; Israel Insider (Israel)
http://web.israelinsider.com/Articles/Security/10962.htm

ISRAEL HOLDS NATIONWIDE DRILL SIMULATING MASSIVE TERROR ATTACKS.

Tuesday, March 20, will mark Israel's Home Front Command's first country-wide drill to simulate major conventional and unconventional terror attacks, Ynetnews reported. All of Israel's rescue services will be involved in the drill, which will begin with the sounding of a siren on Tuesday. The drill is aimed at testing the Home Front's preparedness for different emergency scenarios, with the goal of implementing the lessons learned from the second Lebanon war. Among the scenarios to be tested are a missile attack on a building in Netanya, causing the three-story house to collapse, and a missile landing at the Reading Power Station in Tel Aviv, causing a large number of casualties. The rescue services will be sent to other "missile landing" areas in Petah Tikva and in a community center in Jaffa. In Be'er Sheva the drill will simulate a "mega-terror attack," simultaneous to a heavy barrage of rockets in southern Israel, injuring many people.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2007-04-25 DHS Daily OSIR; New York Times http://www.nytimes.com/2007/04/25/us/25nuke.html

U.S. TAKES STEP TO ADDRESS AIRLINER ATTACKS ON REACTORS.

New nuclear reactors need not be designed to withstand suicide attacks by big airplanes, the Nuclear Regulatory Commission (NRC) decided Tuesday, April 24. Instead, the commission proposed that designers be required to analyze how their reactors can be built to mitigate the effects of such an attack, “to the extent practicable.” The commission has already approved two designs, one by General Electric and one by Westinghouse, for which no such analysis was required. One design now pending before the commission, a French-German model called the EPR, was devised to meet a European requirement that reactors be built to withstand airplane crashes. And General Electric said Tuesday that it had assessed the capabilities of its two new reactor designs, including the one already approved, and that both “have the capability to withstand the effects of an aircraft crash.” Most of several new designs incorporate features that could be helpful in case of a plane crash, like locating emergency water supplies inside the containment building, at an elevation above the reactor vessel, instead of in a tank outside the building.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2007-05-10 DHS Daily OSIR; Department of Homeland Security http://www.dhs.gov/xnews/releases/pr_1178811654577.shtm

DHS AWARDS $445 MILLION TO SECURE NATION'S CRITICAL INFRASTRUCTURE.

The Department of Homeland Security (DHS) announced on Thursday, May 10, final awards totaling $445 million in grant programs that strengthen the ability of ports, transit, and intercity bus systems to prevent, protect against, respond to and recover from terrorist attacks, major disasters and other emergencies. The awards are part of the fiscal year 2007 Infrastructure Protection Program, which has provided nearly $2 billion in grants to strengthen critical infrastructure facilities and transportation systems. "These grants will help to protect our nation's critical infrastructure from threats and hazards that could cause major loss of life, economic impact, and disruption of services," said Homeland Security Deputy Secretary Michael Jackson. "These risk-based investments will increase security for vital assets such as ports, mass transit systems, long-distance bus carriers, chemical facilities, and nuclear power plants." Funding was directly allocated in January to Tier I Transit grants, the Buffer Zone Protection Program and the Trucking Security Program. This announcement outlines the final competitively-bid portions of these grants, which includes Port Security grants, Tier II Transit Security grants, and Intercity Bus Security grants. For the list of individual grants and further information on the Infrastructure Protection Program: http://www.dhs.gov

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2007-05-14 DHS Daily OSIR; U.S. Air Force http://www.af.mil/news/story.asp?id=123053186

MILITARY, CIVILIAN EMERGENCY COMMUNICATIONS TESTED.

A two-week national-level exercise involving local, state, and federal government agencies is proving the capabilities of a system designed to provide effective communication and organization between different emergency responders. Being tested at Ardent Sentry/Northern Edge 2007, the Incident Command System (ICS) is part of the Federal Emergency Management Agency's (FEMA) National Incident Management System, which is being implemented nationwide. The ICS is a unified command and control system driven by a presidential directive that covers the Department of Defense and civilian federal government agencies, said Major Darren Deroos, the 3rd Wing chief of inspections and exercises at Elmendorf Air Force Base, Alaska. The incident command system is a combination of facilities, equipment, operators, procedures and communications designed to aid in domestic incident management activities. It can be used for a broad spectrum of emergencies, according to FEMA's national incident management system Website. May 8 and 9, military, civilian and federal authorities partnered to respond to two incidents -- a simulated train collision involving hazardous materials and mass casualties here, and a simulated terrorist attack on the North Pole Refinery Complex in nearby North Pole, Alaska. During both incidents, emergency responders used ICS to coordinate their efforts.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2007-05-21 DHS Daily OSIR; Department of Homeland Security http://www.dhs.gov/xnews/releases/pr_1179773665704.shtm

DHS COMPLETES KEY FRAMEWORK FOR CRITICAL INFRASTRUCTURE PROTECTION.

The Department of Homeland Security announced on Monday, May 21, the completion of 17 Sector-Specific Plans (SSPs) in support of the National Infrastructure Protection Plan (NIPP). The NIPP outlines a comprehensive risk management framework that defines critical infrastructure protection roles and responsibilities for all levels of government and private industry. Homeland Security Presidential Directive 7 identified 17 critical infrastructure and key resource sectors that require protective actions to prepare for, or mitigate against, a terrorist attack or other hazards. The sectors are: agriculture and food; banking and finance; chemical; commercial facilities; commercial nuclear reactors, including materials and waste; dams; defense industrial base; drinking water and water treatment systems; emergency services; energy; government facilities; information technology; national monuments and icons; postal and shipping; public health and healthcare; telecommunications; and transportation systems including mass transit, aviation, maritime, ground or surface, rail and pipeline systems. The vast majority of the nation's critical infrastructure is owned and operated by private industry. SSPs define roles and responsibilities, catalog existing security authorities, institutionalize already existing security partnerships, and establish the strategic objectives required to achieve a level of risk reduction appropriate to each individual sector.
National Infrastructure Protection Program Sector-Specific Plans Fact Sheet:
http://www.dhs.gov/xnews/gc_1179776352521.shtm

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2007-05-28 DHS Daily OSIR; Press of Atlantic City (NJ)
http://www.pressofatlanticcity.com/top_three/story/7481826p- 7376794c.html

TEXT MESSAGES COULD BE LIFE-SAVER IN EMERGENCY.

A hurricane can cut off electricity and shut down roads. Lingering storms can make it impossible to call relatives. But the same technology that teenagers use to text message could help emergency responders continue to communicate, a state researcher says. Elizabeth Gomez, an information specialist, said that during disasters and heavy weather, cell-phone signals could degrade to the point that speech is not possible. "But there's nearly always enough signal to send text," Gomez said. That is because texting works in quick bursts and requires significantly less signal to send. But even though a text message can get through, Gomez said, digital space and time are limited. "You have to know how to shrink your dialogue to 160 characters," she said. "That's the architecture of text messaging on the phone." "The most important thing is knowing what to say in a crisis," Gomez said. Gomez said speak plainly and get to the point.

Category 16.4 Homeland Security preparations, plans, drills, & government actions

2007-05-29 DHS Daily OSIR; Federal Emergency Management Agency
http://www.fema.gov/news/newsrelease.fema?id=36592

FEMA TRAINS 700 RESPONDERS ON HOMELAND SECURITY EQUIPMENT AT NEW ORLEANS CONFERENCE.

More than 700 emergency responders from 47 states and Puerto Rico will travel to New Orleans this week to receive training on equipment their departments will receive through the Department of Homeland Security Federal Emergency Management Agency's (FEMA) Fiscal Year 2006 Commercial Equipment Direct Assistance Program. This includes representtives from 19 departments who will receive accelerated training and equipment delivery because they are located in areas at high risk for hurricanes, tornados, or wildfires. Representatives from the 19 "high-risk" departments will receive training on equipment to improve incident communications, either an incident commanders' radio interface or radio interoperability system. Other responders will be trained on thermal imagers, devices used to detect humans and other warm-blooded creatures through building walls, a smoke-filled room, or in darkness.

16.5 Military perspectives on cyberwar & battlespace

Category 16.5 Military perspectives on cyberwar & battlespace

2006-01-16 DHS Daily OSIR; http://www.networkworld.com/news/2006/011606-military-security.html

MILITARY CLAMPING DOWN ON SECURITY

Lt. General Charles Croom, commander of the Joint Task Force (JTF) on Global Network Operations (GNO) and director of the Defense Information Systems Agency (DISA), last week said a sweep is underway of all Department of Defense (DoD) networks to uncover security holes amid a get-tough policy. "The attacks are coming from everywhere and they're getting better," said Croom in his keynote address at the DoD Cyber Crime Conference last week. The discovery of a botnet last November 5th inside DoD networks contributed to the decision to clamp down security. So far, the results are troubling. "Almost 20 percent of our accounts are unauthorized or had expired," Croom said, noting that military personnel tend to move every two or three years and accounts are sometimes left open. The exact tally of improper accounts won't be known until March, he said. The biggest changes to come may be in the next six months as the JTF-GNO, the organization set up to centralize decisions about security and operations in the Army, Navy, Air Force and Marines, evaluates a possible redesign of its two primary global IP-based military networks.

Category 16.5 Military perspectives on cyberwar & battlespace

2006-03-08 DHS Daily OSIR; http://www.gcn.com/online/vol1_no1/40075-1.html

INTERNET "CLOAKING" EMERGES AS NEW WEB SECURITY THREAT.

Terrorist organizations and other national enemies have launched bogus Websites that mask their covert information or provide misleading information to users they identify as federal employees or agents, according to Lance Cottrell, founder and chief scientist at Anonymizer of San Diego, CA. The criminal and terrorist organizations also increasingly are blocking all traffic from North America or from Internet Protocol addresses that point back to users who rely on the English language, Cottrell told an educational seminar in Washington at the FOSE 2006 trade show's Homeland Security Center Tuesday, March 7. Among the risks of the terrorist cloaking practice are that the organizations can provide bogus passwords to covert meetings. By doing so they can pinpoint federal intelligence agents who attend the meetings, making them vulnerable to being kidnapped or becoming the unwitting carriers of false information, Cottrell said.

Category 16.5 Military perspectives on cyberwar & battlespace

2006-05-03 TechTarget http://tinyurl.com/nnf72

DIGITAL DOOMSDAY CAN BE AVOIDED WITH PREPARATION

Bill Brenner began his report in TechTarget's SearchSecurity with the following paragraphs which reflect a scenario long described by Winn Schwartau since the early 1990s:

"A common nightmare scenario in the business world is that a hacker will crack a company's digital defenses, steal sensitive data or disable the network. Scott Borg, director and chief economist at the U.S. Cyber Consequences Unit (US-CCU), an independent organization that churns out information security data on behalf of the government, says enterprises face a darker possibility.

Online outlaws could quietly penetrate the network and, over six to eight months, alter critical data so that it's no longer accurate. For instance, an attacker could access a health insurance company's patient records and modify information on a person's prescriptions or surgical history. Or an attacker could access an automotive company's database and tamper with specifications on various car parts."

Category 16.5 Military perspectives on cyberwar & battlespace

2006-05-15 DHS Daily OSIR; Federal Computer Week http://fcw.com/article94524-05-15-06-Web

MILITARY INTEROPERABILITY TEST: COMBINED ENDEAVOR 2006

Combined Endeavor 2006, a two-week operation to test the interoperability of vital communication systems for multinational forces, began on Monday, May 15 in Lager Aulenbach, Germany. The U.S. European Command, in cooperation with the German Ministry of Defense, is sponsoring the communications and information systems interoperability exercise. Forty-one countries, including members of NATO and Partnership for Peace, are participating. The vendor providing the core network infrastructure for the exercise will test communications deployed in humanitarian, peacekeeping, and disaster relief efforts.

Category 16.5 Military perspectives on cyberwar & battlespace

2006-05-25 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article94650-05-25-06-Web

DOD: CHINA FIELDING CYBERATTACK UNITS.

China is stepping up its information warfare and computer network attack capabilities, according to a Department of Defense (DoD) report released last week. The Chinese People's Liberation Army (PLA) is developing information warfare reserve and militia units and has begun incorporating them into broader exercises and training. Also, China is developing the ability to launch pre-emptive attacks against enemy computer networks in a crisis, according to the document, "Annual Report to Congress: Military Power of the People's Republic of China 2006." The Chinese approach centers on using civilian computer expertise and equipment to enhance PLA operations, the DoD report states.

The referenced report can be found at: http://www.defenselink.mil/pubs/china.html

* * *

EXECUTIVE SUMMARY

China's rapid rise as a regional political and economic power with global aspirations is an important element of today's strategic environment – one that has significant implications for the region and the world. The United States welcomes the rise of a peaceful and prosperous China. U.S. policy encourages China to participate as a responsible international stakeholder by taking on a greater share of responsibility for the health and success of the global system from which China has derived great benefit.

China's leaders face some important choices as its power and influence grow. These choices span a range of issues: challenges of China's economic transition and political reform, rising nationalism, internal unrest, proliferation of dangerous technologies, adoption of international norms, and China's expanding military power.

The People's Liberation Army (PLA) is in the process of long-term transformation from a mass army designed for protracted wars of attrition on its territory to a more modern force capable of fighting short duration, high intensity conflicts against high-tech adversaries. Today, China's ability to sustain military power at a distance is limited. However, as the 2006 Quadrennial Defense Review Report notes, "China has the greatest potential to compete militarily with the United States and field disruptive military technologies that could over time offset traditional U.S. military advantages."

In the near term, China's military build-up appears focused on preparing for Taiwan Strait contingencies, including the possibility of U.S. intervention. However, analysis of China's military acquisitions suggest it is also generating capabilities that could apply to other regional contingencies, such as conflicts over resources or territory.

The PLA's transformation features new doctrine for modern warfare, reform of military institutions and personnel systems, improved exercise and training standards, and the acquisition of advanced foreign (especially Russian) and domestic weapon systems. Several aspects of China's military development have surprised U.S. analysts, including the pace and scope of its strategic forces modernization. China's military expansion is already such as to alter regional military balances. Long-term trends in China's strategic nuclear forces modernization, land- and sea-based access denial capabilities, and emerging precision-strike weapons have the potential to pose credible threats to modern militaries operating in the region.

China's leaders have yet to adequately explain the purposes or desired end-states of their military expansion. Estimates place Chinese defense expenditure at two to three times officially disclosed figures. The outside world has little knowledge of Chinese motivations and decision-making or of key capabilities supporting PLA modernization.

This lack of transparency prompts others to ask, as Secretary of Defense Rumsfeld did in June 2005: Why this growing investment? Why these continuing large and expanding arms purchases? Why these continuing robust deployments? Absent greater transparency, international reactions to China's military growth will understandably hedge against these unknowns.

Category 16.5 Military perspectives on cyberwar & battlespace

2006-05-30 RISKS; DoD http://www.defenselink.mil/pubs/pdfs/China%20Report%202006.pdf

CHINA CONTINUES PUSH FOR CYBERWAR CAPABILITIES

The annual "Military Power of the People's Republic of China" for 2006 was presented to Congress by the US DoD in May. Two sections in particular speak to concerns about information warfare capabilities (pp. 35-36):

Exploiting Information Warfare The PLA considers active offense to be the most important requirement for information warfare to destroy or disrupt an adversary's capability to receive and process data. Launched mainly by remote combat and covert methods, the PLA could employ information warfare preemptively to gain the initiative in a crisis.

Specified information warfare objectives include the targeting and destruction of an enemy's command system, shortening the duration of war, minimizing casualties on both sides, enhancing operational efficiency, reducing effects on domestic populations and gaining support from the international community.

The PLA's information warfare practices also reflect investment in electronic countermeasures and defenses against electronic attack (e.g., electronic and infrared decoys, angle reflectors, and false target generators.

Computer Network Operations. China's computer network operations (CNO) include computer network attack, computer network defense, and computer network exploitation. The PLA sees CNO as critical to seize the initiative and achieve "electromagnetic dominance" early in a conflict, and as a force multiplier. Although there is no evidence of a formal Chinese CNO doctrine, PLA theorists have coined the term "Integrated Network Electronic Warfare" to outline the integrated use of electronic warfare, CNO, and limited kinetic strikes against key C4 nodes to disrupt the enemy's battlefield network information systems. The PLA has established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics and measures to protect friendly computer systems and networks. The PLA has increased the role of CNO in its military exercises. For example, exercises in 2005 began to incorporate offensive operations, primarily in first strikes against enemy networks.

Formation of Information Warfare Reserve and Militia Units

The Chinese press has discussed the formation of information warfare units in the militia and reserve since at least the year 2000. Personnel for such units would have expertise in computer technology and would be drawn from academies, institutes, and information technology industries. In 2003, an article in a PLA professional journal stated "coastal militia should fully exploit its local information technology advantage and actively perform the information support mission of seizing information superiority." Militia/reserve personnel would make civilian computer expertise and equipment available to support PLA military training and operations, including "sea crossing," or amphibious assault operations. During a military contingency, information warfare units could support active PLA forces by conducting "hacker attacks" and network intrusions, or other forms of "cyber" warfare, on an adversary's military and commercial computer systems, while helping to defend Chinese networks.

The PLA is experimenting with strategy, doctrine, and tactics for information warfare, as well as integrating militia and reserve units into regular military operations. These units reportedly participate with regular forces in training and exercises.

Category 16.5 Military perspectives on cyberwar & battlespace

2006-06-06 DHS Daily OSIR; GovExec
http://govexec.com/story_page.cfm?articleid=34254&dcn=todays news

ROBOTICS SEEN AS GROWTH AREA FOR DOD.

The Department of Defense (DoD) is working to advance scientific efforts on robotics, but technology may be outpacing policy before it is even crafted, panelists said Monday, June 5. "Policy and procedure need to catch up with technology," said Stephen Welby, a tactical technology officer for the Defense Advance Research Projects Agency. Although U.S. military efforts have greatly considered fusion with modern robotics technology, there are fundamental challenges -- like securing adequate funding. They also noted that robotics can aid U.S. troops in military maneuvers. The terrain in the Middle East presents a problem to troops, but robotics can take them further out of harm's way. Welby noted that robots have "the ability to do things beyond human capability." Competition with uncertainty may be the second largest factor dampening the robotics movement. And while the majority of robotics investments are in the industrial sector, possible programs at the Pentagon hope to realize the need for robotics in the U.S. military.

Category 16.5 Military perspectives on cyberwar & battlespace

2006-06-07 DHS Daily OSIR; Government Computer News
http://www.gcn.com/online/vol1_no1/40968-1.html

DOD MOVES FORWARD WITH PORTAL.

The Army and the Defense Information Systems Agency (DISA) are moving forward with the vision of a single enterprise service online portal for all of the Department of Defense (DoD). Along with representatives from the Navy, Air Force and the other military agencies, the Army and DISA are leading the working groups to create the initial requirements and standards, and figure out what existing components can be reused to develop the Defense Knowledge Online (DKO) portal. John Garing, DISA CIO, said there are some challenges to making DKO happen, including ensuring that it can scale to the number of users and that the contracting language is appropriate.

[MK notes: hmm, a nice single point of failure for an insider attack in an information warfare conflict. Let's hope DISA puts strong I&A, IDS and logging in place to spot unusual activity.]

Category 16.5 Military perspectives on cyberwar & battlespace

2006-10-24 DHS Daily OSIR; National Journal
http://www.govexec.com/story_page.cfm?articleid=35335&dcn=todaysnews

DEFENSE OFFICIAL: CHANGES NECESSARY TO MEET 'NET-CENTRIC' GOALS.

The defense community's prevailing "information is power" attitude must evolve into "a culture that embraces and leverages the power of information," a senior Department of Defense official told the Military Communications Conference on Tuesday, October 24. The "need to know" regime is changing to one that focuses on "the need to share," said John Grimes, assistant secretary of defense for networks and information integration. "We must be stewards of the information, not the owners." Connecting people with data leads to information, which leads to knowledge, he said. Attaining DoD's "network-centric goals" involves changing the way it does business and the way it acquires capabilities quicker and cheaper, based on commercial practices, Grimes said. "Some will impact your business models," he warned attendees, many of whom were from the private sector. The Pentagon "must stop buying individual, highly tailored proprietary systems," and turn instead to vendors that can provide solutions for use within and across the military, he said. Grimes, who is also DoD's chief information officer, said the military is shifting to a portfolio management concept, emphasizing managed services and service-oriented architectures, he said. A year ago, the catchphrase was "information assurance," but today he said "it's all about data."

Category 16.5 Military perspectives on cyberwar & battlespace

2006-10-31 DHS Daily OSIR; Federal Times http://federaltimes.com/index.php?S=2323081

HACKERS -- FROM LOCALS TO CHINESE -- CHALLENGE DATA SECURITY.

From the Chinese government to homegrown hackers, groups are increasingly targeting agencies' networks, data security experts claim. "The Chinese are in half of your agencies' systems," Alan Paller, research director of the SANS Institute, told attendees Monday, October 30, at the Executive Leadership Conference. Paller cited 2005 reports that hackers using servers in China stole designs for an aviation mission-planning system for Army helicopters, and, on one night in 2004, found vulnerabilities in computers at the Defense Information Systems Agency, the Naval Ocean Systems Center in San Diego, the Army Information Systems Engineering Command at Fort Huachuca, AZ, and the Army Space and Strategic Defense Installation in Huntsville, AL. Officials believe the attacks were sponsored by the Chinese government. Paller argued that many information security metrics established by the Federal Information Security Management Act do not measure how well agencies protect data. Agencies must report the number of systems for which they complete reports on security vulnerabilities, but most reports are written by consultants and never read by top managers, Paller said. Agencies are also required to count the number of officials who complete security awareness training, but do not have to measure what skills they acquired, he said.

Category 16.5 Military perspectives on cyberwar & battlespace

2006-11-02 DHS Daily OSIR; Reuters http://www.washingtonpost.com/wp-dyn/content/article/2006/11/02/AR2006110200613.html

AIR FORCE TO CREATE CYBERSPACE COMMAND.

The U.S. Air Force plans to set up what could become a major command aimed at safeguarding U.S. military and civilian cyberspace, Air Force Secretary Michael Wynne said on Thursday, November 2. Wynne said the new command would be part of the 8th Air Force based at Barksdale Air Force Base in Louisiana. The mission of bombers now within the 8th Air Force would remain, and the new cyber-command reflects the Air Force's growing reliance on computer networks, data and electronic warfare. Wynne said he hoped the new command would eventually be on par with such major Air Force units as the Space Command and the Air Combat Command. In creating what could become a unit led by a four-star Air Force general, the Air Force would set the stage for significant budget resources and congressional interest. The Air Force will seek funding for the cyber-command in fiscal 2009, which begins October 1, 2008, he said.

Category 16.5 Military perspectives on cyberwar & battlespace

2007-01-24 DHS Daily OSIR; IDG News Service http://www.infoworld.com/article/07/01/24/HNmilitarywiki_1.html

EXPERT: U.S. MILITARY NEEDS WIKIS, VIDEO-SHARING.

The U.S. military should embrace user-driven Web services such as wikis, video-sharing sites, andsocial-networking sites as its focus grows to include providing more security and reconstruction help, a defense analyst recommended Wednesday, January 24. The U.S. military is increasingly moving toward a role where it will share responsibilities with organizations outside the U.S. government, including charitable organizations, international aid groups, and even private businesses, said Guy Ben-Ari, a fellow in the Defense-Industrial Initiatives Group at the Center for Strategic and International Studies, a Washington, DC, think tank. In those cases -- where the military is helping with reconstruction or security following a natural or human-made disaster -- U.S. forces need to find better ways to communicate with other groups, said Ben-Ari, speaking at the Network Centric Warfare conference in Washington. Too often, the U.S. military has been reluctant to share even unclassified information with other groups working for the same goals, he said.

Category 16.5 Military perspectives on cyberwar & battlespace

2007-02-08 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article97614-02-08-07-Web

DISA COULD SPEND CLOSE TO $1 BILLION ON SECURITY OVER THREE YEARS.

The Defense Information Systems Agency (DISA) plans to spend $959 million on network and information systems security over the next three years, with an emphasis on protecting against insider threats and defending classified networks, according to 2008 budget documents. Funding for DISA's Information Systems Security Program (ISSP), from fiscal 2007-2009, includes $819 million in operations and maintenance and $140 million for procurements. DISA has budgeted $247 million for ISSP in 2007, with $251 million requested for 2008 and $319 million planned for 2009. The ISSP budget calls for increased defense against internal security threats. The agency plans to deploy tools to 1,500 locations worldwide to analyze, detect and respond to insider threats against information and information systems, according to the budget documents. DISA also is stepping up its defense of the Secret Internet Protocol Router Network.

Category 16.5 Military perspectives on cyberwar & battlespace

2007-02-09 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article97645-02-09-07-Web

ATTACK BY KOREAN HACKER PROMPTS DOD CYBER DEBATE.

The Department of Defense (DoD) computer networks are probed and attacked hundreds of time each day. But a recent attack on the civilian Internet is causing DoD officials to re-examine whether the policies under which they fight cyber battles are tying their hands. "This is an area where technology has outstripped our ability to make policy," said Air Force Gen. Ronald Keys, Commander of Air Combat Command. "We need to have a debate and figure out how to defend ourselves." Unlike in the war on terror, DoD can't go after cyber attackers who plan or discuss crimes until they act, Keys said. Websites in other countries are beyond DoD's reach, he added. "If they're not in the United States, you can't touch 'em." Keys said it would probably take a cyber version of the 9/11 attacks to make the U.S. realize that barriers to action in cyberspace should be re-evaluated.

Category 16.5 Military perspectives on cyberwar & battlespace

2007-03-06 DHS Daily OSIR; Government Computer News
http://www.gcn.com/online/vol1_no1/43260-1.html

DOD INTERTWINES DATA SECURITY, INTEROPERABILITY CHALLENGES.

The Department of Defense (DoD) is spending $2.5 billion on information assurance in fiscal 2007, and a good portion of those funds are to ensure the military can share data safely and more easily with the intelligence community. John Grimes, DOD CIO, said Monday, March 5, the key to information sharing is security. "We are looking at those two areas in our architecture and in the next generation of security technology, and how we may change the nonclassified IP router network," he said in Orlando, FL, at the Information Processing Interagency Conference, sponsored by the Government IT Executive Conference. "The only way to get to net-centricity is to ensure we can share information and it is interoperable." One program DoD is working on with the Department of Homeland Security (DHS) and other agencies is the National Command Coordination Center, which will improve information sharing among federal, state and local agencies. To ensure data interoperability, DoD is moving more toward communities of interest, including one recently set up in the maritime community with the Coast Guard, Navy and other agencies. Grimes said the Office of Management and Budget is paying close attention to how these communities succeed. Conference Website: http://www.ipicconference.org/

Category 16.5 Military perspectives on cyberwar & battlespace

2007-04-05 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article98157-04-05-07-Web

ARMY CONSIDERING ADDING CYBERSPACE TO TACTICAL DOMAINS.

The Army may follow the Air Force's lead in setting up a cyber command. "Cyber war is emerging as just as important as kinetic war, some say more important," said Vernon Bettencourt, the Army's deputy chief information officer at the recent AFCEA Belvoir chapter/Program Executive Office Enterprise Information Systems industry day in Bethesda, MD. The Air Force announced it would create a cyber command last November that would be located at the 8th Air Force at Barksdale Air Force Base, LA and fully operational by October 2009. "The Air Force did not just create a new command...The Air Force changed its mission statement to say that it fights in three domains: air, space and cyberspace. A development like that is worthy of our assessment," he said. To that end, a high-level Army delegation recently visited the Air Force Cyber Command. Bettencourt said, "They have amalgamated some capabilities together...They have consolidated network operations and defense on a global basis." He added that the Army already has done some of the same by co-locating parts of its Information Operations Command, its computer emergency response teams and its Network Enterprise Technology Command together at Fort Belvoir, VA.

Category 16.5 Military perspectives on cyberwar & battlespace

2007-04-16 DHS Daily OSIR; Washington Technology
http://www.washingtontechnology.com/online/1_1/30465-1.html

DARPA WANTS CREATIVE CONCEPTS TO SOLVE COMPLEX CATASTROPHES.

The Defense Advanced Research Projects Agency (DARPA) is seeking innovative ideas and concepts that can advance the area of strategic collaboration. The agency wants interested individuals and organizations to submit white papers on technologies and concepts that could form the basis for a DARPA program to develop a network-enabled collaborative environment. Ultimately, the networked environment would bring together large numbers of people with different experiences, cultures and expertise to address the complex problems of large-scale disaster recovery and relief operations. The recent and increasing prominence of Stability, Security, Transition and Reconstruction (SSTR) and Humanitarian Assistance and Disaster Relief (HADR) operations pose new challenges for the U.S. military, according to DARPA. These operations involve a large, diverse mix of military organizations, nonmilitary government organizations, regional and international government agencies, nongovernmental organizations, private volunteer organizations, individual volunteers and the local population, the request for information states. These disaster relief and reconstruction operations exceed the ability of any one actor or organization to solve or even comprehend, DARPA officials said. Participants in SSTR/HADR operations have to collaborate across domains, organizations, cultures and languages.

Category 16.5 Military perspectives on cyberwar & battlespace

2007-05-01 DHS Daily OSIR; Frederick News Post (MD)
http://www.fredericknewspost.com/sections/business/display.htm?StoryID=59604

ROBOTS ARE BEING DEVELOPED FOR FUTURE BATTLEGROUND RESCUE EFFORTS.

An improvised explosive device detonates in Iraq, taking down a U.S. service member. Troops, rather than sending one or two medics to drag him to safety, deploy an unmanned robotic extraction vehicle. The robot pulls the wounded service member onto a board and drives him to a first responder. The scenario sounds futuristic, but it's not. Researchers headquartered at Fort Detrick in Frederick, MD, and others around the country are gaining headway on making extraction robots a reality. Ideally, robotic extraction wouldn't require human participation. Robotic casualty evacuation is needed not only to shield medics from harm but to involve fewer medics in basic operations, freeing them up for urgent work. Robotic extraction, though reducing risks to medics and other first responders, isn't without its challenges, said Gary Gilbert, the robotics program manager at the Telemedicine and Advanced Technology Research Center (TATRC). The robots must be sensitive so they don't cause further injury to wounded troops and maintain a level of bedside manner, providing comfort to the service member in the same way a human medic would.

16.6 Hacktivists, terrorists & state-sponsored attackers

Category 16.6 Hacktivists, terrorists & state-sponsored attackers

2006-02-07 DHS Daily OSIR; http://www.securitypipeline.com/news/179101482

ISLAMIC MESSAGES DEFACE HUNDREDS OF DANISH SITES.

Muslim protests over editorial cartoons originally published by a Danish newspaper have spilled onto the Internet and resulted in defacements of nearly 600 Danish Websites with anti-Dane, pro-Muslim messages in the past week, Helsinki-based F-Secure said Tuesday, February 7. This has been the latest fallout in the uproar over cartoons that include one depicting Mohammed with a bomb for a turban. The defacements included warnings of suicide bombings, Arabic-language messages sprawled across home pages, and threats such as "die plez."

Category 16.6 Hacktivists, terrorists & state-sponsored attackers

2006-03-27 http://www.usdoj.gov/criminal/press_room/press_releases/2006_4527_3-27-06Hansen.pdf

TELEMARKETING FIRM OFFICIAL INDICTED IN NEW HAMPSHIRE PHONE JAMMING CASE

WASHINGTON, DC – Shaun Hansen, former co-owner of Idaho-based telemarketing firm Mylo Enterprises, appeared in a federal court in New Hampshire today to face charges for conspiring to commit, and aiding and abetting the commission of, interstate telephone harassment relating to a scheme to jam several New Hampshire telephone lines on Election Day, 2002, the Department of Justice announced today.

The two-count indictment was returned under seal on March 8, 2006, and unsealed today upon his appearance in court. Hansen, 34, is charged with conspiracy to commit telephone harassment and aiding and abetting telephone harassment.

The indictment alleges that Hansen was contacted by others involved in the scheme and asked to assist in making harassing phone calls to five telephone numbers associated with the New Hampshire Democratic Party and one number associated with the Manchester Professional Firefighters Association on Election Day, November 5, 2002. Hansen allegedly agreed that, in return for $2,500, employees of Mylo Enterprises would place repeated hang-up calls to those numbers on that day. The indictment charges that, at Hansen's direction, employees of Mylo Enterprises in Idaho placed several hundred hang-up calls to those New Hampshire telephone numbers on that morning before the scheme was discontinued.

If convicted, Hansen faces a maximum penalty of five years in prison on the conspiracy charge, and a maximum penalty of two years in prison on telephone harassment charge. Hansen is the fourth individual charged in the Justice Department's investigation into the phone jamming scheme. Allen Raymond, former president of a Virginia communications consulting company, and Charles McGee, former Executive Director of the New Hampshire Republican State Committee, have each pleaded guilty to one count of conspiracy to commit telephone harassment. McGee was sentenced to seven months in prison and Raymond was sentenced to three months. James Tobin, former New England Regional Chairman of the Republican National Committee, was convicted after a December 2005 jury trial on for conspiring to commit, and aiding and abetting the commission of, interstate telephone harassment. Tobin will be sentenced on May 17, 2006.

Category 16.6 Hacktivists, terrorists & state-sponsored attackers

2006-03-31 DHS Daily OSIR; http://www.shanghaidaily.com/press/2006/03/31/attacks-on-gov 11 - websites-skyrocket/

ATTACKS ON CHINESE GOVERNMENT WEBSITES SKYROCKET.

Hackers cracked various levels of the Chinese government official Websites and changed information on the Web pages 2,027 times last year, doubling that of 2004. Additionally, more than 13,000 Chinese Websites were altered last year, one-sixth of which were government Websites.

Category 16.6 Hacktivists, terrorists & state-sponsored attackers

2006-06-19 DHS Daily OSIR; IDG News Service http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=cybercrime_hacking&articleId=900127 9&taxonomyId=82

HACKERS HIT MICROSOFT FRANCE SITE.

Part of Microsoft Corp.'s French Website was taken offline by hackers, who apparently took advantage of a misconfigured server at the software vendor's Web hosting provider. The experts.microsoft.fr Website was defaced Sunday, June 18, with the word "HACKED!" written across the top, just above a note that attributed the job to a group of Turkish hackers. The site remained out of operation on Monday morning, June 19. The defacement led to rumors that the hackers may have used a new undisclosed vulnerability in the company's Internet Information Services 6.0 Web server. Microsoft dismissed these rumors on Monday, saying that the hack was due to a misconfigured Web server.

Category 16.6 Hacktivists, terrorists & state-sponsored attackers

2006-06-28 DHS Daily OSIR; CNET News http://news.com.com/2061-10789_3-6089019.html

GAZA HACK ATTACK.

Hundreds of Israeli Websites were defaced Wednesday, June 28, allegedly by Moroccan hacker group Team Evil, according to a Haaretz.com post. The Website defacements, whose targets included banks and hospitals, carried the message: "Hacked By Team-Evil Arab hackers u KIll palestin people we Kill Israel servers," according to a posting on Zone-h Internet thermometer Website.

Category 16.6 Hacktivists, terrorists & state-sponsored attackers

2006-07-13 DHS Daily OSIR; Information Week http://www.informationweek.com/news/showArticle.jhtml

STATE DEPARTMENT RELEASES DETAILS OF COMPUTER SYSTEM ATTACKS.

The State Department confirmed that attacks last month on some of its computer systems originated in the East Asia-Pacific region, targeting U.S. embassies there, and worked their way toward State's headquarters in Washington, DC. The department hasn't indicated whether it has a specific suspect (or suspects) in mind, but State says it's working with Carnegie Mellon University's Computer Emergency Response Team and the FBI on an investigation. The systems affected by the hack were unclassified computer systems, State Department spokesperson Sean McCormack said during a press briefing Wednesday, July 12. The State Department has taken some precautionary steps, including changing some passwords.

Category 16.6 Hacktivists, terrorists & state-sponsored attackers

2006-08-08 DHS Daily OSIR; Time http://www.time.com/time/world/article/0,8599,1224273,00.html

HOW HEZBOLLAH HIJACKS THE INTERNET.

Hackers from the militant Lebanese group Hezbollah are trolling the Internet for vulnerable sites to communicate with one another and to broadcast messages from Al-Manar television. In today's asymmetrical warfare, the Internet is vital to groups like Hezbollah who use it to recruit, raise money, communicate and propagandize. The recent hijacking of a South Texas cable operator is a case study in how Hezbollah moves in. The Texas cable company has an agreement with a New York-based satellite communications aggregator, which moves feeds to a variety of customers from throughout the world, including Lebanon. A technician in New York made an improper connection and that opening was detected by Hezbollah. Al-Manar linked to the small cable company's Internet Protocol (IP) address, which can be thought of, in simple terms, as a telephone number. Hezbollah essentially added an extension on that telephone line allowing their traffic to flow. Hezbollah then gets the word out through e-mail and blogs that it can be found at that IP address and the hijack is complete.

Category 16.6 Hacktivists, terrorists & state-sponsored attackers

2006-08-15 DHS Daily OSIR; Government Computer News http://www.gcn.com/online/vol1_no1/41669-1.html

CHINESE SEEK MILITARY ID INFORMATION.

The Pentagon's primary Internet backbone, the Global Information Grid, comes under siege some 3 million times a day by outsiders looking for a way to penetrate military networks. Maj. Gen. William Lord, director of information, services and integration in the Secretary of the Air Force Office of Warfighting Integration and Chief Information Officer, told an audience of civilian Air Force personnel attending the Air Force IT Conference that "China has downloaded 10 to 20 terabytes of data from the NIPRNet. They're looking for your identity, so they can get into the network as you." Lord said that this is in accordance with the Chinese doctrine about the use of cyberspace in conflict. Lord said that the Air Force Research Laboratories are undertaking projects to mitigate the threat, possibly to look at offensive actions that could be launched, but "the rules of engagement have to change before we're fully engaged in cyberspace."

Category 16.6 Hacktivists, terrorists & state-sponsored attackers

2007-04-06 DHS Daily OSIR; Computerworld http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9015900&intsrc=hm_list

PRIVACY ADVOCATE TARGETS MASSACHUSETTS SECRETARY OF STATE'S WEBSITE.

A privacy advocate on Friday, April 6, threatened to publicly post on her Website the names of prominent individuals in Massachusetts whose Social Security numbers and other personal data she was able to pull from public records posted on the commonwealth secretary of state's Website. In addition, Betty "B.J." Ostergren said detailed instructions will be provided on her site telling others how to access the data from the site. Ostergren, a Virginia-based privacy advocate, runs a Website called The Virginia Watchdog, which she uses to draw attention to -- and put pressure on -- county and state government officials who post unredacted public records online. The threat to publicize the information stems from the continued refusal by Massachusetts Secretary of State William Galvin to break links to the records. The documents, which pertain to loans taken out by individuals and businesses in Massachusetts, are considered public records and are accessible to anyone with an Internet connection. Brian McNiff, a spokesperson for Galvin's office said "These documents are necessary for commerce. These are business documents that lenders file with the state to indicate what someone has pledged as collateral for a loan."

Category 16.6 Hacktivists, terrorists & state-sponsored attackers

2007-05-17 DHS Daily OSIR; IDG News Service http://www.infoworld.com/article/07/05/17/estonia-denial-of- service-attack_1.html

ESTONIA RECOVERS FROM MASSIVE DENIAL-OF-SERVICE ATTACK.

A spree of denial-of-service attacks against Websites in Estonia appears to be subsiding, as the government calls for greater response mechanisms to cyber attacks within the European Union. The attacks, which started around April 27, have crippled Websites for Estonia's prime minister, banks, and less-trafficked sites run by small schools, said Hillar Aarelaid, chief security officer for Estonia's Computer Emergency Response Team, on Thursday, May 17. But most of the affected Websites have been able to restore service. "Yes, it's serious problem, but we are up and running," Aarelaid said. Aarelaid said analysts have found postings on Websites indicating Russian hackers may be involved in the attacks. However, analysis of the malicious traffic shows that computers from the U.S., Canada, Brazil, Vietnam, and others have been used in the attacks, he said. Experts from the North Atlantic Treaty Organization are helping Estonia investigate the attacks, Aarelaid said.

Category 16.6 Hacktivists, terrorists & state-sponsored attackers

2007-05-29 DHS Daily OSIR; Chicago Tribune http://www.chicagotribune.com/technology/chi-estonia_rodriguezmay29,1,6793241.story

ATTACKS ON ESTONIA MOVE TO NEW FRONT.

After Estonia relocated a Soviet war memorial out of downtown Tallinn last month, furious Russians rioted in the Estonian capital, tried to attack Estonia's ambassador in Moscow, and hastily engineered de facto economic sanctions against the tiny Baltic nation. But the salvo from the Russian side that has most worried Estonians is a carefully crafted three-week cyber attack on Estonian government, bank and media Websites that has wreaked havoc in a country heavily dependent on the Internet for everything from banking and voting to paying taxes. The onslaught of "denial-of-service" attacks, many of which have originated from Russian computers, has raised questions about whether such attacks will become a tactic in future political conflicts. U.S. Deputy Secretary of State John Negroponte said the cyber sabotage in Estonia shouldprompt countries to shore up defenses against hackers and cyber-terrorists. Hackers routinely use Internet-connected computers as a conduit for attacks without the owner's knowledge. And Estonian officials have yet to prove that the Russian government instigated the sabotage.

16.7 Disinformation, PSYOP, propaganda

Category 16.7 Disinformation, PSYOP, propaganda

2006-04-02 RISKS; AP http://209.157.64.201/focus/f-news/1606953/posts

FAKE E-MAIL TOPPLES JAPANESE OPPOSITION PARTY

Japan's opposition party suffered a fresh humiliation Friday [March 31, 2006] when its leadership resigned en masse over a fake e-mail scandal, handing Prime Minister Junichiro Koizumi an uncontested grip on power in his last six months in office. … Party leader Seiji Maehara and his lieutenants stepped down after the party's credibility was torpedoed by one of its own lawmakers, who used a fraudulent e-mail in an apparent attempt to discredit Koizumi's ruling Liberal Democratic Party.

[Abstract by Peter G. Neumann]

Category 16.7 Disinformation, PSYOP, propaganda

2006-05-05 DHS Daily OSIR; http://news.zdnet.com/2100-1040_22-6068963.html

ISLAMIC MILITANTS RECRUIT USING U.S. VIDEO GAMES.

The creators of combat video games have unwittingly become part of a global propaganda campaign by Islamic militants to exhort Muslim youths to take up arms against the U.S., defense officials said on Thursday, May 4. Tech-savvy militants from al-Qaeda and other groups have modified video war games so that U.S. troops play the role of bad guys in running gunfights against heavily armed Islamic radical heroes, Department of Defense officials and contractors told Congress. The sites use a variety of emotionally charged content, from images of real U.S. soldiers being hit by snipers in Iraq to video-recordings of American televangelists making disparaging remarks about Islam. The underlying propaganda message, officials say, is that the U.S. is waging a crusade against Islam in order to control Middle Eastern oil, and that Muslims should fight to protect Islam from humiliation.

Category 16.7 Disinformation, PSYOP, propaganda

2006-05-05 RISKS

SUBWAY SIGNS ACCUSE CANADIAN PRIME MINISTER OF CANNIBALISM

Criminal hackers using a $25 remote control device reprogrammed several electronic message boards in Toronto's GO Transit subway cars to read "Stephen Harper Eats Babies" in endless loops. A colleague of the Prime Minister said, "I worked with Stephen Harper for five years and never once did he, in that time, eat a baby."

[MK adds: Note the qualifier, "in that time."]

17.1 Penetration

Category 17.1 Penetration

2006-05-25 EDUPAGE; CNET http://news.com.com/2100-7349_3-6077212.html

LIST OF HACKED UNIVERSITIES GROWS

Sacred Heart University, in Fairfield, Connecticut, has acknowledged that its computer systems have been hacked. The intrusion took place on May 8, according to officials from the university, though they declined to provide further details. The university did say it has notified local police and the FBI. A local television station reported that the university has notified about 135,000 individuals that the incident may have put their personal information at risk, including Social Security numbers. An unnamed source reportedly told the station that the university had informed him that information he provided as part of the school's entrance exams was included in the compromised data. Colleges and universities have been the targets of a number of data breaches in recent years, and some analysts fault school officials for not taking adequate precautions. Avivah Litan, a security analyst with research firm Gartner, said institutions do not put enough emphasis--or money--into computer security.

Category 17.1 Penetration

2006-06-20 DHS Daily OSIR; Associated Press http://www.seacoastonline.com/news/06202006/maine/108355.htm

HACKER TAPS INTO NEWSPAPER WEBSITES.

Hackers broke into the Websites of MaineToday.com early Saturday morning, June 17. MaineToday.com operates a Website under its own name as well as Internet sites for the Portland Press Herald, Kennebec Journal and Morning Sentinel. The hackers, who were apparently out of Brazil, managed to find security weaknesses that enabled them to break into the sites and replace the pages with banners stating "YOU ARE OWNED." MaineToday.com has changed its server configuration to prevent future problems. The attack did not compromise user accounts or passwords, or allow access to sensitive customer information, which is stored on a remote, secure server.

Category 17.1 Penetration

2006-10-03 DHS Daily OSIR; TechWeb http://www.techweb.com/wire/security/193101569

HACKER KIT USE SURGES, MEANS MORE MALICIOUS SITES.

About one in every six sites set up by criminals to steal information is created with hacking-for-dummies-style "toolkits," a security researcher said Tuesday, October 3. "About 15 percent of malicious sites designed to steal information have kit code or a derivation of kit code," said Dan Hubbard of Websense. Although Websense only began counting sites that use code from a toolkit late last year, the ratio is a major uptick, added Hubbard. Near the end of 2005, only 5 percent of the sites in a smaller sampling were using kit code. "They also don't
appear to be selling just kits," he said. "They also sell services. They'll infect Websites for you, collect data for you. I call it a 'managed insecurity service,'" said Hubbard. The most popular hacker toolkits are made and sold by Russian entrepreneurs, and include the well-known "WebAttacker" and the less-familiar "Nuclear Grabber" (aka "Haxdoor"). They range in price from $25 to over $2,500.

Category 17.1 Penetration

2006-11-03 DHS Daily OSIR; IDG News Service http://www.infoworld.com/article/06/11/03/HNchangingsecuritythreat_1.html

SECURITY THREAT CHANGING, SAYS SYMANTEC CEO.

The threat posed to computer users and companies by hackers is shifting from attacks on the computers to attacks on electronic transactions, according to the head of one of the world's largest security software vendors. John Thompson, chairman and CEO of Symantec, said the change has been taking place over the last few years but has recently been accelerating. "The attacks that we see today are more targeted and more silent and their objective is to create true financial harm as opposed to visibility for the attackers," he said. The head of Symantec's Asia Pacific business, Bill Robbins, explained in an interview that this changing threat would mean businesses will have to spend more time and energy on making sure that data is not just secure but also recording which users are accessing and manipulating information stored in corporate databases.

Category 17.1 Penetration

2007-01-18 DHS Daily OSIR; Boston Globe
http://www.boston.com/business/globe/articles/2007/01/18/tjx_credit_data_stolen_wide_impact_feared?mode=PF

TJX CREDIT DATA STOLEN; WIDE IMPACT FEARED. TJX COS.

Wednesday, January 17, said credit and debit card information was stolen from its computer systems, a breach that could affect a broad swath of customers of T.J. Maxx, Marshalls, and other stores. The retailer, which operates 2,500 outlets, said it does not know yet how much data was taken, though one banking official estimated that up to millions of cardholders could be affected. Data leaks are becoming an increasing threat to consumers and to the payment systems that handle millions of transactions per day. But the TJX case is unusual since it was the result of theft rather than the more common inadvertent losses. TJX said that it learned in mid-December it had "suffered an unauthorized intrusion" into the parts of its computers that process and store details of customer purchases. The intrusion involved the portion of the company's network that handles credit card, debit card, check, and merchandise return functions of various stores in the United States and Canada, and potentially locations in Britain and Ireland as well. A second potentially larger group's data covering periods in 2003 and 2006 "may have been accessed," the company said. TJX knows of no misuse of customer data so far.

17.2 Web vandalism

Category 17.2 Web vandalism

2006-05-03 DHS Daily OSIR; http://www.theregister.co.uk/2006/05/03/canadian_train_sign_ hack/

HACKERS LIBEL CANADIAN PRIME MINISTER ON TRAIN SIGNS.

Bewildered Toronto, Canada, train passengers were left scratching their heads after a hacker altered advertising signs in order to mock Stephen Harper, the country's prime minister, on the westbound Lakeshore GO Transit train. Scrolling LED signs on several trains repeated the message "Stephen Harper Eats Babies" every three seconds during the duration of the attack. Security specialists told the Toronto Star that the attack was probably carried out by a remote control device that can be used to program scrolling electronic signs. The kit can be bought over the counter at electronic hobby stores, such as Sam's Club.

17.3 Phreaking, PBX subversion, cramming

Category 17.3 Phreaking, PBX subversion, cramming

2006-08-15 DHS Daily OSIR; Consumer Affairs
http://www.consumeraffairs.com/news04/2006/08/modem_hijacking.html

DIAL-UP USERS FACE "MODEM HIJACKING" RISK.

Consumers using a dial-up Internet connection not only have to put up with painfully slow connection speeds, they also face the risk of "modem hijacking," resulting in hundreds of dollars in unauthorized charges. Even by inadvertently clicking on a popup, users can be disconnected from the Internet and then reconnected using international or premium rate phone exchanges.

Category 17.3 Phreaking, PBX subversion, cramming

2006-08-24 DHS Daily OSIR; Register (UK)
http://www.channelregister.co.uk/2006/08/24/pizza_fraud_scam/

TELEPHONE REDIRECT RUSE HITS CALIFORNIA.

U.S. scammers were able to pose as a pizza outlet after an AT&T service rep redirected calls from cooks to crooks. Con men claiming that the phone at pizza outlets was malfunctioning persuaded the rep to set in place a call forwarding request to a number of their choosing. AT&T failed to make any checks. As a result, orders for pizzas were fielded by scammers, who insisted advanced payments needed to be made by credit card. Payment details were subsequently used to make fraudulent Internet purchases under the name of unsuspecting pizza customers. The beauty of this simple ruse is the potential victims would have no reason to be suspicious, because they initiated the orders. Two incidents of the scam have been reported in southern California, but it's unclear if the ruse has been replicated elsewhere.

Category 17.3 Phreaking, PBX subversion, cramming

2006-09-07 DHS Daily OSIR; Federal Trade Commission
http://www.ftc.gov/opa/2006/09/websource.htm

COURT HALTS ILLEGAL PHONE BILLING SCHEME.

A U.S. district court has entered an order barring unlawful activities by an operation that allegedlycrammed unauthorized charges on the phone bills of small businesses or nonprofits for Website services that, in many cases, they didn't know they had and didn't request. The original complaint names defendants WebSource Media, L.L.C., BizSitePro, L.L.C., Eversites, L.L.C., Telsource Solutions, Inc., Telsource International, Inc., Marc R. Smith, Kathleen A. Smalley, Keith Hendrick, Steven Kennedy, John O. Ring, and James E. McCubbin, Jr. An amended complaint was filed later, adding defendant WebSource Media, L.P. The court has appointed a receiver to oversee the business operations and frozen defendants' assets, pending trial. At trial, the Federal Trade Commission will seek a permanent halt to the operation's activities and ask the court to order consumer redress for thousands of consumers who were illegally billed.

Category 17.3 Phreaking, PBX subversion, cramming

2006-10-24 DHS Daily OSIR; Computer World
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9004381&source=rss_topic85

EXPLOIT IN ASTERISK PBX SOFTWARE PATCHED.

A vulnerability in the Asterisk PBX server that enables an attacker to gain complete control of a PBX system has been discovered by the Australian and New Zealand security outfit, Security-Assessment.com. The exploit allows an attacker to spoof caller IDs, sniff voice calls on the network and take complete control of the system. No public exploits of the vulnerability have been released. Asterisk was notified of the discovery on Tuesday, October 17. A patch for the vulnerability was released by Asterisk on Wednesday, October 18.

17.4 Piggybacking, shoulder surfing

Category 17.4 Piggybacking, shoulder surfing

2006-05-23 DHS Daily OSIR; Finextra http://finextra.com/fullstory.asp?id=15349

NEW SECURITY DEVICE AIMS TO PROTECT CHIP AND PIN USERS FROM SHOULDER SURFERS.

A new chip and PIN security device that has been designed to protect cardholders from "shoulder surfing" thieves at ATMs is being piloted by a UK health and beauty retailer. Researchers at Warwick University originally designed the device, which features a specially-designed magnifying lens, to help visually impaired customers see the keys on a chip and PIN terminal. But the device is now being marketed to retailers and banks after it was realized that only the customer directly in front of the lens could view the keypad clearly. The lens distorts the view of the keypad from any other angle and so allows PINs to be protected from shoulder surfing criminals or hidden cameras.

Category 17.4 Piggybacking, shoulder surfing

2007-02-15 DHS Daily OSIR; InformationWeek http://www.informationweek.com/showArticle.jhtml

SMOKERS OPEN THE DOOR FOR HACKERS ... LITERALLY.

With companies banning smoking inside their offices, smokers are forced outside -- usually to specific smoking areas in the back of the building. The doors leading out to them are a major security hole, according to a social engineering study undertaken by NTA Monitor Ltd. a UK-based Internet security tester. NTA's tester was able to easily get inside a corporate building through a back door that was left open so smokers could easily and quickly get out and then back in to work, according to the company. Once inside, he reportedly gained access to a meeting room unchallenged and was then able to connect his laptop to the company's VoIP network. "We are experiencing a surge in demand for social engineering tests as hackers are turning to social techniques to infiltrate corporate networks. This latest social engineering test has proved that once inside a corporate building, an attacker can use social methods on employees to gain access to restricted areas and information if a rigid staff pass system is not in place, " said Roy Hills, technical director at NTA Monitor.

17.5 Social engineering

Category 17.5 Social engineering

2006-05-30 DHS Daily OSIR; Sweetwater Reporter (TX)
http://www.sweetwaterreporter.com/articles/2006/05/30/news/news2.txt

SCAM ALERT IN TEXAS.

The Sweetwater, TX Police Department is warning residents about a current scam to steal bank account information. An official-looking letter claims the recipient has won the "El Gordo Spanish Sweepstake Lottery/International Promotions Program." The recipient is asked to supply information, including the name, date of birth, identification number (Social Security number), and bank account information so they can identify the winner and deposit the winnings. The scam is distributed via a "confidential" and professional-looking form which the recipient is asked to fill out and fax to the company with a copy of identification.

Category 17.5 Social engineering

2006-11-24 DHS Daily OSIR; Associated Press
http://www.philly.com/mld/dailynews/living/16087082.htm?source=rss&channel=dailynews_living

CONSUMERS WARNED OF OPRAH TICKET SCAM.

Online thieves are using the lure of tickets to "The Oprah Winfrey Show" to rip off the identities of consumers, officials said. The thieves have been sending unsolicited e-mails asking people to send them personal information, verify financial information or wire money to a third party for tickets to the show, Illinois state Attorney General Lisa Madigan said. The show, taped in Chicago, doesn't sell tickets. It takes reservations to attend tapings for free. Madigan's office couldn't say how widespread the messages had reached.

Category 17.5 Social engineering

2007-03-25 DHS Daily OSIR; Computerworld
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9014218&intsrc=hm_list

MICROSOFT ACKNOWLEDGES XBOX LIVE PRETEXTING.

Months after Xbox Live users began complaining of hacked accounts, Microsoft Corp on Saturday, March 24, acknowledged that the service's support staff is at fault, victims of "pretexting" calls by identity thieves. Reports of account theft on Xbox Live have been making the rounds of its member forums since at least December. But Microsoft responded only after noted security researcher -- Kevin Finisterre of "Month of Apple Bugs" fame -- last week went public about how his account was hijacked. Larry Hryb, director of programming at Xbox Live, said they are examining the policies and have already begun retraining the support staff and partners to help make sure we reduce this type of social engineering attack.

18.1 Stolen equipment or media

Category 18.1 Stolen equipment or media

2006-05-22 RISKS; ConsumerAffairs.Com http://tinyurl.com/loluu; USA Today http://tinyurl.com/mwugq

VAST DATA CACHE ABOUT VETERANS HAS BEEN STOLEN

Personal electronic information on up to 26.5 million military veterans, including their names, Social Security numbers, and birth dates, was stolen from the residence of a Department of Veterans Affairs employee who had taken the data home without authorization. …Comments about no evidence of data misuse (yet) and no health/financial records, but deeply embarrassing to VA. No mention of a statement that this incident was not reported for several weeks….

[Abstract by Peter G. Neumann]

Martin Bosworth, writing for ConsumerAffairs.Com, wrote "In every public case, company representatives insist the laptops are stolen simply for their resale value, as opposed to the data they contain. The more skeptical might say that as consumers get smarter about not sharing their information on the Web, enterprising hackers and data thieves are taking advantage of other holes in the security fence -- namely slipshod government and business policies. Whether it's a criminal conspiracy or good old-fashioned incompetence, public and private agencies are not adequately protecting the personal information that's entrusted to them and, in many cases, are less than forthcoming about the circumstances surrounding laptop losses."

The FirstGov.gov Web portal included an extensive Web page entitled "Latest Information on Veterans Affairs Data Security" at < http://www.firstgov.gov/veteransinfo.shtml >.

In early June, the VA revealed that the stolen data included information about 2.2 million active-duty military personnel and National Guard troops. According to an Associated Press report, a class-action lawsuit filed by a coaltion of veterans' groups demanded "that the VA fully disclose which military personnel are affected by the data theft and [sought] $1,000 in damages for each person — up to $26.5 billion total. The veterans are also seeking a court order barring VA employees from using sensitive data until independent experts determine proper safeguards." The complaint added, "VA arrogantly compounded its disregard for veterans' privacy rights by recklessly failing to make even the most rudimentary effort to safeguard this trove of the personally identifiable information from unauthorized disclosure."

Category 18.1 Stolen equipment or media

2006-06-02 EDUPAGE; Wall Street Journal (sub. req'd) http://online.wsj.com/article/SB114921264072869450.html

TWO MONTH DELAY IN ANNOUNCING THAT UNENCRYPTED DATA WERE ON LAPTOP STOLEN FROM AUDITOR'S CAR TRUNK

A laptop was stolen from the trunk of an Ernst & Young employee's car, compromising the names and credit card numbers of 243,000 customers of Hotels.com, which was on the machine. The theft occurred in February, but Ernst & Young was not able to determine what was on the computer until early May, at which time it and Hotels.com began notifying the affected individuals. Those affected can avail themselves of a free credit-monitoring service. This incident marks the third time this year the auditor has exposed data belonging to its clients, following an incident that compromised data from Goldman Sachs and another incident involving several companies. Ernst & Young said it has no reason to believe the thief was specifically seeking the information on the computer. It has since added new security protections to the laptops of its 30,000 employees in the United States and Canada.

Category 18.1 Stolen equipment or media

2006-06-20 DHS Daily OSIR; Associated Press http://www.nytimes.com/aponline/business/AP-Equifax-Data-Loss.html

EQUIFAX: LAPTOP WITH EMPLOYEE DATA STOLEN.

Equifax Inc., one of the nation's three major credit bureaus, said Tuesday, June 20, a company laptop containing employee names and Social Security numbers was stolen from an employee who was traveling by train near London. The theft, which could affect as many as 2,500 of the Atlanta-based company's 4,600 employees, happened May 29 and all employees were notified June 7, spokesperson David Rubinger said. Employee names and partial and full Social Security numbers were on the computer's hard drive, though Rubinger said it would be almost impossible for the thief to decipher the information because it was streamed together. The employee whose laptop was stolen has been disciplined for violating company policy, which prohibits storage of company information on a hard drive, Rubinger said.

Category 18.1 Stolen equipment or media

2006-06-23 EDUPAGE; CNET http://news.com.com/2100-1029_3-6087218.html

FTC LAPTOPS STOLEN

Two computers belonging to employees of the Federal Trade Commission (FTC) were stolen from a locked car last week, putting personal information on about 110 individuals at risk. An FTC official said the laptops, which belonged to two FTC attorneys, were password protected, but she noted that the computers contained names, Social Security numbers, addresses, and some financial information. The FTC has notified the individuals affected and offered them free credit monitoring for one year. The agency is working on a new policy that would forbid employees from taking computers with personal information out of FTC offices without explicit permission to do so. This incident follows other recent cases of government loss of personal information, including one in which the Department of Veterans Affairs lost a hard drive with information on 26.5 million veterans.

Category 18.1 Stolen equipment or media

2006-06-30 EDUPAGE; New York Times (registration req'd) http://www.nytimes.com/aponline/us/AP-Vets-Data-Theft.html

VA LAPTOP RECOVERED

A stolen laptop containing personal information on 26.5 million people has been recovered, and authorities believe the data on the computer was not accessed. The laptop, which belonged to the Department of Veterans Affairs, was stolen on May 3 from the home of a VA employee. The agency was harshly criticized for waiting until May 22 to disclose the theft, and some veterans sued the government for $1,000 per person affected--a total of $26.5 billion. Following the announcement of a $50,000 reward, an individual contacted law enforcement officials and led them to the laptop. Initial forensic examinations indicated that the sensitive data had not been accessed since the laptop was stolen. Further tests are scheduled to try to confirm that. The VA had said it would pay for credit-monitoring services for one year for those affected. The agency is reevaluating that offer, given the recovery of the laptop. Joe Davis, spokesperson for the Veterans of Foreign Wars, said the VA should honor its pledge to pay for the monitoring services unless it can show that the data were definitely not compromised.

Category 18.1 Stolen equipment or media

2006-07-26 DHS Daily OSIR; Associated Press http://www.chron.com/disp/story.mpl/ap/politics/4074633.html

NAVY COMPUTERS WITH PERSONAL DATA STOLEN.

Two laptop computers with personal information on about 31,000 Navy recruiters and their prospective recruits were stolen from Navy offices in New Jersey in June and July, the Navy disclosed on Wednesday, July 26. "There have been no reports of illegal usage of personal data identified by these incidents," said Navy spokesperson, Lt. Bashon W. Mann, adding that the Navy is identifying the affected individuals. He said the information on the laptops was secured by several layers of password protection. One laptop was reported stolen from a recruiting station in Trenton, NJ, in early June, and the other was taken from a Jersey City, NJ, recruiting station in early July. Information on the computers included a list of applicants and recruiters as well as information from selective service and school lists. About 4,000 included Social Security numbers. The police and the Navy Criminal Investigative Service are investigating.

Category 18.1 Stolen equipment or media

2006-08-30 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article95848-08-30-06-Web

EDUCATION DATA AT RISK AGAIN.

The Department of Education is a victim of data exposure for the second time in less than a month. DTI Associates, a professional services contractor based in Arlington, VA, acknowledged that two laptop computers were stolen August 11 from its Washington, DC, office. The laptops contained information on 43 reviewers who were assessing grant applications for Education's Teacher Incentive Fund, said Bruce Rankin, vice president of DTI. The only personal data that may have been in the laptops were the educators' Social Security numbers, used for payroll identification purposes, he said.

Category 18.1 Stolen equipment or media

2006-09-15 DHS Daily OSIR; Government Computer News
http://www.gcn.com/online/vol1_no1/42012-1.html

SECOND STOLEN COMPUTER WITH VA DATA RECOVERED.

Law enforcement has recovered the desktop computer stolen from Unisys that contained personal information of about 16,000 patients treated in Department of Veterans Affairs (VA) medical centers in Philadelphia and Pittsburgh, according to the FBI and VA's Office of Inspector General. Khalil Abdullah-Raheem, who worked for a company that provides temporary labor to Unisys, was charged Thursday, September 14 with theft of government property. VA secretary Jim Nicholson said, "It appears that the Unisys computer was not targeted for the veteran information it may have contained." The VA data contained insurance claim information with names, addresses, and personal identifiers, VA said. The FBI is conducting a forensics analysis to determine whether VA data was compromised.

Category 18.1 Stolen equipment or media

2006-09-15 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/06/09/15/HNunisyscontractor arrested_1.html

UNISYS CONTRACTOR ARRESTED IN VA THEFT.

Authorities have charged a 21-year-old Unisys Corp. subcontractor with stealing a desktop computer with billing information on as many as 38,000 U.S. Department of Veterans Affairs medical patients. Khalil Abdulla-Raheem was charged Wednesday, September 13, with theft of government property. He is the employee of an unnamed company that "provides temporary labor to Unisys," according to a statement released by the Veterans Affairs (VA) department's Office of Inspector General. The computer was stolen in late July from Unisys's Reston, Virginia, offices. It contained records on about 16,000 living patients who had received treatment at VA medical centers in Philadelphia and Pittsburgh, as well as information on another 2,000 who are deceased. Data on an additional 20,000 patients may have been stored on the computer, according to the VA. The VA said that these records may have contained Social Security numbers, addresses, and insurance information. The U.S. Federal Bureau of Investigation (FBI) is now analyzing the computer to determine whether this information has been compromised, but investigators do not believe that Abdulla-Raheem was after the VA data.

Category 18.1 Stolen equipment or media

2007-01-26 DHS Daily OSIR; Business Week
http://www.businessweek.com/ap/financialnews/D8MRSCTG0.htm

BANKERS DETECT FRAUD FROM TJX HACK.

Customer data stolen by computer hackers from TJX Cos. has been used to make fraudulent debit card and credit card purchases in the United States and overseas, the Massachusetts Bankers Association (MBA) said Wednesday, January 24. The fraudulent purchases have been made in Florida, Georgia, and Louisiana, and overseas in Hong Kong and Sweden, the association said. Nearly 60 banks have reported they've been contacted by credit and debit card companies about compromised cards, the association said. The number is likely to grow because less than half of the association's 205 banks have reported to it on the issue. The association said banks are notifying customers about fraudulent purchases, and reissuing cards, in some cases. Last week, TJX said hackers had broken into a system that handles credit and debit card transactions, as well as checks and merchandise returns for customers in the U.S. and Puerto Rico and may involve customer accounts from the U.K. and Ireland.

Category 18.1 Stolen equipment or media

2007-02-05 DHS Daily OSIR; Associated Press http://www.nytimes.com/aponline/us/AP-Security-Breach.html

VA HARD DRIVE WITH PERSONAL DATA MISSING.

A portable hard drive that may contain the personal information of up to 48,000 veterans may have been stolen, the Department of Veterans Affairs (VA) and a lawmaker said Friday, February 2. An employee at the VA medical center in Birmingham, AL reported the external hard drive missing on January 22. The drive was used to back up information on the employee's office computer. It may have contained data from research projects, the department said. The employee also said the hard drive may have had personal information on some veterans, although portions of the data were protected. Secretary of Veterans Affairs Jim Nicholson said that the VA and the FBI are investigating. Representative Spencer Bachus (R-AL) said that the personal information of up to 48,000 veterans was on the hard drive and the records of up to 20,000 of them were not encrypted. Pending results of the investigation, VA is planning to send individual notifications and to provide a year of free credit monitoring to anyone whose information is compromised.

Category 18.1 Stolen equipment or media

2007-03-21 DHS Daily OSIR; InformationWeek
http://www.informationweek.com/news/showArticle.jhtml

STOLEN DATA LEADS TO FLORIDA FRAUD.

Data stolen from TJX has surfaced in Florida, where it's been used to help thieves steal about $8 million in merchandise from Wal-Mart stores. The thieves used the stolen TJX customer data to create dummy credit cards for purchasing Wal-Mart and Sam's Club gift cards, and then used those to hit stores in 50 of Florida's 67 counties. The Gainesville Police Department and Florida Department of Law Enforcement investigation began in November. After analysis of transaction records and video footage of the perpetrators, investigators arrested six suspects and issued warrants for the arrest of four more. Those arrested were charged with organized scheme to defraud, a first-degree felony. The fraud ring was uncovered after Wal-Mart employees became suspicious of certain shoppers who were using multiple gift cards--many of them worth $400--to pay for their purchases. The $400 denomination was used because gift cards valued at $500 or more require the customer to provide some form of identification.

Category 18.1 Stolen equipment or media

2007-05-07 DHS Daily OSIR; InformationWeek
http://www.informationweek.com/security/showArticle.jhtml

PRISON PAYS $6,000 TO CHANGE LOCKS AFTER KEYS SOLD ON EBAY.

Iowa's Anamosa State Penitentiary officials just paid $6,000 to have the outer locks changed in the Iowa maximum security men's prison that houses 1,289 inmates. Fred Scaletta, a spokesperson for the Iowa Department of Corrections told InformationWeek that changing the locks was a precautionary measure because they're not sure if the keys sold on the popular online auction site, eBay, were actually for the prison. But they certainly could be, so prison officials weren't going to take any chances. Scaletta explained that a man who used to work as a locksmith for the prison was allowed to work from his home. He retired in 1974 and has since died. When the man's wife died, their estate, including some keys that are thought to be for the prison, went on sale. No one at the corrections department knew there was anything amiss until an employee pointed the sale out to them and said some keys might be involved. Scaletta also noted that the prison updates its locks periodically but he wasn't sure if the locks that these keys might have opened had been changed since the '70s or not.

18.2 Lost or missing equipment or media

Category 18.2 Lost or missing equipment or media

2006-02-24 EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/13952271.htm

MCAFEE AUDITOR LOSES EMPLOYEE DATA

Deloitte and Touche, the external auditor of computer-security firm McAfee, has lost a CD containing unencrypted data on more than 9,000 McAfee employees. The CD was left in a seat pocket on an airliner on December 15, though the loss was not reported to Deloitte officials until January 8, and it took until January 30 to determine what was on the disk. A spokesperson for McAfee, Siobhan MacDermott, said auditors commonly have access to the kind of data that was on the CD and that the decision not to encrypt the data was Deloitte's. MacDermott said, "We have policies in place to prevent this from happening" and noted that McAfee and Deloitte are working to prevent such a loss from happening again. Ken McEldowney, executive director of Consumer Action, expressed dismay at the news. "How hard would it be to encrypt the data?" he said. "How hard would it be to make sure important information like that is not on CDs that are not under tight control by the company?"

Category 18.2 Lost or missing equipment or media

2006-02-25 The Register < http://www.theregister.co.uk/2006/03/30/ey_nokia_lapop/ >

ERNST & YOUNG LOSES LAPTOP COMPUTER WITH CUSTOMER DATA

The international consulting firm Ernst & Young lost a series of laptop computers in 2006. In February, the firm admitted that a laptop with confidential customer data -- including the SSN of Scott McNealy, CEO of Sun Microsystems -- had been lost or stolen in January. McNealy reported that his identity had in fact been compromised.

Then a March report in the Miami Herald stated that some Ernst & Young auditors went to lunch on Feb 9 -- leaving their laptop computers in a conference room in the office building where they were working. Two men stole four laptops. E&Y declined to issue a public statement about these breaches of security, although they did assure the public that "password protection" sufficed to compensate for loss of control over the data.

On March 15, The Register's Ashlee Vance, indomitable reporter that she is, wrote that E&Y lost yet another laptop computer -- this one stolen in January from an employee's car. It contained financial and tax records compromising the security of "thousands" of IBM employees and ex-employees. Once again, the company refused to issue a public statement about the theft and informed the potential victims of identity theft two months after the incident. On March 23, Vance found out that E&Y had admitted to BP that 38,000 employees were included in the January laptop theft.

Category 18.2 Lost or missing equipment or media

2006-06-29 DHS Daily OSIR; Call 6 (IN) http://www.theindychannel.com/call6/9448883/detail.html

VETERANS RECORDS TAPE MISSING FROM INDIANAPOLIS OFFICE.

A backup tape with more than 16,000 records from the Department of Veterans Affairs Regional Counsel Office in Indianapolis, IN, is missing. The revelation came Thursday, June 29, during a hearing of the House Committee on Veterans' Affairs in Washington. The tape, missing since May 5, had records of 16,537 legal cases and 12,349 records containing personally identifiable information of individuals. The records contain dates of birth, medical records and social security numbers for an unknown number of veterans. The Indianapolis incident happened two days after a laptop containing the personal information of more than 26 million veterans was reported stolen.

Category 18.2 Lost or missing equipment or media

2006-08-08 EDUPAGE; Internet News http://www.internetnews.com/security/article.php/3625256

MORE VA DATA GOES MISSING

Following the theft in May and subsequent recovery of a Veterans Administration (VA) laptop containing personal information on more than 26 million veterans, a subcontractor to the agency now says a desktop computer is missing, putting information on as many as 38,000 veterans at risk. The computer belongs to Unisys, which confirmed that data including names, Social Security numbers, and dates of birth for 18,000 people were definitely on the computer. Another 20,000 records may have also been on the machine; the VA and Unisys are trying to determine whether those additional records were compromised. Unisys and the VA are working to contact those affected by the incident.

Category 18.2 Lost or missing equipment or media

2006-09-22 EDUPAGE; ZDNet http://news.zdnet.com/2100-1009_22-6118495.html

COMMERCE DEPARTMENT MISSING 1,100 LAPTOPS

A statement issued by the U.S. Department of Commerce indicates that the agency cannot account for 1,137 laptops that should be in its inventory of about 30,000. Of those that are missing--whether lost or stolen--249 reportedly contained personally identifiable information from the U.S. Census Bureau. The agency said that it has received no reports that the information contained on the missing computers has been misused, noting that the data are protected by passwords, encryption, and complex database software. The Commerce Department's statement did acknowledge, however, that since 2003, nearly 300 cases of compromised personal information had been reported. Those instances involved 217 laptops, 15 handheld devices, 46 other devices, including USB flash drives.

Category 18.2 Lost or missing equipment or media

2006-11-02 DHS Daily OSIR; Associated Press
http://www.tulsaworld.com/NewsStory.asp?ID=061102_Ne_A6_Areav63279

OKLAHOMA VETERANS' PERSONAL DATA REPORTED LOST.

Three computer disks containing the Social Security numbers and other personal information of about 1,400 veterans treated at a McAlester, OK, clinic are missing, federal officials said. The Veterans Affairs Hospital in Muskogee, OK, confirmed the loss in a letter mailed Tuesday, October 31, to patients of the McAlester clinic. The lost information includes patients' names, Social Security numbers, amount billed, and amount paid for services they received at the outpatient clinic, which operated through a contract with the Choctaw Nation. The hospital says there is no information to indicate this personal information has been misused. The disks were mailed May 10, June 10, and July 10. The hospital did not notify veterans earlier because it had to wait for officials in Washington to approve the wording of the letter, she said, which didn't come until October 26.

Category 18.2 Lost or missing equipment or media

2007-02-12 DHS Daily OSIR; GovExec
http://www.govexec.com/story_page.cfm?articleid=36113&dcn=todaysnews

ALABAMA VA LOSES SENSITIVE INFORMATION ON 1.3 MILLION DOCTORS.

The hard drive that went missing from a Birmingham, AL, Veterans Affairs (VA) Department facility last month contained highly sensitive information on nearly all U.S. physicians and medical data for about 535,000 VA patients, agency officials announced over the weekend. The data for the 1.3 million physicians who have billed Medicaid and Medicare, both living and deceased, could result in widespread fraud, such as the creation of fake Medicare and Medicaid invoices. There are 902,053 physicians in the United States, according to the American Medical Association. VA officials are not sure at this point whether the data was stolen or simply lost. They are arranging to provide one year of free credit monitoring to those whose information was compromised. The incident marks the third major breach at the VA in less than a year.

Category 18.2 Lost or missing equipment or media

2007-04-01 DHS Daily OSIR; New York Times
http://www.mercurynews.com/politics/ci_5569889?nclick_check=1

SECURITY AGENCY COMPUTERS MISSING.

The office in charge of protecting American technical secrets about nuclear weapons from foreign spies is missing 20 desktop computers, at least 14 of which have been used for classified information, the Department of Energy (DOE) inspector general reported Friday, March 30. This is the 13th time in a little over four years that an audit has found the department, whose national laboratories and factories do most of the work in designing and building nuclear warheads, has lost control over computers used in working on the bombs. "Problems with the control and accountability of desktop and laptop computers have plagued the department for a number of years," the report said. In January, Linton F. Brooks was fired as the administrator of the National Nuclear Security Agency, the DOE agency in charge of bombs, because of security problems. Previous incidents of wayward computers have involved nuclear-weapons information. But the office involved in this breach has a special responsibility, tracking and countering efforts to steal bomb information. Its computers would have material on what the department knew about foreign operatives and efforts to steal sensitive information.

Category 18.2 Lost or missing equipment or media

2007-04-06 DHS Daily OSIR; Hortica Press Release http://www.hortica-insurance.com/hotTopics/26.PDF

INSURANCE COMPANY ALERTING PUBLIC TO LOSS OF BACKUP TAPES.

Florists' Mutual Insurance Company (Hortica), an Illinois-based provider of employee benefits and insurance to companies in the horticultural industry, Friday, April 6, announced that a locked shipping case containing magnetic backup tapes cannot be located. Hortica believes that the backup tapes contained personal information including names, Social Security numbers, drivers' license numbers, and/or bank account numbers. The locked shipping case was being transported by UPS from a secure offsite facility to the company's Illinois headquarters. Hortica is continuing its investigation of this incident and is working with various law enforcement agencies to locate the shipping case. "UPS and law enforcement agencies have no evidence to indicate an unauthorized individual has possession of the tapes," said Robert McClellan, president and chief executive officer. "It is important for customers to note that these tapes cannot be read without specific computer equipment and software." Mr. McClellan said Hortica has since altered its backup tape storage procedures so shipment of backup tapes by common carrier is no longer required. No unusual activity involving customer information has been reported to the company.

Category 18.2 Lost or missing equipment or media

2007-05-25 DHS Daily OSIR; Government Computer News http://www.gcn.com/online/vol1_no1/44344-1.html

ENERGY REPORTS LOSING 1,400 LAPTOPS IN SIX YEARS.

The Department of Energy (DOE) notified Congress Thursday, May 24, that it has lost 1,427 laptop PCs over the past six years. The department said none of the laptops contained classified information. The figure represents approximately two percent of its current inventory of laptop computers, or approximately 71,874 units used either by agency personnel or contractors. The Energy Department statement broke down the missing laptops by year, with 144 reported missing for 2001, 248 in 2002, 256 in 2003, 258 in 2004, 223 in 2005 and 205 in 2006. Another

81 laptops were identified as missing, though the years those went missing were not disclosed. The agency revealed the information in response to a Freedom of Information Act request filed by WTOP, a Washington, DC, news radio station. As a result of these findings, which track missing units up until June 2006, Energy secretary Samuel Bodman directed a full inventory of laptops, which subsequently recovered 100 of these units, Energy spokesperson Megan Barnett said.

18.3 Data disposal & remanence (Dumpster® diving, discarded media

Category 18.3 Data disposal & remanence (Dumpster® diving, discarded media

2006-08-30 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2163176/pdas-sold-ebay-loaded-sensitive

PDAS SOLD ON EBAY LOADED WITH SENSITIVE DATA.

Many of the used smart phones and PDAs for sale online are loaded with sensitive data ranging from banking records to corporate e-mails that can easily be retrieved by hackers and data thieves. According to a sampling by mobile security software provider Trust Digital, much of this sensitive information is retained in the Flash memory of the devices because of a widespread failure to perform the advanced hard reset required to delete data. Trust Digital claimed that its engineers were able to recover nearly 27,000 pages of personal, corporate and device data from nine out of 10 mobile devices purchased through eBay for the project.

Category 18.3 Data disposal & remanence (Dumpster® diving, discarded media

2006-09-07 DHS Daily OSIR; Reuters http://www.foxnews.com/story/0,2933,212739,00.html

CHASE THROWS OUT PERSONAL INFORMATION ON 2.6 MILLION CREDIT CARD HOLDERS.

Personal information on 2.6 million past and current Circuit City credit card holders was mistakenly thrown out as trash by Chase Card Services, a division of J.P. Morgan Chase. Chase Card Services issues bank-branded and private-label credit cards for Circuit City. The company said Thursday, September 7, that it believes the tapes, inside a locked box, were compacted, destroyed, and buried in a landfill. Chase has begun notifying customers and monitoring affected accounts, but the company says it has not identified any misuse of personal information. No other Chase accounts are involved in this incident, the bank said.

Category 18.3 Data disposal & remanence (Dumpster® diving, discarded media

2006-09-28 DHS Daily OSIR; Capitol Media Services (AZ) http://www.azcentral.com/abgnews/articles/0928abg-record0928.html

NEW ARIZONA LAW MANDATES THAT BUSINESSES DESTROY RECORDS WITH PERSONAL DATA.

Companies must start shredding or otherwise destroying records with personal customer and employee information when they've finished with the records. A law that takes effect October 1 in Arizona makes it a crime for businesses to knowingly dispose of paper records if identifying information can be read. The Identity Theft Data Clearinghouse, administered by the Federal Trade Commission, reported more than 9,300 complaints of identity theft filed last year. The new requires that records must be destroyed, or at least the information obliterated, if it contains at least an individual's first initial and last name if it also contains other identifying numbers. That list includes Social Security, credit and debit cards, bank accounts, and driver's licenses. The law exempts entities that must comply with federal laws, including financial institutions and health care providers. It also is crafted to apply solely to paper records, not electronic files.

Category 18.3 Data disposal & remanence (Dumpster® diving, discarded media

2006-10-28 DHS Daily OSIR; Agence France-Press http://news.yahoo.com/s/afp/20061028/wl_uk_afp/britainmoneybanking_061028121036

BANKS DISPOSE OF CUSTOMER ACCOUNT INFORMATION IN TRASH RECEPTACLES.

Some banks have been using garbage bags to dispose of customer information in "wholly unacceptable" breaches of data protection rules, Britain's information commissioner has said. Richard Thomas said that his office was investigating branches of HSBC, Halifax, NatWest, and Royal Bank of Scotland as well as a post office. "A number of banks have been very careless with people's personal information," he told the Times newspaper, adding he had seen rubbish bags full of bank statements and details of a $948,000 bank transfer. "...if the banks themselves are being careless with the information, that seems to me to be wholly unacceptable." The banks could face unlimited fines if the information commissioner's office was to take them to court but the spokesperson said Thomas wanted banks to "sort this out" themselves. Ian Mullen of the British Bankers' Association told BBC radio that instances of documents being found in dustbin bags were isolated and it was not clear whether banks were at fault.

Category 18.3 Data disposal & remanence (Dumpster® diving, discarded media

2006-11-27 DHS Daily OSIR; Associated Press
http://www.myrtlebeachonline.com/mld/myrtlebeachonline/news/local/16109822.htm

SOUTH CAROLINA SCHOOL DISTRICT SOLD COMPUTERS WITH PERSONAL INFORMATION.

The Greenville County school district sold computers that contained Social Security numbers and birthdates for roughly 100,000 students and at least 1,000 employees. The two buyers never released the information found in computers they bought at a dozen school district auctions between 1999 and last March, but worry about other computers sold, their attorney David Gantt told The Greenville News. The businessmen went public about their findings after the district repeatedly ignored their warnings and continued to sell computers without removing the data, Gantt said. "Their concern is, and frankly a reasonable concern is, who else might have gotten access to this information?" he said. "They didn't buy everything at these sales." Discovered data included addresses, phone numbers, medical information, personnel evaluations, driver's license numbers and Department of Juvenile Justice records.

Category 18.3 Data disposal & remanence (Dumpster® diving, discarded media

2007-02-21 DHS Daily OSIR; Government Computer News
http://www.gcn.com/online/vol1_no1/43189-1.html

AUDITORS FAULT DOE'S COMPUTER DISPOSAL METHODS.

The Department of Energy's (DOE) Inspector General, Gregory H. Friedman, has found fault with the Idaho National Laboratory's (INL) technical procedures for removing restricted nuclear data and confidential data from old computers. DOE agreed with the conclusions of a report Friedman's office issued, which essentially recommended that the Idaho laboratory adopt and enforce all department policies regarding the handling of excess computers. The IG's auditing staff found that INL had sold a computer containing unclassified controlled information, including personal information, at a public auction in October 2004. "We concluded that INL did not have adequate policies and internal controls for excessing computers and other electronic memory devices to prevent the unauthorized dissemination of unclassified controlled information," the report stated. They added that they did not uncover any additional releases of the controlled information. The auditors toured INL's facilities for storing excess computers and shipping them offsite for disposal after degaussing. They found many hard drives kept in a wooden box outdoors in the lab's property protection area. Report: http://www.ig.energy.gov/documents/IG-0757.pdf

Category 18.3 Data disposal & remanence (Dumpster® diving, discarded media

2007-03-13 DHS Daily OSIR; Finextra http://www.finextra.com/fullstory.asp?id=16653

UK BANKS CENSURED FOR DUMPING CUSTOMER DATA IN BINS.

The UK's Information Commissioner's Office (ICO) has found 11 financial institutions in breach of the Data Protection Act after they dumped customers' personal details in outdoor bins. The banks involved are HBOS, Alliance & Leicester, Royal Bank of Scotland, Scarborough Building Society, Clydesdale Bank, Natwest, United National Bank, Barclays Bank, Co-operative Bank, HFC Bank, Nationwide Building Society. The UK's Post Office was also found in breach of the act. The watchdog has now ordered the firms to sign a formal undertaking to comply with the principles of the Data Protection Act. Failure to abide by the rules will lead to further enforcement action and could result in prosecution.

Category 18.3 Data disposal & remanence (Dumpster® diving, discarded media

2007-03-15 DHS Daily OSIR; Orlando Sentinel (FL)
http://www.orlandosentinel.com/news/local/orange/orl-airport1707mar17%2C0%2C625703.story?coll=orl-home-promo

SENSITIVE PLANS, MAPS FOUND IN OIA DUMPSTER.

Orlando International Airport (OIA) officials already scrambling to plug security gaps had a new concern to explain Friday, March 15: how sensitive documents detailing the airport's layout, fuel-storage facilities, communications systems, and power lines wound up in a dumpster. The documents, part of an OIA 20-year growth master plan updated in August 2004, are labeled "sensitive security information" that should not be released without a "need to know." Instead, the documents somehow made their way into a trash bin next to a warehouse owned by the Greater Orlando Aviation Authority just east of the airport perimeter. A teenage aviation enthusiast who was exploring the area around the warehouse two weeks ago came upon the discarded documents and collected them as a souvenir. A parent delivered the material to the Sentinel last week in the wake of recent reports about OIA security problems. The airport's top security official, Robert Raffel, stressed that the binders contained planning documents that were widely distributed to airport managers, staff and planners -- and were not the airport's ultra-sensitive security plan. Still, he has ordered airport-security officials to conduct random checks of dumpsters and will send out warnings to workers about proper handling and disposal of sensitive documents.

Category 18.3 Data disposal & remanence (Dumpster® diving, discarded media

2007-03-21 DHS Daily OSIR; Pacific Business News (HI)
http://www.bizjournals.com/pacific/stories/2007/03/19/daily29.html

STATE OF HAWAII SUES FORMER TITLE COMPANY EXECUTIVE OVER DUMPED RECORDS.

Stephen Marn, who paid a handyman to take boxes of confidential records to the dump, has been formally accused of violating Hawaii consumer protection laws. The Hawaii Department of Commerce and Consumer Affairs (DCCA) sued the Hawaii Kai resident Wednesday, March 21, after its Office of Consumer Protection investigated. The boxes, found by PBN Editor Jim Kelly in a Niu Valley recycling dumpster, contained thousands of documents on hundreds of Hawaii residents, including names, addresses, Social Security numbers and other personal information. Marn was the president of Fidelity Escrow Services Corp., which went out of business in 2004. The DCCA alleges that
Marn broke not one but several state laws, including the new "Dumpster-diving law" that impels companies to dispose of records by burning or shredding them. It calls for fines of up to $2,500 per violation.

Category 18.3 Data disposal & remanence (Dumpster® diving, discarded media

2007-04-17 DHS Daily OSIR; Reuters
http://www.reuters.com/article/bondsNews/idUSN1731988520070417

TEXAS ATTORNEY GENERAL SUES CVS OVER CUSTOMER RECORDS.

Texas Attorney General Greg Abbott sued CVS/Caremark Corp. on Tuesday, April 17, after finding customer records with personal information such as driver license and credit card numbers in the trash behind one of the drugstore chain's Texas stores. Investigators with the office of the attorney general found the documents in a dumpster behind a CVS store in Liberty, Texas, near Houston, Abbott's office said. Medical prescription forms with name, address, date of birth, issuing physician and the types of medication prescribed were found, along with hundreds of active debit and credit card numbers with expiration dates, his office said. The store was either vacant or being vacated, according to a document filed with the court. Refund slips with a customer's name, driver's license number and telephone contact were also found, according to the document. The attorney general said investigators are working to determine if any exposed data was used illegally. He cautioned customers who used the Liberty store to carefully monitor
their financial statements for any signs of suspicious activity and said they should consider obtaining free copies of their credit reports.

19.1 Software piracy

Category 19.1 Software piracy

2006-06-09 DHS Daily OSIR; CNET News http://news.zdnet.com/2100-1009_22-6082334.html?tag=zdfd.newsfeed

MICROSOFT TO EASE UP ON PIRACY CHECK-INS.

Microsoft plans to update the Windows Genuine Advantage (WGA) Notifications program so that it only checks in with Microsoft once every two weeks, instead of after each boot-up. By year's end, the tool will stop pinging Microsoft altogether. The changes come after critics likened the antipiracy tool to spyware because the program, designed to validate whether a copy of Windows has been legitimately acquired, checks in with Microsoft on a daily basis. "We are changing this feature to only check for a new settings file every 14 days," Microsoft said in a statement on its Website. "Also, this feature will be disabled when WGA Notifications launches worldwide later this year."

Microsoft's statement: http://www.microsoft.com/presspass/features/2006/jun06/06-08 wgaqa.mspx

Category 19.1 Software piracy

2006-07-18 EDUPAGE; Wired News http://www.wired.com/news/wireservice/0,71404-0.html

MICROSOFT FILES PIRACY SUITS

Microsoft has filed 26 lawsuits in the United States against companies accused of selling pirated copies of the company's software to businesses and consumers. Because of the increasing saturation of the global market for software, Microsoft has more to gain by ensuring that the copies of its Windows and Office software that are bought are legitimate. The lawsuits are intended to raise awareness and encourage buyers and sellers to avoid pirated software, according to Microsoft, rather than to recoup money lost to counterfeit copies. The U.S. suits follow aggressive action in overseas markets, including China, Russia, and India, which are thought to be havens for software pirates. Ted Schadler, analyst with Forrester Research, said that although the rate of piracy is much lower in the United States than in other countries, Microsoft likely believes its influence with foreign governments will be stronger if it takes a tough line on domestic piracy. The lawsuits reportedly followed letters to those suspected of piracy, though at least one defendant denied that he had received such a letter.

Category 19.1 Software piracy

2007-04-06 DHS Daily OSIR; IDG News Service http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9015904&intsrc=hm_list

MOTHERBOARD MAKER'S WEBSITE HACKED.

The Website for computer parts manufacturer ASUStek Computer Inc. has been hacked and has been serving up attack code that exploited a critical Windows vulnerability, patched earlier last week. The exploit is hidden in an HTML element on the front page of ASUStek's Taiwanese Website, which then attempts to download the code from another server, according to Roger Thompson of Exploit Prevention Labs Inc. As of Friday, April 6, the server that downloaded the attack code was not operational, mitigating the risk of this attack, although attackers could easily redirect their attacks to a live server, he said. The malware is of particular concern because it exploits a critical flaw, patched just this past week, in the way Windows processes .ani animated cursor files. Reliable exploit code that targets this flaw has been circulating for more than a week now, and users who visit the ASUStek Web site before installing the MS07-017 patch could have their PCs compromised.

19.2 Music piracy

Category 19.2 Music piracy

2006-01-08 EDUPAGE; http://www.finfacts.com/irelandbusinessnews/publish/article_10004404.shtml

LEGAL DOWNLOADS SURGE AFTER CHRISTMAS

Sales of music tracks online surged over the holidays, indicating what might be new baseline levels for the market. During the Christmas week, 9.5 million tracks were downloaded from legal online music services, a new record for single-week sales. The following week, that number jumped to nearly 20 million tracks, triple the number sold during the same week a year earlier. Analysts attribute much of the gain to the ballooning number of portable MP3 players in the hands of consumers and to strong sales of gift cards. For the year, legal downloads rose 147 percent to 142.6 million. Although a drop always follows the holiday spike, analysts said the holiday numbers could indicate a market that will grow to perhaps 750 million or 1 billion tracks in 2006. Such numbers still pale compared to downloads on P2P services, which are estimated at 250 million per week, but experts say the upswing in legal downloads signals a changing tide for online music.

Category 19.2 Music piracy

2006-01-19 EDUPAGE; http://chronicle.com/daily/2006/01/2006011901t.htm

STUDENTS BLAME I2HUB FOR THEIR DOWNLOADING HABITS

A group of students at the University of Massachusetts at Amherst are demanding that the operators of the now-shuttered i2hub pay for their settlements with the Recording Industry Association of America (RIAA). According to Lisa Kent, an attorney at the university's Student Legal Services Office, which is representing the 42 students, i2hub deceived students into believing the service was endorsed by the university. This deception led to their believing that downloading materials over the network was legal. Unless i2hub pays the $157,500 that the RIAA is seeking from the students, the student legal office will file a lawsuit, said Kent. Charles S. Baker, the attorney for Wayne Chang, who created i2hub when he was a sophomore at UMass Amherst, rejected Kent's argument, saying that the software that Chang wrote was technically legal. "i2hub," he said, "is not responsible if your clients used the software for an improper purpose." Fred von Lohmann, a lawyer for the Electronic Frontier Foundation, compared the students' legal argument to "a shooter deciding to sue a gun company, saying, 'The gun made me do it.'"

19.4 Books / e-books piracy

Category 19.4 Books / e-books piracy

2006-04-20 EDUPAGE; http://www.pearsoned.com/pr_2006/041806.htm

PUBLISHERS SETTLE COPYRIGHT LAWSUITS, MORE PENDING

Two academic publishers have settled six of 20 lawsuits filed against individuals for selling copies of instructors' manuals online. The manuals accompany specific textbooks but are intended for faculty only because they include answers to homework and quiz questions in the texts. The individuals involved in the settlements were accused of making copies of instructors' manuals and selling them online, according to William Dunnegan, an attorney representing Pearson Education and John Wiley & Sons. Terms of the settlement were not released, nor were the names of the defendants. Other cases are still pending, and the publishers involved said the lawsuits are just one part of a larger campaign to address the problem of illegal online sales of copyrighted academic texts. Dunnegan said he hopes other academic publishers will join Pearson and Wiley, saying, "It will be easier to enforce as part of a group effort."

19.6 Counterfeit currency, credit-cards, other negotiable tokens

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

2006-06-06 DHS Daily OSIR; MosNews
http://www.mosnews.com/news/2006/06/06/ballettickets.shtml

RUSSIAN CENTRAL BANK WARNS OF "BALLET TICKET" COUNTERFEIT BILLS.

Scammers have designed counterfeit Russian ruble banknotes that have "Ballet Ticket" printed where "Bank of Russia" should be, the Russian Central Bank reports. According to Interfax, the bills, with a face value of 1,000 rubles (approximately $35), appeared in the Nizhny Novgorod region. The counterfeit notes are printed on good paper with water marks, all have II II 888888 as the serial number, and are a bit paler than authentic currency. Moreover, where regular notes have "one thousand rubles" and "Bank of Russia" printed, the false ones have "One thousand bubbles" and "Ballet Ticket".

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

2006-07-20 DHS Daily OSIR; East Texas Review
http://www.easttexasreview.com/story.htm?StoryID=3712

NEW SCAM, COUNTERFEIT U.S. POSTAL MONEY ORDER.

According to Texas Attorney General Gregg Abbott, "recently, in a troubling new twist, Texas financial institutions and consumers have been reporting the existence of high quality counterfeit U.S. Postal money orders that are being used to fool consumers into cashing them and wiring part of the money abroad. Finding that consumers have caught on to the counterfeit check scam, scammers are now using phony U.S. Postal money orders instead of cashier's checks. Cashier's checks and postal money orders are generally considered much safer than personal checks, since they are issued by financial institutions that have already verified the existence of sufficient funds. These counterfeits are so good sometimes that even bank tellers have been fooled."

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

2006-07-31 DHS Daily OSIR; Associated Press
http://www.belleville.com/mld/belleville/news/state/15162426.htm

COUNTERFEIT MONEY BEING PRINTED ON LESSER-VALUE NOTES.

A scheme has been hatched to pass off counterfeit money for goods and services, according to the U.S. Secret Service. Lower denomination bills are being bleached then reprinted as notes of higher value, using off-the-shelf computer scanners and printers. Secret Service officials say more and more of these bogus notes have shown up at their offices all over the country in recent months. The fakes now make up 90 percent of the $19,000 in counterfeit cash that the Secret Service's Chicago office receives each week. They are sold on the street for 40 or 50 cents on the fake dollar, in a burgeoning black market, said Xavier Morales, supervisor of the Secret Service's Chicago counterfeit squad. "It's not yet a national problem, but they figured it out here," Morales said. The fakes are printed on bleached bills, the finished product is on the real linen and cotton paper used by the Federal Reserve. The technique gives counterfeiters several advantages, including the fact that the paper feels legitimate, according to Morales. Most counterfeit bills that wind up in the hands of Secret Service agents in Chicago are received from banks after being deposited by fast-food outlets or other small businesses.

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

2006-08-07 DHS Daily OSIR; Associated Press http://www.washingtonpost.com/wp-dyn/content/article/2006/08/07/AR2006080700046_pf.html

U.S. FIGHTS NORTH KOREA OVER FAKE CURRENCY.

For those who have handled them, North Korean "supernotes" are virtually indistinguishable from the $100 bills they mimic -- near-perfect forgeries of the most widely circulated American bank note outside the U.S. In congressional testimony, court papers, and interviews, current and former U.S. officials have described what they say is an unprecedented effort by a reclusive,communist-led government to support itself with criminal activity, including counterfeit $100 bills. The supernotes' trail begins in 1989, when the bills were detected in the Philippines, and stretches from Asia to Europe to both coasts of the U.S. The fakes, say David Asher, a former State Department official on North Korea, "have been detected essentially on every continent in the world in the last 15 years." North Korea denies the counterfeiting charges. But the Secret Service has seized about $50 million worth of supernotes worldwide. Analysts say much more is likely in circulation. Still, the problem the supernotes pose for the U.S., officials say, is not the quantity but the high quality of the bills, which mimic the real thing right down to similar "reverse-engineered paper" and security features, such as special red and blue fibers, threads, and a watermark.

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

2006-10-20 DHS Daily OSIR; U.S. Department of the Treasury http://www.treasury.gov/press/releases/hp143.htm

DEPARTMENT OF THE TREASURY SECRETARY TO UNVEILS CURRENCY WITH NEW SIGNATURE.

Department of the Treasury Secretary Henry M. Paulson visited the Bureau of Engraving and Printing (BEP) on Monday, October 23, for the unveiling of the first paper currency with the new Secretary's signature. BEP engravers first transferred the Secretary's signature to steel plates, which will be used to print all new U.S. paper currency. Since the introduction of the smaller-size notes in 1929, the signatures of 25 Treasury Secretaries and 16 Treasurers -- including Secretary Paulson and Treasurer Anna Escobedo Cabral -- have appeared on U.S. paper currency. The new $20 Series 2006 Paulson-Cabral notes are expected to be sent to the Federal Reserve for distribution as needed.

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

2006-10-25 DHS Daily OSIR; Dow Jones http://www.nasdaq.com/aspxcontent/NewsStory.aspx?cpath=20061025%5cACQDJON200610251751DOWJONESDJONLINE001245.htm

U.S. GOVERNMENT SAYS COUNTERFEIT DOLLARS NOT SERIOUS PROBLEM TO ECONOMY.

Only about one in 10,000 U.S. currency notes is likely to be counterfeit, despite a mostly overseas market for U.S. dollars and new technologies that make it easier to produce phony money, according to an interagency U.S. government report Wednesday, October 25. "Counterfeiting is not currently a serious problem for the U.S. economy as a whole," according to an interagency report to Congress by the Federal Reserve, the Department of the Treasury, and the U.S. Secret Service. Counterfeiting remains low largely because of diligent investigation and prosecution, deterrent currency design and effective public education, the report says. Meanwhile, counterfeiters have benefited from the growing availability and falling cost of computers, software, and inkjet printers that can more easily mimic genuine currency. While counterfeiting in general appears to be "quite small" in relative terms, the report lists countries that have had the biggest seizures of fake dollars. In fiscal 2005, Peru topped the list, followed by Sri Lanka, Hong Kong, the Philippines, Singapore, China, Chile, Bolivia, Mexico and Taiwan.

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

2007-02-06 DHS Daily OSIR; CBC News (Canada) http://www.cbc.ca/consumer/story/2007/02/06/counterfeit.html

BANK OF CANADA TO REDESIGN BILLS AGAIN TO FOIL COUNTERFEITERS.

The Bank of Canada is planning another redesign of Canadian banknotes as part of a strategy to stay ahead of counterfeiters, the central bank's deputy governor says. "As I speak, my colleagues at the bank are hard at work designing the next generation of banknotes, planned for introduction beginning in 2011," David Longworth said during a Chamber of Commerce speech in Kitchener-Waterloo, Ontario, on Tuesday, February 7. The most common counterfeited bills are $10 and $20 notes, Royal Canadian Mounted Police figures show. "By 2009, we aim to reduce the level of counterfeiting to fewer than 100 counterfeits detected annually per million notes in circulation," Longworth said. That's down from 225 per million in 2006, 326 per million in 2005 and 470 per million in 2004. An internal bank report made public last year revealed that the bank felt counterfeiting had reached "dangerous levels," according to documents obtained by the Canadian Press. The central bank considers anything over 120 counterfeits per million to be a problem.

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

2007-02-26 DHS Daily OSIR; Associated Press http://www.whbf.com/Global/story.asp?S=6143306

STUDY SUGGESTS NEW WAYS TO BATTLE COUNTERFEITERS.

A new study estimates 30 out of every million 100-dollar bills is a fake. So to overcome those increasingly creative counterfeiters, the National Research Council has some suggestions. They're calling on the government to use plastic for low-denomination notes. They also recommend using complex starburst patterns that copiers can't reproduce. Other ideas include using inks that change color according to temperature, and varying the feel of the paper or other material that notes are printed on. The Council's report warns that within ten years, even low-skill amateurs will be able to duplicate almost any two-dimensional image.

Report: http://books.nap.edu/catalog/11874.html

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

2007-05-13 DHS Daily OSIR; Los Angeles Times http://www.orlandosentinel.com/business/orl-ymchecks1307may13,0,6726320,print.story?coll=orl-business-head

CHECK WASHING SCAM IS BACK.

An ordinary check made out to person A is bathed in a chemical available at any hardware store. In just a few minutes, it is blank again and made out to person B -- who is a thief. This process, which has been around for decades, is known as "check washing" among con men, and in an era of high-tech crimes it seems almost quaint. Except that it's back. Along with other check crimes. "It's a backlash after so much effort made by banks to boost security on their Websites," said Will Wade of the journal American Banker. "Some of the scammers are going old school with the easier stuff." U.S. banks lost $711 million because of check fraud in 2005. But losses to individuals andbusiness owners, many of whom will never realize they have been scammed, probably push that figure far higher. But not all the schemes are stuck in the past. A new fake-check fraud, which often makes use of digital printers and the Internet, has proved to be particularly potent. The National Consumers League last year received more complaints about fake checks than any other scam, except those involving online auctions and purchases.

19.8 Plagiarism & cheating

Category 19.8 Plagiarism & cheating

2006-03-26 EDUPAGE; http://news.bbc.co.uk/2/hi/uk_news/education/4848224.stm

PHONE CHEATING INCREASING

According to the Qualifications and Curriculum Authority (QCA), cheating on examinations in the United Kingdom is increasing, due in part to the number of cell phones being taken into exams. Although the incidence of cheating remains relatively low, officials from the country's testing agencies have begun to separate the kinds of cheating they discover. New data indicate that in 60 percent of the cases reported, the infraction involved bringing a cell phone into a test. Despite acknowledging that many times the phones were brought accidentally, the QCA said in its report that "it is essential that [the cheating] is actively addressed to ensure that learners, parents, and employers can continue to have confidence in the examination system." A spokesperson from the Department for Education and Skills echoed those sentiments, saying, "We expect schools to maintain high standards of discipline." The spokesperson continued, "There is no place for mobile phones in the classroom, let alone in the examining hall."

Category 19.8 Plagiarism & cheating

2006-05-02 http://www.pbs.org/newshour/bb/entertainment/jan-june06/viswanathan_05-02.html

STUDENT NOVELIST WITHDRAWS FIRST NOVEL BECAUSE OF PLAGIARISM

In early 2006, a 19-year-old sophomore from Harvard University, Kaavya Viswanathan, was in the news when her first novel, “How Opal Mehta Got Kissed, Got Wild, and Got a Life,” was withdrawn from bookstores by the publisher, Little, Brown after she admitted that she had unconsciously and unintentionally plagiarized material from novels by Megan McCafferty.

[Talk about an embarrassing start to a promising career….]

Category 19.8 Plagiarism & cheating

2006-06-17 LA Times; http://www.latimes.com/business/la-fi-termpaper17jun17,0,5819159,full.story?coll=la-home-headlines

TEACHERS ADJUST LESSON PLANS AS WEB FUELS PLAGIARISM

Terril Yue Jones wrote a summary of the effects of widespread plagiarism on educators. "Across the country, teachers and professors are abandoning the traditional academic chore of tidy margins and meticulous footnotes because the Internet offers a searchable online smorgasbord of ready-made papers." In addition to using plagiarism-detection systems such as TurnItIn, "Teachers who still assign long papers — 10 pages or more with footnotes and bibliographies — often require students to attach companion essays that describe every step of their research and writing." Many teachers are shifting their writing assignments to in-class essays; however, "In-class writing assignments are, by necessity, much shorter exercises that can be as brief as a couple of paragraphs and rarely more than a few pages." Jones quotes Nancy Willard of the Center for Safe and Responsible Internet Use as saying, "Kids these days have difficulty writing in depth about anything…. They are used to doing PowerPoint presentations, and the level of superficiality is great compared with term papers."

Category 19.8 Plagiarism & cheating

2006-06-18 EDUPAGE; BBC http://news.bbc.co.uk/2/hi/uk_news/education/5093286.stm

ADDRESSING STUDENT PLAGIARISM

Sally Brown, pro vice chancellor for assessment, learning, and teaching at Leeds Metropolitan University in the United Kingdom, believes that the age of technology has not only made cheating easy but has also engendered a sense among today's students that there is nothing wrong with copying and pasting someone else's work into your own. Many students today, she said, simply do not understand what plagiarism is and why it is wrong. Of the several approaches Brown suggested for fixing the problem, the one she thinks the best is designing coursework around plagiarism. By giving assignments that require personal knowledge or that compel students to provide regular accounts of their studies, an instructor can largely avoid the issue of plagiarism, according to Brown. Other strategies include education, punishments, and changing the culture among students so that cheaters are looked down on by everyone.

Category 19.8 Plagiarism & cheating

2006-06-20 EDUPAGE; ZDNet http://news.zdnet.com/2100-1040_22-6085712.html

HIGH-TECH CHEATING LEADS TO INJURIES

With nearly four students vying for every available spot in China's universities, cheating on entrance exams is rampant. As technology has entered the equation for cheaters, so has it become a tool for proctors trying to defeat the cheaters. Video cameras and cell-phone blocking have become common in Chinese testing centers. Students intent on cheating, then, resort to ever-smaller devices, with some students finding out how small is too small. According to the "China Daily," one student used an earpiece for cheating that was so tiny it entered his ear canal and ruptured his eardrum. Another student had to have an earpiece removed surgically, according to the paper, and yet another was injured when a remote listening device exploded. The device was strapped to the student's body and connected to headphones; the explosion left the student with an open wound in his abdomen.

Category 19.8 Plagiarism & cheating

2006-10-01 http://reasonandbrimstone.blogspot.com/2006/10/rainvilles-stolen-ideas.html;

POLITICAL WRITER RESIGNS IN DISGRACE OVER PLAGIARISM ON CANDIDATE'S WEB SITE

In Vermont in September, 29-year-old political writer Christopher Stewart had to resign from the campaign team of Martha Rainville for using text from other politicians on behalf of his candidate without quotation marks, without attribution and without permission. He eventually called local columnist Peter Freyne, who reported that he said, "I am deeply sorry and embarrassed for my actions…. I, and I alone, take full responsibility for any plagiarized material used by the campaign. I was stupid and I was wrong." In that case, plagiarism cost the enthusiast his job.

Category 19.8 Plagiarism & cheating

2007-05-15 DHS Daily OSIR; Associated Press http://www.fayobserver.com/article_ap?id=105272

NRC: GUARDS AT PROGRESS ENERGY NUKE PLANTED CHEATED ON TESTS.

Cheating on security guard tests could result in enhanced sanctions or civil penalties against Progress Energy and the security firm it contracts with at a nuclear plant in Wake County, the Nuclear Regulatory Commission (NRC) said. Inspectors said three supervisors with Securitas Security Services USA provided answers to guards taking annual recertification tests in 2005. That resulted in unqualified security guards at the Shearon Harris plant. Progress Energy and the security company are being allowed to respond in writing or meet privately to discuss the findings before the commission makes a final decision on penalties for what it deems willful violations. The three supervisors implicated in the case no longer work for Securitas.

19.9 Counterfeit products (hardware, clothing etc.)

Category 19.9 Counterfeit products (hardware, clothing etc.)

2006-08-30 DHS Daily OSIR; U.S. Food and Drug Administration
http://www.fda.gov/bbs/topics/NEWS/2006/NEW01441.html

CONSUMERS WARNED NOT TO BUY OR USE PRESCRIPTION DRUGS FROM VARIOUS WEBSITES THAT SELL COUNTERFEIT PRODUCT.

The U.S. Food and Drug Administration (FDA) is advising consumers not to purchase prescription drugs from Websites that have orders filled by Mediplan Prescription Plus Pharmacy or Mediplan Global Health in Manitoba, Canada, following reports of counterfeit versions of prescription drug products being sold by these companies to U.S. consumers. FDA is investigating these reports and is coordinating with international law enforcement authorities on this matter. Laboratory analyses are underway for intercepted product that was destined for the U.S. market. Preliminary laboratory results to date have found counterfeits of the following drug products from these Websites: Lipitor, Diovan, Actonel, Nexium, Hyzaar, Ezetrol (known as Zetia in the U.S.), Crestor, Celebrex, Arimidex, and Propecia.

Category 19.9 Counterfeit products (hardware, clothing etc.)

2007-02-02 DHS Daily OSIR; New York Sun http://www.nysun.com/article/47938

NEW YORK POLICE COMMISSIONER OUTLINES DANGERS OF COUNTERFEITING GOODS.

The New York Police Department last year increased enforcement against counterfeiters in New York, closing down 75 establishments, making 600 felony arrests, giving out 6,000 summonses, and seizing $18 million worth of fake goods, New York Police Commissioner Raymond Kelly said. Speaking at a summit on the problem of counterfeiting, he emphasized the connection between terrorism and the black market of counterfeit goods, as well as the hidden violent nature of the crime. In two recent cases in Spain and Michigan, he said, groups have used the "low-risk, high-profit" crime to finance an attack on the Spanish commuter trains and to fund Hezbollah. A deputy assistant attorney general at the Department of Justice, Sigal Mandelker, said the sale of counterfeit American products is estimated to be a $250 billion market.

Category 19.9 Counterfeit products (hardware, clothing etc.)

2007-04-04 DHS Daily OSIR; Business 2.0
http://money.cnn.com/magazines/business2/business2_archive/2 007/03/01/8401026/

SMART TECH FIGHTS COUNTERFEIT GOODS.

Though official numbers are scarce, online protection company MarkMonitor says a record $119 billion in knockoff goods will be sold on the Web in 2007, up from $84 billion last year--everything from counterfeit watches to fraudulent pharmaceuticals. But just as fake goods are enjoying a heyday online, so are virtual sleuths. New tech firms are arming brand holders with a smart solution: Web-crawling software that detects fraud and sends warnings to apparent violators, often with minimal human action. About two-dozen companies are using Web-crawling technology to search for counterfeit storefronts and sales. They detect scammers who set up shop using domain names similar to legitimate brands or who plaster brands' trademarks and logos on their online storefronts. The companies also monitor counterfeit sales, looking for keywords like "cheap," "discount," "authentic," and "factory variants." They flag colors that the original product wasn't made in and prices that are far too low.

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

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

2006-01-05 DHS Daily OSIR; http://www.press-citizen.com/apps/pbcs.dll/article?AID=/2006 0105/NEWS01/601050310/1079

IOWA COMPANY WINS $11 BILLION SPAM JUDGMENT

A Clinton, IA-based Internet service provider was awarded an $11.2 billion judgment against a Florida man for sending millions of unsolicited e-mails advertising mortgage and debt consolidation services. The lawsuit, filed in 2003 by CIS Internet Services owner Robert Kramer III, also prompted earlier judgments against companies in Florida and Arizona worth more than one billion. The most recent judgment was issued Friday, December 23, against James McCalla of Florida, who is also barred from accessing the Internet for three years. The lawsuit claimed that McCalla sent more than 280 million illegal spam e-mails into CIS's network, which provides Internet connections in Eastern Iowa and parts of Illinois. Kramer's lawsuit initially named numerous defendants, many of whom were dropped from the lawsuit the last couple years. John Mozena, co-founder and vice president of Coalition Against Unsolicited Commercial E-mail (CAUCE), said Kramer's lawsuit will likely not solve the spamming problem. He said, "There have been regulatory actions and even criminal actions against spammers, but it has not made much of a dent in the total volume of spam we see...Spam is still roughly two-thirds of all e-mail on the Internet."

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

2006-03-28 NEWSFACTOR < http://tinyurl.com/ouefj >

INDUSTRIAL ESPIONAGE COUPLE GETS JAIL TIME

The perpetrators of the Trojan Horse scandal that rocked Israel in May 2005 were sent to jail in March 2006. The husband-and-wife team installed Trojan horse software that functioned as keystroke loggers and transmitted confidential data for use in industrial espionage. They also had to pay about ½MU$ in restitution to their victims. Michael Haephrati, who wrote the software, went to prison for four years; Ruth Brier-Haephrati was jailed for two years for her role in selling the code to dishonest private investigators.

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

2006-04-19 DHS Daily OSIR; http://www.sophos.com/pressoffice/news/articles/2006/04/spyw arechen.html

HEFTY FINE FOR MAN WHO MARKETED BOGUS ANTI-SPYWARE SOFTWARE.

SophosLabs reports a man has been fined almost $84,000 for marketing a bogus anti-spyware program, but has warned Web surfers that there are many other fake protection products being unethically promoted on the Internet. Zhijian Chen of Portland, OR, was found to have made thousands of dollars by sending spam messages that fooled people into believing that their computers were infected by spyware, and claiming that a product called "Spyware Cleaner" was the cure. According to court documents, Chen sent out e-mails and advertisements promoting the "Spyware Cleaner" software in exchange for a 75 percent commission on each $49.95 sale.

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

2006-05-09 DHS Daily OSIR; http://news.yahoo.com/s/nm/20060509/tc_nm/crime_botmaster_dc ;_ylt=AuAzPlcqryDNlBx5rov1ohkjtBAF;_ylu=X3oDMTA5aHJvMDdwBHNl YwN5bmNhdA--

BOTMASTER GETS NEARLY FIVE YEARS IN PRISON.

Jeanson James Ancheta, a well-known member of the "Botmaster Underground" who pleaded guilty in January to federal charges of conspiracy, fraud and damaging U.S. government computers, was sentenced Monday, May 8, to nearly five years in prison for spreading computer viruses. Prosecutors say 11 the case was unique because Ancheta was accused of profiting from his attacks by selling access to his "bot nets" to other hackers and planting adware into infected computers.

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

2006-06-04 RISKS

TEXAS MEGA-SPAMMER SETTLES WITH STATE, MICROSOFT

The Associated Press reported, "One of the world's most notorious spammers has settled lawsuits with the state of Texas and Microsoft Corp. that cost him at least $1 million, took away most of his assets and forced him to stop sending the nuisance e-mails. Ryan Pitylak, 24, who graduated from the University of Texas[in May 2006], has admitted sending 25 million e-mails every day at the height of his spamming operation in 2004…. Pitylak, who plans to help Internet companies fight spam, said he would sell his $430,000 house and a 2005 BMW to help pay his fines and legal bills."

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

2006-06-23 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2158925/phishing-site-oper ator-gets-21

PHISHER GETS 21-MONTH JAIL TERM.

A 23-year-old phishing site operator from Iowa has been sentenced to 21 months in jail and will have to pay $57,294 in restitution. Jayson Harris had pleaded guilty to two counts of wire fraud and fraud. Harris operated a bogus MSN billing Website between January 2003 and June 2004, guiding visitors to the site through spam e-mail messages. The e-mails asked MSN customers to visit the Website and update their account information and credit card numbers in exchange for a 50 percent discount for the next month's MSN service. Microsoft tracked down the phisher and forwarded the information to the FBI. Microsoft is known for hunting down online criminals, but its actions have mostly resulted in the arrest and conviction of botnet operators. The Harris case is the first time that the company has assisted in the conviction of a phisher.

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

2006-06-24 DHS Daily OSIR; Associated Press http://www.kesq.com/Global/story.asp?S=5074358&nav=9qrx

HACKER GETS A YEAR IN PRISON FOR PUTTING 'TIME BOMB' ON COMPUTER.

William Shea was sentenced Thursday, June 22, for placing a "time bomb" on his employer's computer that corrupted more than 57,000 company records at the Silicon Valley-based debt collection company, Bay Area Credit Services. The malicious code on the computer network that was set to delete and modify data at the end of the month.

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

2006-06-30 DHS Daily OSIR; Channel Register (UK) http://www.channelregister.co.uk/2006/06/30/shadowcrew_sentencing/

SHADOWCREW MASTERMIND CONVICTED.

The co-founder of a carding Website that prosecutors describe as one of the biggest online forums for identity theft has been jailed. Andrew Mantovani plead guilty last November to various credit card fraud offences over his involvement with the infamous Shadowcrew website, the Associated Press reports. Mantovani is among 28 people arrested in October 2004 following a year-long undercover investigation, codenamed Operation Firewall, mounted by the U.S. Secret Service against Shadowcrew.com, a members-only underground website that became an online marketplace for credit card scammers and counterfeit identification document forgers. An estimated 4,000 Shadowcrew members allegedly trafficked in at least 1.7 million stolen credit card numbers and caused total losses in excess of $4 million. Victims of this carding activity included banks and credit card companies, who bore the brunt of losses, as well as consumers whose identities and credit histories were damaged by identity theft.

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

2006-08-15 http://news.bbc.co.uk/2/hi/uk_news/england/bristol/somerset/4795633.stm?ls

UK GAMES PIRATE JAILED FOR 18 MONTHS

Nicholas Hunter, a 40 year-old man from Bristol, England, was jailed after pleading guilty to 17 counts of violations under the Trade Marks Act for making and selling hundreds of titles of video games and some business software. The BBC reported that investigators "discovered copying equipment capable of producing 16 fake CDs every seven minutes, packaging materials and hundreds of illegally-copied games."

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

2006-08-25 http://www.cybercrime.gov/ferrerSent.htm

MILLIONARE OPERATOR OF BUYUSA PIRACY WEBSITE SENTENCED TO SIX YEARS IN PRISON

WASHINGTON- The owner of a massive for-profit software piracy website was sentenced in federal court to six years in prison, Assistant Attorney General Alice S. Fisher of the Criminal Division and U.S. Attorney Chuck Rosenberg of the Eastern District of Virginia announced [25 Aug 2006].

In addition to the prison term, Danny Ferrer, 37, of Lakeland, Fla., was also ordered by U.S. District Judge T.S. Ellis III to forfeit the proceeds of his illegal conduct, pay restitution of more than $4.1 million, and perform 50 hours of community service. The ordered forfeiture involves a wide array of assets, including numerous airplanes, a helicopter, boats, and cars, which Ferrer had purchased with the profits from his illegal enterprise. In particular, Ferrer forfeited a Cessna 152; a Cessna 172RG; a Model TS-11 ISKRA aircraft; a RotorWay International helicopter; a 1992 Lamborghini; a 2005 Hummer; a 2002 Chevrolet Corvette; two 2005 Chevrolet Corvettes; a 2005 Lincoln Navigator; an IGATE G500 LE Flight Simulator; a 1984 twenty-eight foot Marinette hardtop express boat; and an ambulance. Ferrer has also agreed to surrender the proceeds of sales of two fire trucks that were also bought with his illegal proceeds.

"Danny Ferrar obtained millions of dollars worth of luxury items by stealing and pirating the works of others. But now, the cars and planes and boats he paid for with the proceeds of his crime are being taken by the government, and he will spend six years in jail," said Assistant Attorney General Fisher. "The Department of Justice is committed to vigorous enforcement of the law and protection of intellectual property rights."

"Modern day pirates ought to expect modern day penalties," said U.S. Attorney Rosenberg. "We are very pleased with the sentence imposed today - one of the longest ever imposed for software piracy - and trust that it sends a strong message to those who pilfer the intellectual property of others."

Beginning in late 2002 and continuing until its shutdown by the FBI on Oct. 19, 2005, Ferrer and his co-conspirators operated the www.BUYSUSA.com website, which sold copies of software products that were copyrighted by companies such as Adobe Systems Inc., Autodesk, and Macromedia Inc. at prices substantially below the suggested retail price. The software products purchased on the website were reproduced on CDs and distributed through the mail. The operation included a serial number that allowed the purchaser to activate and use the product. Further investigation established that, during the time of its operation, www.BUYSUSA.com illegally sold more than $4.1 million of copyrighted software. These sales resulted in losses to the owners of the underlying copyrighted products of nearly $20 million.

After receiving complaints from copyright holders about Ferrer's website, an undercover FBI agent made a number of purchases of business and utility software from the site, which were delivered by mail to addresses in the Eastern District of Virginia.

Ferrer pleaded guilty before Judge Ellis on June 15, 2006, to one count of conspiracy and one count of criminal copyright infringement for selling pirated software through the mail.
. . . .

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

2006-08-25 EDUPAGE; San Jose Mercury News
http://www.siliconvalley.com/mld/siliconvalley/15361600.htm

FLORIDA SOFTWARE PIRATE SENTENCED

A federal judge in Virginia sentenced a Florida man to six years in prison for selling millions of dollars worth of pirated software. Danny Ferrer admitted that he sold bogus copies of software on his Web site, BuysUSA.com, using fake serial numbers that he obtained online. The FBI is continuing an investigation into those responsible for the fake serial numbers. Prosecutors said Ferrer's activities cost the software industry as much as $20 million between 2002 and 2005. Ferrer told the judge that he initially sold the counterfeit software to pay for a feeding tube for his wife but that "there was probably a certain amount of greed." Ferrer bought a number of airplanes, exotic cars, and other goods with the proceeds of his activities. The judge in the case ordered that Ferrer's assets be sold and the proceeds used to pay $4.1 million in restitution to Adobe Systems Inc., Autodesk, and Macromedia Inc. "If severe penalties were not attached," said the judge, "people would line up from here to Los Angeles to do what you've done."

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

2006-10-13 http://www.cybercrime.gov/munozSent.htm

CALIFORNIA MAN SENTENCED FOR ELECTRONICALLY STEALING TRADE SECRETS FROM HIS FORMER EMPLOYER, A CONSTRUCTION CONTRACTOR

United States Attorney Carol C. Lam announced that Benjamin Munoz, III, was sentenced today [13 Oct 2006] in federal court in San Diego by United States District Judge John A. Houston to serve six months in federal prison. Mr. Munoz previously pleaded guilty to electronically stealing trade secrets of construction contractor T.B. Penick and Sons, Inc., in violation of Title 18, United States Code, Section 1832.

According to Assistant U.S. Attorney Mitch Dembin, who prosecuted the case, in connection with his guilty plea Mr. Munoz admitted that he had been employed as a Project Manager for Penick and Sons until August 25, 2005. By virtue of that employment, Mr. Munoz knew that Penick and Sons had drafted a bid proposal to provide concrete and related services for a proposed commercial development at Otay Ranch Town Center. After leaving Penick and Sons, Mr. Munoz was hired by a competing contractor. Mr. Munoz further admitted that on September 26, 2005, while employed by the competing contractor, he accessed the computer network of Penick and Sons from his home computer, using an account of a Penick and Sons employee for which he knew the user name and password. Mr. Munoz also admitted that he did not have permission to use that account. After accessing the Penick and Sons computer network without authority, Mr. Munoz printed the draft bid proposal on his home printer and used the information to prepare a competing bid on behalf of his new employer, without his new employer's knowledge. Mr. Munoz knew that the Penick and Sons draft bid was confidential and a trade secret of Penick and Sons. Both Penick and Sons and Munoz's subsequent employer, among others, submitted bids for the Otay Ranch project.

Mr. Munoz's subsequent employer, after being informed of the investigation, withdrew its competing bid and cooperated in the investigation. The bid ultimately was awarded to Penick and Sons. Mr. Munoz acknowledged that the potential loss to Penick and Sons exceeded $400,000.

In addition to having to serve six months in prison, Mr. Munoz was ordered to pay a fine of $5,000 and a $100 special assessment. Upon his release from prison, Mr. Munoz will be subject to supervision by the U. S. Probation Department for a period of three (3) years.

This case was investigated by Special Agents assigned to the Cybercrime Squad of the San Diego Division of the Federal Bureau of Investigation.

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

2006-10-16 http://www.cybercrime.gov/heimSent.htm

CALIFORNIA MAN SENTENCED FOR RECKLESSLY DAMAGING A PROTECTED COMPUTER OWNED BY HIS FORMER EMPLOYER

United States Attorney Carol C. Lam announced that Jay Vern Heim was sentenced today by United States District Judge Roger T. Benitez in federal court in San Diego. Judge Benitez first accepted as final Mr. Heim's previously tendered plea of guilty to a charge of recklessly damaging a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A)(ii).

According to Assistant U.S. Attorney Mitch Dembin, who prosecuted the case, in connection with his guilty plea Mr. Heim admitted that he was a founding partner and employee of Facility Automation Systems ("FAS"), a San Diego company that installs and maintains building automation systems. He left FAS in March 2005. Mr. Heim further admitted that on January 26, 2006, he used the username and password assigned to FAS for its Internet domain, facilityautomationsystems.com, and redirected all FAS Internet traffic, including electronic mail, to a server at Mr. Heim's new employer, the Moreno Valley Unified School District. Mr. Heim knew that redirecting the traffic to that server would make FAS' web site and electronic mail services inaccessible. The cost to FAS in lost productivity and restoring services exceeded $6,000.

Mr. Heim was sentenced to two years of probation and required to pay a $500 fine in addition to having to make restitution to his victim, Facility Automation Systems, in the amount of $6,050.

This case was investigated by Special Agents assigned to the Cybercrime Squad of the San Diego Division of the Federal Bureau of Investigation.

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

2006-10-17 http://www.cybercrime.gov/stanleySent.htm

VIRGINIA MAN SENTENCED IN PEER-TO-PEER PIRACY CRACKDOWN

United States Attorney John L. Brownlee announced today [17 Oct 2006] that GRANT T. STANLEY, age 23, of Wise, VA, was sentenced to five months in prison to be followed by five months of home detention for his role in a BitTorrent peer-to-peer (P2P) network previously known as Elite Torrents.

United States District Court Judge James P. Jones also sentenced STANLEY to a $3,000 fine and three years supervised release. The defendant had previously pleaded guilty to a two count felony information charging conspiracy to commit copyright infringement and criminal copyright infringement in violation of the Family Entertainment Copyright Act.

"This is the first criminal enforcement action against copyright infringement on a P2P network using BitTorrent technology," said United States Attorney John Brownlee. "We hope this case sends the message that cyberspace will not provide a shield of anonymity for those who choose to break our copyright laws."

Stanley is one of three defendants convicted to date as a result of Operation D-Elite, a federal crackdown against the first providers (or suppliers) of pirated works to the technologically-sophisticated P2P network known as Elite Torrents. At its prime, the Elite Torrents network attracted more than 133,000 members and facilitated the illegal distribution of more than 2 million copies of movies, software, music, and games. On May 25, 2005, federal agents shut down the Elite Torrents network by seizing its main server and replacing its log-in web page with the following notice: "This Site Has Been Permanently Shut Down by the FBI and U.S. Immigration and Customs Enforcement (ICE)." Within the first week alone, this message was viewed over half a million times.

The Elite Torrents P2P network offered a virtually unlimited content selection, including illegal copies of copyrighted works before their availability in retail stores or movie theatres. Operation D-Elite is a joint investigation by ICE and the FBI as part of the Computer and Technology Crime High-Tech Response Team (CATCH), a San Diego task force of specially trained prosecutors and law enforcement officers focused on high-tech crime. Federal and state member agencies of CATCH include ICE, the FBI, the Department of Justice, the San Diego District Attorney's Office, San Diego Police Department, the San Diego Sheriff's Department, and San Diego County Probation.

Andrea Sharrin, Senior Counsel for the Department of Justice Criminal Division's Computer Crime and Intellectual Property Section and S. Randall Ramseyer, Assistant U.S. Attorney for the Western District of Virginia, prosecuted this case on behalf of the government. The Motion Picture Association of America also provided substantial assistance to this investigation.

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

2006-11-14 DHS Daily OSIR; Computeractive
http://www.pcw.co.uk/computeractive/news/2168530/jail-men-guilty-carousel-fraud

JAIL FOR GROUP GUILTY OF HI-TECH CAROUSEL FRAUD.

Seven UK men have been jailed for the skimming of VAT on items such as mobile phones and computer chips. The men were sentenced to more than 16 years imprisonment after being found guilty of millions in evasion and the laundering of the proceeds of these frauds. Known as carousel fraud, the scam involves the criminals importing high-value goods such as mobile phones and computer chips, free of VAT, from other countries in the European Union. These goods are then sold in the UK with VAT attached, but the criminals disappear with the tax they have collected.

1A5 Criminal hacker organizations

Category 1A5 Criminal hacker organizations

2006-03-30 DHS Daily OSIR; http://software.silicon.com/security/0,39024655,39157704,00. htm

CRIMINAL GANGS RECRUITING HACKERS.

Speaking at the e-Crime Congress in London Thursday, March 30, Alan Paller, director of research for SANS, said weak digital security in businesses is helping hackers fund criminal activity. Paller said he had recently seen cases of criminal gangs recruiting hackers by threatening to harm their families unless they agree to carry out denial-of-service extortion attacks. Paller said the FBI is currently receiving more than one report of cyber extortion every day.

Category 1A5 Criminal hacker organizations

2006-06-28 http://www.usdoj.gov/criminal/press_room/press_releases/2006_4666_06-28-06-DefendantsSentenced.pdf

OPERATION FASTLINK WINS PRISON TERMS FOR LND FIRST-RELEASE WAREZ GANG MEMBERS

WASHINGTON - David Chen Pui, 27, of Fountain Valley, Calif., and David Lee Pruett, 35, of Auburn, Washington, were sentenced to prison terms of 12 and 18 months, respectively. . . today [28 Jun 2006]. Pui and Pruett were sentenced for their involvement with online software piracy. They were prosecuted as a result of the Charlotte, NC component of Operation FastLink.

Pui and Pruett each pled guilty to a single felony count of conspiracy to commit copyright infringement, Pui for distributing pirated works from his own and other Internet sites, and Pruett for his involvement in the software release group “Legenda Never Die” or “LND.” On June 27, United States District Court Judge Graham Mullen sentenced Pui to 12 months imprisonment, and today Mullen sentenced Pruett to 18 months imprisonment. The sentencing of Pui and Pruett follow the recent sentencing of Franklin Edward Littel and Shawn Laemmrich in United States District Courts in Indianapolis and Marquette, Mich., respectively. The four defendants were investigated and charged as part of the same FBI undercover operation headquartered in Charlotte. Both Little and Laemmrich were sentenced to eight months in prison to be followed by eight months of home confinement.

These are the first federal criminal sentences for members of the so-called “warez scene” from the Charlotte component of Operation FastLink, an ongoing federal crackdown against the organized piracy groups responsible for most of the initial illegal distribution of copyrighted movies, software, games and music on the Internet. Operation FastLink has resulted, to date, in more than 120 search warrants executed in 12 countries; the confiscation of hundreds of computers and illegal online distribution hubs; and the removal of more than $50 million worth of illegally-copied copyrighted software, games, movies and music from illicit distribution channels.

. . . .

These four defendants were members of or affiliated with software release groups. Three of these individuals were active members of warez groups that acted as "first-providers" of copyrighted works to the Internet – the so-called "release" groups that are the original sources for a majority of the pirated works distributed and downloaded via the Internet. Once a group prepared a stolen work for distribution, the material was distributed in minutes to secure computer servers throughout the world. From there, within a matter of hours, the pirated works are distributed globally, filtering down to peer-to-peer and other public file sharing networks accessible to anyone with Internet access. The fourth defendant, Pui, operated his own distribution server.

Operation FastLink was the culmination of multiple FBI undercover investigations across the country. To date, 31 defendants have been convicted of felony copyright infringement offenses as a result of the Department of Justice anti-piracy initiative.
. . . .

Category 1A5 Criminal hacker organizations

2006-07-11 http://www.usdoj.gov/criminal/press_room/press_releases/2006_4676_CRM_06-424_ccips_Hatten_sentencing.pdf

OPERATION FIREWALL BAGS ANOTHER SHADWOCREW MEMBER

WASHINGTON – Chad Hatten, 36, of Houston, Texas, was sentenced today to 90 months in federal prison, to be followed by three years of supervised release, the Justice Department announced today [11 Jul 2006].

Hatten was sentenced by U.S. District Judge Lee H. Rosenthal in the Southern District of Texas to 66 months on four counts of access device fraud. He was also sentenced to 24 additional months for aggravated identity theft, which will be served consecutively to the access device fraud counts, pursuant to the Identity Theft Penalty Enhancement Act enacted in July 2004.

Hatten entered a plea of guilty on November 1, 2005, to a five-count superseding indictment charging him with four counts of access device fraud and one count of aggravated identity theft. As part of his plea, Hatten admitted to being a member of the Shadowcrew criminal organization, an international criminal organization with numerous members that promoted and facilitated a wide variety of criminal activities including the electronic theft of personal identifying information, credit card and debit card fraud, and the production and sale of false identification documents. Hatten used the Shadowcrew website to assist with his credit card fraud; he also purchased gift cards from retail stores using counterfeit credit cards and resold the gift cards for a percentage of their actual value. In addition to possessing and using stolen credit card numbers to obtain items of value, Hatten was also charged with possessing equipment used to encode counterfeit credit cards with stolen numbers.

Hatten's conviction is part of a continuing effort to prosecute individuals targeted during Operation Firewall, a year-long investigation undertaken by the U.S. Secret Service, working in cooperation with the U.S. Attorney's Office for the District of New Jersey, the Criminal Division's Computer Crime and Intellectual Property Section and other U.S. Attorneys' offices and law enforcement agencies. The undercover investigation led to the arrests of 21 individuals in the United States on criminal complaints in October 2004. Additionally, several individuals were arrested in foreign countries in coordination with the domestic arrests. For more information, visit: < http://www.cybercrime.gov/mantovaniIndict.htm >
. . . .

Category 1A5 Criminal hacker organizations

2006-08-06 DHS Daily OSIR; IDG News Service
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9002230&taxonomyId=17

CYBERCRIMINALS TAKING CUES FROM MAFIA, SAYS FBI.

The Website offered to sell stolen credit card information for $100, but it was the title of the poster that caught FBI agent Thomas X Grasso Jr.'s attention. The cybercriminal identified himself as a "Capo di capo" -- a boss of bosses, in Mafia parlance. As money has become the driving force behind online threats, cyber criminals have adopting the same kind of organizational structures as organized crime groups, Grasso said Friday, August 4, at the Defcon hacker conference. "This organized crime group, Carderplanet, organized themselves into the same structure as the Italian Mafia," said Grasso. The FBI estimates that cybercrime cost the U.S. more than $67 billion last year, Grasso said. Grasso then played a slick promotional video offering Carderplanet "business" services. It could easily have been mistaken for a legitimate IT consulting ad. Carderplanet is just one part of a larger confederation of online criminals called the International Carder's Alliance. They use known Websites and IRC (Internet Relay Chat) channels to coordinate their online attacks. Many other cybercrime groups, such as Mazafaka, Shadowcrew, and IAACA (the International Association for the Advancement of Criminal Activity), are affiliated with Carderplanet.

Category 1A5 Criminal hacker organizations

2007-02-09 DHS Daily OSIR; CNET News
http://news.com.com/Price+of+cybercrime+tools+shrinks/2100-7349_3-6158025.html

PRICE OF CYBERCRIME TOOLS SHRINKS.

It's becoming cheaper and easier to get hold of the tools needed to launch a cybercrime attack, according to security company RSA. Jens Hinrichsen, the company's product marketing manager for fraud auction, said Thursday, February 8, that RSA has been monitoring the Websites and ICQ channels where malicious hackers and cybercriminals interact. These sites allow participants to share feedback and even review one another's products. Addressing an audience at the RSA Conference 2007, Hinrichsen showed several screengrabs to illustrate that the prices being asked for hacking tools have been dropping, with many participants embracing volume discounts and other incentives. One example was a post offering a "Super Trojan," which could be used to install malicious code on a victim's PC, for $600.

Category 1A5 Criminal hacker organizations

2007-03-28 DHS Daily OSIR; IDG News Service
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9014675&intsrc=hm_list

CARDERIM: HACKERS BUILD ENCRYPTED IM TO KEEP OUT LAW ENFORCEMENT.

Hackers have built their own encrypted instant-message (IM) program to shield themselves from law enforcement trying to spy on their communication channels. The application, called CarderIM, is a sophisticated tool hackers are using to sell information such as credit-card numbers or e-mail addresses, part of an underground economy dealing in financial data, said Andrew Moloney, business director for financial services for RSA during a presentation at the International e-crime Congress in London on Wednesday, March 28. The name, CarderIM, is a reference to the practice of "carding," or converting stolen credit-card details into cash or goods. It's not known how widely CarderIM is being used, but its distribution appears to be limited, Moloney said. "To get ahold of it [CarderIM] you need to be part of one of the trusted groups, which we have agents within," Moloney said. The application supposedly uses encrypted servers that are "offshore" and does not record IM conversations.

Category 1A5 Criminal hacker organizations

2007-04-04 DHS Daily OSIR; Computerworld
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9015588&intsrc=hm_list

HACKERS NOW OFFER SUBSCRIPTION SERVICES, SUPPORT FOR THEIR MALWARE.

As organized gangs increasingly turn to cybercrime, Websites that sell malicious code are coming to represent the new face of malware development and distribution. Unlike malicious code writers of the past who tended to distribute their code to a tight group of insiders or in underground newsgroups, the new breed is far more professional about how it sells its wares, security researchers said. In return for downloading the malware to their sites, Website owners are promised at least $66 every Monday, with the potential for even more for "clean installs" of the malicious code on end user systems. The exploit code is usually encrypted and uses a range of morphing techniques to evade detection by security software. It is designed to use various vulnerabilities to try to infect a target system. And many exploit providers simply wait for Microsoft Corp.'s monthly patches, which they then reverse-engineer to develop new exploit code against the disclosed vulnerabilities, said Gunter Ollmann, director of security strategies at IBM's Internet Security Systems X-Force team.

1A6 Criminal hacker psychology & methods

Category 1A6 Criminal hacker psychology & methods

2006-04-13 DHS Daily OSIR; http://news.zdnet.co.uk/internet/security/0,39020375,3926334 1,00.htm

NASA HACKER TO SPEAK AT SECURITY SHOW.

NASA hacker Gary McKinnon will be joined by other hackers and security experts on a panel discussion at the Infosecurity Europe conference Thursday, April 27, in London. McKinnon faces the prospect of an indefinite stay in Guantanamo Bay, but this won't prevent him from appearing on the Infosecurity panel and discussing hacking at a UK security conference. The NASA hacker is currently fighting extradition to the U.S. in what has been a protracted trial. He is charged with gaining unauthorized access to 97 U.S. government computers, including machines belonging to NASA and the Department of Defense. He claims he was searching for evidence of UFOs.

Category 1A6 Criminal hacker psychology & methods

2006-11-10 DHS Daily OSIR; Computer World http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9004967

MUTATE, FRAGMENT, HIDE: THE NEW HACKER MANTRA.

Hackers working for criminal gain are using increasingly sophisticated methods to ensure that the malware they develop is hard to detect and remove from infected systems, security researchers warned at this week's Computer Security Institute trade show in Orlando. The most popular of these approaches involve code mutation techniques designed to evade detection by signature-based malware blocking tools; code fragmentation that makes removal harder; and code concealment via rootkits. Unlike mass-mailing worms such as MS Blaster and SQL Slammer, most of today's malware programs are being designed to stick around undetected for as long as possible on infected systems, said Matthew Williamson, principal researcher at Sana Security Inc. The goal in developing such malware is not to simply infect as many systems as possible but to specifically steal usage information and other data from compromised systems, he said. An increasingly popular way of attempting this is with the use of polymorphic code that constantly mutates. Many malicious hackers also now use "packers" to encrypt malware to evade detection.

Category 1A6 Criminal hacker psychology & methods

2006-11-19 DHS Daily OSIR; Columbus Dispatch (OH) http://www.columbusdispatch.com/news-story.php?story=dispatch/2006/11/19/20061119-A3-01.html

PRISON NO OBSTACLE FOR CUNNING ID THIEF; MAN ACCUSED OF TWO NEW SCHEMES.

Anthony F. Forte is accused of accessing personal account information -- including Social Security numbers, addresses and phone numbers -- while locked up in a state prison in Lancaster, OH. Bristow was able to mine the personal information of unsuspecting motorists by obtaining copies of their traffic tickets. Bristow took blank, pre-signed subpoena forms from a lawsuit he filed in an Indiana municipal court, filled in the case numbers (randomly picked) of 10 traffic tickets of which he wanted copies, and mailed the requests to Fairfield County Municipal Court. Court Clerk Sherry L. Eckman said the simple public-records request was met without question because officials are not allowed to ask why records are needed. Bristow is also accused stealing credit-card numbers and is suspected of using people's personal information to set up a phone account and circumvent the prison's system. In the alleged scam involving hotels in seven states, Bristow posed as a Holiday Inn executive who called and told the desk clerks that Ohio law-enforcement officers wanted help pursuing a prison escapee who had checked in. Then he conned desk clerks into giving up the names of men who had checked in, along with their credit card information.

Category 1A6 Criminal hacker psychology & methods

2006-11-27 DHS Daily OSIR; ZDNet Asia
http://www.zdnetasia.com/news/security/0,39044215,61969925,00.htm

HACKERS RIDE ON WEB APPLICATION VULNERABILITIES.

According to Watchfire, the most vulnerable area in the enterprise information ecosystem is Web applications. The company specializes in software and services to audit the security and regulatory compliance of Websites. Danny Allan, Watchfire's director of strategic research, noted that network perimeters bore the brunt of attacks in the past. Given that networks today are adequately protected by a range of security tools, Web applications are now not only easier to target, they are also linked to backend servers and databases containing a wealth of information. However, businesses are currently not spending enough to protect their Web applications, said Allan. Citing research by Gartner, he pointed out that 90 percent of IT security spending is on network protection and only 10 percent is spent on Web applications.

Category 1A6 Criminal hacker psychology & methods

2007-01-23 DHS Daily OSIR; Information Week
http://www.informationweek.com/news/showArticle.jhtml?ArticleID=196902970

ONE HACKER KIT ACCOUNTS FOR 71 PERCENT OF ATTACKS.

A multi-exploit hack pack was responsible for nearly three-fourths of all Web-based attacks during December, a security company said Tuesday, January 23. Tagged with the moniker "Q406 Roll-up," the attack kit was behind 70.9 percent of last month's attacks, reported Atlanta, GA-based Exploit Prevention Labs. Up to a dozen different exploits make up the kit, which includes several exploits derived from the proof-of-concept code that researcher HD Moore published in July 2006 during his "Month of Browser Bugs" project. It's difficult to tell the exact number of exploits in the package, said Exploit Prevention's chief technology officer, Roger Thompson, because the kit is heavily encrypted. The most common exploits found in the kit are setSlice, VML, XML, and (IE COM) Createcomobject Code. "The dominance of this package reinforces the fact that the development and release of exploits frequently parallels legitimate software businesses," Thompson said in a statement.

Category 1A6 Criminal hacker psychology & methods

2007-02-22 DHS Daily OSIR; SC Magazine http://scmagazine.com/us/news/article/635172/former-fbi-agent-youth-turning-cybercrime-money/

FORMER FBI AGENT: YOUTH TURNING TO CYBERCRIME FOR THE MONEY.

Young technology graduates from developing countries are being drawn into organized cybercrime believing they'll make more money than at legitimate jobs, according to Ed Gibson, chief security adviser for Microsoft U.K. Gibson, who addressed delegates at a security conference organized by Claranet in London Thursday, February 22, warned: "In countries like Ukraine, it is tempting for young people with a technology background to work for these hacking gangs because there is not a lot of money in legal jobs. Even when a person wants out, their family is threatened with violence so they continue to work for these organized criminals." The former FBI agent said that cybercrime gangs are operating in emerging nations--such as Ukraine and Bulgaria--to run online fraud campaigns because of lax law enforcement and lack of cooperation between authorities there in the West. "The police here in the U.K. and other developed countries are territorially and jurisdictionally bound," he said. "They can't just go to these emerging countries, where these cybercriminals are working, and liaise with the authorities there."

1A7 Contests

Category 1A7 Contests

2006-02-15 DHS Daily OSIR; http://www.windowsitpro.com/windowspaulthurrott/Article/ArticleID/49416/windowspaulthurrott_49416.html

IDEFENSE OFFERS $10,000 BOUNTY FOR CRITICAL BUG BY 31 MARCH 2006

iDefense announced that it will pay $10,000 to anyone who discovers a bug in a Microsoft product that results in a new Microsoft Security Bulletin with a severity rating of critical. But there's one slight catch: The bug must be reported by midnight March 31, 2006, EST. The company has paid for vulnerability reports for some time now. However iDefense is changing its tactics to some extent. A spokesperson for iDefense said, "Going forward, on a quarterly basis, we will select a new focus for the challenge and outline the rules for vulnerability discoveries that will qualify for the monetary rewards." iDefense competes against a growing underground market for vulnerability reports and exploit code, where reports and code are sometimes sold the highest bidder and other times sold to everyone who can pay the asking price.

Category 1A7 Contests

2006-03-06 DHS Daily OSIR; http://www.gcn.com/online/vol1_no1/40053-1.html

OPEN-SOURCE BUG HUNT RESULTS POSTED.

Coverity Inc. of San Francisco, CA, has released the results of a Department of Homeland Security (DHS)-funded bug hunt that ranged across 40 popular open-source programs. The company found less than one-half of one bug per thousand lines of code on average, and found even fewer defects in the most widely used code, such as the Linux kernel and the Apache Web server. To test the programs, Coverity deployed analysis software first developed by Stanford's computer science department. Ben Chelf, chief technology officer of Coverity, warned that this automated bug scan is not definitive, but it can point to bugs traditional in-house code review techniques can miss. The results are the first deliverable of a $1.2 million, three-year grant DHS awarded to a team consisting of Coverity, Stanford University and Symantec Corp. of Cupertino, CA. DHS wants to reinforce the quality of open-source programs supporting the U.S. infrastructure.

Category 1A7 Contests

2006-03-08 DHS Daily OSIR; http://www.informationweek.com/security/showArticle.jhtml?articleID=181502078

HACK-MY-MAC CHALLENGE LEAVES SYSTEM SHIPSHAPE.

Dave Schroeder, a University of Wisconsin systems engineer who said a Swedish Hack-My-Mac contest was too easy, closed down his own challenge Tuesday, March 7. The machine ran Mac OS X 10.4.5 with the latest security updates and had two local accounts. In addition, Schroeder left both SHH and HTTP open. The mini garnered attention and lots of traffic, said Schroeder, who logged 4,000 attempts. The machine weathered two denial-of-service attacks, various Web exploit scripts, SSH dictionary attacks, and untold probes by scanning tools, he added.

Category 1A7 Contests

2007-01-10 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2082014,00.asp

VERISIGN OFFERS HACKERS $8,000 BOUNTY ON VISTA, IE 7 FLAWS.

VeriSign's iDefense Labs has placed an $8,000 bounty on remote code execution holes in Windows Vista and Internet Explorer (IE) 7. The Reston, VA, security intelligence outfit threw out the monetary reward to hackers as part of a challenge program aimed at luring researchers to its controversial pay-for-flaw Vulnerability Contributor Program. The launch of the latest hacking challenge comes less than a month after researchers at Trend Micro discovered Vista flaws being hawked on underground sites at $50,000 a pop and illustrates the growth of the market for information on software vulnerabilities. iDefense isn't the only brand-name player in the market. 3Com's TippingPoint runs a similar program, called Zero Day Initiative, that pays researchers who agree to give up exclusive rights to advance notification of unpublished vulnerabilities or exploit code. The companies act as intermediaries in the disclosure process -- handling the process of coordinating with the affected vendor -- and use the vulnerability information to beef up protection mechanisms in their own security software, which is sold to third parties.

Category 1A7 Contests

2007-04-20 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/07/04/20/HNmachackedatconference_1.html

HACKER SHOWS MAC BREAK-IN.

A hacker managed to break into a Mac and win a $10,000 prize as part of a contest started at the CanSecWest security conference in Vancouver. In winning the contest, he exposed a hole in Safari, Apple's browser. "Currently, every copy of OS X out there now is vulnerable to this," said Sean Comeau, one of the organizers of CanSecWest. The conference organizers decided to offer the contest in part to draw attention to possible security shortcomings in Macs. Initially, contestants were invited to try to access one of two Macs through a wireless access point while the Macs had no programs running. No attackers managed to do so, and so conference organizers allowed participants to try to get in through the browser by sending URLs via e-mail. Dino Di Zovie, who lives in New York, sent along a URL that exposed the hole. Because the contest was only open to attendees in Vancouver, he sent it to a friend who was at the conference and forwarded it on. The URL opened a blank page but exposed a vulnerability in input handling in Safari.

1B1 Adult pornography

Category 1B1 *Adult pornography*

2006-02-01 DHS Daily OSIR; http://www.computerworld.com/securitytopics/security/story/0,10801,108267,00.html?SKC=security-108267

CONVICTION SECOND-EVER FOR TRANSMISSION OF OBSCENE E-MAIL MESSAGES.

A California man accused of managing the computer system to send hundreds of thousands of pornography-related e-mail messages has pleaded guilty to violating a U.S. antispam law. Kirk F. Rogers of Manhattan Beach, CA, pleaded guilty in U.S. federal court in Arizona Tuesday, January 31, to violating the U.S. CAN-SPAM Act, according to the U.S. Department of Justice (DOJ). Rogers' plea is the second-ever U.S. conviction related to the transmission of obscene e-mail messages, the DOJ said. Rogers agreed to forfeit money obtained in his spamming operation and faces a maximum sentence of five years in prison for a one-count violation of CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing Act). Sentencing is scheduled for June 5.

Category 1B1 *Adult pornography*

2006-06-01 http://www.usdoj.gov/criminal/press_room/press_releases/2006_4616_1_06-01-06obscenityfivestarPR.pdf

FEDERAL GRAND JURY CHARGES ARIZONA AND CALIFORNIA COMPANIES AND THEIR OWNERS WITH OBSCENITY VIOLATIONS

WASHINGTON – A Chatsworth, California film production company and a Tempe, Arizona video distributor and retailer, along with three owners of the businesses, have been charged by a federal grand jury in Phoenix, Arizona with operating an obscenity distribution business and related offenses. . . today [1 Jun 2006].

In an indictment unsealed yesterday, Five Star Video, LLC, of Tempe, Arizona, and Phoenix residents Christopher Warren Ankeney and Kenneth James Graham were charged with four counts of using an interactive computer service to sell and distribute DVDs containing obscene matter – identified as "Gag Factor 18," "Filthy Things 6," "Gag Factor 15" and "American Bukkake 13" – and three counts of using an interstate common carrier to transport obscene DVDs. In addition, Five Star was charged in a separate count with using the mails to deliver a DVD containing obscene matter. Jeff Norton Productions of Chatsworth, California, also known as JM Productions, and Mike Leonard Norton, who resides in Woodland Hills, California, were charged with six counts of using an interstate common carrier to transport DVDs that are obscene. All of the defendants were also charged with three counts of engaging in the business of selling and transferring obscene matter. The government is also seeking forfeiture of certain obscene materials and profits, together with Internet domain name and website ownership rights.

According to the indictment, JM Productions and Norton distributed to Five Star via UPS various obscene films in DVD format that were in turn sold and distributed to the public by Five Star, Ankeney and Graham via UPS and the mails. If convicted, the defendants face a maximum penalty of five years in prison on each of the obscenity counts.
. . . .

1B2 Child pornography

Category 1B2 Child pornography

2006-07-14 http://www.usdoj.gov/criminal/press_room/press_releases/2006_4684_CRM_06-438_ceos_Mitchel_sentencing.pdf

VIRGINIA MAN SENTENCED TO 150 YEARS IN PRISON ON CHILD PORNOGRAPHY CHARGES

WASHINGTON – A Virginia man was sentenced today [14 Jul 2006] in federal court in Roanoke, Va., to 150 years in prison on multiple charges involving the sexual exploitation of minors and the operation of child pornography websites, Assistant Attorney General Alice S. Fisher for the Criminal Division and U.S. Attorney John L. Brownlee of the Western District of Virginia announced today.

Gregory John Mitchel, 39, of Dublin, Va., received the sentence today at a hearing in federal court in the Western District of Virginia. Mitchel pleaded guilty on Jan. 27, 2006 to the production, distribution, sale and possession of child pornography. Mitchel had been convicted previously of child pornography offenses.

“Today's 150-year sentence is strong evidence of our commitment to punish severely child predators like Mr. Mitchel,” said U.S. Attorney Brownlee. “With the imposition of this sentence, Mr. Mitchel is no longer a danger to our children.”

The investigation that resulted in Mitchel’s conviction revealed that Mitchel facilitated and assisted in the daily operation of child pornography websites. The sites Mitchel administered—including a website called JustinFriends.com—sold membership subscriptions to individuals looking to obtain videos of minor boys engaging in sexually explicit conduct. Mitchel was also directly responsible for producing content for the websites by filming videos of minors engaging in sex acts. Mitchel and others received proceeds from the membership subscriptions.
. . . .

Category 1B2 Child pornography

2007-05-10 DHS Daily OSIR; Channel Register (UK)
http://www.channelregister.co.uk/2007/05/10/ore_credit_card_fraud/

CREDIT CARD FRAUD FEARS CLOUD OPERATION ORE.

Operation Ore, the UK's biggest ever child pornography investigation, involved the prosecution of 2,000 suspects among 7,000 Brits whose credit cards were used to pay for access to images of child abuse via a U.S.-based portal run by Landslide Inc. Nearly half a million people worldwide paid to access the depraved material. Lawyers and computer security experts suspect that many of those arrested may have been victims of credit card fraud. The police admit the possibility that third parties used fraudulently obtained credit card details to pay for child porn. U.S. authorities raiding Landslide found a list of credit card purchases on its servers. They passed over the details of UK suspects to British police, prompting the launch of Operation Ore in May 2002. Experts argue that the police failed to carry out proper checks designed to determine whether the suspects might have been victims of fraud. "The police just didn't look for and didn't understand the evidence of wholesale card fraud," Ross Anderson of Cambridge University told the BBC. "And as a result, hundreds of people... have been put through a terrible mill with threats of prosecution for child pornography."

1B3 Pedophilia, kidnapping, Net-adoption fraud

Category 1B3 Pedophilia, kidnapping, Net-adoption fraud

2006-08-02 EDUPAGE; BBC http://news.bbc.co.uk/2/hi/technology/5238992.stm

CHILD ONLINE IDENTITY CARD DEBUTS

An online identity service for children has debuted in the United Kingdom, the United States, Canada, and Australia. Conceived by U.K. businessman Alex Hewitt, the NetIDMe system requires parents to apply for ID cards for their kids and to supply a credit card as verification. Another person who knows the child must countersign the application. Once an ID is established, users can communicate with others online with the assurance that users who say they are children are not in fact adults who prey on kids. The service, which costs 10 pounds per year, is only effective if both communicating parties participate. Jim Gamble, chief executive of the Child Exploitation and Online Protection Centre, said that this effort, like any other that works to verify the age and identity of Internet users, will help prevent children from becoming victims of online predators. Detective Chief Superintendent Tom Porter of the Scottish Crime and Drug Enforcement Agency noted that Web users should nonetheless be cautious. "We would advise all parents and young people to…ensure no personally identifiable information is shared with online strangers."

1B5 Gambling

Category 1B5 Gambling

2006-04-12 RISKS; NYT; http://tinyurl.com/ou6jf

CASINO CAN REPROGRAM SLOT MACHINES IN SECONDS

As an enormous operational improvement, the 1,790 slot machines in Las Vegas's Treasure Island Casino can now be reprogrammed in about 20 seconds from the back-office computer. Previously this was an expensive manual operation that required replacing the chip and the glass display in each machine. Now it is even possible to have different displays for different customers, e.g., changing between "older players and regulars" during the day and a different crowd at night ("younger tourists and people with bigger budgets". (Slot machines generate more than $7B revenue annually in Nevada.) Casinos are also experimenting with chips having digital tags that can be used to profile bettors, and wireless devices that would enable players to gamble while gamboling (e.g., in swimming pools!). . . .

There are various risks of interest to RISKS. Regulators are concerned that machines might be "invaded by outsiders", while bettors are concerned that casinos could be intentionally manipulating the odds -- for example, giving preferential treatment to high rollers. Internal and external manipulation are clearly potential issues, which of course could be exacerbated by compromisible wireless security. By Nevada law, odds cannot be manipulated while someone is playing, although with four-minute timeouts before and afterward, machines may be reprogrammed on the fly.

If it were still April Fools' Day, I might suggest that the slot machines could be reprogrammable for use as voting machines on election day. That way you could have instant payoff if you vote the right way.

[Abstract and commentary by Peter G. Neumann]

Category 1B5 Gambling

2006-07-11 EDUPAGE; CNET http://news.com.com/2100-1030_3-6092852.html

HOUSE CLAMPS DOWN ON INTERNET GAMBLING

The U.S. House of Representatives has approved a bill that supporters said would place considerable and needed restrictions on Internet gambling. Opponents called it political maneuvering ahead of the November election and said the bill is full of huge loopholes. Under the terms of the Unlawful Internet Gambling Enforcement Act, restrictions would be placed on Internet service providers and on services that process financial transactions in their dealings with offshore gambling sites. Calling Internet gambling a "scourge," Rep. Bob Goodlatte (R-Va.) said the bill is necessary to prevent the practice from growing to include not only PCs but also cell phones and other mobile devices. Rep. John Conyers (D-Mich.) noted that an exemption has been carved out of the bill for horse racing, betting on which would still be allowed online. Previous efforts to pass such legislation have died on the vine, including a bill passed by the House in 2003 that the Senate did not act on.

Category 1B5 Gambling

2006-10-02 EDUPAGE; Red Herring http://www.redherring.com/Article.aspx?a=18906&hed=Snake+Eyes+for+Online+Gambling#

US LAW ATTACKS ONLINE GAMBLING

President George W. Bush is expected to sign legislation passed by the U.S. Congress outlawing Internet gambling in the United States. The law, called the Safe Port Act, was passed Saturday. The legislation could halve the $12 billion Internet gambling industry. Several companies have already suspended operations in the United States. RedHerring correspondent C. Medford writes, "One of the industry's best-known firms, PartyGaming, on Monday said it will suspend its U.S. business indefinitely if the president signs the Safe Port Act, a bill passed on Saturday that includes provisions that make the receipt of funds in connection with online wagering illegal in the U.S. . . . A second company, 888.com, which like PartyGaming is listed on the London Stock Exchange, also believes the president will sign the bill, and as a result announced its plans to terminate its U.S.-facing business."

Category 1B5 Gambling

2007-04-02 DHS Daily OSIR; KLAS-TV (NV) http://www.klas-tv.com/Global/story.asp?S=6315668

ASIAN ORGANIZED CRIME ON THE RISE IN LAS VEGAS.

Law enforcement officers from all over the United States and the world are in Las Vegas, NV. They're trying to find solutions to the growing problem of Asian organized crime. Experts say these gangs are absolutely connected to specific types of crimes. They say these Asian gang members focus on crimes where a lot of money is involved including -- selling methamphetamine, counterfeiting, and human smuggling. The draw of Las Vegas, for Asian organized crime gangs, is money. And for them, it comes in a number of different ways. The gang members are known to try to clean their dirty money, or launder it, by gambling and betting on sports. They're also responsible for infusing counterfeit money into the economy, and they have a hand in the illegal businesses of human smuggling and dealing methamphetamine. Rich Staka, with the St. Paul, MN, Police Department, is in Las Vegas to teach police officers about Asian gangs. Experts say these gang members are technologically sophisticated, good at planning and communicating their orders by computers.

1B6 Auctions, sales

Category 1B6 Auctions, sales

2006-08-03 DHS Daily OSIR; Register (UK) http://www.channelregister.co.uk/2006/08/03/ebay_scam_automation/

EBAY SCAMMING AUTOMATION PRIMED FOR FRAUD.

Scammers are starting to use automated bots in a bid to establish a bogus eBay reputation that will later allow them to dupe gullible users through bogus auctions. By automating the process of creating an account with an ostensibly good reputation, crooks can avoid the tedious business of building up a decent profile before looking to cash in with a scam auction. The "eBay scamming automation" begins with the creation of randomly named, fake user accounts. These fake users, powered by automated Web spider software, search eBay for extremely low value "buy it now" items, such as eBook or wallpapers, and place a purchase. As Fortinet points out, most one-cent-plus-no-delivery-cost sellers automate the whole transaction: should someone buy their eBooks, a script e-mails it automatically to the buyer, and leaves a standard feedback comment on the buyer's profile. The fake user then automatically responds with a standard feedback comment on the seller's profile. Software bots talk to software bots, and scammers can build up multiple fake accounts.

Category 1B6 Auctions, sales

2006-11-16 DHS Daily OSIR; Bankrate http://biz.yahoo.com/brn/061116/19824.html?.v=1

'SECOND-CHANCE' ONLINE AUCTION SCAMS.

Scammers sometimes watch bidders in high-dollar auctions, especially on big-name auction sites, such as eBay, and try to dupe unsuspecting buyers out of their money after an auction closes. The scheme, known as a second-chance auction scam, is just one of many types of Internet auction fraud -- the leading type of offense reported to the Internet Crime Complaint Center (IC3). Second-chance scams are one of the most popular auction fraud complaints currently reported to the center, says Aaron Naternicola of the IC3. Of the 17,933 auction fraud complaints it received within the past 12 months, 1,381, or 7.7 percent, involved second-chance online scams. Second-chance scammers wait until auctions end and then offer non-winning bidders a phony second chance to purchase the item -- usually through a wire transfer service. April Wall of the National White Collar Crime Center explains that by targeting bidders in specific auctions, the scammer can cash in on the victim's invested interest in the product. A majority of second-chance auction fraud complaints come through eBay auctions, says Wall, but "this is more than likely simply a function of the huge popularity of the eBay site...All auction sites have the potential for this type of fraud."

Category 1B6 Auctions, sales

2006-11-24 DHS Daily OSIR; Mirror (UK) http://www.mirror.co.uk/news/tm_headline=boy-who-built-a-nuclear-reactor-in-his-basement-%26method=full%26objectid=18150199%26siteid=94762-name_page.html

BOY USED PARTS BOUGHT ON EBAY TO BUILD A NUCLEAR REACTOR AT HIS HOME.

A teenager has created a working nuclear reactor in the basement of his family home. Thiago Olson, 17, bought spare parts on eBay and persuaded manufacturers to give him discounts to create the machine. It took 1,000 hours over two years to build the fusion reactor, which creates energy by combining atoms. During the process, a 40,000-volt charge is supplied from a gutted mammogram scanner.

Category 1B6 Auctions, sales

2007-01-09 DHS Daily OSIR; Finextra (UK) http://finextra.com/fullstory.asp?id=16346

ENTROPIA UNIVERSE TO AUCTION VIRTUAL BANKING LICENSES.

The company behind Entropia Universe -- an online role-playing game that has a real world cash economy -- says it will auction five virtual banking licenses that will allow financial firms to set up real world banking systems in the online universe. Online science fiction game Entropia Universe has over 500,000 members and had a turnover of over $160 million in 2005. The cyber world has a currency that has a fixed exchange rate with the U.S. Dollar. Cash can be moved between Entropia Universe and the real world using an ATM card. Now MindArc, the company that developed Entropia, is offering banks two-year exclusive licenses that will enable them to set up operations in the online world. The licenses will be available through the public auction beginning mid January 2007. The virtual banks will work in a similar way to real world firms and will initially be provided with secure systems enabling them to lend money to citizens and collect interest payments.

Category 1B6 Auctions, sales

2007-01-18 DHS Daily OSIR; Associated Press
http://news.yahoo.com/s/ap/20070118/ap_on_hi_te/ebay_fraud

EBAY HEIGHTENS SECURITY PRECAUTIONS.

Executives at eBay Inc. are touting security as their top priority in 2007 after an internal survey showed that online scammers may be denting the company's reputation. The company began a program last year to safeguard members' identities by concealing their user names on expensive listings. That measure could make it harder for con artists to contact losing bidders and goad them into "second chance offers," where customers wire cash to the scammers' accounts. Engineers also want to reduce counterfeit items and clamp down on scams between buyers and sellers from different countries, said William C. Cobb, president of eBay North America. Cobb said, "Where we've historically put an emphasis on transparency and free choice, today the security threats are more complex, and we're more actively protecting our buyers from fraud." The emphasis on security enhancements is billed as the most important initiative in the company's 12-year history. EBay says less than one-hundredth of one percent of the listings on its Website are fraudulent. But even by that measure, 58,300 auctions may have been fraudulent in one three-month period. More concerning, fraud disproportionately strikes high-end categories such as automobiles, electronics and jewelry.

Category 1B6 Auctions, sales

2007-04-06 DHS Daily OSIR; Washington Post http://www.washingtonpost.com/wp-dyn/content/article/2007/04/05/AR2007040502086.html

RETAILERS JOIN FORCES TO TRACK THEFT RINGS.

Two of the shopping industry's largest trade groups are joining forces with the FBI to create a database that tracks retail crime gangs, which they say are becoming increasingly organized. About 35 companies are participating in the database. The Law Enforcement Retail Partnership Network, or LERPnet, launched Monday, April 9, for retailers, and law enforcement will have access in a few months. The Retail Industry Leaders Association and the National Retail Federation (NRF), which have each launched similar databases recently, teamed up to create the new online catalogue. About 14,000 incidents have been recorded in the NRF database alone. Although theft has always existed in retail, technology has broadened criminals' reach and allowed them to become more sophisticated. The industry estimates it lost $37.5 billion to theft and fraud in 2005. Gangs often steal items from several stores, then sell the goods for about 70 percent of the retail value at online auction sites in a practice known as "e-fencing." In other cases, the gangs may even return items to stores with fraudulent receipts for the original value, plus tax.
LERPnet: http://www.nrf.com/lerpnet/press.htm

1B7 Hate groups

Category 1B7 Hate groups

2006-05-04 DHS Daily OSIR; http://abcnews.go.com/Technology/wireStory?id=1925141

REPORT: HATE GROUPS USE U.S. INTERNET SERVERS.

Hate groups around the world, including Islamic militants, often use Internet servers based in the U.S. to send propaganda and instructions to followers, according to a report released Thursday, May 4, by the Simon Wiesenthal Center (SWC). The Center said it had logged some 6,000 Websites in the past year used by racists and bigots to incite violence. Extremist anti-Americans often find it easier and cheaper to use a site hosted in America since the U.S. has free speech and little Internet censorship. Recently, the center also has been intercepting an increased number of online tutorials and how-to manuals aimed at sympathizers who might actually be recruited to carry out attacks. SWC press release: http://www.wiesenthal.com/site/apps/nl/content.asp?c=fwLYKnN 8LzH&b=312458&content_id={433F72C6-2173-4360-8981-0BB7B508C4 87}&notoc=1 SWC's interactive report will be available for purchase May 2006: http://www.wiesenthal.com/site/pp.asp?c=fwLYKnN8LzH&b=242023

Category 1B7 Hate groups

2006-08-31 EDUPAGE; Houston Chronicle http://www.chron.com/disp/story.mpl/ap/fn/4155909.html

JUDGE IN BRAZIL ORDERS GOOGLE TO TURN OVER DATA

A judge in Brazil has ordered Google to release user information relating to an investigation of child pornography and hate speech. Prosecutors in the country allege that users of Orkut, a networking site operated by Google, use the site to exchange illegal photographs and to post hate speech targeting blacks, Jews, and homosexuals. Officials from Google said that although the company has been cooperating with investigative requests from Brazilian authorities, Google does not maintain information on users of Orkut. The judge in the case rejected that argument and ordered Google to turn over requested information or face fines of $23 million per day. "It is not relevant that the data are stored in the United States," said Judge Jose Marcos Lunardelli, "since all the photographs and messages being investigated were published by Brazilians, through Internet connection in national territory."

Category 1B7 Hate groups

2007-03-04 DHS Daily OSIR; Associated Press
http://www.cnn.com/2007/US/03/04/white.supremacist.gang.ap/index.html

GROWING WHITE SUPREMACIST GANG INVOLVED IN IDENTITY THEFT.

The white supremacist gang Public Enemy No. 1 began two decades ago as a group of teenage punk-rock fans from upper-middle class bedroom communities in Southern California. Now, the violent gang that deals in drugs, guns and identity theft is gaining clout across the West after forging an alliance with the notorious Aryan Brotherhood, authorities say. In the past three years, its ranks have doubled to at least 400, but authorities suspect there could be hundreds of other members operating under the radar. They said heavy recruiting is taking place throughout California and Arizona, and members have been picked up by police in Nevada and Idaho. Public Enemy is now involved in identity theft. Cpl. Nate Booth, a gang detective with the Buena Park Police Department in Orange County, said the gang has gone from swiping personal information from mailboxes and trash to stealing entire credit profiles with the help of girlfriends and wives who take jobs at banks, mortgage companies and even state motor vehicle departments. Money from those operations is used to fuel its methamphetamine business, he said. Authorities worry that Public Enemy is using stolen credit information to learn the home addresses of police and their families.

1C2 Identity theft

Category 1C2 Identity theft

2006-06-05 DHS Daily OSIR; Consumer Affairs
http://www.consumeraffairs.com/news04/2006/06/scammers_credit_cards.html

MANY SCAMMERS PREFER BANK ACCOUNTS TO CREDIT CARDS (YOURS)

Scammers have a number of ways to steal from you, but the credit card is losing popularity among the criminal class. As consumers have become more protective of their credit card information in recent years and as credit card companies have improved security, scammers have had to look for alternate ways to commit their crimes. Since consumers are protected from large unauthorized charges, banks are more likely to go after credit card thieves. Today, a scammer would rather get access to a bank account number than a credit card. With the bank account number, a scammer can access an account and take all the money in it.

Category 1C2 Identity theft

2006-06-23 DHS Daily OSIR; Business Week
http://www.idanalytics.com/pdf/BusinessWeek_IDTheftMore_Hype_Than_Harm062306.pdf

ID THEFT: MORE HYPE THAN HARM.

All told, as many as 88 million Americans -- more than one in four -- had digital data exposed in the past 18 months. With each report, the feeling of helplessness grows. But for all of the drama over ID theft, what is not often pointed out is how rarely it results in actual financial loss for consumers. There's reason to believe that the actual losses may be a little more than a tenth of the $48 billion annual estimate that often gets thrown around. In fact, at the same time that regular folks are getting the wits scared out of them about security breaches, experts in the field are growing less worried about the impact. Law enforcement officials, who braced for a wave of financial fraud following all those well-publicized incidents, admit they've been struck by the lack of follow-through by criminals. "What we've seen has not been significant...Given the high profile, we would have expected to have seen more," says Daniel Larkin, who heads the Internet Crime Complaint Center for the FBI. The conclusion of the article points out a common misconception: “Perhaps the most spooky thing about the ID-theft scare is that chances are high the data weren’t stolen by some shadowy hacker in Estonia, after all, but someone very close to you. Fully one-fourth of the respondents in the 2003 FTC study who had been the victim of a financial fraud said they knew who had committed the crime, and in half those instances the perpetrator turned out to be a friend, relative, or neighbor.”

Category 1C2 Identity theft

2006-06-27 DHS Daily OSIR; Associated Press http://news.com.com/2100-1029_3-6088997.html

EXPERTS TO FORM ID THEFT RESEARCH CENTER.

An alliance of businesses, colleges, and federal crime fighters will combine their expertise at a new research center that will study the problems of identity theft and fraud. Founding partners of the Center for Identity Management and Information Protection include LexisNexis Inc. and IBM Corp., the U.S. Secret Service, and the FBI. The center will be established in New York at Utica College. Research will focus on critical issues in identity management, information sharing policy, and data protection, said Dr. Gary Gordon, a Utica College professor and expert in cybercrime and identity fraud. One of the initial research projects at the center will examine current and emerging criminal groups that perpetrate identity fraud and theft, with a focus on their methods of operation. It also will look at developing stronger identity authentication systems. The center will share its research through training sessions, symposiums, publications, and its Website.

Center for Identity Management and Information Protection: http://www.cimip.org

* * *

[MK adds: From http://www.utica.edu/academic/institutes/cimip/about/index.cfm]

WELCOME TO CIMIP

Utica College's Center for Identity Management and Information Protection is a research collaborative dedicated to furthering a national research agenda on identity management, information sharing, and data protection. Founded in June 2006, its ultimate goal is to impact policy, regulation, and legislation, working toward a more secure homeland.

CIMIP's partners are committed to working together to provide resources, gather subject matter experts, provide access to sensitive data, and produce results that will be acted upon. Completing research and publishing papers based on the results is not enough. The results must be put into action in the form of best practices, new policies, regulations, and legislation, training opportunities, and proactive initiatives for solving the growing problems of identity fraud and theft, secure sharing of information, and information protection.

Please visit this website often to see the latest projects and results. Information about becoming involved is provided under Partners and Supporters.

Category 1C2 Identity theft

2006-07-18 http://www.fdic.gov/news/news/press/2006/pr06071.html

US AGENCIES PROPOSE IDENTITY THEFT RED FLAGS

The federal financial institution regulatory agencies and the Federal Trade Commission are soliciting comments on a Notice of Proposed Rulemaking (NPRM) concerning identity theft "red flags" and address discrepancies. The NPRM, which has been reviewed and approved by each of the listed agencies, implements sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003.

The regulations that the agencies are jointly proposing would require each financial institution and creditor to develop and implement an identity theft prevention program that includes policies and procedures for detecting, preventing, and mitigating identity theft in connection with account openings and existing accounts. The proposed regulations include guidelines listing patterns, practices, and specific forms of activity that should raise a "red flag" signaling a possible risk of identity theft. Under the proposed regulations, an identity theft prevention program established by a financial institution or creditor would have to include policies and procedures for detecting any "red flag" relevant to its operations and implementing a mitigation strategy appropriate for the level of risk.

The proposed regulations also would require credit and debit card issuers to develop policies and procedures to assess the validity of a request for a change of address followed closely by a request for an additional or replacement card.

Additional proposed regulations would require users of consumer reports to develop reasonable policies and procedures that they must apply when they receive a notice of address discrepancy from a consumer reporting agency.

Category *1C2* *Identity theft*

2006-07-25 EDUPAGE; CNET http://news.com.com/2100-1029_3-6098246.html

BRITS CONSIDER PRISON FOR IDENTITY THIEVES

British legislators are considering amending the Data Protection Act to allow for prison terms for identity thieves in addition to the fines currently allowed by the law. The proposal followed a report from Richard Thomas, data protection watchdog information commissioner, which argued that the existing penalties are insufficient to deter potential identity criminals. The amendment would allow for prison terms of up to two years for those found guilty of intentionally misusing personal information; individuals who mistakenly disclose or otherwise mishandle personal information would not be subject to the new provisions. Thomas welcomed the proposal, saying it would serve to discourage those who might be considering identity theft. A review of the proposal will run through October.

Category *1C2* *Identity theft*

2006-08-09 DHS Daily OSIR; Scotsman (UK) http://thescotsman.scotsman.com/index.cfm?id=1153962006

ONE IN TEN BRITONS SUFFERS ID THEFT.

One in ten Britons has been the victim of identity fraud, according to new research which suggests the problem of stolen personal information is much worse than previously thought. Nine percent of those interviewed for the study believed they had been a victim of ID theft -- the equivalent of six million people. Experts said the number of fraudulent incidents was far higher than reported. The most vulnerable were those under 30, because they are the least aware when it comes to protecting their personal information. According to CIFAS, the UK's fraud prevention service, identity theft has risen from 20,000 reported cases in 1999 to 137,000 in 2005. Professor Martin Gill, identity theft specialist and professor of criminology at Leicester University, said: "Official statistics relating to cases of ID theft are not indicative of the true scale of this growing crime, many cases go unrecorded or undetected.

Category *1C2* *Identity theft*

2006-08-11 DHS Daily OSIR; Dallas Morning News http://www.dallasnews.com/sharedcontent/dws/news/city/collin/stories/081106dnccocountyIDtheft.2108934.html

ONLINE RECORDS RAISE IDENTITY THEFT CONCERNS.

These days, an identity thief could access sensitive, personal information by surfing through online records that once were available only at the county courthouse. These photographic images of deeds, divorce settlements, tax liens and bankruptcies -- particularly older records -- may contain Social Security numbers, driver's license numbers, and credit card and bank account information. Now, county officials in Texas and around the country are evaluating yet another trade-off created by technology: Does the public convenience of online government records outweigh the individual's need for financial privacy? Some counties are deleting sensitive data from online documents but keeping it on original courthouse records. The theory is that identity thieves are less likely to show themselves in a public office. They're more comfortable with the anonymity of sitting at home on the computer. Other counties have begun charging for online records to discourage casual snoops. Still others provide all public documents for free without alteration. The Texas Supreme Court is studying recommendations from an advisory group to regulate access to online public civil and criminal court records containing sensitive information. Other states also are looking at ways to protect personal identifying information from full public view.

Category *1C2* *Identity theft*

2006-09-04 DHS Daily OSIR; New York Times http://www.nytimes.com/2006/09/04/us/04theft.html

SOME ID THEFT IS NOT FOR PROFIT, BUT TO GET A JOB.

Though most people think of identity theft as a financial crime, one of the most common forms involves illegal immigrants using fraudulent Social Security numbers to conduct their daily lives. With tacit acceptance from some employers and poor coordination among government agencies, this practice provides the backbone of some low-wage businesses and a boon to the Social Security trust fund. In the 1990's, mismatches accounted for $20 billion in Social Security taxes paid. "It's clear that it is a different intent than trying to get someone's MasterCard and charge it up, knowing they're going to get the bill," said Richard Hamp, a Utah assistant attorney general. The Federal Trade Commission, which estimates that 10 million Americans have their identities stolen annually, does not distinguish between people who steal Social Security numbers so they can work and those who intend to steal money.

Category 1C2 Identity theft

2006-09-27 DHS Daily OSIR; Associated Press
http://www.buffalonews.com/editorial/20060927/4027571.asp

PATAKI SIGNS THREE BILLS TO COMBAT IDENTITY THEFT.

New York Governor George Pataki (R) has signed into law three bills to combat identity theft. The Consumer Communication Records Privacy Act prohibits the sale, fraudulent transfer, or solicitation of a person's telephone records without his consent. The second bill puts new limits on the use of Social Security numbers, restricting businesses from printing the numbers on mailings and prohibiting companies from requiring an individual to transmit his encrypted Social Security number over the Internet. It also requires businesses to institute safeguards to protect customers' identities. A third measure strengthens existing laws to prosecute those who intentionally steal personal information or plant programs such as spyware on personal computers without authorization.

Category 1C2 Identity theft

2006-10-25 DHS Daily OSIR; Computerworld
http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=data_control_and_ip&articleId=9004429&taxonomyId=144

ONLINE ID FRAUD IS HYPED; REAL PROBLEM IS OFF-LINE.

The problem of online identity theft is vastly hyped when compared with its more prevalent off-line equivalent, according to Javelin Strategy & Research. While keylogging software, phishing e-mails that impersonate official bank messages, and hackers who break into customer databases may dominate headlines, more than 90 percent of identity fraud starts off conventionally, with stolen bank statements, misplaced passwords, or other similar means, according to Javelin. While scammers often use the Internet to access existing bank, phone or brokerage accounts or to create new ones using stolen details, in only one out of 10 of those incidents did the actual theft of the personal data take place through e-mail or the Web or somewhere else on the Internet, according to Javelin. Bank customers in the U.S. are not the most frequent targets of the most common form of online identity theft, phishing attacks. McAfee reports that more than half of all recent phishing attacks involved e-mails from a sender masquerading as VolksBank, a German bank, with another quarter targeting customers of U.K. bank Barclays PLC.

Category 1C2 Identity theft

2006-10-29 DHS Daily OSIR; Daily Mail (UK) http://www.thisismoney.co.uk/credit-and-loans/idfraud/article.html?in_article_id=414157&in_page_id=159

ID THIEVES INFILTRATE CALL CENTERS.

As more businesses move away from direct customer contact, call centers have become the latest front in the war on identity theft as criminals search for new ways of accessing secret customer information and stealing from accounts. Up to a tenth of call centers in one UK city alone have already been targeted. There are some 5,700 call centers in the UK, meaning nearly 600 could potentially have been infiltrated. Call centers are not used just by banks, but by other groups such as insurers, shops, and catalogue companies. Criminals have tapped into call centers after recognizing how easy it is to operate in such a large industry with a high staff turnover. The scammers recruit volunteers to work in the centers who supply them financial information in return for a fee. Employees leaving the call centers are also being approached and coerced into providing data. Disgruntled employees may also turn their hand to fraud. They target large accounts, with sums of money stolen ranging from a few thousand to hundreds of thousands.

Category 1C2 Identity theft

2006-11-07 DHS Daily OSIR; Guardian (UK)
http://money.guardian.co.uk/saving/banks/story/0,,1941239,00.html

ONLINE BANK FRAUD UP BY 55 PERCENT.

Losses from online banking fraud have risen sharply following a surge of nearly 1,500 percent in the number of bogus bank Websites used by criminals to plunder people's accounts, new figures show. Cash machine fraud has also risen by 37 percent, driven by criminals using miniature cameras to spy on people keying in pin numbers, says the Association for Payment Clearing Services (Apacs). But overall, credit and debit card fraud losses have fallen. For the six months to June 30, they were down five percent on the losses recorded during the same period last year. Online banking fraud losses were up 55 percent on losses racked up during the same period last year. These losses involved "phishing" scams. The chip and pin regime has made so-called card-not-present fraud more attractive for scammers. It accounts for almost half of all losses but, even though there has been an explosion in the numbers of people shopping online, this type of fraud grew by only five percent year-on-year, said Apacs. Despite all the headlines about identity theft, credit, and debit card ID fraud fell seven percent over the period.

Category 1C2 *Identity theft*

2006-12-08 EDUPAGE; ZDNet http://news.zdnet.com/2100-1009_22-6141989.html

STUDENTS RECRUITED FOR CYBERCRIME

According to a new report from computer security firm McAfee, gangs of criminals are recruiting college students to do the dirty work of cybercrimes. In an annual report, McAfee compared the gangs' tactics to those of agents working for the USSR during the Cold War, saying that recruiters scan computer clubs and other online venues looking for individuals with strong aptitude for technology. Those people, many of them undergraduates, are brought in to the criminal gang, where they write viruses, commit identity theft, and launder money. McAfee said the growing business of cybercrime is more lucrative than illegal drugs. "Although organized criminals may have less of the expertise and access needed to commit cybercrimes," said the report, "they have the funds to buy the necessary people to do it for them." The report is based in part on information from the FBI and European intelligence agencies, according to McAfee.

Category 1C2 *Identity theft*

2007-02-01 DHS Daily OSIR; Reuters http://today.reuters.com/news/articlenews.aspx?type=domesticNews&storyID=2007-02-01T083003Z_01_N31383185_RTRUKOC_0_US-IDTHEFT.xml&WTmodLoc=Home-C5-domesticNews-2

STUDY: U.S. IDENTITY THEFT LOSSES FALL IN 2006.

Americans lost about $49.3 billion in 2006 to criminals who stole their identities, an 11.5 percent decline that may reflect increased vigilance among consumers and businesses, a study released on Thursday, February 1, shows. Losses declined from a revised $55.7 billion in 2005, according to the third annual study by Javelin Strategy & Research. They had increased in each of the prior two years. The average identity theft fraud fell 9 percent to $5,720 from $6,278, while the median -- where half were larger and half were smaller -- held steady at $750. "Businesses are doing a better job screening, and consumers are doing better at locking up information and monitoring their accounts," said James Van Dyke, founder and president of Javelin. Notwithstanding the apparent decline in fraud, security experts say identity theft remains a big problem, as scammers try to stay one step ahead of consumers and businesses. Some are fighting back. U.S. regulators, for example, ordered banks by the end of last year to require a second form of identification before letting many customers transact online.

Category 1C2 *Identity theft*

2007-03-05 DHS Daily OSIR; Patriot-News (PA) http://www.pennlive.com/news/patriotnews/index.ssf?/base/news/1173061508187020.xml&coll=1

YOUNG ADULTS ARE LIKELY IDENTITY THEFT VICTIMS.

Identity theft is a common problem, particularly for young adults and college students, authorities say. From 2003-2005, almost 30 percent of identity theft victims were ages 18 to 29, according to the Federal Trade Commission. Younger adults can be exposed to the dangers of identity theft since they are more comfortable in making purchases online, said Lauren Bozart, a spokesperson for the Pennsylvania state attorney general's office. Jason Kozoowski, a senior at Penn State York, makes sure his credit card number is not visible to others when he gets ready to swipe his card in the machine. "Cell phones now have cameras in them, and anyone can take a picture of my credit card number," said Kozoowski, 24. Many colleges strive to teach their students identity-theft prevention tips. With social networking Websites such as Facebook and MySpace, students are vulnerable to attackers. Rosemary Yuhas, interim vice president of student affairs at Lebanon Valley College, said the college offered a program on the pros and cons of social networking sites.

Category 1C2 *Identity theft*

2007-05-04 DHS Daily OSIR;
Webuser (UK) http://www.webuser.co.uk/news/news.php?id=118654

NEW METHODS ENRICH CYBER THIEVES.

VirusPC Computer hackers are making more money than drug dealers by engineering sophisticated new methods of attack, a report has revealed. According to anti-virus company PC Tools, new crime-based online threats have soared by 120 percent in the last few months. PC Tools claims that new methods, such as creating "stealth mode viruses" -- which run on a computer without being detected -- have increased dramatically. Also on the rise are metamorphoses of Trojans, where basic signatures of threats are constantly changed to confound anti-virus programs, and rootkits which remain hidden for weeks or even months before unleashing dangerous attacks. “Cyber thieves are making as much money as drug dealers, according to a recent global identity theft report," said Michael Greene, vice president of Product Strategy at PC Tools.

1C4 Anonymity

Category 1C4 Anonymity

2006-01-30 EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4663388.stm

ISPS IN BRITAIN ORDERED TO DISCLOSE IDENTITIES

In the United Kingdom, the High Court has ordered 10 ISPs to disclose the identities of 150 individuals suspected of trading copyrighted software. The Business Software Alliance estimates that one-quarter of all software used in the United Kingdom is illicit. The court ruling came after a group called the Federation Against Software Theft (FAST) petitioned the court to order the disclosures, noting that software pirates hide behind fake names and bogus e-mail addresses and are notoriously difficult to track down. FAST said that after it has obtained the identities of those suspected of illegally trading software, it will consult with law enforcement authorities. John Lovelock, an official at FAST, said the group intends to make an example of software pirates, and the group's legal counsel said the current court action is "only the first wave of an ongoing strategy."

Category 1C4 Anonymity

2006-03-06 RISKS; Slashdot http://yro.slashdot.org/article.pl?sid=06/03/06/1736234

NEW JERSEY BILL WOULD HAVE BANNED ANONYMOUS POSTINGS

A firestorm broke out on Slashdot and other Internet-centric discussion sites after someone posted the following announcement: "The New Jersey legislature is considering a bill that would require operators of public forums to collect users' legal names and addresses, and effectively disallow anonymous speech on online forums. This raises some serious issues, such as to what extent local and state governments can go in enacting and enforcing Internet legislation."

Vigorous discussion ensued, including this cogent posting by "orthogonal":

MR. JUSTICE Hugo Black, writing for the Supreme Court of the United States in Talley v. California, 362 U.S. 60 (1960), declaring unconstitutional a California ordinance requiring that handbills and pamphlets be signed:

>Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all. The obnoxious press licensing law of England, which was also enforced on the Colonies was due in part to the knowledge that exposure of the names of printers, writers and distributors would lessen the circulation of literature critical of the government. The old seditious libel cases in England show the lengths to which government had to go to find out who was responsible for books that were obnoxious [362 U.S. 60, 65] to the rulers. John Lilburne was whipped, pilloried and fined for refusing to answer questions designed to get evidence to convict him or someone else for the secret distribution of books in England. Two Puritan Ministers, John Penry and John Udal, were sentenced to death on charges that they were responsible for writing, printing or publishing books…. Before the Revolutionary War colonial patriots frequently had to conceal their authorship or distribution of literature that easily could have brought down on them prosecutions by English-controlled courts. Along about that time the Letters of Junius were written and the identity of their author is unknown to this day. Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names. It is plain that anonymity has sometimes been assumed for the most constructive purposes.

We have recently had occasion to hold in two cases that there are times and circumstances when States may not compel members of groups engaged in the dissemination of ideas to be publicly identified. Bates v. Little Rock, 361 U.S. 516 ; N. A. A. C. P. v. Alabama, 357 U.S. 449, 462 . The reason for those holdings was that identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance. This broad Los Angeles ordinance is subject to the same infirmity. We hold that it, like the Griffin, Georgia, ordinance, is void on its face. [362 U.S. 60, 66]<

[MK notes that by June 2006, the NJ legislature's Web site no longer had any reference to the proposed bill.]

Category 1C4 Anonymity

2006-03-10 Effector Online http://www.eff.org/Privacy/Anonymity/

CONSUMER ALERT: ADVICEBOX. COM ISN'T ANONYMOUS EMAIL.

EFF is warning the public about a so-called anonymous email service located at Advicebox.com. Advicebox.com's tagline is "Anonymous email made easy" but this service does not provide real anonymity -- it's a trap for the unwary and should not be used by battered spouses, whistleblowers and others who need real protection. We were alerted to the AdviceBox.com trap by someone who believed the tagline and paid to send an "anonymous," extremely critical email about a former employer. After the employer ran to court, AdviceBox.com handed the critic's name over and gave our critic less than a three days notice -- not nearly enough time to find an attorney and make a motion to protect his identity. He has lost his current job as a result. So has AdviceBox.com violated its promise? Certainly if you look at the way this service is marketed. The Website is filled with stuff like "Send your anonymous email here!" and "What is anonymous email? The ability to send email without revealing your identity to the recipient." But AdviceBox.com doesn't really provide anonymous email -- the small print in the terms of service make this clear. AdviceBox. com won't protect you if anyone "claims that any content violates the rights of third parties." And what critical speech isn't vulnerable to claims that it violates the rights of people being criticized? Advicebox.com will respond to "legal process" like subpoenas, but we've long seen that legal process is used to silence criticism. It's difficult to see how Advicebox.com's service is any more protective of your identity than simply choosing the name smoochy@myisp. com. Most ISPs don't go around handing out their customer's identities either. People who need real anonymity would be much better off setting up a free webmail account without giving identifying information and using Tor to hide their IP address. This will not only give them better protection, it will save them the $4.95 per month that AdviceBox.com charges.
For this post: http://www.eff.org/deeplinks/archives/004460.php#004460
To learn more about Tor: http://tor.eff.org/
To learn more about anonymity online: http://www.eff.org/Privacy/Anonymity/

Category 1C4 Anonymity

2007-01-23 Effector Online http://www.eff.org/deeplinks/archives/005079.php

NEWSPAPER PUBLISHER TRIES TO THWART FIRST AMENDMENT.

The Santa Barbara News-Press needs a lesson in the FirstAmendment. Insisting that an anonymous comment posted for a few hours on a news blog skewed a labor unionization vote, the publisher of the newspaper is demanding that Google disclose the blogger's account information. It all started last September, three months after several editors walked off the job amid allegations that News-Press owner and co-publisher Wendy McCaw had improperly interfered in editorial decisions. The remaining employees were struggling to form a union to negotiate with McCaw, and McCaw did not take kindly to the unionization effort or even commentary about it. In fact, she has sued two newspapers based on their coverage of the labor dispute and threatened defamation suits against individual citizens who posted pro-union signs in their windows. The legal campaign has made headlines around the country. Enter pseudonymous blogger Sara de la Guerra. Sara reports and comments on current events in Santa Barbara and has been critical of McCaw's anti-union tactics. In early September, a third party submitted a comment advocating various acts of cybersabotage against News-Press management. The comment was taken down within hours, but News-Press later issued a press release quoting and complaining about the comment. When the employees then voted to form a union, News-Press filed objections with the National Labor Relations Board, arguing that the comment had influenced the election. Three months later, just a few days before the hearing on the objections, News-Press issued a subpoena to Google seeking information relating to Sara's account. News-Press has apparently forgotten a basic principle of the journalistic profession--respect for the First Amendment, which protects the right to anonymous speech. Court after court has recognized that discovery requests that seek to pierce the anonymity of online speakers must be carefully scrutinized. Moreover, courts have recognized the need for a particularly high level of protection when the discovery request seeks information about a nonparty. Such protection is especially important here, given McCaw's proclivity for retaliating against critics. Sara's important but fragile anonymity interests must be shielded unless News-Press can show that its claims are viable and that the requested evidence is necessary to advance those claims. And therein lies the rub: The hearing to which the information would be relevant was held two weeks ago, with no reference to the subpoena. Thus, even assuming the information was relevant to some claim, the need for that information has passed. EFF has written a letter to the NLRB judge explaining the free speech interests at stake and asking him to confirm the subpoena is moot. Here's hoping that the judge will bring a quick end to this dangerous skirmish in the News- Press' anti-union campaign.
For this post and related links: http://www.eff.org/deeplinks/archives/005079.php

---

Category 1C4 Anonymity

2007-01-24 INNOVATION (NewScientist.com 12 Jan 2007) <http://www.newscientist.com/channel/tech/mg19325865.500-how-to-leak-a-secret-and-not-get-caught.html>

WIKILEAKS OFFERS HAVEN FOR WHISTLEBLOWERS

Whistleblowers can breath easier if a nascent project called WikiLeaks moves forward. The site is designed to allow anyone to post documents anonymously, ensuring that authorities cannot track them down for prosecution. According to the group's Web site, www.wikileaks.org, targeted populations include China and Russia, as well as oppressive regimes in Eurasia, the Middle East and sub-Saharan Africa. To hide an e-mail's origin, WikiLeaks uses an anonymizing protocol called The Onion Router (Tor), which routes data through a network of servers that use cryptography to scramble the path the packets took. Organizers recognize that the anonymity offered could be misused: "The initiative could drown in fabricated documents, pornographic records or become hijacked to serve vendettas," says Steven Aftergood of the Federation of American Scientists. But the WikiLeaks team says the antidote to abuse will be oversight by the community of users, which they count on to sniff out and flag false postings. "WikiLeaks will provide a forum for the entire global community to examine any document relentlessly for credibility," the site claims.

Category 1C4 Anonymity

2007-05-09 Effector Online http://www.eff.org/news/archives/2007_05.php#005232

CORPORATE CRITIC FIGHTS TO KEEP INTERNET ANONYMITY. CHEMICAL COMPANY ON QUEST TO IDENTIFY ONLINE SPEAKER.

San Francisco - The Electronic Frontier Foundation (EFF) and the California First Amendment Coalition (CFAC) have asked a California appeals court to scrutinize a chemical company's attempt to strip the anonymity from a participant in an online message board. The participant posted information that H.B. Fuller Co. claims could only have been obtained through a company "town hall meeting," in violation of an employee confidentiality agreement. However, the poster has submitted a declaration to the court swearing that he or she is not an employee and that the information posted on the message board could have been gleaned from any follower of Fuller's business practices. A lower court ruled the message board poster should be identified to Fuller. In an amicus brief filed last Wednesday, however, EFF and CFAC argue that the lower court undervalued the right to anonymity and set a dangerously low threshold for stripping Internet users of its protection. "Liberal protection for the right to engage in anonymous communication to speak, read, listen, and associate anonymously is fundamental to a free society," said EFF Staff Attorney Corynne McSherry. "That is why courts must strike the appropriate balance between the competing interests of subpoenaing parties and the anonymous speakers they seek to unmask, recognizing that once an online user's anonymity and privacy have been eviscerated, they cannot be repaired." EFF and CFAC urged the appeals court to adopt a test for this case and others that would protect the rights of Internet critics. That test should include notice to the anonymous speaker, an assessment of the merits of the legal claims and other alternatives for finding the source of harm, and careful consideration of the balance of harms.
For the full amicus brief in Fuller v. Doe: http://www.eff.org/legal/cases/fuller_v_doe/fuller_v_doe_amicus.pdf
For more on anonymity on the Internet: http://www.eff.org/Privacy/Anonymity
For this release: http://www.eff.org/news/archives/2007_05.php#005232

1C5 Phishing & pharming

Category 1C5 Phishing & pharming

2006-01-31 DHS Daily OSIR; Computing http://www.vnunet.com/computing/news/2173899/phishing-overtakes-spam

PHISHING OVERTAKES SPAM FOR THE FIRST TIME.

For the first time the proportion of phishing attacks has exceeded the number of threats from virus or Trojan attacks, according to MessageLabs. The increase in phishing attacks is due to several factors. Firstly, virus attacks have become more targeted and are no longer occurring as one large outbreak. Secondly, online merchants have recently shifted toward deploying two-factor authentication methods which have given rise to 'man-in-the-middle' phishing sites. An increasing number of phishing sites are now using Flash content rather than HTML in an attempt to evade anti-phishing technology deployed in Web browsers. Successive virus outbreaks, such as StormWorm appear to be moving toward the Warezov model. The large numbers of new variants combine a number of anti-countermeasure features, like the use of rootkit technology, which make the virus increasingly difficult to detect and remove using traditional anti-virus methods.

Category 1C5 Phishing & pharming

2006-05-25 DHS Daily OSIR; IDG News Service http://www.infoworld.com/article/06/05/25/78676_HNrootofecrime_1.html

PHISHING PUSHES E-CRIME FURTHER UPSTREAM.

"The Web is under attack," said Phillip Hallam-Baker of VeriSign Inc, who gave a session Thursday, May 25, 2006 on Internet crime at the W3C (World Wide Web) conference in Edinburgh, Scotland. The tools to commit e-crime are for sale on the Internet. Mounting an attack on millions of Internet users can be done for a little as U.S. $300, Hallam-Baker said. Networks of computers under the control of hackers, called botnets, can be rented to send spam. Also for sale are lists of up to 100 million e-mail addresses. Hallam-Baker said one Russian hacker will create a custom rootkit -- a method to hide a piece of malicious software deep in a computer's operating system -- for about $60. If users are tricked into clicking on an attachment with a piece of malware, it can mean all of their personal data, such as passwords and credit card numbers, can be recorded and sent back to the hacker, who may resell them to other criminals.

Category 1C5 Phishing & pharming

2006-07-11 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,1987544,00.asp

FBI REPORTS A SURGE IN ONLINE JOB SCAMS.

According to a report issued by the Federal Bureau of Investigation (FBI) on July 5, individuals in the market for a new job have more to fear than rejection—online job scams are becoming prevalent as more individuals hunt for new employment opportunities online. In a cautionary report, the FBI explains that identity thieves have been known to take advantage of the personal information that is disclosed when applying for a job: names, home addresses and phone numbers, work numbers, e-mail addresses, and sometimes even dates of birth and social security numbers. Report: http://www.fbi.gov/page2/july06/job_scams070506.htm

Category 1C5 Phishing & pharming

2006-07-27 DHS Daily OSIR; TechWeb http://www.techweb.com/wire/security/191501877

EBAY, PAYPAL USERS HIT HARDEST BY PHISHING

Three out of every four phishing attacks target users of online auctioneer eBay and its electronic payment system PayPal, Sophos said Thursday, July 27. Of the phishing e-mails captured so far in 2006 by Sophos' network of spam traps 54.3 percent took aim at PayPal users and 20.9 percent tried to dupe users of eBay. Graham Cluley of Sophos said, "Although bank customers do also suffer from phishing attacks, they tend to be less likely to have the global reach that these net giants have." Sophos' numbers differ from the Anti-Phishing Working Group, of which the security company is a member. According to the APWG's most recent data, 92 percent of phishing attacks in May were directed at brands and companies in the financial services sector. That number hasn't changed significantly since the start of 2006.

Category 1C5 Phishing & pharming

2006-08-25 DHS Daily OSIR; Security Focus http://www.securityfocus.com/brief/289

THE DANGER OF USING "FREE" IN SEARCH QUERIES.

Building on a Wall Street Journal analysis of the 20 million search queries leaked by America Online that found "free" to be the most popular search term, Web safety firm SiteAdvisor warned that the results produced by such searches frequently lead to malicious Websites. The top three search queries including the word "free" that led to malicious sites include "free screensavers," "free ringtones," and "free music," the company stated. More than half of all sites returned for a search of "free screensavers" were malicious, not legitimate, SiteAdvisor stated.

Category 1C5 Phishing & pharming

2006-08-31 DHS Daily OSIR; Carnegie Mellon University http://www.cmu.edu/PR/releases06/060831_phishing.html

CARNEGIE MELLON CYLAB RESEARCHERS CREATE NEW SYSTEM TO ADDRESS PHISHING FRAUD.

Carnegie Mellon University's CyLab researchers have developed a new anti-phishing tool to protect users from online transactions at fraudulent Websites. A research team led by Electrical and Computer Engineering Professor Adrian Perrig has created the Phoolproof Phishing Prevention system that protects users against all network-based attacks, even when they make mistakes. The innovative security system provides strong mutual authentication between the Web server and the user by leveraging a mobile device, such as the user's cell phone or PDA. The system is also designed to be easy for businesses to implement. "The mobile device acts like an electronic assistant, storing a secure bookmark and a cryptographic key for each of the user's online accounts," said Perrig. For further detail: http://sparrow.ece.cmu.edu/~parno/phishing/

Category 1C5 Phishing & pharming

2006-09-01 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2163387/phishing-sophisticated

EXPERTS WARN OF DEVIOUS PHISHING ATTACKS.

Phishing attacks will use more sophisticated social engineering, targeting consumers for financial and identity theft and businesses for intellectual property theft. This is the main conclusion of the August 2006 global malware report released Friday, September 1, by security firm MessageLabs. The days of crude phishing e-mails which consumers have learned to spot are coming to a close, warns the report. Cyber-criminals are now developing personalized approaches that ape legitimate businesses' customer relationship management techniques, or "victim relationship management." "The latest wave of phishing attacks uses social engineering techniques by harvesting personal data from social networking sites like MySpace," said Mark Sunner, chief technical officer at MessageLabs.

Category 1C5 Phishing & pharming

2006-09-06 DHS Daily OSIR; ElectricNews.net http://uk.news.yahoo.com/06092006/95/high-tech-crime-forum-fight-phishing.html

HIGH-TECH CRIME FORUM TO FIGHT PHISHING.

Irish banks have responded to internet scams such as phishing by setting up the High-Tech Crime Forum to share information. Last month it emerged that a number of Bank of Ireland customers had lost hundreds of thousands of dollars through a fraudulent e-mail scam. Eight banks will work with the Garda Bureau of Fraud Investigation, the Irish Payment Services Organization, the Internet Service Providers Association of Ireland, and the Department of Justice's Internet Advisory Bureau. This discussion forum replaces the previous system in which banks shared information on an informal basis. Educational campaigns will highlight the threat of online fraud to consumers, and the forum is pushing for clearer warnings about potential online crime on banking Websites as part of its aim to increase general public awareness. Police authorities involved in the forum will enable members to have access to the latest fraud and cyber crime developments worldwide from Europol and Interpol.

Category 1C5 Phishing & pharming

2006-09-12 DHS Daily OSIR; Agence France-Presse
http://news.yahoo.com/s/afp/20060912/tc_afp/afplifestyleusinternetcrimecompanyyahoo

YAHOO AIMS TO PROTECT WEBSITE USERS FROM SCAMS.

Yahoo launched a sign-in service that allowed users of the search engine to create custom seals to thwart scammers out to trick them by imitating the search engine's pages. The security feature was aimed at exposing "phishing" cons in which people are duped into entering log-in or other information on bogus Websites that resemble legitimate Web pages, according to Yahoo. Yahoo users were given the option of creating a "sign-in seal" consisting of a secret message or image to be remembered on their computer and then displayed when they go to Yahoo log-in pages for services such as e-mail.

Category 1C5 Phishing & pharming

2006-11-03 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/06/11/03/HNantiphishingmalware_1.html

TERMINATION SQUAD FORMED TO COMBAT MALWARE.

The volunteers behind the Phishing Incident Reporting and Termination Squad (PIRT) have started a new project to crack down on malware. Called the Malware Incident Reporting and Termination Squad (MIRT), the effort was launched earlier last week, according to Paul Laudanski, owner of Computer Cops LLC and the leader of the project. MIRT works in much the same way as PIRT, an antiphishing project launched in March of this year. It invites users to submit samples of potentially malicious code to a database of "unknown files," which are then analyzed and reverse-engineered by MIRT's team of volunteers. MIRT then will publish reports on the malicious software and make its findings known to authorities and security companies, Laudanski said.

Category 1C5 Phishing & pharming

2006-11-15 DHS Daily OSIR; PC World http://blogs.pcworld.com/staffblog/archives/003156.html

PHISHERS TAKE WEEKENDS OFF.

According to research by Symantec, there is over a 30 percent dip in the number of new phishing sites on weekends. "That indicates that phishers are working phishing as their regular job," according to Oliver Friedrichs, of Symantec's Security Response team. So now we're dealing with 9-to-5, punch-the-clock criminal enterprise. Prevention is challenging to say the least. These criminals know what they are doing, and they limit their exposure. "The average life cycle of a phishing site is four hours," says Friedrichs.

Category 1C5 Phishing & pharming

2007-04-26 DHS Daily OSIR; ComputerWorld
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9017862&intsrc=hm_list

ENTREPRENEURIAL HACKERS BUY SPONSORED LINKS ON GOOGLE.

A hacker scheme that involved buying search keywords on Google and then routing users to a malicious site when they clicked on sponsored links was revealed Wednesday, April 25, by a security company. According to Roger Thompson, chief technology officer at Exploit Prevention Labs, the ploy involved sponsored links (the text ads that appear alongside search results on Google), a malicious intermediary and malware that steals online banking usernames and passwords. Those keywords put the criminals' sponsored links at the top of the page when searches were run for brand name sites like the Better Business Bureau or Cars.com, using phrases such as "betterbusinessbureau" or "modern cars airbags required." But when users clicked on the ad link, they were momentarily diverted to smarttrack.org, a malicious site that used an exploit against the Microsoft Data Access Components (MDAC) function in Windows to plant a back door and a "post-logger" on the PC.

Category 1C5 Phishing & pharming

2007-04-27 DHS Daily OSIR; Associated Press http://www.mercurynews.com/business/ci_5762859

GOOGLE HALTS 'HIJACKED' ADS USED TO STEAL PERSONAL DATA.

Google yanked paid advertisements that online criminals were using to steal banking and other personal information from Web surfers looking for the Better Business Bureau and other sites.
The ads, linked to 20 popular search terms, directed those who clicked on them to a booby-trapped site where their information could be captured. It was unclear how many people were affected before the breach was discovered this week, but computer security experts said Thursday, April 26, the attack appears to be isolated and only targeting Windows XP users who had not properly updated their machines. Google said it dismantled the offending links and shut down the problem AdWords accounts Tuesday. The company is working with advertisers to identify any other malware-loaded sites that might be on the network, it said. The attack targeted the top sponsored links tied to Google search results, installing a program on victims' computers to capture private information used to access online accounts for 100 different banks.

Category 1C5 Phishing & pharming

2007-04-30 DHS Daily OSIR; Bank Net 360
http://www.banknet360.com/news/NewsAbstract.do?na_id=8689&service_id=1&bi_id=

PHISHING SCAMS BEING DEFEATED FASTER.

Security researchers are getting better at limiting the damage caused by phishing. An example is the work of the Phishing Incident Reporting and Termination Squad (PIRT). PIRT is dedicated to taking down phishing Websites. The 15 PIRT security research volunteers have honed the time it takes to dismantle a phishing site to as little as 11 minutes. The average time, however, is a couple of hours, because of the volume of received phishing notices, said Robin Laudanski, PIRT team leader. By developing working relationships with global Internet service providers, as well as law enforcement, PIRT team members can orchestrate take-downs of phishing Websites hosted by both U.S.-based and international ISPs. Laudanski says dealing with overseas ISPs is not any harder than dealing with domestic ones, because of the established relationships. PIRT also stores and distributes the information it collects to law enforcement, financial institutions, and other corporations that request it. Banks and credit unions are the No.1 target for phishers. Recently, MIRT -- Malware Incident Reporting and Termination, and SIRT -- Spam Incident Reporting and Termination were launched to combat malware and spam in the same fashion.

Category 1C5 Phishing & pharming

2007-05-02 DHS Daily OSIR; British Computer Society (UK)
http://www.bcs.org/server.php?show=conWebDoc.11398

PHISHING THREAT GROWING, SAYS REPORT.

Phishing tactics are being used more and more to the extent that they have been reclassified as malware rather than spam by many anti-virus firms, according to new research. SoftScan has found that an increase in the proportion of Web traffic identified as malware last month is primarily because more messages were classified as phishing instead of spam. Its scan for April found that 88.93 percent of all emails were spam, with 1.92 percent classified as viruses. Diego d'Ambra of noted that phishing messages were seen as a pest rather than a serious danger to Web users 18 months ago. "Since then phishing has become far more sophisticated and their success rate at finding victims has also increased, making the threat overall far more prevalent," he commented.

1D1 Organizations, cooperation, treaties for law enforcement

Category 1D1 Organizations, cooperation, treaties for law enforcement

2006-06-19 DHS Daily OSIR; Computer Crime Research Center http://www.crime-research.org/news/19.06.2006/2060/

FBI OPENS NEW CYBERCRIMES UNIT.

On Tuesday, June 13, the FBI announced the creation of the Metro East Cyber Crimes and Analysis Task Force (MCCA) to assist local police agencies in their investigations. Participating Illinois police departments include Glen Carbon, Southern Illinois University Edwardsville, and the Madison County Sheriff's Department. Janice Fields of the FBI said the FBI and local police are "going to be working as a cohesive group to identify and neutralize one of the most significant threats we have -- cybercrime." She added: "This is a huge agenda for the FBI. Without the assistance from our local law enforcement, we could not do it." In the Metro East, 15 local, state, and federal agencies will share information and resources. The MCCA will be the FBI's 94th cybercrimes task force nationwide.

Category 1D1 Organizations, cooperation, treaties for law enforcement

2006-08-02 DHS Daily OSIR; IDG News Service http://www.pcworld.com/article/id,126632;c,cybercrime/article.htmlIDG News Service http://www.pcworld.com/article/id,126632;c,cybercrime/article.html

FBI JOINS WITH INDUSTRY TO TACKLE ID THEFT.

The U.S. Federal Bureau of Investigation (FBI) is stepping up its fight against online fraud with a new initiative called OperationIdentity Shield, according to a senior FBI official. The project, which is already in operation, is one of a growing number of collaborations between the FBI and the technology industry. "It's sort of an evolution of what we've seen in the phishing area," said Daniel Larkin, chief of the FBI's Internet Complaint Center, speaking at the Black Hat USA conference in Las Vegas on Wednesday, August 2. The FBI's antiphishing effort, called Digital PhishNet, was launched in late 2004 with backing from companies like Microsoft, America Online, and VeriSign, as well as the U.S. Secret Service and the U.S. Postal Inspection Service. The FBI plans to publicize OperationIdentity Shield in the coming months, but already Larkin credits the effort as contributing to a number of arrests.

Category 1D1 Organizations, cooperation, treaties for law enforcement

2006-08-08 Effector Online http://www.eff.org/deeplinks/archives/004864.php

SENATE SNEAKS THROUGH CYBERCRIME TREATY

After substantial pressure from the White House, the Senate ratified the sweeping Convention on Cybercrime treaty. Ratifying the Cybercrime treaty introduces not just one bad Internet law into this country, but also invites the enforcement of all the world's worst Internet laws. The treaty requires that the U.S. government help enforce other countries' "cybercrime" laws -- even if the act being prosecuted is not illegal in the United States. Countries that have laws limiting free speech on the Net could oblige the FBI to uncover the identities of anonymous U.S. critics or monitor their communications on behalf of foreign governments. American ISPs would be obliged to obey other jurisdictions' requests to log their users' behavior without due process or compensation. Instead of this one-way enforcement ratchet, Congress should be focusing on strengthening protections for your rights. ZDNet's Declan McCullagh on the treaty: http://news.zdnet.com/2100-1009_22-5973735.html
For the original version of this post: http://www.eff.org/deeplinks/archives/004864.php

Category 1D1 Organizations, cooperation, treaties for law enforcement

2006-09-17 DHS Daily OSIR; BBC http://news.bbc.co.uk/2/hi/business/5353568.stm

NEW CRIME BODY BLOCKS BANK SCAM.

A major scam aimed at hundreds of Internet banking customers has been averted, the UK's new Serious Organized Crime Agency (Soca) has said. The unit, launched in April, prevented the fraud -- targeting account passwords and names -- by issuing a new style of alert to financial institutions. It led to an arrest in a foreign country, said Soca director-general Bill Hughes. Soca, which has been dubbed the UK's FBI, brings together 4,000 police, customs, and immigration experts. One of Soca's predecessors, the National Criminal Intelligence Service, issued similar alerts but Hughes said his organization had a closer relationships with business and had developed the system of alerts. Warnings can be made in writing or on CD, and in urgent cases Soca -- which is not revealing details of the current case -- would telephone banks to issue an alert.

Category 1D1 Organizations, cooperation, treaties for law enforcement

2006-09-28 DHS Daily OSIR; U.S. House of Representatives Committee on Homeland Security http://hsc-democrats.house.gov/press/index.asp?ID=141

LEAP: CONGRESSMAN PROPOSES SEVEN CRITICAL STEPS TO ENABLE LAW ENFORCEMENT INFORMATION SHARING.

Thursday, September 28, Congressman Bennie G. Thompson (D-MS), Ranking Member of the Committee on Homeland Security, issued a report that analyzes institutional failures and a lack of initiative to enable law enforcement officers as first preventers in the War on Terror. The report, entitled “LEAP: A Law Enforcement Assistance and Partnership Strategy,” finds that a lack of information sharing between Federal, state, local, and tribal law enforcement dangerously limits the capabilities of police officers. The report lays out seven necessary initiatives, including: 1) Plans to establish a National Center for Intelligence-Led Policing; 2) Help major city chiefs defray the costs of a foreign liaison detail program; 3) Develop a “border intelligence” resource at border state fusion centers; 4) Fund local and tribal participation at those centers; 5) Establish a program at the National Counterterrorism Center to incorporate law enforcement officers in the intelligence production process; 6) A system to get law enforcement executives who need them security clearances; 7) An initiative that can track the progress of these and other intelligence-led policing efforts. Full report: http://hsc-democrats.house.gov/SiteDocuments/20060927193035- 23713.pdf

Category 1D1 Organizations, cooperation, treaties for law enforcement

2006-10-24 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2036619,00.asp

FBI: COMPANIES NEED TO REPORT CYBER ATTACKS.

Companies should do more to report cyber-crimes such as hacking and phishing to help federal authorities investigate and ensure that additional data isn't compromised beyond initial attacks, a high-ranking FBI official said. "A huge issue for us is the underreporting of successful or almost successful hacking," Special Agent Mark Mershin, the assistant director-in-charge of the FBI's New York City Office, told a crowd gathered at the Infosecurity Conference and Exhibition on Tuesday, October 24. The agency is troubled by a pattern of behavior among corporations and businesses who are not consistently reporting when their infrastructure has been hacked, or even when their companies have become the unsuccessful target of hackers and other cyber-crooks. Most companies, Mershin said, worry about the bottom line and feel any publicity or investigation into a cyber-crime will hurt profits.

Category 1D1 Organizations, cooperation, treaties for law enforcement

2006-11-17 DHS Daily OSIR; Washington Post http://www.washingtonpost.com/wp-dyn/content/article/2006/11/16/AR2006111601424.html

GROUP WILL SORT TERRORISM ALERTS FOR LOCAL GOVERNMENTS.

A new plan to improve information sharing about terrorism, signed by President Bush and delivered to Congress on Thursday, November 16, establishes a Washington-based "threat assessment group" that includes federal, state and local officials. It also aims to reduce more than 100 restrictive and confusing categories of "sensitive" federal information to a half-dozen or fewer so local-level officials can better understand what they are told. State and local governments and law enforcement officials have long complained of a lack of coordination among the federal agencies that send terrorism-related alerts, analysis and instructions. The new plan allows state and local officials to participate in deciding what players outside the federal government need to know and designates an online channel to distribute the information. The 165-page plan complies with part of the intelligence reorganization mandated by Congress in 2004, which created the Office of the Director of National Intelligence and the National Counterterrorism Center to facilitate coordination within the federal intelligence community. The newly released plan "restructures the way we handle intelligence and other information so that state and local customers get products that they can use," said Thomas E. McNamara, whose office, under Director of National Intelligence John D. Negroponte, wrote it with input from across the government.

Category 1D1 Organizations, cooperation, treaties for law enforcement

2007-03-09 DHS Daily OSIR; Department of Homeland Security
http://www.dhs.gov/xnews/releases/pr_1173477460607.shtm

NATIONAL COMPUTER FORENSIC INSTITUTE UNVEILED.

The Department of Homeland Security and Alabama state officials unveiled, Friday, March 9, the National Computer Forensic Institute in Hoover, AL, that will assist in the field of computer forensics and digital evidence analysis. The institute will be developed by the U.S Secret Service and is partially funded by the department's National Cyber Security Division. It will serve as a national cyber crimes training facility where state and local police officers, as well as prosecutors and judges, will be offered training and equipment. Law enforcement agencies routinely encounter computer or digital evidence and the level of training for state and local police departments is diverse. The facility will include classrooms, a computer forensic lab with an advanced research and development area, an evidence vault, storage and server rooms, public education exhibit space, and a conference room. Training will be based on the current U.S. Secret Service curriculum and include: basic electronic crimes investigation, network intrusion investigation and computer forensics.

Category 1D1 Organizations, cooperation, treaties for law enforcement

2007-04-11 DHS Daily OSIR; Reuters
http://today.reuters.com/news/articlenews.aspx?type=politicsNews&storyid=2007-04-11T194336Z_01_N11235745_RTRUKOC_0_US-SECURITY-USA-MCCONNELL.xml&src=rss&rpc=22

DNI ROLLS OUT NEW INTEGRATION PLAN.

The new Director of National Intelligence (DNI), Mike McConnell, on Wednesday, April 11, unveiled a broad new program to enhance collaboration between agencies and expand the number of intelligence workers with Middle Eastern and Asian backgrounds. A 100-day plan seeks to further integrate the 16-agency intelligence community by establishing new performance and career incentives for officers to do joint duty at other agencies. The plan also formalizes new clarity standards for official intelligence reports, encourages greater communication between spies and agency analysts, and seeks to impose financial audits to better measure the way the community spends an annual budget said by independent experts to exceed $40 billion. McConnell, who became director of national intelligence in February, said his office is prepared to seek help from Congress if new legislation is needed to push through changes and alter the power and scope of his own office. The plan would set community wide standards for recruiting new intelligence officers from the American Arab and Muslim communities in the hope of acquiring language and cultural skills necessary to combat al Qaeda and other Islamist militant groups. Official DNI press release: http://www.dni.gov/press_releases/20070411_release.pdf

Category 1D1 Organizations, cooperation, treaties for law enforcement

2007-05-01 DHS Daily OSIR; Finextra (UK) http://finextra.com/fullstory.asp?id=16876

CHINESE BANKS GET TOGETHER TO TACKLE ONLINE BANKING FRAUD.

Sixteen banks and the China Financial Certification Association are working together on anti-fraud mechanisms to improve security for online banking customers. The banks involved are Industrial and Commercial Bank of China, Agricultural Bank of China, China Construction Bank, Bank of Communications, CITIC Bank, China Everbright Bank, Huaxia Bank, China Minsheng Bank, China Merchants Bank, Guangdong Development Bank, Shenzhen Development Bank, Shanghai Pudong Development Bank, Industrial Bank, Beijing City Commercial Bank, Nanjing Bank, and Tianjin Bank. They have agreed to create and share an online banking "blacklist", and to cooperate on any investigations of fraudulent activity. They also propose working together to monitor the latest security technology developments and will organize seminars and forums to share information.

1D2 Technology for law enforcement

Category 1D2 Technology for law enforcement

2006-01-11 INNOVATION (NewScientist.com 5 Jan 2006)
<http://www.newscientist.com/article.ns?id=mg18925335.800>

UNDERCOVER LIE DETECTOR

The U.S. Defense Dept. is working on a lie detector that can be used without the subject knowing it. The Remote Personnel Assessment (RPA) device could be used to pinpoint fighters hiding in a combat zone or to spot signs of stress that could signal suicide bomber intentions. The RPA will use microwave or laser beams reflected off the subject's skin to assess pulse, respiration rate and changes in electrical conductance, known as the "galvanic skin response." Because these parameters are the same as those used by a polygraph lie detector, DoD says it will also be able to assess the subject's psychological state. Whether it will actually work is questionable, says one electrical engineer at the University of Sussex, U.K., who specializes in non-invasive sensors: "They might capture a breathing rate with an infrared laser that senses chest vibration, but how they will measure a pulse through clothes, for instance is a very big question." And of course there are concerns about the accuracy of the methodology as well as privacy concerns, with one conflict analyst predicting the RPA could introduce a "chill factor" into everyday life.

Category 1D2 Technology for law enforcement

2006-05-10 INNOVATION (Government Technology 2 May 2006)
<http://www.govtech.net/magazine/story.print.php?id=99373>

ARTIFICIAL INTELLIGENCE TURNS CRIMEBUSTER

Since most crimes are committed by repeat offenders, a staple of police work is identifying patterns that link crimes together. A new neural network may soon help. Neural networks, which are considered artificial intelligence, attempt to create connections between processing elements -- the equivalent of neurons to the computer system. The Chicago PD's new Classification System for Serial Criminal Patterns (CSSCP) will comb through police IT systems, searching for patterns or clusters of data elements that might tie together a string of crimes and give police the data they need to find the perpetrators. The system assigns numerical values to different data elements in each crime, including type, suspect description, getaway vehicle, etc. The system uses pattern-recognition software that is "trained" to find those clusters of data. "We picked (top detective's) brains for the type of patterns they looked for. We looked at what they did, and found there was no one way they did their work," said Dr. Tom Muscarello, an assistant professor at DePaul University, who developed CSSCP. "Some concentrated on the victim, some on the time of day, but they all concentrated on something, and it helped them solve the crime. We picked out the best data features to look at," then programmed the system to look for patterns the same way. CSSCP should be ready for deployment later this year.

Category 1D2 Technology for law enforcement

2006-07-06 DHS Daily OSIR; Associated Press http://abcnews.go.com/US/wireStory?id=2161304

GANGS USE INTERNET TO SHOWCASE EXPLOITS.

Some of the country's most notorious street gangs have gotten Web-savvy, showcasing illegal exploits, making threats, and honoring killed and jailed members on digital turf. Crips, Bloods, MS-13, 18th Street and others have staked claims on various corners of cyberspace. George W. Knox, director of the National Gang Crime Research Center, said he has trained hundreds of police officials in how to cull intelligence on gang membership, rivalries, territory and lingo from these Webpages. "In order to understand any subculture, be it al Qaeda, witches, devil worshippers or gangs, you have to be able to know their own language," Knox said. Knox said it's important for police to learn how to read between the lines on gang Websites and blogs. Time on the Web may help them understand arcane Web clues. Knox and others fear gangs are using the Internet to recruit new members.

Category 1D2 Technology for law enforcement

2006-11-03 DHS Daily OSIR; KCAL-TV (CA) http://cbs2.com/topstories/local_story_307142326.html

WEB-BASED NETWORK IN TERRORISM TECHNOLOGY UNVEILED.

A secure Web-based network that will allow local law enforcement agencies to share information on improvised explosive devices (IEDs) was unveiled Friday, November 3, in Los Angeles, CA. The U.S. Department of Homeland Security will use the Technical Resource for Incident Prevention, or TRIPwire, to connect the Los Angeles Police Department and Los Angeles County Sheriff's Department to other agencies across the country to share information about bombs and terrorism threats. TRIPwire will focus on improvised explosive devices because they are commonly used by terrorists, as seen in bombings in London, Madrid, Israel and Iraq. Many inexpensive ingredients can be used to make an IED, homeland security officials said.

Category 1D2 *Technology for law enforcement*

2007-01-17 DHS Daily OSIR; Washington Post http://www.washingtonpost.com/wp-dyn/content/article/2007/01/16/AR2007011601506.html

MARYLAND OFFICIALS CREDIT COMPUTER DATA AND TRAFFIC STOPS FOR CRIME DROP.

Violent crime and property offenses in Prince George's County, MD, dropped nearly 21 percent last year because of a variety of police strategies that included computer analysis of crime trends and increased traffic stops, County Executive Jack B. Johnson and Police Chief Melvin C. High said Tuesday, January 16. Johnson and High attributed the drop to police strategies that they said prevented crime and led to the arrests of career criminals. They also credited the involvement of law-abiding community members who provided officers with information. High said police used computerized data of criminal activity to direct patrol officers and investigators to high-crime areas. Traffic stops have been a particularly effective tactic, said Assistant Chief Roberto Hylton, who heads the patrol bureau. In 2005, county police conducted 52,205 traffic stops; last year, officers made 94,674 traffic stops, an increase of more than 81 percent. Officers often find illegal firearms and drugs during such stops, Hylton said. Officers also sometimes find suspects who are named in arrest warrants, Hylton said.

Category 1D2 *Technology for law enforcement*

2007-02-28 DHS Daily OSIR; CNET News http://news.com.com/Cybercops+drowning+in+data/2100-7348_3-6162882.html

CYBER INVESTIGATORS OVERWHELMED WITH DATA.

Cyber investigators are nearly drowning in the massive amounts of digital data seized from criminal suspects, a government official said Wednesday, February 28. As digital evidence increases in importance, authorities seize anything that can hold data. This includes computers, CDs, USB keys, MP3 players, cell phones and game consoles, Jim Christy, a director of the U.S. Department of Defense Cyber Crime Center, said in a presentation at the Black Hat DC Briefings & Training event in Arlington, VA. Digital evidence can answer key questions in a legal case, but efficient tools to sift through massive amounts of data don't exist today, Christy said. Cybercrime investigators need more tools because they are stretched thin. There are only about a dozen accredited digital-forensics labs in the United States. Digital evidence is used in many more cases than DNA analysis, for example, which appears in only 1 percent of U.S. criminal cases, Christy said.
Black Hat DC Briefings & Training:
http://www.blackhat.com/html/bh-dc-07/bh-dc-07-speakers.html #Christy

Category 1D2 *Technology for law enforcement*

2007-04-05 DHS Daily OSIR; Associated Press http://www.nytimes.com/aponline/technology/AP-Retail-Crime-Data-Base.html

RETAIL TRADE, FBI FIGHT ORGANIZED THEFT.

Two leading retail industry associations have teamed up with the Federal Bureau of Investigation (FBI) to create a national online database that will allow merchants to share information to fight organized retail theft. The database, scheduled to debut Monday, April 9, with 40 retailers, consolidates efforts made by the National Retail Federation (NRF) and the Retail Industry Leaders Association. Both organizations had launched their own password-protected online national crime data bases last year. Previously, merchants had never shared information, so organized rings could hit various stores in one area without being detected. Joseph LaRocca, NRF's vice president of loss prevention, said that this database called Law Enforcement Retail Partnership Network will become the "national platform" for sharing retail crime information. In a statement, FBI Supervisory Special Agent Brian Nadeau, program manager for the FBI's Organized Retail Theft program, said that this tool "will create a stronger partnership between retailers and law enforcement to tackle a growing problem and disrupt criminal organizations." NRF, the industry's largest trade group, estimates that shoppers pay almost two cents on every dollar to cover the cost of retail theft.

1D3 Litigation, legal rulings, judgements (not search & seizure, warrants, wiretaps)

Category 1D3 Litigation, legal rulings, judgements (not search & seizure, warrants, wiretaps

2006-02-06 DHS Daily OSIR; http://www.securityfocus.com/brief/129

THREE CHARGED WITH WIRETAPPING, RACKETEERING.

A federal grand jury indicted private investigator Anthony Pellicano and two associates for the alleged illegal use of law enforcement data and wiretapping using a custom software program, prosecutors announced on Monday, February 6. The 110-count indictment charges Pellicano and his associates with creating a criminal enterprise in which the private detective allegedly paid tens of thousands of dollars to police officers to provide him with confidential law enforcement information on numerous individuals. In addition, the indictment charges Pellicano and the two associates -- a software developer and a telecommunications engineer -- with creating a program known as Telesleuth in 1995 and using it as early as 1997 to wiretap such people as Herbalife co-founder Mark Hughes, actor Sylvester Stallone and journalist Anita Busch. Monday's indictment was originally issued under seal on Wednesday, February 1. Among the other charges are 31 counts of wire fraud and five counts of identity theft. Four other defendants were charged wiretapping and wire fraud.

Category 1D3 Litigation, legal rulings, judgements (not search & seizure, warrants, wiretaps

2006-02-13 EDUPAGE; http://www.itworld.com/Man/2683/060213iipa/

INTELLECTUAL PROPERTY GROUP CALLS FOR FOCUS ON RUSSIA

In comments submitted to the U.S. Trade Representative (USTR), the International Intellectual Property Alliance (IIPA) urges the agency to identify Russia as a Priority Foreign Country, a designation for countries considered most threatening to intellectual property. The IIPA estimates that piracy rates in Russia are as high as 85 percent for business software, 67 percent for music, 81 percent for movies, and 82 percent for entertainment software. In addition, the Priority Foreign Country list indicates countries whose antipiracy efforts are minimal. The IIPA has previously requested that Russia be put on the list, but only Ukraine is on the highest-priority list. According to the IIPA, Ukraine should be moved down a step, to the Priority Watch List, with 15 other countries, including China, Egypt, Thailand, and Venezuela. The IIPA said countries including Pakistan, Brazil, and Taiwan had improved efforts during 2005 to address intellectual property concerns.

Category 1D3 Litigation, legal rulings, judgements (not search & seizure, warrants, wiretaps

2006-07-06 DHS Daily OSIR; Reuters
http://news.com.com/U.K.+agrees+to+extradite+alleged+hacker+to+U.S./2100-7348_3-6091493.html?tag=cd.top

UNITED KINGDOM AGREES TO EXTRADITE ALLEGED HACKER TO U.S.

Britain on Thursday, July 6, approved the extradition of a computer expert accused by the United States of perpetrating the world's "biggest military hack of all time." Gary McKinnon was arrested in June last year following charges by U.S. prosecutors that he illegally accessed 97 U.S. government computers, including the Pentagon, Army, Navy and NASA systems, and causing $700,000 worth of damage.

Category 1D3 Litigation, legal rulings, judgements (not search & seizure, warrants, wiretaps

2006-07-19 EDUPAGE; Federal Computer Week http://www.fcw.com/article95339-07-19-06-Web

BILL WOULD REQUIRE NOTICE OF SECURITY BREACHES

Rep. Tom Davis (R-Va.) has introduced a bill that would outline requirements for federal agencies to disclose computer security breaches that put individuals at risk of identity theft or fraud. The introduction of the bill follows several instances where government computers were compromised but the agency responsible for the system took a long time to notify those affected. In one case, the Energy Department did not make public a security breach until more than a year after it happened. "Sadly, this legislation is necessary to ensure that federal agencies are taking the proper steps to notify the public, the potential victims, and appropriate government officials," according to Davis. Under the legislation, the Office of Management and Budget would implement policies and procedures concerning notification when personal information is lost or stolen.

1D4 Government funding for law enforcement

Category 1D4 Government funding for law enforcement

2006-01-08 DHS Daily OSIR; http://www.nj.com/news/gloucester/local/index.ssf?/base/news-2/1136625344302990.xml&coll=8

NEW JERSEY LAW ENFORCEMENT UNITS COMBINE TO FIGHT COMPUTER CRIME

Three state law enforcement units in New Jersey will combine to fight computer crime. The new Computer Crime Task Force, formed by New Jersey state Attorney General Peter C. Harvey, will include personnel from the Division of Criminal Justice's (DCJ) Computer Analysis and Technology Unit (CATU), the New Jersey State Police Digital Technology Investigations Unit, and the state police Cyber Crimes Unit. The new task force will include three investigative units staffed with state troopers, DCJ investigators, and FBI special agents and will focus on computer hacking and viruses, Internet fraud, and the creation and distribution of child pornography. The Incident Response Unit investigations will focus on computers, computer networks, telecommunication devices, and other devices used in the commission of crimes. It will also provide cyber crime awareness outreach services to the public and train law enforcement regarding network intrusion crimes. The Cyber Crime Unit will investigate the use of computers in fraud and identity theft. A training committee will coordinate community outreach programs. The task force will aim to increase the reporting of cyber crime and computer intrusions. A Computer Crimes Task Force hotline is available at 1-888-648-6007, in addition to an online incident reporting form at http://www.cctf.nj.gov.

21.1 General QA failures

Category 21.1 General QA failures

2001-12-04 RISKS

DATA ENTRY ERROR & POOR USER INTERFACE DESIGN COSTS MILLIONS

According to the _Wall Street Journal_, "Dentsu Inc., one of the world's biggest advertising companies, was making its trading debut Friday on the Tokyo Stock Exchange after completing one of the year's biggest initial public offerings -- a deal arranged by UBS Warburg, a unit of Switzerland's UBS AG. . . . Before the Tokyo market opened Friday, a UBS Warburg trader entered what was intended to be an order to sell 16 Dentsu shares at 610,000 yen ($4,924.53) each or above. Instead, the trader keyed in an order to sell 610,000 Dentsu shares at 16 yen apiece. . . . The order was canceled by 9:02 AM, but not before 64,915 shares, almost half of the 135,000 shares in the IPO, had been sold. The price of Dentsu shares, which had been bid up to 600,00 yen before the market opened, fell to 405,000 yen. Now, UBS Warburg is obligated to deliver the shares it sold, and will have to buy them on the open market."

George C. Kaplan, who contributed this item to RISKS, cogently pointed out, "The article doesn't say anything about sanity checks in UBS's trading software. These have their own risks, of course, but you'd think that an error of 4 orders of magnitude in the selling price would at least merit an "Are you sure?" before the order went through. Once again, we see how computers let people make really big mistakes quickly."

Category 21.1 General QA failures

2006-01-25 DHS Daily OSIR; http://www.techweb.com/wire/security/177103864

GARTNER BASHES ORACLE OVER SECURITY.

Oracle security practices are raising red flags, a Gartner analyst recently warned, and administrators should hunker down in protecting their database systems. Just five days after Oracle released a critical security update that patched 82 vulnerabilities, a Gartner researcher said in an online advisory that "Oracle can no longer be considered a bastion of security." Rich Mogull wrote, "The range and seriousness of the vulnerabilities patched in this update cause us great concern.... The database products alone include 37 vulnerabilities, many rated as easily exploitable and some potentially allowing remote database access. Oracle has not yet experienced a mass security exploit, but this does not mean that one will never occur." Mogull noted that Oracle administrators had avoided patching by relying on the database's strong security and the fact that the software was deployed deep within an enterprise's defenses. That no-patching procedure won't cut it now. To keep databases secure, Mogull recommended that companies shield all Oracle systems, patch known bugs -- "because incomplete information from Oracle will make shielding incomplete," he said in an aside -- and pressure Oracle to get on the security stick.

Category 21.1 General QA failures

2006-02-11 RISKS; http://tinyurl.com/rq8p8

TRUSTING THE COMPUTER CAUSES TAX REVENUE SHORTFALL FOR TOWN

In Valparaiso, Indiana, someone pressed the wrong key in the municipal-tax program and accidentally altered the property value for a house originally evaluated at $121,900 so that it was appraised at $400M. No one noticed. The tax bill went from $1,500 to $8M, causing a significant increase in the anticipated municipal tax revenues. Although the faulty tax bill was corrected, the town planners had already lowered the property tax rate to take into account the imaginary $8M windfall and therefore faced a budget deficit for municipal services and schools.

Category 21.1 General QA failures

2006-03-09 Language Log http://itre.cis.upenn.edu/~myl/languagelog/archives/002911.html

THE CUPERTINO EFFECT

Benjamin Zimmer posted an amusing analysis of a peculiar automatic correction in some word processing software: the misspelling "cooperatino" (for "cooperation") is corrected to "Cupertino." Apparently some European translators have dubbed this problem "The Cupertino Effect." Zimmer writes,

>Here's a brief sampling of the hundreds of Cupertinos one can find on the ".int" domain used by international groups like the UN, the EU and NATO:

* Within the GEIT BG the Cupertino with our Italian comrades proved to be very fruitful. (NATO Stabilisation Force, "Atlas raises the world," 14 May 2003)

* The fact that Secretary General Robertson is going to join this session this afternoon in the European Union headquarters gives you already an idea of how close and co-ordinated this Cupertino is and this action will be. (NATO Press Point, 19 Mar. 2001)

* Safe blood transfusion services are being addressed in Freetown and Lungi, using WHO RB funds in Cupertino with the Red Cross Society of Sierra Leone and in Bo by MSF/Belgium. (WHO/EHA report on Sierra Leone, 1 May 2000)

* Could you tell us how far such policy can go under the euro zone, and specifically where the limits of this Cupertino would be? (European Central Bank press conference, 3 Nov. 1998)

* Co-ordination with the World Bank Transport and Trade Facilitation Programme for South East Europe will be particularly important in the area of trade facilitation and shall be conducted through regular review mechanisms and direct Cupertino. (European Agency for Reconstruction, "Focal area: Justice and home affairs") . . . .<

Apparently another automatic correction changes "coperation" to "copulation" as in the following examples:

* "Albania was very interested in concluding a customs copulation agreement."

* "The Heads of State and Government congratulated SATCC for the crucial role it plays in strengthening copulation and accelerating the implementation of regional programmes in this strategic sector. (Southern African Development Community, Communique from the 1982 SADC Summit)"

* "The Western Balkan countries confirmed their intention to further liberalise trade amongst each other. They requested that they be included in the pan-european system of diagonal copulation, which would benefit trade and economic development. (International Organization for Migration, Foreign Ministers Meeting, 22 Nov. 2004)"

Category 21.1 General QA failures

2006-03-10 RISKS

MS-EXCEL DAMAGES EXPERIMENTAL DATA

Biomedical researchers reported that MS-Excel converted some gene names into dates, damaging data sets and causing rejection of the damaged data. The authors listed 30 gene names such as DEC1 that got converted to dates (e.g., to 1-Dec). A worse problem occurred when data identifiers contained the letter E in a string of digits; these identifiers were irreversibly converted to floating point numbers in scientific notation. The authors wrote,

>There is another default conversion problem for RIKEN clone identifiers identifiers of the form nnnnnnnEnn, where n denotes a digit. These identifiers are comprised of the serial number of the plate that contains the library, information on plate status, and the address of the clone. A search … identified more than 2,000 such identifiers out of a total set of 60,770. For example, the RIKEN identifier "2310009E13" was converted irreversibly to the floating-point number "2.31E+13." A non-expert user might well fail to notice that approximately 3% of the identifiers on a microarray with tens of thousands of genes had been converted to an incorrect form, yet the potential for 2,000 identifiers to be transmogrified without notice is a considerable concern. Most important, these conversions to an internal date representation or floating-point number format are irreversible; the original gene name cannot be recovered.<

Peter G. Neumann commented, "If some computer virus or trojan did this sort of damage to the results of thousands of high-cost biomedical experiments, I imagine that we'd see a serious effort to put some people in jail. I'm not suggesting that any similar sort of retribution is appropriate here, but perhaps some rehabilitation would be in order. . . ."

Category *21.1* *General QA failures*

2006-03-28 RISKS; AP http://tinyurl.com/o45wj

DEBIT CARD TYPO RENDERS COUPLE PENNILESS

An AP item datelined Palmdale, California notes that George Beane was charged $4,334.33 for four burgers at Burger King. To make a long story short, the cashier entered $4.33 and then forgetfully reentered the same amount again, resulting in a debit-card charge that instantly was paid out of his Bank of America account, wiping out their balance. After this was discovered, the bank insisted the funds were on a three-day hold and the debit could not be be reversed. [The AP article said, "Burger King did not charge the Beanes for their meal, and the couple got their $4,334.33 back on Friday."] "For those three days, those were the most expensive value burgers in history," Pat Beane said.

[Abstract by Peter G. Neumann; additions by MK]

Mark Feit added in RISKS 24.23:

>[Debit-card] Transactions at countertop terminals do have a bounds check, but it happens at the wrong point in the transaction. The customer receipt and store copy are printed *after* the charge has been committed to the clearing house, leaving the cardholder with no way to approve the amount. (Even restaurants, which have an extra step where you add a gratuity, have this problem, because the final figure is still un-verified by the customer.) Even if the customer refuses to consummate the transaction by signing, it's still a done deal and the only recourse for correcting it is to take it up with the bank.

I suspect that's what happened in this case, and it's a very good reason to use a real credit card instead of a debit card.<

Category *21.1* *General QA failures*

2006-05-09 RISKS

RISKS OF INADEQUATE TESTING HIT BELL CANADA

In the 613 area code (Ottawa, Eastern Ontario) in Canada, BELL Canada prepared to switch to requiring the area code for all calls including local ones. Rod Davidson reported on a glitch that appeared because of poor testing and planning:

>There is a local 866 exchange so that the phone number 866-1234 (just made up) is a local call. As of this morning, when I tried to dial 1-866-123-4567 I received the message "This is not a long distance call." as soon as I pressed the "4" in the sequence. Dialing "866-1234" got me the message "The mailbox of 866-1234 is full." I'm not really surprised.<

The situation was made worse by BELL Canada operators, who either ignored his explanation of the problem or proposed a service call for a problem that resided at the central office. Davidson pointed out, "When someone reports unusual system behavior (and reports they observed it on several different phone lines) it should raise some sort of red flag."

Category *21.1* *General QA failures*

2006-05-23 RISKS

PARKING METER CHARGES $8M FOR 63-YEAR PARKING STAY

A humor column in today's _LA Times_ featured a photograph of a self-pay parking kiosk with a mis-set date of 16 May 1943, showing an amount due of $8,082,022.84.

Sanity checking, you ask? Not bloody likely. An auxiliary display shows the fee in larger characters; it reads 8.1E+6. When you have an programmer so clueless as to calculate money values in floating point, there is little hope for subtleties like sanity checking.

As a side point, I'm fascinated that things like parking kiosks now use chips powerful enough to have floating-point support, at least as a library. A 4-bitter would be adequate for the task, though it's not clear to me that this particular programmer could have written the code needed to compute the fee on a 4-bit machine.

[Abstract and commentary by Geoff Kuenning]

Category *21.1* *General QA failures*

2006-10-26 DHS Daily OSIR; Finextra http://finextra.com/fullstory.asp?id=16073

CUSTOMERS CLEAN OUT 'DOUBLE YOUR MONEY' RBS ATM.

Hundreds of customers waited for up to three hours in Bristol, UK, on Saturday, October 21, to use a faulty cash machine owned by Royal Bank of Scotland (RBS) that started dispensing twice the amount of money requested. According to UK press reports, customers flocked around the ATM as news of the fault spread for a chance to "double their money." Another RBS ATM at the same location, which was operating normally, remained unused. Many customers withdrew cash then waited in line again. The unit eventually ran out of cash Saturday evening. A RBS spokesperson told reporters that due to a "manual error," the machine began dispensing incorrect bills.

Category *21.1* *General QA failures*

2007-01-16 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2172616/databases-come-under-security

ORACLE FLAGS 52 SECURITY FLAWS.

Oracle has issued its first pre-release security patch announcement, flagging up no fewer than 52 critical updates, just as a security company has highlighted the vulnerability of many databases. However, security firm Secerno warned that weaknesses in the development process are often more serious than any vendor vulnerabilities. "This is another step in the right direction by Oracle. As ever, forewarned is forearmed and this move allows IT managers to get to grips earlier with essential patching," said Secerno chief executive Paul Davie. "But users need to beware that it is not the vendor vulnerabilities that they need to focus on, but the critical weaknesses in their development
processes." Vulnerabilities in vendor solutions can be mitigated to some extent by timely patching, but users cannot rely on patch management to solve database security problems, according to Davie. Secerno believes that the continuous pressure on developers to drag more and more functionality out of their database should be a much greater cause for concern. Deployment errors caused by poorly configured databases, inappropriate access permissions or badly engineered applications accessing the database are an increasingly worrying trend.

21.2 Security product QA failures

Category 21.2 Security product QA failures

2006-01-12 RISKS; http://tinyurl.com/atvlo

CISCO/CISCO = SILLY/SILLY

Gadi Evron analyzed a Cisco advisory entitled "Default Administrative Password in Cisco Security Monitoring, Analysis and Response System" which revealed a back door to root:

"The security issue is basically a user account on the system that will give you root when accessed.

The account is:
1. Hidden.
2. Default.
3. With a pre-set password."

Evron also noted that many Cisco routers still use a canonical "Joe" account (same string for account and password):

"On the other hand, the most common practice to hack routers today, is still to try and access the devices with the notoriously famous default login/password for Cisco devices: cisco/cisco.

Cisco/cisco is the single most used default password of our time. It got more routers pwned than any exploit in history, and it still does. One would think that a company such as Cisco, especially with this history, would stay away from such 'default' accounts? But the fact that this account is hidden makes it something different."

Category 21.2 Security product QA failures

2007-01-12 DHS Daily OSIR; CNET News
http://news.com.com/CA+addresses+backup+software+flaws/2110-73493-6149978.html

CA ADDRESSES BACKUP SOFTWARE FLAWS.

CA, formerly known as Computer Associates International, on Thursday, January 11, issued updates for its BrightStor ARCserve Backup software to address several security vulnerabilities. The most serious of the flaws could be exploited to compromise a vulnerable system. "CA BrightStor ARCserve Backup contains multiple overflow conditions that can allow a remote attacker to execute arbitrary code," CA said in an alert. The problems affect only Windows systems, the company said. The BrightStor ARCserve Backup Tape Engine service, Mediasvr service, and ASCORE.dll file are affected, it said. CA Alert: http://www3.ca.com/securityadvisor/newsinfo/collateral.aspx?cid=97428

Category 21.2 Security product QA failures

2007-02-08 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2092841,00.asp

HIGHLY-CRITICAL FLAW DISCOVERED IN TREND MICRO PRODUCTS.

A dangerous buffer-overflow flaw in Trend Micro anti-virus software products was reported by Trend Micro and confirmed by security researchers at iDefense Labs. Researchers at Secunia have also posted an advisory on this vulnerability and have deemed this to be highly critical. This flaw can be exploited in both Windows and Linux systems, and could be used to gain access to machines, cause denial-of-service activity and allow attackers total control of affected systems. Trend Micro responded to the vulnerability by pushing out a patch that a
company spokesperson says fixes the issue. The vulnerability targets all scan engine and pattern file technology in Trend Micro products due to an error within UPX compressed executables. Secunia Advisory: http://secunia.com/advisories/24087/

Category 21.2 Security product QA failures

2007-02-28 DHS Daily OSIR; CNET News http://news.com.com/Symantec+incorrectly+flags+Yahoo+Mail+as+a+virus/2100-1002_3-6163068.html

SYMANTEC INCORRECTLY FLAGS YAHOO MAIL AS A VIRUS.

Yahoo's e-mail service is not infected with a computer virus, despite a warning from Symantec that says it is. Starting sometime on Tuesday, February 27, accessing the beta version of Yahoo Mail on a PC with Symantec's updated antivirus software caused alarm bells to go off. The security software reported finding the "Feebs" worm on the Yahoo Webpages. That warning was in error, Symantec said Wednesday. "Symantec antivirus products...triggered a false-positive alert with Yahoo Mail beta," said Vincent Weafer, a senior director at Symantec Security Response.

Category 21.2 Security product QA failures

2007-03-12 DHS Daily OSIR; Security Focus http://www.securityfocus.com/brief/458

MICROSOFT ONECARE DELETED OUTLOOK E-MAILS.

Recent reports suggest Microsoft's OneCare anti-virus offering suffered a bug that could have caused it to delete or quarantine all e-mail in a user's Outlook inbox, in certain cases when it finds a virus. A short brief by Virus Bulletin suggests that the problem was confirmed and then fixed in version 1.0, but reappeared in version 1.5 of OneCare. There are workarounds for users, such as preventing OneCare from scanning Outlook's .PST file. A note by the Windows OneCare forum moderator on Microsoft's site confirmed the issue. Users have been pointed to Microsoft Support for technical assistance, and it is suggested that Windows users should also backup their Outlook .PST files regularly. Microsoft appears to have now fixed the issue, but it is not clear how many users were affected by the bug.
Microsoft forum: https://forums.microsoft.com/WindowsOneCare/ShowPost.aspx?PostID=1307595&SiteID=2&PageID=0
Virus Bulletin: http://www.virusbtn.com/news/virus_news/2007/03_12.xml

Category 21.2 Security product QA failures

2007-05-21 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2190301/millions-pcs-zapped-bad

BAD NORTON UPDATE ZAPS 'MILLIONS' OF PCS.

A faulty update to Symantec's Norton Antivirus package has disabled "millions" of PCs in China, according to local press reports. One report carried by China's official news agency put the number of affected PCs in the millions, although others said that the figure was more like thousands or tens of thousands. The affected PCs cannot be started up. PCs running Windows XP began to fail after they downloaded a virus definitions update file on Friday, May 18. The regular updates are automatically pushed out from Symantec's servers. Users explained that nothing went wrong immediately, but that the next restart showed the infamous Windows 'Blue Screen of Death' instead of the normal start-up sequence. The PCs could not be restored to operation by any normal means. Symantec's China office explained in a statement that the software had mistakenly detected a virus in some key Windows XP system files. These files were either deleted or quarantined.

Category 21.2 Security product QA failures

2007-05-24 DHS Daily OSIR; CNET News http://news.com.com/Flawed+Symantec+update+cripples+Chinese+PCs/2100-1002_3-6186271.html

FLAWED SYMANTEC UPDATE CRIPPLES CHINESE PCS.

A Symantec antivirus signature update mistakenly quarantined two critical system files in the Simplified Chinese version of Windows XP last week, crippling PCs throughout China. According to the Chinese Internet Security Response Team (CISRT), users of Norton Antivirus, Norton Internet Security 2007 and Norton 360 who installed an antivirus signature update released by Symantec on May 17 could not reboot their PCs. The update reportedly mistook two Windows system files--"netapi32.dll" and "lsasrv.dll"--as the Backdoor.Haxdoo Trojan horse. The two files were subsequently quarantined. CISRT said the flawed Symantec update only affects users of the Simplified Chinese version of Windows XP Service Pack 2 that have been patched with a particular Microsoft software fix available since November 2006. According to Symantec China's Website, affected customers can resolve the problem by initiating another LiveUpdate, if they have not restarted their PCs after installing the flawed update. Systems that have already been restarted can be returned to the previous state by recovering the two system files from the Windows XP disc.

21.3 Embedded processors

Category 21.3 Embedded processors

2006-04-07 DHS Daily OSIR; http://www.fcw.com/article94004-04-07-06-Web&RSS=yes

CYBER ATTACKERS CAN EXPLOIT PENTIUM SELF-DEFENSE.

Your computer could hand itself over to cyber attackers when it's trying to cool off. That warning was issued this week at the CanSecWest/Core06 Conference in Vancouver, British Columbia. Computers with Intel Pentium processors can be hijacked through a built-in mode designed to protect the processor's motherboard, said Loïc Duflot, a security engineer and researcher for the scientific division of France's Central Directorate for Information Systems Security. The vulnerability affects every computer that runs on x86 architecture, including the millions that the U.S. government and industry use, said Dragos Ruiu, the conference's organizer.

Category 21.3 Embedded processors

2006-06-14 DHS Daily OSIR; Los Angeles Times
http://www.mercurynews.com/mld/mercurynews/news/world/14814370.htm?source=rss

MEXICO CRACKS DOWN ON RIGGED GASOLINE PUMPS.

Nine in 10 gasoline stations in Mexico have rigged their pumps to dispense less than what their meters promise, according to federal authorities, who calculated that purloined petrol cost consumers at least $1 billion last year. Random checks have revealed that the average retailer skims a little more than a liter of gasoline for every 20 sold. Profeco, the nation's chief consumer watchdog, has mounted surprise inspections, gathering evidence with the help of undercover agents armed with video cameras and vehicles outfitted with gas tanks that can be removed for lab analysis. About 900 stations, more than 10 percent of the nation's total, have been caught in the dragnet this year. Profeco is closing outlets and fining owners. It plans to post inspection results on the Internet to expose swindlers. It has launched a public relations campaign to urge motorists to report gasoline cheats. Station owners have been known to dilute their fuel with additives to stretch their profits, causing engine damage to clients down the road.

Category 21.3 Embedded processors

2006-08-04 DHS Daily OSIR; IDG News Service
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9002199&source=rss_topic85

SERIOUS FLAW PUTS XEROX PRINTERS AT RISK.

Xerox Corp. is scrambling to update a security patch following the disclosure of a major security flaw in its WorkCenter multifunction printers. By taking advantage of a configuration error in the printers' Web interface, security researcher Brendan O'Connor was able to run unauthorized software on the printers, compromise network traffic and access sensitive information being printed on the machines. He shared details of how to compromise the printers during a presentation at the Black Hat USA conference in Las Vegas Thursday, August 3. O'Connor said he was not trying to "pick on Xerox," but rather using his hack as a case study to draw attention to the security threat posed by increasingly powerful embedded devices.

21.4 SCADA (supervisory control & data acquisition) systems, vehicle controls

Category 21.4 SCADA (supervisory control & data acquisition) systems, vehicle controls

2006-05-08 DHS Daily OSIR; http://fcw.com/article94273-05-08-06-Print

INDUSTRIAL CONTROL SYSTEMS POSE LITTLE-NOTICE SECURITY THREAT.

The electronic control systems that act as the nervous system for all critical infrastructures are insecure and pose disastrous risks to national security, cybersecurity experts warn. Supervisory control and data acquisition and process control systems are two common types of industrial control systems that oversee the operations of everything from nuclear power plants to traffic lights. Their need for a combination of physical security and cybersecurity has largely been ignored, said Scott Borg, director and chief economist at the U.S. Cyber Consequences Unit, an independent research group funded by the Department of Homeland Security. Control systems security is one of six areas of critical vulnerabilities Borg included in a new cybersecurity checklist released in April by the research group. The private-sector owners of critical infrastructure refuse to release data and deny that their aging, inherently insecure systems pose any security risk, said Dragos Ruiu, an information technology security consultant to the U.S. government who runs several hacker conferences. Average hackers can break into the systems, said Robert Graham, chief scientist at Internet Security Systems. He, Borg and other experts fear that major cyberattacks on control systems could have socio-economic effects as severe and far-reaching as Hurricane Katrina.

Category 21.4 SCADA (supervisory control & data acquisition) systems, vehicle controls

2007-03-25 DHS Daily OSIR; Physorg http://www.physorg.com/news94025004.html

VULNERABILITY FOUND IN PROTOCOL HANDLING VITAL NATIONAL INFRASTRUCTURE.

Researchers on March 21 announced that the systems which control dams, oil refineries, railroads and nuclear power plants have a vulnerability that could be used to cause a denial of service or a system takeover. The flaw, reported by Neutralbit, is the first remotely exploitable SCADA (supervisory control and data acquisition) security vulnerability, according to the security services provider. Neutralbit identified the vulnerability in NETxAutomation NETxEIB OPC (OLE for Process Control) Server. OPC is a Microsoft Windows standard for easily writing GUI applications for SCADA. It's used for interconnecting process control applications running on Microsoft platforms. OPC servers are often used in control systems to consolidate field and network device information. Neutralbit reports that the flaw is caused by improper validation of server handles, which could be exploited by an attacker with physical or remote access to the OPC interface to crash an affected application or potentially compromise a vulnerable server. Neutralbit has also recently published five vulnerabilities having to do with OPC.

21.5 Robots

Category 21.5 *Robots*

2006-04-19 INNOVATION (Knowledge@Wharton 5 Apr 2006)
<http://knowledge.wharton.upenn.edu/index.cfm?fa=viewArticle&id=1435>

ROBOTS: THE NEXT BIG THING

At home, they vacuum floors. In Iraq, they defuse bombs. That may not be surprising for a company whose mission statement is, "Build cool stuff, deliver great product, make money, have fun, and change the world." Consumer and military products company iRobot has not only sold more than 1.5 million Roomba vacuum- cleaning robots, they have also deployed more than 300 tactical military robots in Iraq. CEO Helen Greiner says her robots have been credited with saving the lives of dozens of U.S. soldiers. Elsewhere, iRobots helped National Geographic explore uncharted parts of the Great Pyramids in Giza. Robots were sent deep into shafts that people had never explored, shafts that hadn't been seen in the 5,000 years since they were built. Robots were the only way to move cameras and sensors into places where the archeologists wanted to get more information. In schools, kids are hacking robots to learn about technology by tinkering with the robots'
internal systems. "That's another reason we put an open interface on the Roomba," Greiner says. What's ahead? On the consumer front, they're working on a robot that mops floors. "People hate to vacuum, but they absolutely loathe mopping," Greiner says. One day, she predicts, robots will assist law enforcement, first responders, even the elderly who want to live independently in their own homes.

Category 21.5 *Robots*

2006-04-26 INNOVATION (USA Today 14 Apr 2006)<http://www.usatoday.com/tech/news/techinnovations/2006-04-13-robot-soldiers_x.htm>

ROBOTS ON THE FRONT LINES

The US military is countering the risks from roadside bombs and terrorist ambushes by replacing troops with battlefield robots, including new versions armed with machine guns. "Just a few years ago we almost had to beg people to try an unmanned ground vehicle," says Marine Col. Terry Griffin, manager of the Robotic Systems Joint Project Office in Huntsville, Ala. Not anymore. In Iraq, where improvised explosive devices (IEDs) are the largest killer of U.S. troops, hundreds of small robots are helping bomb squads examine or disarm explosives from a safe distance. Sophisticated new ground- and sea-based robots are being developed and tested, including an unmanned vehicle intended to patrol around domestic bases, self-driving convoy trucks, and driverless versions of the Army's Stryker armored personnel carrier. Robots that can enter a building, look for an enemy and send back a map of the interior are being tested for the Marine Corps. The military also is responding to some creative tinkering by the troops, who have modified their robots to carry grenades and other weapons into buildings or other potentially unsafe targets. "Soldiers and Marines are very innovative," says Griffin. Meanwhile, much larger and more ambitious robot weapons are in testing, including the tank-like, 1,600-pound Gladiator, which can fire a variety of guns or tear gas.

Category 21.5 *Robots*

2007-04-04 INNOVATION (Wired Mar 2007)
<http://www.wired.com/wired/archive/15.03/bemore.html>

BUILDING A BETTER SOLDIER

The Defense Advanced Research Projects Agency is funding dozens of so-called human augmentation projects around the globe, ultimately aimed at creating a strain of super soldiers. DARPA has pushed the development of some things that have already become part of the fabric of military and civilian life: wearable computers, long-range drone aircraft, night vision, even the M16 rifle and the computer mouse. Now the agency is tackling the life sciences in hopes of developing a more capable armed forces. One experimental contraption fits over your hands to create a vacuum that pulls blood to the surface of your hand. Then it chills your blood to rejuvenate a sweaty, exhausted soldier, or warms it to revive one who's freezing. In another experiment, psychologists are using transcranial magnetic stimulation to counter fatigue. Another DARPA contractor is working on a mechanical exoskeleton that could make a GI's 100-pound pack feel feather-light. Boeing is developing a controller that may someday allow a single pilot to fly entire squadrons of robotic planes. It uses functional near-infrared spectroscopy to monitor the pilot's brain, suggest targets and ultimately take over the flying. Finally, to boost a soldier's energy level, a cocktail of green tea, quercetin and B vitamins is being tested to boost the production of mitochondria. With the drink, world-class cyclists shaved 3% off their times in a 30-kilometer ride.

21.6 Zero-day exploits

Category 21.6 Zero-day exploits

2006-01-31 DHS Daily OSIR; Information Week http://www.informationweek.com/showArticle.jhtml

MICROSOFT CHALLENGES NEWEST WORD ZERO-DAY.

Microsoft on Wednesday, January 31, disputed a security company's claim that a fifth unpatched vulnerability in Microsoft Word was being actively exploited by criminals. On Tuesday, Symantec notified users it had multiple exploit samples that represented new targeted attacks using a zero-day bug in Word 2003. In a warning sent to customers of its DeepSight threat management service, Symantec said that the attacks were "exploiting a previously undocumented and currently unpatched vulnerability." Opening a malformed Word 2003 document triggers the vulnerability, which then allows the exploit -- a form of the Mdropper.x Trojan horse -- to inject several malicious files onto the PC. Microsoft said Wednesday afternoon, however, that its research came to a different conclusion. "Microsoft's initial investigation shows that this is not a new vulnerability but a duplicate of an already known issue" first reported in mid-December, a company spokesperson said in an e-mail.

Category 21.6 Zero-day exploits

2006-06-19 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,1978835,00.asp

MICROSOFT POSTS EXCEL ZERO-DAY FLAW WORKAROUNDS.

Microsoft's security response center is recommending that businesses consider blocking Excel spreadsheet attachments at the network perimeter to help thwart targeted attacks that exploit an unpatched software vulnerability. The software giant published a pre-patch advisory on Monday, June 19, with a list of workarounds that include blocking Excel file-types at the e-mail gateway. File extensions associated with the widely deployed Microsoft Excel program are: xls, xlt, xla, xlm, xlc, xlw, uxdc, csv, iqy, dqy, rqy, oqy, xll, xlb, slk, dif, xlk, xld, xlshtml, xlthtml and xlv. The company's guidance comes just a few days after public confirmation that a new, undocumented Excel flaw was being used in an attack against an unidentified business target. The attack resembles a similar exploit that targeted Microsoft Word users, prompting suspicion among security researchers that the attacks may be linked.

Microsoft pre-patch advisory: http://www.microsoft.com/technet/security/advisory/921365.mspx

Category 21.6 Zero-day exploits

2006-09-04 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2011765,00.asp

MICROSOFT "BROWSERSHIELD": POTENTIAL SOLUTION TO ZERO-DAY BROWSER EXPLOITS.

Microsoft researchers are experimenting with an automatic code zapper for the company's Internet Explorer (IE) Web browser. Researchers at the company have completed work on a prototype framework called BrowserShield that promises to allow IE to intercept and remove, on the fly, malicious code hidden on Web pages, instead showing users safe equivalents of those pages. The BrowserShield project -- the brainchild of Helen Wang, a project leader in Microsoft Research's Systems & Networking Research Group -- could one day even become Microsoft's answer to zero-day browser exploits such as the Windows Metafile attack that spread like wildfire in December 2005. "This can provide another layer of security, even on unpatched browsers," Wang said. "If a patch isn't available, a BrowserShield-enabled tool bar can be used to clean pages hosting malicious content."

Category 21.6 Zero-day exploits

2006-09-30 DHS Daily OSIR; CNET News http://news.com.com/Hackers+claim+zero-day+flaw+in+Firefox/2100-1002_3-6121608.html

HACKERS CLAIM ZERO-DAY FLAW IN FIREFOX.

The open-source Firefox Web browser is critically flawed in the way it handles JavaScript, two hackers said Saturday, September 30. An attacker could commandeer a computer running the browser simply by crafting a Webpage that contains some malicious JavaScript code, Mischa Spiegelmock and Andrew Wbeelsoi said in a presentation at the ToorCon hacker conference. The flaw affects Firefox on Windows, Apple Computer's Mac OS X and Linux, they said. The flaw is specific to Firefox's implementation of JavaScript, a 10-year-old scripting language widely used on the Web. In particular, various programming tricks can cause a stack overflow error, Spiegelmock said. The implementation is a "complete mess," he said. "It is impossible to patch."

Category 21.6 Zero-day exploits

2007-01-24 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2087034,00.asp

THE ZERO-DAY DILEMMA.

The recent surge in malware attacks against zero-day flaws in some of the most widely used software packages is confirmation of an IT administrator's worst nightmare: Stand-alone, signature-based anti-virus software offers no protection from sophisticated online criminals. During 2006, there was a wave of zero-day attacks against Microsoft Office applications that bypassed all anti-virus protection at the network and desktop level. Because traditional anti-virus technology depends on the ability to quickly capture malware samples, reverse the code for the specific characteristics, and then write and release detection signatures, the zero-day attack presents a major dilemma. "Signatures have been dead for a long time now," said Roger Thompson, an anti-virus pioneer who now runs the Atlanta-based Exploit Prevention Labs. "[Attackers] use new packers or tweak their code so that it's different enough to bypass signatures for a short while. By the time you get a signature out, it's too late. They've already hit enough targets." The death of stand-alone, signature-driven anti-virus software has forced incumbent security software vendors to reshape their product lineups.

Category 21.6 Zero-day exploits

2007-04-10 DHS Daily OSIR; CNET News http://news.com.com/Office+zero-day+bugs+spoil+Patch+Tuesday/2100-1002_3-6175011.html

OFFICE ZERO-DAY BUGS SPOIL PATCH TUESDAY.

A trio of what appear to be new, yet-to-be-patched flaws in Microsoft Office has surfaced, according to security researchers at McAfee. The vulnerabilities were reported in online security forums on Monday, April 9, according to a posting on the McAfee Avert Labs blog on Tuesday. All but one of the flaws results in denial-of-service, meaning the application would crash, according to the blog post. "There is one heap-overflow flaw that might be exploited for code execution," Karthik Raman, a McAfee researcher wrote on the blog on Tuesday. Typically such flaws are exploited by tricking a targeted victim into opening a rigged Office document. Microsoft is investigating the bug reports as well, a company representative said in an e-mailed statement. Microsoft is not aware of any attacks that exploit any of the issues at this time, the representative said. Word of the flaws comes on the day that Microsoft issued five security bulletins as part of its monthly patch cycle. McAfee blog: http://www.avertlabs.com/research/blog/?p=253

21.7 Proof-of-concept code

Category 21.7 Proof-of-concept code

2006-04-07 DHS Daily OSIR; http://www.computerworld.com/printthis/2006/0,4814,110330,00 .html

KASPERSKY WARNS OF CROSS-PLATFORM VIRUS PROOF-OF-CONCEPT.

Kaspersky Labs is reporting a new proof-of-concept virus capable of infecting both Windows and Linux systems. The cross-platform virus is relatively simple and appears to have a low impact, according to Kaspersky. Even so, it could be a sign that virus writers are beginning to research ways of writing new code capable of infecting multiple platforms, said Shane Coursen, senior technical consultant at Kaspersky. The new virus, which Kaspersky calls Virus.Linux.Bi.a/Virus.Win32.Bi.a, is written in assembler and infects only those files in the current directory. "However, it is interesting in that it is capable of infecting the different file formats used by Linux and Windows," Kaspersky said.

Category 21.7 Proof-of-concept code

2006-07-07 DHS Daily OSIR; Sophos http://www.sophos.com/pressoffice/news/articles/2006/07/gattman.html

GATTMAN COMPUTER VIRUS USES NEW METHOD OF INFECTION.

Sophos researchers have discovered a proof-of-concept virus, called W32/Gattman-A, which works in a novel way. Unlike the majority of malicious software, which are Windows programs targeting the Windows operating system, this virus deliberately targets an analysis tool which is widely used by security researchers. The Gattman virus spreads through the program Interactive Disassembler Pro (IDA), produced by DataRescue. The Gattman virus, which is believed to have been written by members of the "Ready Rangers Liberation Front" and "The Knight Templars" virus-writing gangs, works by infecting IDC files. IDC is a script programming language similar to ANSI C, which allows researchers to customize and enhance the behavior of the IDA tool. They are often useful in unscrambling esoteric or hidden parts of malicious code, and are often exchanged with other researchers as part of the effort of taking apart a new piece of malware.

Category 21.7 Proof-of-concept code

2007-04-06 DHS Daily OSIR; MacNewsWorld http://www.macnewsworld.com/story/E5SKyrF5GUatOL/iPod-Proof- of-Concept-Virus-No-Teeth-No-Legs.xhtml

SECURITY RESEARCHERS CREATE IPOD VIRUS.

It was only a matter of time before someone developed a proof-of-concept virus aimed at the iPod. Discovered by Kaspersky Lab, the virus is a file that can be launched and run on an iPod. The good news for the majority of iPod users is that Linux must be installed on the device for the virus to function; iPods running Linux are a decidedly smaller subset. If the virus, dubbed "Podloso," should manage to latch onto such an iPod, it would install itself in the folder that contains the program demo versions. Once launched, according to Kaspersky Lab, the virus scans the device's hard disk and infects all executable .elf format files. When the user tries to access these files, a message is displayed on the screen that says, "You are infected with Oslo the first iPodLinux Virus." Podloso is a typical proof-of-concept virus, according to Kaspersky, created in order to show that it is possible to infect a specific platform. Like most of the ballyhooed mobile phone viruses, Podloso is unable to spread.

Category 21.7 Proof-of-concept code

2007-04-12 DHS Daily OSIR; InformationWeek http://www.informationweek.com/windows/showArticle.jhtml

ANOTHER MS VULNERABILITY DISCLOSED WITH PROOF-OF-CONCEPT CODE.

The so-called heap-overflow vulnerability affects Windows help files in multiple versions of Windows XP, Windows Server 2003, Windows NT, and Windows 2000. Researchers at SecurityFocus reported that the Help File viewer is prone to a heap-overflow vulnerability because it fails to perform boundary checks before copying user-supplied data into insufficiently sized memory buffers. The problem arises when the application handles a malformed or malicious Windows Help File. Hon Lau, a member of the Security Response Team at Symantec, wrote in a blog entry on Thursday that researchers there have not seen the vulnerability being actively exploited. Lau said Symantec analyzed a sample of the proof-of-concept code and released the Bloodhound.Exploit.135 to detect threats that exploit the vulnerability. Symantec blog: http://www.symantec.com/enterprise/security_response/weblog/2007/04/new_vulnerability_in_windows_h.html

---

22.1 Denial-of-service (DoS) attacks

Category 22.1 Denial-of-service (DoS) attacks

2006-05-03 DHS Daily OSIR; http://www.techweb.com/wire/security/187200053

MASSIVE DOS ATTACK KNOCKS TYPEPAD, LIVEJOURNAL BLOGS OFFLINE.

Millions of blogs hosted by LiveJournal and TypePad were unavailable throughout Tuesday night, May 2, and into Wednesday morning, May 3, as a massive denial-of-service attack struck their servers. The attack that brought down the servers at Six Apart -- the San Francisco company behind the LiveJournal and TypePad services, and the Moveable Type blogging software -- began at 4 p.m. PDT Tuesday, according to an advisory posted to the firm's Website by Michael Sippey, the vice president of product. According to Sippey, service was interrupted for the following: TypePad, LiveJournal, TypeKey, sixapart.com, movabletype.org and movabletype.com.

Category 22.1 Denial-of-service (DoS) attacks

2007-05-06 DHS Daily OSIR; Associated Press
http://www.nhregister.com/site/news.cfm?newsid=18306355&BRD=1281&PAG=461&dept_id=31007&rfi=6

EXXON MOBIL CANCELS STATE GOVERNMENT'S GASOLINE CREDIT CARDS AMID TAX DISPUTE.

Exxon Mobil Corp. has canceled the Connecticut government's gasoline credit cards as part of a tax dispute with the state, the Republican-American of Waterbury reported Saturday, May 5. The state comptroller's office notified state agencies on Friday not to use state-issued Exxon Mobil cards because retailers won't accept them. The notice said card use had been suspended indefinitely because of a tax dispute with Exxon Mobil. It advised agencies to use alternative means for buying gas for the time being.

Category 22.1 Denial-of-service (DoS) attacks

2007-05-28 DHS Daily OSIR; SecurityFocus http://www.securityfocus.com/news/11466

PEER-TO-PEER NETWORKS CO-OPTED FOR DOS ATTACKS.

A flaw in the design of a popular peer-to-peer network software has given attackers the ability to create massive denial-of-service attacks that can easily overwhelm corporate Websites, a security firm warned last week. Over the past three months, more than 40 companies have endured attacks emanating from hundreds of thousands of Internet protocol addresses (IPs), with many of the attacks producing more than a gigabit of junk data every second, according to security solutions provider Prolexic Technologies. The latest attacks came from a collection of computers running peer-to-peer software known as DC++. The software is based on Direct Connect, a protocol which allows the exchange of files between instant messaging clients. The directories of where to find certain files resides in a few servers, known as hubs. Older versions of the hub server software have a flaw that allows an attacker to direct clients to get information from another server, said Fredrik Ullner, a developer for the DC++ project. Maliciously redirecting those client results in a large number of computers continuously demanding data from the victim's Web server, overwhelming it with requests.

22.2 Distributed DoS (DDos) attacks

Category 22.2 Distributed DoS (DDos) attacks

2006-03-20 DHS Daily OSIR; http://www.securiteam.com/securityreviews/5GP0L00I0W.html

PAPER ON DOMAIN NAME SYSTEM AMPLIFICATION ATTACKS RELEASED.

In recent months several attackers massively exploited recursive name servers to amplify distributed denial-of-service (DDoS) attacks against several networks utilizing IP spoofing. Analysis of three of these attacks makes up the bulk of a recent study released Friday, March 17. The paper outlines a DDoS attack which abuses open recursive Domain Name System name servers using spoofed UDP packets. To access the full report: http://www.isotf.org/news/DNS-Amplification-Attacks.pdf

22.4 Accidental availability disruptions (e.g., backhoe attacks)

Category 22.4 Accidental availability disruptions (e.g., backhoe attacks)

2006-03-29 RISKS

THE SPIDER OF DOOM

Alex Papadimoulis had a fascinating tale of a disappearing Web site. In brief, a government Web site was converted to a content-management system that would allow employees to manage their own Web pages without having to go through a Web designer. It worked fine for five days, but on the sixth day all the content was gone! The entire Website had been erased by an external user that turned out to be the GOOGLE web crawling spider.

>After quite a bit of research (and scrambling around to find a non-corrupt backup), Josh found the problem. A user copied and pasted some content from one page to another, including an "edit" hyperlink to edit the content on the page. Normally, this wouldn't be an issue, since an outside user would need to enter a name and password. But, the CMS authentication subsystem didn't take into account the sophisticated hacking techniques of Google's spider. Whoops.

As it turns out, Google's spider doesn't use cookies, which means that it can easily bypass a check for the "isLoggedOn" cookie to be "false". It also doesn't pay attention to Javascript, which would normally prompt and redirect users who are not logged on. It does, however, follow every hyperlink on every page it finds, including those with "Delete Page" in the title. Whoops.

After all was said and done, Josh was able to restore a fairly older version of the site from backups. He brought up the root cause -- that security could be beaten by disabling cookies and javascript -- but management didn't quite see what was wrong with that. Instead, they told the client to NEVER copy paste content from other pages.<

Steve Summit added in RISKS 24.23

>I can see Joe Loughry's tongue in his cheek pretty clearly from here, but it might not be obvious to a casual reader that this was manifestly *not* a "hacking" attempt by Google. That a simple and naïve traversal of some hyperlinks could cause content to be deleted makes it pretty obvious that something was badly wrong with the site's editing and access-control model.

Needless to say (or, it *ought* to be needless, but is actually pretty needful), security that assumes that visitors *will* have cookies and JavaScript enabled, that can be compromised if these features are disabled, is no security at all. That content could have been inadvertently deleted by any visitor to the vulnerable website; google's spider just happened to get to it all first.<

Category 22.4 Accidental availability disruptions (e.g., backhoe attacks)

2006-06-01 DHS Daily OSIR; Pueblo Chieftain (CO) http://www.chieftain.com/metro/1149176562/22

CONTRACTOR CUT QWEST CABLE IN COLORADO.

A construction worker in Huerfano County cut a Qwest fiber optic cable between Walsenburg and Pueblo, severing cable TV, Internet and phone service to thousands of Southern Colorado residents Tuesday, May 30. The outage affected the 8,000-square-mile San Luis Valley, as well as the Trinidad and Walsenburg areas, for five hours. The outage also affected 911 service. The patrol was able to bypass the problem by using microwave towers, but residents outside the Alamosa exchange could not contact the patrol.

Category 22.4 Accidental availability disruptions (e.g., backhoe attacks)

2006-07-05 DHS Daily OSIR; Palladium-Item (IN) http://www.pal-item.com/apps/pbcs.dll/article?AID=/20060705/NEWS01/60705004

VERIZON OUTAGE IMPACTS THOUSANDS.

About 22,000 Verizon customers in the Richmond, IN, area were without service Wednesday afternoon, July 5, when excavating crews working near the Interstate 70 and U.S. 27 interchange damaged one of Verizon's major fiber optic lines. The outage also knocked out Randolph County's 911 system.

Category 22.4 Accidental availability disruptions (e.g., backhoe attacks)

2006-08-31 DHS Daily OSIR; NUNet http://www.vnunet.com/vnunet/news/2163310/error-knocks-thousands-spanish

ERROR KNOCKS OUT THOUSANDS OF SPANISH SITES.

An error in Spain's central domain registry resulted in thousands of Websites being unavailable for two hours last week. A failed software update resulted in 400,000 sites being knocked offline on Tuesday, August 29. The error was due to a hardware fault and lasted just over an hour. The outage only affected Websites hosting their domains through Network Solutions. While Network Solutions had a backup system in place to ensure continued service in case of failures, it did not prevent the crash.

Category 22.4 Accidental availability disruptions (e.g., backhoe attacks)

2006-10-10 DHS Daily OSIR; Cibola County Beacon (NM) http://www.cibolabeacon.com/articles/2006/10/10/news/news2.txt

PARAGLIDER CAUSES MAJOR ELECTRIC OUTAGE.

About 7,000 residents in Grants, San Rafael, Laguna, Acoma, and communities in east Cibola County, NM, lost power for approximately four hours Saturday morning, September 30, after a paraglider flew into an electrical transmission line at I-40 and Rio Puerco. A paraglider came into contact with a 115,000-volt transmission line owned by the Public Service Company of New Mexico (PNM). Continental Divide Electric Co-op Supervisor Mark Bahl said if the outage lasted several hours, or the weather was bad and people needed to heat their homes, Continental Divide was prepared to "jump" power from operating wires out of Milan, Bluewater, and western service areas. Those areas still had power, because they receive electricity from the Tri-State Generation and Transmission Association Plains Esclante station. But that process would have taken time and "create hardship" for everyone who receives power from the Co-op, Bahl reported. The feed would have required shutting down power in Milan and Bluewater.

Category 22.4 Accidental availability disruptions (e.g., backhoe attacks)

2007-01-05 DHS Daily OSIR; Reuters http://news.yahoo.com/s/nm/20070105/wr_nm/china_earthquake_domain_dc

CHINESE WEB USERS LOSE 10,000 DOMAIN NAMES IN QUAKES.

Chinese Web users lost around 10,000 Internet domain names due to disruption caused by last month's earthquakes off Taiwan, state media said on Friday, January 5. The domain names -- or Website addresses -- vanished after Chinese users were unable to update them or failed to re-register them on their expiry, the official Xinhua news service said, citing China International Network Information Center.

Category 22.4 Accidental availability disruptions (e.g., backhoe attacks)

2007-03-05 DHS Daily OSIR; Reuters http://today.reuters.com/news/articleinvesting.aspx?type=companyNews&storyid=37366+06-Mar-2007+RTRS&WTmodLoc=InvArt-L2-CompanyNews-2

ANIMALS TRIP LOS ANGELES-AREA REFINERIES, BOOST GASOLINE PRICES.

A raccoon and an opossum separately set off electrical power disruptions at two Los Angeles-area refineries on Sunday night, March 4, and Monday morning, boosting gasoline prices on the U.S. West Coast. Wholesale gasoline prices jumped seven cents in the Los Angeles market at word of the upsets on Monday morning. An opossum in a Southern California Edison commercial customer substation and a raccoon in a Los Angeles Department of Water and Power substation upset power supplies to the refineries within an hour of each other late Sunday night. The Southern California Edison substation in Torrance, CA, tripped offline at about 9 p.m. PST on Sunday, spokesperson Tom Boyd said. Exxon Mobil Corp.'s 150,000-barrel-per-day (bpd) Torrance refinery lost power at about that time, setting off a two-hour disruption in operations, said spokesperson Carolin Keith. At about 10:20 p.m. PST Sunday, a Los Angeles Water and Power substation in Wilmington, CA, switched offline, cutting power to a Shell Oil Co. refinery for about 10 seconds, said the utility's spokesperson Kim Hughes. Animals crawling into electrical substations and transformers is not uncommon and disrupting power is not uncommon, Hughes said.

Category 22.4 Accidental availability disruptions (e.g., backhoe attacks)

2007-04-17 DHS Daily OSIR; Associated Press
http://www.azcentral.com/business/consumer/articles/0417biz-fcctv17-ON.html

DIGITAL TV WILL CAUSE ANALOG BLACKOUT.

Federal Communications Commission (FCC) Commissioner Michael Copps on Tuesday, April 17, called for greater efforts to educate the public about a government-mandated switch-over to digital television signals in two years. Copps, appearing alongside fellow Commissioner Deborah Taylor Tate, told the annual convention of the National Association of Broadcasters that there was a possibility of serious disruptions when analog TV signals go off the air on February 17, 2009. When the change to digital television or "DTV" occurs, viewers who don't have digital-compatible televisions and use traditional antennas won't be able to view broadcast TV signals unless they have a digital converter box. With the deadline less than two years away, concerns have been growing that not enough people are aware of the switch-over or what will need to be done to make sure their sets still work. Many are also concerned that not enough is being done to prepare for a smooth switch-over. Digital converter boxes aren't in stores yet and aren't likely to go on sale until next January, about a year before the change. Copps called for more efforts in both the private and public sector to educate the public about the issue.

Category 22.4 Accidental availability disruptions (e.g., backhoe attacks)

2007-04-20 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2119111,00.asp

RIM: SOFTWARE UPGRADE CAUSED BLACKBERRY FAILURE.

BlackBerry maker Research In Motion (RIM) announced late Thursday, April 19, that it has determined the apparent cause of the shutdown that stopped e-mail service to BlackBerry users throughout North America earlier in the week. According to a statement from the Waterloo, Ontario-based company, the shutdown on April 17 was related to a software upgrade that went awry, followed by a failover process that also didn't work properly. The BlackBerry blackout happened when the company introduced a new, noncritical system routine into its database, officials said. The routine, according to RIM, was designed to improve cache optimization but instead caused a series of interaction errors between the databases and the cache.

23.2 JavaScript

Category 23.2 JavaScript

2006-06-13 DHS Daily OSIR; Information Week http://www.informationweek.com/news/showArticle.jhtml?articleID=189400799&subSection=Breaking+News

YAHOO MAIL WORM MAY BE FIRST OF MANY AS AJAX PROLIFERATES.

The Yamanner worm that infested Yahoo Mail was quickly countered by making a change to the Internet servers that administer Yahoo's popular e-mail program. Nevertheless, over a 36-hour period, the world got a glimpse of what's in store for it unless stricter measures are followed in building Web applications. Yahoo Mail relied on a JavaScript function in connection with uploading images from a message to their mail server. JavaScript is a key component of Ajax, a set of technologies that is being used more and more frequently for Web applications. "This kind of worm shouldn't be a surprise to anyone. We can expect to continue to see viruses" as long as Websites and enterprises are implementing Ajax applications without understanding their vulnerabilities, said David Wagner, assistant professor of computer science at the University of California at Berkeley. Without careful, designed-in security, Web applications using Ajax will open many additional doors to malicious code writers. "The problem isn't that Yahoo is incompetent. The problem is that filtering JavaScript to make it safe is very, very hard," said Wagner. Not only is hard to defend against misuse of JavaScript, it's easy for skilled hackers to find the openings.

Category 23.2 JavaScript

2006-07-28 DHS Daily OSIR; CNET News http://news.com.com/JavaScript+opens+doors+to+browser-based+attacks/2100-7349_3-6099891.html?tag=cdlede

JAVASCRIPT OPENS DOORS TO BROWSER-BASED ATTACKS.

Security researchers have found a way to use JavaScript to map a home or corporate network and attack connected servers or devices, such as printers or routers. The malicious JavaScript can be embedded in a Webpage and will run without warning when the page is viewed in any ordinary browser, the researchers said. It will bypass security measures such as a firewall because it runs through the user's browser, they said. "We have discovered a technique to scan a network, fingerprint all the Web-enabled devices found and send attacks or commands to those devices," said Billy Hoffman, lead engineer at Web security specialist SPI Dynamics. "This technique can scan networks protected behind firewalls such as corporate networks." A successful attack could have significant impact.

Category 23.2 JavaScript

2006-09-18 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2017407,00.asp

ZERO-DAY IE ATTACKS SPOTTED IN WILD.

Security researchers at Sunbelt Software have discovered an active malware attack against fully patched versions of Microsoft's Internet Explorer (IE) browser. There are at least three different sites hosting the malicious executables, which are being served up on a rotational basis. According to Eric Sites, vice president of research and development at Florida-based Sunbelt Software, the vulnerability is a buffer overflow in the way the world's most widely used browser handles Vector Markup Language code. The attack is linked to the WebAttacker, a do-it-yourself malware installation toolkit that is sold at multiple underground Websites. "Once you click on the site, the exploit opens an MS-DOS box and starts installing spyware," Sites said. He said the exploit can be mitigated by turning off JavaScript in the browser.

Category 23.2 JavaScript

2007-01-04 DHS Daily OSIR; CNET News
http://news.com.com/PDF+security+risk+greater+than+originall+thought/2100-1002_3-6147428.html

PDF SECURITY RISK GREATER THAN ORIGINALLY THOUGHT.

A recently discovered security weakness in the widely used Acrobat Reader software could put Internet users at more risk than previously thought, experts warned Thursday, January 4. Initially, security professionals thought that the problem was restricted and exposed only Web-related data or could support phishing scams. Now it has been discovered that miscreants could exploit the problem to access all information on a victim's hard disk drive, said Web security specialists at WhiteHat Security and SPI Dynamics. Key to increased access is where hostile links point. When the issue was first discovered, experts warned of links with malicious JavaScript to PDF files hosted on Websites. While risky, this actually limits the attacker's access to a PC. It has now been discovered that those limits can be removed by directing a malicious link to a PDF file on a victim's PC. "This means any JavaScript can access the user's local machine," said Billy Hoffman, lead engineer at SPI Dynamics. "Depending on the browser, this means the JavaScript can read the user's files, delete them, execute programs, send the contents to the attacker, et cetera. This is much worse than an attack in the remote zone."

Category 23.2 JavaScript

2007-02-15 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/07/02/15/HNdrivebywebattack_1.html

DRIVE-BY WEB ATTACK COULD HIT HOME ROUTERS.

If you haven't changed the default password on your home router, do so now. That's what researchers at Symantec and Indiana University are saying, after publishing the results of tests that show how attackers could take over your home router using malicious JavaScript code. For the attack to work, the attackers would need a couple of things to go their way. First, the victim would have to visit a malicious Website that served up the JavaScript. Second, the victim's router would have to still use the default password that it's pre-configured with it out of the box. In tests, the researchers were able to do things like change firmware and redirect a D-Link Systems DI-524 wireless router to look up Websites from a Domain Name System server of their choosing. They describe these attacks in a paper, authored by Sid Stamm and Markus Jakobsson of Indiana University, and Symantec's Zulfikar Ramzan. "By visiting a malicious Webpage, a person can inadvertently open up his router for attack," the researchers write. "A Website can attack home routers from the inside and mount sophisticated...attacks that may result in denial-of-service, malware infection, or identity theft."
Research: http://www.cs.indiana.edu/pub/techreports/TR641.pdf

23.3 ActiveX

Category 23.3 ActiveX

2007-01-10 DHS Daily OSIR; Security Focus http://www.securityfocus.com/brief/404

ACER SHIPS LAPTOPS WITH ACTIVEX SECURITY HOLE.

Computer maker Acer has shipped its notebook computers with an ActiveX control that lets any Website install software on the machine, security researchers warned this week. The ActiveX control -- named LunchApp.ocx -- appears to be a way for the company to easily update customer laptops, but also allows others to do the same thing, anti-virus firm F-Secure stated in a blog post on Tuesday, January 9. The security problem, first discovered in November by security researcher Tan Chew Keong, was confirmed by antivirus F-Secure. "The library, named LunchApp.ocx, is probably supposed to help with browsing the vendor's Website, enable easy updates and such," wrote F-Secure's research team. "It turns out it also makes all those machines vulnerable to a specially crafted HTML file that could instantly download malicious file(s) onto the user's machine and then execute them."

Category 23.3 ActiveX

2007-05-07 DHS Daily OSIR; InformationWeek http://www.informationweek.com/news/showArticle.jhtml?ArticleID=199300005

MONTH OF ACTIVEX BUGS REVEALS CRITICAL VULNERABILITIES.

Researchers posted details of a denial-of-service bug in Office OCX PowerPoint Viewer. It's an ActiveX control that enables software to communicate with Microsoft PowerPoint files. The French Security Incident Response Team (FrSIRT) called the bug critical. There are also several holes in the Excel Viewer OCX that Secunia rates as "highly critical." "The vulnerabilities are caused due to boundary errors within the Excel Viewer ActiveX control (ExcelViewer.ocx)," wrote Secunia analysts. "These can be exploited to cause stack-based buffer overflows via overly long arguments passed to certain methods (e.g. "HttpDownloadFile()" or "OpenWebFile()"). Successful exploitation may allow execution of arbitrary code when a user visits a malicious Website." The vulnerabilities, according to Secunia, are confirmed in version 3.2.0.5, but other versions also may be affected.
Secunia: http://secunia.com/
FrSIRT: http://www.frsirt.com/english/

Category 23.3 ActiveX

2007-05-10 DHS Daily OSIR; CRN http://www.crn.com/security/199500662

MCAFEE, SYMANTEC EXTERMINATE ACTIVEX BUGS.

Two ActiveX vulnerabilities were reported this week, one in McAfee Security Center, a management interface for its antivirus and antispam software, and the other in Symantec's Norton Antivirus product. The "McSubMgr.DLL" ActiveX control in McAfee Security Center contains a flaw that could enable an attacker to corrupt memory by sending an excessive amount of data, opening the door to remote code execution, Symantec said Wednesday, May 9. McAfee said the flaw affects products that are managed through Security Center, including Total Protection 2007, VirusScan 8.x, 9.x, 10.x, and VirusScan Plus 2007. McAfee said it fixed the vulnerability in March with Security Center updates 7.2.147 and 6.0.25, which many of its customers received automatically. Symantec this week acknowledged a buffer overflow vulnerability in the ActiveX control that ships with its popular Norton Antivirus software. Symantec said it has released an update for Norton that fixes the flaw and has made it available to customers through its LiveUpdate service. McAfee Security Bulletin: McAfee SecurityCenter 7.2.147 or higher fixes vulnerability: http://ts.mcafeehelp.com/faq3.asp?docid=419189
Symantec COM object security bypass:
http://www.symantec.com/avcenter/security/Content/2007.05.09.html

23.4 HTML, XML, browsers

Category 23.4 HTML, XML, browsers

2006-01-26 DHS Daily OSIR; http://www.hackerscenter.com/archive/view.asp?id=22251

MICROSOFT INTERNET EXPLORER DOES NOT HONOR ACTIVEX.

Internet Explorer (IE) fails to properly check the kill bit for ActiveX controls, which may allow a remote attacker to execute arbitrary code on a vulnerable system. By convincing a user to view a specially crafted HTML document an attacker could execute arbitrary code with the privileges of the user. Depending on the ActiveX control being used, an attacker may be able to take other actions. There are a number of significant vulnerabilities in technologies involving the IE domain/zone security model, local file system (Local Machine Zone) trust, the Dynamic HTML (DHTML) document object model in particular, proprietary DHTML features; the HTML Help system, MIME type determination, the graphical user interface (GUI), and ActiveX. These technologies are implemented in operating system libraries that are used by IE and many other programs to provide Web browser functionality. IE is integrated into Windows to such an extent that vulnerabilities in IE frequently provide an attacker significant access to the operating system.

Category 23.4 HTML, XML, browsers

2006-01-30 DHS Daily OSIR; http://www.securityfocus.com/bid/16427/references

MOZILLA FIREFOX XBL -MOZ-BINDING PROPERTY CROSS DOMAIN SCRIPTING VULNERABILITY.

The Mozilla and Mozilla Firefox browsers are vulnerable to a cross domain scripting attack by which a malicious Webpage could access trusted sites' properties and execute arbitrary script code in the context of an arbitrary domain. The issue affects the "-moz-binding" property supported by the Mozilla Extensible Binding Language. XBL is a markup language for describing bindings that can be attached to elements in other documents. Bindings can be attached to elements using either cascading stylesheets [CSS] or the document object model [DOM]. A malicious site could access the properties of a trusted site and facilitate various attacks including disclosure of sensitive information.

Category 23.4 HTML, XML, browsers

2006-01-31 DHS Daily OSIR; http://www.techworld.com/security/news/index.cfm?NewsID=5276 &Page=1&pagePos=6&inkc=0

BROWSERS FACE TRIPLE THREAT.

Polish security researcher Michael Zalewski has highlighted three bugs in the handling of cookies that he says could be used to carry out attacks on commercial Websites. The bugs, for which Zalewski has coined the term "cross site cooking," are fundamental to the design and implementation of cookies. The first problem involves the way browsers handle the domain specified in a cookie. Browsers should theoretically reject cookies where the domain is specified too broadly, but the mechanism doesn't work in Mozilla-based browsers, though Internet Explorer doesn't seem to be affected, Zalewski said. A variant on this bug is that browsers don't check to see if anything is between the periods in a domain name specified by a cookie. The third problem Zalewski outlined is a trick that he said could be easily used to force random visitors to a site to accept and relay malicious cookies to third-party sites. "Using this trick, a brand new identity may be temporarily bestowed upon the user, and used to perform certain undesirable or malicious tasks on the target site," he said.

Category 23.4 HTML, XML, browsers

2006-02-07 DHS Daily OSIR; http://www.computerworld.com/securitytopics/security/holes/story/0,10801,108469,00.html ?SKC=security-108469

ATTACK CODE PUBLISHED FOR FIREFOX FLAW.

A hacker Tuesday, February 7, published code that exploits a vulnerability found in the latest version of Mozilla Corp.'s Firefox browser. The code, which targets the Firefox 1.5 browser, was posted Tuesday on The Metasploit Project site by a hacker known as H D Moore. Metasploit is a widely used hacking tool. Moore said that a hacker by the name of Georgi Guninski reported the flaw to the Mozilla Foundation on December 6, and that he had simply implemented and posted the technique described by Guninski. Mozilla published an advisory about the exploit last Wednesday as it released the Firefox 1.5.0.1 browser, which included a patch for the flaw. According to the advisory, the vulnerability, which had been rated as moderate, causes a corruption in the browser's memory that could be exploitable to run arbitrary code. Hacker Aviv Raff on Tuesday criticized Mozilla in his blog for under-rating the flaw. He has blasted the open-source group in the past for downplaying the seriousness of vulnerabilities that have been found in its software.

Category 23.4 HTML, XML, browsers

2006-03-23 DHS Daily OSIR; http://www.techweb.com/wire/security/183702421

MICROSOFT WARNS OF DANGEROUS INTERNET EXPLORER EXPLOIT.

An exploit for a new zero-day bug in Internet Explorer appeared Thursday, March 23, causing security companies to ring alarms and Microsoft to issue a security advisory that promised it would patch the problem. Just a day after anti-virus vendors warned of a new zero-day vulnerability in Internet Explorer -- the second such alert since Friday, March 17 -- companies including Symantec and Secunia boosted security levels as news of a public exploit spread. Although the publicly-posted exploit only launches a copy of the Windows calculator, "replacing the shellcode in this exploit would be trivial even for an unskilled attacker," Symantec continued. Microsoft confirmed the severity of the bug and the success of the exploit in its own advisory, issued late Thursday. Microsoft advisory: http://www.microsoft.com/technet/security/advisory/917077.mspx

Category 23.4 HTML, XML, browsers

2006-04-12 DHS Daily OSIR; http://www.securityfocus.com/news/11387

BROWSER CRASHERS WARM TO DATA FUZZING.

Last month, security researcher HD Moore decided to write a simple program that would mangle the code found in Webpages and gauge the effect such data would have on the major browsers. The result: hundreds of crashes and the discovery of several dozen flaws. The technique -- called packet, or data, fuzzing -- is frequently used to find flaws in network applications. Moore and others are now turning the tool on browsers to startling results. In a few weeks, the researcher had found hundreds of ways to crash Internet Explorer and, to a lesser extent, other browsers. In another example, it took less than an hour at the CanSecWest Conference last week for Moore and information-systems student Matthew Murphy to hack together a simple program to test a browser's handling of cascading style sheets, finding another dozen or so ways to crash browsers. "Fuzzing is probably the easiest way to find flaws, because you don't have to figure out how the application is dealing with input," said Moore, a well-known hacker and the co-founder of the Metasploit Project.

Category 23.4 HTML, XML, browsers

2006-04-26 DHS Daily OSIR; http://www.washingtonpost.com/wp-dyn/content/article/2006/04/25/AR2006042501910.html

IE REVISED IN RESPONSE TO SECURITY CONCERNS, LOSS OF USERS.

Internet users were given a peek Tuesday, April 25, at a revamped version of Microsoft Corp.'s Internet Explorer (IE), a response to criticism that the most popular tool for Web surfing and hacking made users vulnerable to the Internet's dangers and caused them to defect to alternative browsers. A test version of IE 7 is available for download from Microsoft's Website, with tighter security protection and more advanced tools to give the user greater control in navigating the Web, said Dean Hachamovitch, general manager of IE. The company has improved its ability to write secure code, but it's unclear if the latest tools will address other dangers on the Internet, which require users to be more savvy, said Bruce Schneier, chief technical officer at Counterpane Internet Security Inc.

Category 23.4 HTML, XML, browsers

2006-06-06 DHS Daily OSIR; Tech Web http://www.techweb.com/wire/security/188702202

IE AND FIREFOX SPORT NEW ZERO-DAY FLAW.

Multiple security organizations warned Tuesday, June 6, that Internet Explorer, Firefox, Mozilla, and SeaMonkey -- on Windows, Linux, and the Mac -- are vulnerable to a JavaScript bug that could allow a determined attacker to dupe users into giving up sensitive personal information such as credit card or bank account numbers and passwords. According to Symantec, which issued an alert late afternoon Tuesday, all versions of the Microsoft and Mozilla browsers could be used to harvest data through a JavaScript key-filtering vulnerability. Symantec advised users to avoid unfamiliar Web neighborhoods and/or disable scripting or active content capabilities of the affected browsers. S
ecurity Focus Advisory: http://www.securityfocus.com/bid/18308/discuss

Category 23.4 HTML, XML, browsers

2006-09-25 DHS Daily OSIR; IDG News Service http://www.infoworld.com/article/06/09/25/HNbrowserbugssurge_1.html

SYMANTEC: 'THERE IS NO SAFE BROWSER'.

According to Symantec's twice-yearly Internet Security Threat Report, hackers found 47 bugs in Mozilla's open-source browsers and 38 bugs in Internet Explorer (IE) during the first six months of this year. That's up significantly from the 17 Mozilla and 25 IE bugs found in the previous six months. While Internet Explorer remained the most popular choice of attackers, no one is invulnerable. According to the report, 31 percent of attacks during the period targeted more than one browser, and 20 percent took aim at Mozilla's Firefox. "There is no safe browser," said Vincent Weafer, senior director with Symantec Security Response. "If you've got a browser, make sure you're configuring it correctly," he added. "That's a far better strategy than running some browser just because you haven't heard of it." Browser bugs are also relatively easy to find and exploit, said Marc Maiffret, chief technology officer with eEye Digital Security. "Everyone has realized that targeting the applications on the desktop is a better way to break into businesses and consumers and steal things than server flaws," he said. Symantec's report: http://eval.veritas.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_x_09_20 06.en-us.pdf

Category 23.4 HTML, XML, browsers

2007-01-04 DHS Daily OSIR; Security Focus http://www.securityfocus.com/brief/400

IE USERS AT RISK FOR 284 DAYS IN 2006.

Exploits and unpatched critical vulnerabilities put the users of Internet Explorer (IE) at risk 77 percent of the time last year, according to the latest number crunching by Brian Krebs of the Washington Post's Security Fix blog. Based on data published by Microsoft and interviews with researchers, Krebs found that critical security issues remained unpatched in IE for 284 days during 2006. The Mozilla Foundation's Firefox browser only suffered a single period of vulnerability lasting nine days, according to the analysis.

Category 23.4 HTML, XML, browsers

2007-04-23 DHS Daily OSIR; ComputerWorld http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9017598&intsrc=hm_list

SAFARI, FIREFOX, IE ALL VULNERABLE IF QUICKTIME IS INSTALLED, SAY RESEARCHERS.

The vulnerability that put $10,000 into the pocket of a New Yorker last Friday, April 20, during a Mac hacking contest is in Apple Inc.'s QuickTime media player, researchers said Monday, April 23. The contest, held at the CanSecWest security conference in Vancouver last week, pitted a pair of MacBook Pro notebooks, each with all currently-available security patches installed, against all comers. On Friday, Sean Comeau, one of the CanSecWest organizers, said the bug was in Safari, the Apple browser bundled with Mac OS X. But Monday, researchers at Matasano Security LLC, a New York-based consultancy, said the flaw is actually in QuickTime. "Dino's finding targets Java handling in QuickTime," said Matasano researcher Thomas Ptacek on the group's blog. "Any Java-enabled browser is a viable attack vector, if QuickTime is installed. Apple's vulnerable code ships by default on Mac OS X (obviously) and is extremely popular on Windows, where this code introduces a third-party vulnerability." Ptacek confirmed that both Safari and Mozilla Corp.'s Firefox can be exploited through the new QuickTime bug. Matasano also said it assumes that Firefox is vulnerable on Windows PCs if QuickTime's plug-in is installed.

23.5 E-mail, instant messaging, chat

Category 23.5 E-mail, instant messaging, chat

2006-03-22 DHS Daily OSIR; http://www.uscert.gov/cas/techalerts/TA06-081A.html

US-CERT TECHNICAL CYBER SECURITY ALERT TA06-081A: SENDMAIL RACE CONDITION VULNERABILITY.

A race condition in Sendmail may allow a remote attacker to execute arbitrary code. Sendmail contains a race condition caused by the improper handling of asynchronous signals. In particular, by forcing the SMTP server to have an I/O timeout at exactly the correct instant, an attacker may be able to execute arbitrary code with the privileges of the Sendmail process. Systems affected: Sendmail versions prior to 8.13.6. Solution: Upgrade Sendmail: Sendmail version 8.13.6 has been released to correct this issue: http://www.sendmail.org/8.13.6.html Patches to correct this issue in Sendmail versions 8.12.11 and 8.13.5 are also available. Version 8.12.11: ftp://ftp.sendmail.org/pub/sendmail/8.12.11.p0 Version 8.13.5: ftp://ftp.sendmail.org/pub/sendmail/8.13.5.p0

Category 23.5 E-mail, instant messaging, chat

2006-04-20 DHS Daily OSIR; http://www.informationweek.com/news/showArticle.jhtml?articleID=186500318

MICROSOFT PATCH 'ERASES' OUTLOOK EXPRESS ADDRESSES.

Another Microsoft patch from the batch released last week is apparently causing problems, at least according to numerous Windows users on the Redmond, WA, developer's official message boards. After applying the patch from security bulletin MS06-016, say dozens of users, their Outlook Express e-mail client's address book disappeared and form-style messages can't be sent. The problem said users, including several Microsoft MVPs, was the MS06-016 patch (also tagged as KB911567). Uninstalling the patch returned the address book to its prior state and allowed template-based messages to be e-mailed normally.

Category 23.5 E-mail, instant messaging, chat

2006-06-05 DHS Daily OSIR; Reuters http://today.reuters.com/news/newsArticle.aspx?type=internet News&storyID=2006-06-01T221008Z_01_N01382932_RTRUKOC_0_US-ME DIA-AOL-EMAIL.xml

AOL: E-MAIL SOFTWARE GLITCH FIXED.

Internet service AOL said on Thursday, June 1, it had resolved a software problem that delayed the transmission of millions of e-mails since the late morning. In the interim, AOL was sending e-mails that it had stored in its queue during the day at the rate of 500,000 messages per minute.

Category 23.5 E-mail, instant messaging, chat

2006-06-21 DHS Daily OSIR; CNET News http://news.com.com/Yahoo+outages+frustrate+some+users/2100-1032_3-6086485.html?tag=nefd.top

YAHOO OUTAGES FRUSTRATE SOME USERS.

Outages across the country left some registered Yahoo users without e-mail or instant-messaging capability on Tuesday, June 20, and Wednesday, June 21. While the company acknowledged an early morning outage Wednesday, some Yahoo user reports indicated that services were also out on Tuesday night in some areas. There were also complaints of Yahoo Sports Fantasy Baseball being unavailable. While Yahoo's e-mail and messenger services were inaccessible for some people, Yahoo Search, Yahoo News and the Yahoo home pages seem to have been unaffected. Yahoo did not release any details on the percentage of users affected, or what specifically caused the "software-related issues."

Category 23.5 E-mail, instant messaging, chat

2006-09-07 DHS Daily OSIR; IDG News Service
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9003091&taxonomyId=17&intsrc=kctop

BUG FOUND IN "CLASSIC" ICQ CLIENT.

AOL LLC is advising users of its ICQ instant message service to update to the latest version of the instant messaging software following the discovery of a bug in an older version of the product. Security researchers at Core Security Technologies Inc. reported Thursday, September 7, that they had discovered the flaw in ICQ Pro 2003b, a version of the ICQ client that AOL still offers for download, billing it as a "veteran version" of the product for users who prefer the earlier look-and-feel. Although the bug doesn't affect more recent ICQ software such as ICQ 5.1, it could mean serious problems for ICQ Pro 2003b users, according to Max Caceres, director of product management at Core, a vendor of penetration testing software. Core researchers have developed proof-of-concept code that causes ICQ Pro 2003b to crash and they believe that this vulnerability could eventually be exploited to run unauthorized software on a user's PC.

For further detail: http://www.coresecurity.com/index.php5?module=ContentMod&action=item&id=1509

23.6 Web-site infrastructure, general Web security issues

Category 23.6 Web-site infrastructure, general Web security issues

2007-03-26 DHS Daily OSIR; Associated Press
http://www.abcnews.go.com/Politics/wireStory?id=2983511

GIULIANI CAMPAIGN FIXES DANGEROUS FLAW ON NEW WEBSITE.

Republican presidential front-runner Rudy Giuliani's campaign hurriedly fixed its official Website late Monday, March 26, to remove a dangerous design flaw that could have allowed hackers to expose personal information submitted by volunteers. The vulnerability affecting Giuliani's site could have exposed confidential information stored in the campaign's databases. The Website failed to block commands that can instruct it to improperly display sensitive information, a popular hacking technique known as "structured query language injection." No personal information was compromised, spokesperson Maria Comella said.

23.7 VoIP

Category 23.7 VoIP

2006-01-23 DHS Daily OSIR; http://www.informationweek.com/security/showArticle.jhtml?articleID=177102457

CISCO SECURITY ALERTS SERVE AS VOIP WAKE-UP CALL.

Cisco Systems' revelation last week of two security alerts and fixes for CallManager, the processing component of its voice-over-IP (VoIP) technology, reminds us that while VoIP offers all sorts of benefits, there's no getting around its vulnerability as a software application. CallManager's vulnerability to denial of service attacks and attacks that would let users increase their access privileges seem mild compared with threats aimed at stealing customer data or blocking Website access. But as more voice communication travels over the Internet, reducing that threat becomes increasingly important. Cisco CallManager extends business telephony functions to IP phones, media-processing devices, VoIP network gateways, and multimedia applications. The denial of service and privilege-escalation vulnerabilities, for which patches are available, affect CallManager 3.2 and earlier, and some versions of CallManager 3.3, 4.0, and 4.1. Like Microsoft in the software market, Cisco is likely to be the main target of VoIP hackers because of its market-share leadership. Another danger lies in IT staff inexperience: VoIP hasn't been much of a target for hackers, and gaining the security know-how to protect those networks may not be top of mind during deployments, says Ofir Arkin, chief technology officer of network-management company Insightix Ltd.

Category 23.7 VoIP

2006-01-25 DHS Daily OSIR; http://news.com.com/Skype+could+provide+botnet+controls/2100 -7349_3-6031306.html?tag=cd.top

SKYPE COULD PROVIDE BOTNET CONTROLS.

Internet phone services such as Skype and Vonage could provide a means for cybercriminals to send spam and launch attacks that cripple Websites, experts have warned. Moreover, because many voice over Internet protocol (VoIP) applications use proprietary technology and encrypted data traffic that can't easily be monitored, the attackers will be able to go undetected. "VoIP applications could provide excellent cover for launching denial of service (DoS) attacks," the Communications Research Network said Wednesday, January 25. The Communications Research Network is a joint venture between Cambridge University and the Massachusetts Institute of Technology. The group urges VoIP providers to publish their routing specifications or switch to open standards. "These measures would…allow legitimate agencies to track criminal misuse of VoIP," Jon Crowcroft, a professor at Cambridge University in the UK, said in a statement. VoIP applications such as eBay's Skype and Vonage could give cybercriminals a better way of controlling their zombies and covering their tracks, the Communications Research Network said. "If the control traffic were to be obfuscated, then catching those responsible for DoS attacks would become much more difficult, perhaps even impossible," the group said in a statement.

Category 23.7 VoIP

2006-04-26 DHS Daily OSIR; http://www.cio-today.com/news/Is-VoIP-the-Next-Target-/story .xhtml?story_id=130004HC857W

VOIP MAY BE A FUTURE DENIAL OF SERVICE TARGET.

Although there has yet to be a recognized instance of a VoIP-coordinated Denial of Service (DoS) attack, the Communications Research Network (CRN) says it is only a matter of time before the technique becomes mainstream. The CRN working group on Internet security has discovered a security loophole in VoIP applications that could give criminals operating on the Internet a better way of covering their tracks. According to CRN, VoIP tools could offer good cover traffic for DoS attacks because VoIP runs continuous media over IP packets. The ability to dial in and out of VoIP overlays allows for control of an application via a voice network, making tracing the source of an attack almost impossible. In addition, proprietary protocols inhibit the ability of ISPs to track DoS activity. CRN's Jon Crowcroft suggests that the loophole could be resolved if VoIP providers were to publish their routing specifications or switch over to open standards.

Category 23.7 VoIP

2006-06-07 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/06/06/07/79053_HNvoiphack_1 .html

MAN CHARGED WITH SELLING HACKED VOIP SERVICES.

A Miami man was charged Wednesday, June 7 with stealing more than 10 million minutes of Voice over Internet Protocol (VoIP) telephone service and then selling them to unsuspecting customers for as little as US$0.004 per minute. Edwin Pena paid a Washington State computer hacker named Robert Moore about $20,000 to help him illegally route Internet telephone calls through the networks of more than 15 unnamed VOIP companies, according to a complaint filed with the U.S. Attorney's Office. Pena presented himself as a legitimate telecommunications wholesaler,while simultaneously using hacking techniques to steal networking services valued at as much as $300,000 from each of the carriers.

Category 23.7 VoIP

2006-06-09 DHS Daily OSIR; IDG News Service
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9001091

COURT UPHOLDS VOIP WIRETAPPING.

A U.S. Federal Communications Commission (FCC) ruling requiring voice over Internet Protocol (VoIP) providers to give law enforcement agencies wiretapping capabilities is legal, a court ruled today. The U.S. Court of Appeals for the District of Columbia upheld the FCC's August 2004 ruling saying interconnected VoIP providers must allow wiretapping by May 14, 2007. Several groups had appealed the ruling, saying it could introduce security vulnerabilities into VoIP services and drive up costs for customers. The FCC ruling requires VoIP providers that offer a substitute service for traditional telephone service to comply with a 1994 telephone wiretapping law called the Communications Assistance for Law Enforcement Act.

Category 23.7 VoIP

2006-06-21 DHS Daily OSIR; CNET News
http://news.com.com/FCC+approves+new+Internet+phone+taxes/21 00-7352_3-6086437.html

FCC APPROVES NEW INTERNET PHONE TAXES.

An estimated four million subscribers to Internet phone services like Vonage could see new fees on their bills under a plan approved Wednesday, June 21, by federal regulators. The Federal Communications Commission (FCC) voted unanimously at its monthly meeting to require all Voice over Internet Protocol (VoIP) services that connect to the public-switched telephone network -- as opposed to using peer-to-peer technology, like Skype -- to contribute to the Universal Service Fund. The $7.3 billion fund, which has been a feature of U.S. policy for more than 70 years, subsidizes telephone service in rural and low-income areas. It also runs a controversy-plagued program called E-Rate that provides discounted Internet and phone service to schools and libraries. Right now, only telecommunications services, including wireless, pay phone, traditional telephone and DSL providers, are required to contribute a fixed percentage of their long distance revenue to the multibillion-dollar fund. It had been unclear whether VoIP providers must also pay. The same FCC order would also raise the share that cell phone providers must contribute to the pool, though it was not immediately clear how many consumers would see hikes or how much they would be.

Category 23.7 VoIP

2006-07-14 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,1989301,00.asp

RESEARCHERS IN CHINA CLAIM TO HAVE CRACKED SKYPE PROTOCOL.

A claim that a group of researchers in China has successfully cracked the Skype Protocol has set the blogosphere alight, but the company says there is no evidence that the software has been reverse-engineered. "We have no evidence to suggest that this is true. Even if it was possible to do this, the software code would lack the feature set and reliability of Skype," said the company. According to Charlie Paglee, CEO of VoIP startup Vozin Communications, in Fremont, CA, engineers at a small research outfit in China have cracked Skype's proprietary protocol to create a third-party application capable of connecting to Skype's 100 million users. Paglee announced the news on his blog on Friday, July 14, and posted screenshots of Skype connecting directly to a rudimentary application. Paglee, who tested the connection during two voice calls with the Chinese group, noted that his IP address was "100 percent correct" on the third-party software. Paglee's blog: http://www.voipwiki.com/blog/

Category 23.7 VoIP

2006-08-03 DHS Daily OSIR; Register (UK)
http://www.channelregister.co.uk/2006/08/03/voip_hacking_exposed/

VOIP HACKING EXPOSED.

The latest VoIP security threats and countermeasures were outlined by security experts from SecureLogix and 3Com's Tipping Point at a presentation for the Black Hat security conference in Las Vegas on Wednesday, August 2. SecureLogix CTO Mark Collier and David Endler, director of security research at 3Com, explained how the scope and severity of attacks on Voice over Internet Protocol (VoIP) networks is likely to increase as adoption increases. Alongside the talk, the security researchers released 13 new tools designed to illustrate generic flaws on insecure VoIP systems. These tools, released to assist penetration testers and corporate sys admin, illustrated how it might be possible to overload phones with spurious traffic, flood IP telephony phones with calls, force hang-ups, reboot phones or reassign devices to other users.

Category 23.7 VoIP

2006-09-21 EDUPAGE; San Jose Mercury News
http://www.mercurynews.com/mld/mercurynews/business/15576648.htm

SAN JOSE STATE TRIES TO BAN SKYPE

Administrators at San Jose State University (SJSU) have temporarily suspended a ban on Internet phone service Skype but said they would reinstitute the prohibition if concerns over network usage are not adequately addressed. A number of universities have blocked use of Skype because of language in the user agreement that appears to allow individuals not associated with the university to use the campus network for phone calls. Skype works by routing calls through available networks, even for third parties, using computers of users who have accepted the company's terms of use. "It's a fairly subtle problem," said Kevin Schmidt, campus network programmer at the University of California, Santa Barbara, which has also banned Skype. He said the result could be "fair amount of traffic that has nothing to do with university business." Following the ban at SJSU, many students and faculty objected, saying the service has become vital to their efforts to keep in touch with families overseas and to promote educational programs around the globe. Campus officials acknowledged those concerns but said that if eBay, which owns Skype, cannot address the problem, the service will be shut off.

Category 23.7 VoIP

2006-09-28 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2165200/experts-launch-voip-security

U.S. EXPERTS LAUNCH VOIP SECURITY PARTNERSHIP.

A group of U.S. academics and industry experts has been created to explore security issues surrounding Voice over Internet Protocol (VoIP) technology, it was announced Thursday, September 28. The collaboration sees Georgia Tech Information Security Center partnering with BellSouth and Internet Security Systems. The researchers plan to conduct a security analysis of VoIP protocols and implementations, and explore issues such as VoIP authentication for dealing with voice spam, modeling of VoIP traffic and device behavior, mobile phone security, and security of VoIP applications running on user agents.

Category 23.7 VoIP

2006-11-29 EDUPAGE; The Register http://www.theregister.co.uk/2006/11/29/voip_hack_calls/

VOIP LEFT VULNERABLE TO HACKERS

Security company Scanit blames the vulnerability of sensitive data sent using voice over Internet Protocol (VoIP) on inadequate network security, leaving 7 of 10 calls open to wiretapping. Scanit's audit of data transfer at call centers and service providers pinpointed the main cause--assumptions that VoIP vendors on the network had already installed security measures. According to Scanit engineer Sheran Gunasekera, "Administrators at these places lacked adequate skills and understanding of the security aspects of setting a VoIP network up. They relied on the vendor or system integrator to secure it." He said that many networks were running VoIP without encryption.

Category 23.7 VoIP

2007-02-13 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/07/02/13/HNvoipnoimpact_1.html

T-MOBILE: VOIP WILL HAVE NO MAJOR IMPACT.

Don't expect new mobile phone services based on the Internet Protocol to become nearly as prevalent as those running over PCs. That's the view of Hamid Akhavan, CEO of T-Mobile International. Voice over Internet Protocol, or VoIP, services provided over mobile phone networks will have "far less impact" than those offered over fixed-line networks, Akhavan said Tuesday, February 13, on the sidelines of a news conference at the 3GSM conference in Barcelona. "There are all sorts of technical issues that make mobile VoIP services difficult to implement," he said. Technical issues related to how networks pass on IP addresses of mobile users have not been completely resolved, he noted. "Take reachability, for example: How can the call come to me?" Akhavan also said emergency phone service and "always on" connectivity are also big issues, since staying online takes up bandwidth on pricey mobile networks. And then there's price: "When people talk about VOIP, they think free," Akhavan said. "With any mobile service provided over the Internet, you're going to need to buy a data package."

Category 23.7 VoIP

2007-03-02 DHS Daily OSIR; CNET News
http://news.com.com/FCC+Local+phone+companies+must+connect+Net+calls/2100-7352_3-6163789.html

FCC: LOCAL PHONE COMPANIES MUST CONNECT NET CALLS.

In a boost to Internet phone providers, federal regulators have ruled that local telephone companies must connect Net-based calls shuttled over broadband lines owned by wholesalers like Sprint Nextel and Verizon Communications. In a 16-page order to local telephony providers issued Thursday, March 1, the Federal Communications Commission (FCC) effectively overturned decisions by state regulators in South Carolina and Nebraska that had prevented Time Warner Cable from deploying its voice-over Internet Protocol (VoIP) service there. FCC Chairman Kevin Martin said the states had misinterpreted federal telecommunications law. "Our decision will enhance consumers' choice for phone service by making clear that cable and other VoIP providers must be able to use local phone numbers and be allowed to put calls through to other phone networks," Martin said in a statement Thursday. Time Warner Cable, the nation's second-largest cable operator, had petitioned the FCC for relief about a year ago.
FCC's order: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-07-709A1.pdf

Category 23.7 VoIP

2007-03-22 DHS Daily OSIR; Websense
http://www.websense.com/securitylabs/alerts/alert.php?AlertID=757

NEW WAREZOV SPREADING VIA SKYPE.

Websense has discovered a new set of the Warezov/Stration malicious code. This new code is currently spreading through the Skype network. Although the code itself is not self-propagating, when it runs, a URL is sent to all users within the user's Contacts List. Skype users receive a message that says "Check up this," with a URL containing a hyperlink. When users click on the link, they are redirected to a site that is hosting a file named file_01.exe. Users are prompted to run the file (note: there is no vulnerability within Skype). If the user runs the file, several other files are downloaded and run. This attack appears to be the same as the version mentioned on the FSecure Blog on February 27, but with new URL information and a new version of the malicious code. FSecure Blog: http://www.f-secure.com/weblog/archives/archive-022007.html# 00001126,

23.9 Scripting languages (e.g., PERL, CGI scripts, Python, PHP)

Category 23.9 Scripting languages (e.g., PERL, CGI scripts, Python, PHP)

2006-09-28 DHS Daily OSIR; Register (UK)
http://www.channelregister.co.uk/2006/09/28/uk_banking_security_study/

UK BANKING WEBSITES' SECURITY RIFE WITH VULNERABILITIES.

Several major UK bank Websites are subject to security flaws that make it easier for phishing scammers to craft more convincing scams, according to a study by Heise Security. Friday, September 22, Heise published a number of demos to show how phishing scammers might be able to overlay the websites of NatWest, Cahoot, Bank of Scotland, Bank of Ireland, First Direct, and Link with rogue frames, potentially served from Websites controlled by scammers. Cross site scripting attacks against the Websites of USB and the Bank of England's site were also demonstrated. Frame spoofing attacks can be thwarted providing users are using up to date browser software, but the cross-site scripting attacks it demonstrated can't be addressed by client-side security updates, according to Heise. Both types of attacks require a modicum of skill to carry out, but are far from difficult. A number of banks -- including HSBC, Barclays and the Halifax -- were not vulnerable to Heise Security's tests. HSBC, for example, uses JavaScript code to check the integrity of the frameset, an approach that thwarts frame spoofing even if a surfer is using out-of-date browser software.

Category 23.9 Scripting languages (e.g., PERL, CGI scripts, Python, PHP)

2006-09-29 DHS Daily OSIR; Computerworld
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9003710

CROSS-SITE SCRIPTING COULD ENABLE PHISHING.

A recent research report stated that cross-site scripting (XSS) is now the top security risk. In a typical XSS scenario, a Web page might use JavaScript to dynamically generate some document content based on a field in a Uniform Resource Identifier (URI). The site itself would generate legitimate information for that field. If the script that generated the new content did not filter the URI, an attacker could feed the page a custom-designed URI that ran a script. The script could do almost anything, and the user would never know that he wasn't seeing legitimate content. This is one way to enable phishing. For example, a Web page with a cross-site scripting vulnerability that belonged to a bank could enable an attacker to could forge e-mails purporting to be from the bank, with URIs that led to the bank's site. Once a user clicked on the link in the e-mail and logged into the bank site, their login credentials (in the form of cookies) would be transmitted to the attacker, who would be able to take over the user's account as long as the session was active.

Category 23.9 Scripting languages (e.g., PERL, CGI scripts, Python, PHP)

2006-11-28 DHS Daily OSIR; CNET News
http://software.silicon.com/security/0,39024888,39164382,00.htm

GOOGLE SEARCH APPS PACKING 'PHISHING FLAW'.

A security flaw in Google's search appliances could expose Websites that use the products to info-stealing phishing attacks, experts have warned. The Google Search Appliance and Google Mini are used by organizations including banks and universities to add search features to Websites. A flaw in the way the systems handle certain characters makes it possible to craft a Web link that looks as if it points to a trusted site but when clicked serves up content from a third, potentially malicious site. John Herron, a security expert who maintains the NIST.org site, said: "This vulnerability affects a lot of very large Websites. It basically allows a virtual defacement of a Website when following a malicious link." Google notified all customers on November 22 with clear instructions on how to protect their appliances. The vulnerability will also be addressed in the next release of the products. No Google Search Appliance or Google Mini users have reported any exploits of the flaw. The cross-site scripting problem involves 7-bit Unicode Transformation Format (UTF) character encoding. The rigged links will be very long, according to security experts. Users who have not heard from Google should contact the company for a fix.

Category 23.9 Scripting languages (e.g., PERL, CGI scripts, Python, PHP)

2007-01-02 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/07/01/02/HNgmailscripting_1.html

GOOGLE CLOSES GMAIL CROSS-SITE SCRIPTING VULNERABILITY.

Google Inc. has fixed a flaw that would have allowed Websites to harvest information from Gmail contact lists, a problem that could have let spammers collect reams of new e-mail addresses. For an attack to work, a user would have to log into a Gmail account and then visit a Website that incorporates JavaScript code designed to take contact information from Gmail. Proof-of-concept code was publicly posted.

Category 23.9 Scripting languages (e.g., PERL, CGI scripts, Python, PHP)

2007-01-16 DHS Daily OSIR; CNET News
http://news.com.com/Google+plugs+account+hijack+holes/2100-1002_3-6150578.html

GOOGLE PLUGS ACCOUNT HIJACK HOLES.

Google has patched a cross-site scripting vulnerability in one of its Web-hosting services. If left unpatched, the cross-site scripting (XSS) vulnerability could have allowed hackers to modify third-party Google documents and spreadsheets and to view e-mail subjects and search history, according to the Google Blogoscoped blog. Philipp Lenssen, the author of Google Blogoscoped, a third-party site that comments on Google developments, said the vulnerability was similar to another in Blogger Custom Domains reported on Sunday night. "The security hole is connected to an update to a specific Google service which doesn't correctly defend against HTML injections," he said. According to Lenssen, the earlier Custom Domains vulnerability allowed another Google expert, Tony Ruscoe, to create a page that was hosted on a Google.com domain. Ruscoe was able to prove that he could have used code to steal a user's Google cookie and access their Google services. The second vulnerability, reported by Lenssen, would also have enabled a hacker to use JavaScript code to pass cookie data to an external source.

Category 23.9 Scripting languages (e.g., PERL, CGI scripts, Python, PHP)

2007-02-21 DHS Daily OSIR; CRN
http://www.crn.com/sections/breakingnews/dailyarchives.jhtml?articleId=197007769

GOOGLE DESKTOP VULNERABILITY FIXED.

Google has fixed a serious vulnerability in its popular Google Desktop software that could allow remote attackers to access confidential data and gain full control over affected PCs. Google Desktop, which extends Google's Web search and indexing functions to local PC hard drives, is susceptible to a cross-site scripting attack (XSS) because of its failure to properly encode output data, according to researchers at security vendor Watchfire, which discovered the flaw in January. Google issued a fix for the vulnerability soon after being notified by Watchfire, and users are being automatically updated with the patch, according to a Google spokesperson. Although Google has fixed this XSS vulnerability, the fact that the online and offline connection with Google Desktop still exists means that the software could still be vulnerable, according to said Mike Weider, CTO of Watchfire. Original report: http://www.watchfire.com/news/releases/02-21-07.aspx

Category 23.9 Scripting languages (e.g., PERL, CGI scripts, Python, PHP)

2007-03-01 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2099735,00.asp

MONTH OF PHP BUGS BEGINS.

Security expert Stefan Esser has declared war on vulnerabilities in the PHP core with the "Month of PHP Bugs." PHP is an open-source HTML embedded scripting language used to create dynamic Webpages. The month-long effort is an attempt to improve the security of PHP. It follows his contentious departure in December from the PHP Security Response Team, which he founded, after he accused The PHP Group of being too slow to fix problems. Esser stressed, however, that he is not striking back at his old colleagues but is addressing legitimate security issues.

23.A Open-source software

Category 23.A Open-source software

2006-01-10 DHS Daily OSIR; http://news.com.com/Homeland+Security+helps+secure+open-source+code/2100-1002_3-6025579.html?tag=nefd.lede

DEPARTMENT OF HOMELAND SECURITY HELPS SECURE OPEN-SOURCE CODE

The U.S. Department of Homeland Security (DHS) is extending the scope of its protection to open-source software. Through its Science and Technology Directorate, DHS has given $1.24 million in funding to Stanford University, Coverity and Symantec to hunt for security bugs in open-source software and to improve Coverity's commercial tool for source code analysis. The DHS grant will be paid over a three-year period, with $841,276 going to Stanford, $297,000 to Coverity and $100,000 to Symantec. In the effort, which the government agency calls the "Vulnerability Discovery and Remediation, Open Source Hardening Project," Stanford and Coverity will build and maintain a system that does daily scans of code contributed to popular open-source projects. The automated system should be running by March, and the resulting database of bugs will be accessible to developers, they said. Symantec will provide security intelligence and test the source code analysis tool in its proprietary software environment, said Brian Witten, the director of government research at the Cupertino, CA, security software vendor. The list of open-source projects that Stanford and Coverity plan to check for security bugs includes Apache, BIND, Ethereal, KDE, Linux, Firefox, FreeBSD, OpenBSD, OpenSSL. and MySQL, Coverity said.

Category 23.A Open-source software

2006-06-01 DHS Daily OSIR; Security Focus http://www.securityfocus.com/bid/14509/discuss

MYSQL USER-DEFINED FUNCTION BUFFER OVERFLOW VULNERABILITY.

MySQL is prone to a buffer overflow vulnerability.

Analysis: A database user with sufficient access to create a user-defined function can exploit this issue. Attackers may also be able to exploit this issue through latent SQL injection vulnerabilities in third party applications that use the database as a backend.

For a complete list of vulnerable products:
http://www.securityfocus.com/bid/14509/info

Solution: This issue is reportedly addressed in MySQL versions 4.0.25, 4.1.13, and 5.0.7-beta. Symantec has not confirmed these fixes.

For details on obtaining and applying the appropriate updates:
http://www.securityfocus.com/bid/14509/references

Category 23.A Open-source software

2006-06-27 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/06/06/27/79658_HNmicrosoftc odesharing_1.html

MICROSOFT UNVEILS CODE-SHARING WEBSITE.

Microsoft is hoping to fire up a community of developers on a code-sharing forum the company has been testing since May but rolled out officially on Tuesday, June 27. The project, called CodePlex, is a forum for Microsoft code and code from other developers, said Jon Rosenberg, director of community source programs at Microsoft. Code contributed to the site can be posted under any licensing terms, Rosenberg said. Microsoft is offering some of its source code under its own Share Source Initiative licensing plan, which offers access to source code under varying conditions. The site is available at: http://www.codeplex.com/

Category 23.A Open-source software

2006-07-03 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2159541/openoffice-patches-three

OPENOFFICE PATCHES THREE SECURITY HOLES.

OpenOffice.org has released an update for its open source productivity suite that plugs three security vulnerabilities. Security Website Secunia rated the vulnerabilities as "moderately critical," its third most severe designation on a five-step scale. The vulnerabilities affect OpenOffice versions 2 and 1.1.5. An update for version 2 is available for download now. A patch for the previous version will be released shortly. Secunia advisory: http://secunia.com/advisories/20867/

Category 23.A Open-source software

2006-07-06 EDUPAGE; ZDNet http://news.zdnet.com/2100-3513_22-6090912.html & http://news.com.com/2102-7344_3-6090912.html

MICROSOFT AGREES TO WORK WITH OPENDOCUMENT

Reversing earlier statements that it would not support translation of its documents into the OpenDocument format, Microsoft has said it will sponsor the development of software that does just that. Microsoft's Open Office XML format and the OpenDocument format have been vying for the top spot in the emerging area of XML-based formats that allow interoperability of documents and platforms. A number of governments, including those of Massachusetts and Belgium, have committed to using the OpenDocument format, and it was pressure from those governments that persuaded Microsoft to allow translation of its Office files into the competing format, according to Tom Robertson, Microsoft's general manager of interoperability and standards. The software, known as Open XML Translator, will be developed by Clever Age, a French company, with support from Microsoft. Microsoft said it hopes to have a plug-in for Word by the end of this year and similar tools for Excel and PowerPoint next year.

[MK notes: as of May 2007, no further news of this project, which is in progress via OpenForge.]

Category 23.A Open-source software

2006-07-06 DHS Daily OSIR; IDG News Service http://www.pcworld.com/news/article/0,aid,126331,00.asp

MICROSOFT OFFICE 2007 TO SUPPORT ODF STANDARD.

On Wednesday, July 5, Microsoft announced the creation of the Open XML Translator project, so its Office suite will support the OpenDocument Format (ODF) standard. The move comes in response to government requests for Microsoft products to be compatible with ODF, such as the national governments of Belgium and Denmark, and the state government of Massachusetts. The company said that the next edition of Office will include menu options for XML, ODF, and Adobe Systems' PDF formats. A prototype of the first translator for Word's 2007 version was posted Wednesday, July 5, on SourceForge.net, a popular Website for open-source development.

Category 23.A Open-source software

2006-07-20 DHS Daily OSIR; Washington Technology http://www.washingtontechnology.com/news/1_1/defense/28963-1.html

DOD REPORT ADVOCATES OPEN-SOURCE APPROACH FOR SOFTWARE ACQUISITION.

A recently released Department of Defense (DoD) report on technology development methodologies advocates more use of open-source software and suggests ways it can be incorporated into the procurement cycle. Reuse can save money by promoting reuse of software across the different defense agencies, the report contends. The Office of the Deputy Undersecretary of Defense for Advanced Systems and Concepts commissioned the Open Technology Development (OTD) road map, which was published in April but only recently released publicly. The concept of OTD is based on sharing software code developed by the DoD and its contractors, as well as by the worldwide open-source community. OTD road map: http://www.acq.osd.mil/actd/articles/OTDRoadmapFinal.pdf

---

Category 23.A Open-source software

2006-07-28 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/06/07/28/HNgoogleopensource_1.html

GOOGLE TO HOST REPOSITORY FOR OPEN-SOURCE PROJECTS.

Google is offering to host open source software development projects in a move that has been met with mixed reaction from the developer community online. As part of the new offering, launched on Thursday, July 27, developers get 100MB of disk space to store and share their open source project, and can use tools such as issue tracking and mailing list support. Google said it is making the offer in an effort to encourage healthy, productive open source communities. Developers must have a Gmail account to use the service. Project Hosting on Google Code: http://code.google.com/hosting/ Project Hosting Frequently Asked Questions: http://code.google.com/hosting/faq.html

Category 23.A Open-source software

2006-11-13 EDUPAGE; BBC http://news.bbc.co.uk/1/hi/technology/6144748.stm

JAVA GOES OPEN SOURCE

Sun Microsystems announced plans to release Java as open source software in an effort to draw more developers to the language. Java, which is more than 10 years old, is widely used in cell phones and other handheld devices and in servers and personal computers. As an open source application, Java will be accessible to developers to make changes and share those changes with others. Rich Green, executive vice president of software at Sun, said the decision to release Java as open source will result in "more richness of offerings, more capability, more applications that consumers will get to use." Java, he said, "will become a place for innovation." Analysts agreed that a healthy community of Java developers would be beneficial to Sun. Michael Cote, an analyst with RedMonk, noted, "Sun profits from the Java ecosystem thriving." Green said that all of the Java source code should be available by March 2007.

Category 23.A Open-source software

2007-03-27 DHS Daily OSIR; CNET News http://news.com.com/Open-source+bug+hunt+project+expands/2100-1002_3-6171105.html

OPEN-SOURCE BUG HUNT PROJECT EXPANDS.

A year after its original launch, a U.S. government-backed project that scans open-source code for flaws is expanding. The effort, supported by a research contract from the Department of Homeland Security (DHS), is now scanning code of 150 open-source projects, up from the original 50. "This allows open-source developers to find and resolve defects introduced into the project," said David Maxwell, open-source strategist for Coverity. Coverity makes source-code analysis tools and shares the DHS contract with Stanford University and Symantec. Since the start of the project, 6,000 bugs that were found have been fixed. About 700 developers are now registered to access the bug data and 35 million lines of code are scanned every day.

23.B Microsoft programs (e.g., Office, Media Player)

Category 23.B Microsoft programs (e.g., Office, Media Player)

2006-06-11 Network World Security Management Newsletter

EXCEL CAN DAMAGE PERCENTAGE DATA

Warn your users to _turn off_ automated format conversion functions in Excel (or other spreadsheets) when working with production spreadsheets where complex alphanumeric codes are to be entered. It would be better to note and correct an error than to have the software silently make assumptions and modify their input, resulting in data rejection or – worse – acceptance of faulty data.

Use the Tools | Options | Edit sequence and uncheck the "Enable automatic percent entry" because it has two different rules in effect. With that option enabled, input numbers _greater_ than 1 are _divided_ by 100; e.g., entering 10 stores the value 10% (i.e., 0.1) and entering 1 stores 1% (i.e., 0.01). However, numbers _smaller_ than 1 are _not_ converted; thus .1 is stored as 10% and .01 is stored as 1%. As you can see, there are two different numbers that can result in the same stored value (yecchhh). If the data contain numbers that cross the boundary between these (not particularly obvious) rules, the numbers stored in the spreadsheet will not be those intended by the operator.

[Based on an article published in Network World Security Management Newsletter by M. E. Kabay; in press]

Category 23.B Microsoft programs (e.g., Office, Media Player)

2006-06-13 DHS Daily OSIR; U.S. Computer Emergency Readiness Team
http://www.uscert.gov/cas/techalerts/TA06-164A.html

US-CERT TECHNICAL CYBER SECURITY ALERT TA06-164A: MICROSOFT WINDOWS, INTERNET EXPLORER, MEDIA PLAYER, WORD, POWERPOINT, AND EXCHANGE VULNERABILITIES.

Microsoft has released updates that address critical vulnerabilities in Microsoft Windows, Word, PowerPoint, Media Player, Internet Explorer, and Exchange Server. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial-of-service on a vulnerable system. Systems affected: Microsoft Windows; Microsoft Windows Media Player; Microsoft Internet Explorer; Microsoft PowerPoint for Windows and Mac OS X; Microsoft Word for Windows; Microsoft Office; Microsoft Works Suite; Microsoft Exchange Server Outlook Web Access. For more complete information, refer to the Microsoft Security Bulletin Summary for June 2006.

Solution: Apply updates: Microsoft has provided updates for these vulnerabilities in the Microsoft Security Bulletin Summary for June 2006: http://www.microsoft.com/technet/security/bulletin/ms06-jun.mspx

Microsoft Windows updates are available on the Microsoft Update site:
https://update.microsoft.com/microsoftupdate/v6/muoptdefault.aspx?ln=en

Workarounds: Please see the following Vulnerability Notes for workarounds:
http://www.kb.cert.org/vuls/byid?searchview&query=ms06-june

Category 23.B Microsoft programs (e.g., Office, Media Player)

2006-06-20 DHS Daily OSIR; CNET News
http://news.com.com/Critical+Microsoft+fix+breaks+some+Net+connections/2100-1002_3-6086130.html?tag=nefd.top

'CRITICAL' MICROSOFT FIX BREAKS SOME INTERNET CONNECTIONS.

One of the dozen security updates Microsoft released last week with security bulletin MS06-025 is causing network connection trouble for some users, the company said. Problems occur only with dial-up connections that use a terminal window, or dial-up scripting, Microsoft said in an article on its support Website published late Monday, June 19. Microsoft is working on a revised security patch to address the issue. Meanwhile, the company recommends that people who need to use dial-up scripting or terminal window features do not install the security update.

Microsoft-released article on this issue: http://support.microsoft.com/kb/911280

Category 23.B Microsoft programs (e.g., Office, Media Player)

2006-07-17 DHS Daily OSIR; Security Focus http://www.securityfocus.com/bid/18989/references

MICROSOFT WORKS SPREADSHEET MULTIPLE REMOTE VULNERABILITIES.

The spreadsheet component of Microsoft Works is prone to multiple remote vulnerabilities. Analysis: These issues occur because the application fails to handle specifically crafted spreadsheet documents when importing them into Microsoft Works. These vulnerabilities allow remote attackers to execute arbitrary machine code in the context of affected application. Attackers may also crash vulnerable applications, denying service to legitimate users. Microsoft Works version 8.0 is vulnerable to these issues; other versions may also be affected. Vulnerable: Microsoft Works 8.0. Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.

Category 23.B Microsoft programs (e.g., Office, Media Player)

2006-07-17 DHS Daily OSIR; Security Focus http://www.securityfocus.com/bid/18993/references

MICROSOFT POWERPOINT MULTIPLE UNSPECIFIED VULNERABILITIES.

Microsoft PowerPoint is prone to multiple remote vulnerabilities. Three proof-of-concept exploit files designed to trigger vulnerabilities in PowerPoint have been released. It is currently unknown if these three exploit files pertain to newly discovered, unpublished vulnerabilities or if they exploit previously disclosed issues. These issues may allow remote attackers to cause crashes or to execute arbitrary machine code in the context of the affected application, but this has not been confirmed. This BID will be updated and potentially split into individual records as further analysis is completed. Microsoft PowerPoint 2003 is vulnerable to these issues; other versions may also be affected. For more information on vulnerabilities: http://www.securityfocus.com/bid/18993/info Solution: Currently, Security Focus is not aware of any vendor-supplied patches for these issues.

Category 23.B Microsoft programs (e.g., Office, Media Player)

2006-07-20 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,1992128,00.asp

POWERPOINT ZERO-DAY ATTACK POINTS TO CORPORATE ESPIONAGE.

A second Trojan used in the latest zero-day attack against Microsoft Office contains characteristics that pinpoint corporate espionage as the main motive, according to virus hunters tracking the threat. According to an alert from Symantec, a backdoor called Trojan.Riler.F is installing itself as a layered service provider, or LSP, allowing it access to every piece of data entering and leaving the infected computer. An LSP is a legitimate system driver linked deep into the networking services of Windows. Symantec said the Trojan also opens a back door on the compromised system and connects to the "soswxyz.8800.org" domain. The Trojan then listens and waits for commands from a remote attacker. Symantec Alert: http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2006-071812-3213-99&tabid=1

Category 23.B Microsoft programs (e.g., Office, Media Player)

2006-08-08 DHS Daily OSIR; U.S. Computer Emergency Readiness Team http://www.uscert.gov/cas/techalerts/TA06-220A.html

US-CERT TECHNICAL CYBER SECURITY ALERT TA06-220A: MICROSOFT PRODUCTS CONTAIN MULTIPLE VULNERABILITIES.

Microsoft has released updates that address critical vulnerabilities in Microsoft Windows, Office, Works Suite, Visual Basic for Applications, and Internet Explorer. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial-of-service on a vulnerable system. The update for MS06-040 addresses a critical vulnerability in the Windows Server service. US-CERT has received reports of active exploitation of this vulnerability. Systems Affected: Microsoft Windows; Microsoft Office (Windows and Mac); Microsoft Works Suite; Microsoft Visual Basic Basic for Applications (VBA); Microsoft Internet Explorer. Solution: Microsoft has provided updates for these vulnerabilities in the August 2006 Security Bulletins: http://www.microsoft.com/technet/security/bulletin/ms06-aug. mspx When prioritizing updates, it is strongly encouraged to apply the update for MS06-040 first. Updates for Microsoft Windows and Microsoft Office XP and later are available on the Microsoft Update site. Microsoft Office 2000 updates are available on the Microsoft Office Update site: https://update.microsoft.com/microsoftupdate/v6/muoptdefault.aspx Apple Mac OS X users should obtain updates from the Mactopia Website: http://www.microsoft.com/mac/ System administrators may wish to consider using Windows Server Update Services: http://www.microsoft.com/windowsserversystem/updateservices/default.mspx

Category 23.B Microsoft programs (e.g., Office, Media Player)

2006-09-04 DHS Daily OSIR; Security Focus http://www.securityfocus.com/bid/16644/solution

MICROSOFT WINDOWS MEDIA PLAYER PLUGIN BUFFER OVERFLOW VULNERABILITY.

The Microsoft Windows Media Player plugin for non-Microsoft browsers is prone to a buffer-overflow vulnerability. The application fails to do proper boundary checks on user-supplied data before using it in a finite-sized buffer. An attacker can exploit this issue to execute arbitrary code on the victim user's computer in the context of the victim user. This may facilitate a compromise of the affected computer. This issue is exploitable only through non-Microsoft browsers that have the Media Player plugin installed. Possible browsers include Firefox .9 and later and Netscape 8; other browsers with the plugin installed may also be affected. For a complete list of vulnerable products: http://www.securityfocus.com/bid/16644/info Solution: Microsoft has released security advisory MS06-006 with updates to address this issue.

Category 23.B Microsoft programs (e.g., Office, Media Player)

2006-09-27 DHS Daily OSIR; Security Focus http://www.securityfocus.com/bid/20226/references

MICROSOFT POWERPOINT UNSPECIFIED REMOTE CODE EXECUTION VULNERABILITY.

Microsoft PowerPoint is prone to an unspecified remote code execution vulnerability. This issue can allow remote attackers to execute arbitrary code on a vulnerable computer by supplying a malicious PowerPoint document to a user. This issue is being actively exploited in the wild as Trojan.PPDropper.F. This vulnerability is currently known to affect Microsoft Office 2000, Office XP and Office 2003. For a complete list of vulnerable products: http://www.securityfocus.com/bid/20226/info Due to a lack of information, further details cannot be provided. Solution: Security Focus is not aware of any vendor-supplied patches for this issue.

Category 23.B Microsoft programs (e.g., Office, Media Player)

2006-11-08 DHS Daily OSIR; Security Focus http://www.securityfocus.com/bid/18938/discuss

MICROSOFT EXCEL FILE REBUILDING REMOTE CODE EXECUTION VULNERABILITY.

Microsoft Excel is prone to a remote code execution vulnerability. Successfully exploiting this issue allows attackers to corrupt process memory and to execute arbitrary code in the context of targeted users. Note that Microsoft Office applications include functionality to embed Office files as objects contained in other Office files. As an example, Microsoft Word files may contain embedded malicious Microsoft Excel files, making Word documents another possible attack vector. For a complete list of vulnerable products: http://www.securityfocus.com/bid/18938/info Solution: Microsoft has released a security advisory addressing this issue. For more information: http://www.securityfocus.com/bid/18938/references

Category 23.B Microsoft programs (e.g., Office, Media Player)

2007-01-05 DHS Daily OSIR; CNET News
http://news.com.com/Microsoft+pulls+four+planned+patches/210 0-1002_3-6147705.html

MICROSOFT PULLS FOUR PLANNED PATCHES.

Microsoft has pulled four bulletins from its announced list of Patch Tuesday fixes, but did not specify why it was backpedaling on the security releases. It now plans to issue four security bulletins on Tuesday, January 9, rather than the eight originally announced, the software giant said Friday in an updated notice on its Website. Three bulletins will contain fixes for Office, at least one of which will be rated "critical," Microsoft said.

Category 23.B Microsoft programs (e.g., Office, Media Player)

2007-01-18 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2085354,00.asp

MICROSOFT PATCHES BUGGY EXCEL PATCH.

Microsoft has re-released an update issued in its January 2007 patch batch to correct a glitch in the way Excel 2000 processes information. The company announced that the "targeted re-release" was necessary to correct the bug, which occurs in the way Excel 2000 processes the phonetic information embedded in files created using Excel in the Korean, Chinese or Japanese executable mode. The patch was shipped January 9 as part of the MS07-002 bulletin that provided fixes for a total of five Microsoft Excel vulnerabilities.
Microsoft Security Bulletin MS07-002:
http://www.microsoft.com/technet/security/Bulletin/MS07-002.mspx

Category 23.B Microsoft programs (e.g., Office, Media Player)

2007-02-05 DHS Daily OSIR;
InformationWeek http://www.informationweek.com/showArticle.jhtml

GARTNER: DEPLOY OFFICE 2007 FILE CONVERTERS NOW.

Enterprises should gear up now for Microsoft Office 2007 even if they've decided not to upgrade, by equipping workers with tools to handle the suite's new document file formats, a Gartner analyst recommended. "Whether you adopt Office 2007 or not, your organization will be affected by the new document format it introduces, because you can't control the format in which users outside your organization will send documents to users within your organization," said Michael Silver in a research note posted to the Gartner Website. Silver also warned companies some workers might themselves install Office 2007 on company-owned systems -- laptops, presumably -- to muddy the format waters. Office 2007 introduced a new file native file format -- Open XML -- which the suite's Word, Excel, and PowerPoint applications save to by default. Microsoft-made converters should be deployed, advised Silver, so that Office 2000, Office XP, and Office 2003 applications are able to open and save the Open XML formats used by Office 2007.

Category 23.B Microsoft programs (e.g., Office, Media Player)

2007-02-23 DHS Daily OSIR; CNET News.com
http://news.com.com/Flaw+found+in+Office+2007/2100-1002_3-6161835.html

FLAW FOUND IN OFFICE 2007.

Researchers at eEye Digital Security found a file format vulnerability in Microsoft Office Publisher 2007, which could be exploited to let an outsider run code on a compromised PC. An attacker could create a malicious publisher file, said Ross Brown, eEye's chief executive. Once the recipient opens the file, he or she could find the system infected and susceptible to a remote attack. Microsoft, meanwhile, said it is investigating the report of a possible vulnerability in Publisher 2007 and will provide users with additional guidance if necessary.

Category 23.B Microsoft programs (e.g., Office, Media Player)

2007-02-26 DHS Daily OSIR; Computerworld
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=servers&articleId=9011799&taxonomyId=68&intsrc=kc_top

MICROSOFT OFFICE 2003 APPS, EXPLORER HIT WITH NEW CRASH BUGS.

Microsoft's Word 2003 and Excel 2003 can be crashed by attackers who feed the business applications malformed documents, Symantec Corp. reported Monday, February 26. "A remote attacker may exploit this vulnerability by presenting a malicious WMF file to a victim user," said Symantec's report. "The issue is triggered when the application is used to insert the malicious file into a document." Specially crafted WMF (Windows Metafile) image files were the root of a major attack in late 2005 and early 2006 that was launched from hundreds of malicious Websites and compromised thousands of PCs. The Excel flaw can be leveraged by a malformed spreadsheet file rather than a WMF image, Symantec added. Attacks using either vulnerability require users to download malicious files from a Website or open them when they arrive as e-mailed file attachments. Also at risk, said Symantec, is XP's and Server 2003's Windows Explorer, the operating system's file interface. Explorer will crash when attempting to open a malformed WMF image.

Category 23.B Microsoft programs (e.g., Office, Media Player)

2007-04-11 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2113222,00.asp

MS FIRST LOOK: NO WORD 2007 BUGS.

Microsoft says a preliminary investigation into reports of vulnerabilities in its Office 2007 suite has produced no evidence of a threat to users. Reports of new security holes in MS Office have been made public on known exploit sites, including information about four bugs posted on one site. Microsoft has not released specific information about the vulnerabilities, citing potential risk to users. "Microsoft's initial investigation has found that none of these claims demonstrate any vulnerability in Word 2007 or any Office 2007 products," a company spokesperson said April "Our investigation into the possible impact of these claims on other versions of MicrosoftOffice is continuing." The reported flaws were uncovered by Mati Aharoni of Offensive-Security.com, in Israel.

Category 23.B Microsoft programs (e.g., Office, Media Player)

2007-04-18 DHS Daily OSIR; InformationWeek http://www.informationweek.com/news/showArticle.jhtml?ArticleID=199100538

HACKERS ATTACK POWERPOINT MORE THAN MICROSOFT WORD; ALSO E-MAIL BEING TARGETTED

For the first time, PowerPoint has surpassed Microsoft Word as the most common exploit vector, and hackers are increasingly pinpointing their enterprise attacks, according to a report out Wednesday, April 18, from MessageLabs. There's one specific gang that's running up the numbers on PowerPoint attacks. Most of the attacks are originating from an IP address within Taiwan, noted the MessageLabs report. The company also pointed out in its study of March messaging attacks that hackers are foregoing the traditional widespread attack for targeted attacks. Instead of spamming out hundreds of thousands of e-mails to try to trick users into divulging critical information, a hacker sends one very specific e-mail to one or two people in a specific position inside the same company.

Category 23.B Microsoft programs (e.g., Office, Media Player)

2007-05-16 DHS Daily OSIR; SecurityFocus http://www.securityfocus.com/brief/502

MICROSOFT TO GIVE MORE EARLY DATA ON FLAWS.

Microsoft announced on Wednesday, May 16, that the company will release more information on coming patches through its Advanced Notification Service and modify the layout of its security bulletins starting in June. Under the changes, Microsoft's Security Response Center will release advanced notifications and security bulletins under the same URLs, adding in-depth vulnerability information on the second Tuesday each month to the summary of information released five days before as part of its Advanced Notification Service. The summarized information will include maximum severity and impact of the flaws, detection information and the names of affected software.

Category 23.B Microsoft programs (e.g., Office, Media Player)

2007-05-22 DHS Daily OSIR; IDG News Service http://www.infoworld.com/article/07/05/22/ms-tools-keep-bad-office-files-at-bay_1.html

MICROSOFT TOOLS KEEP BAD OFFICE FILES AT BAY.

Microsoft released a pair of tools on Monday, May 21, that help protect computers from Office 2003 files containing malicious software code. Both tools, which were announced earlier this month, are designed to help defend against Office "zero-day" attacks, which take advantage of vulnerabilities before a patch is released by Microsoft. These type of attacks have become more common in recent months as attackers look for holes in Office to penetrate corporate networks. The first tool to defend against these attacks, called Microsoft Office Isolated Conversion Environment (MOICE), is meant to protect users running Office 2003 and 2007 Office. The tool does not work with other versions of Office. The second tool, called File Block Functionality for Microsoft Office 2003 and the 2007 Microsoft Office system, gives system administrators the ability to define which file types can and cannot be opened by users. This gives administrators the ability to block access to certain files when a specific threat arises, Microsoft said. Microsoft detailed MOICE and File Blocker in a security advisory, recommending that both tools be used to protect against malicious Office documents. Microsoft Advisory: http://www.microsoft.com/technet/security/advisory/937696.mspx

23.D VPNs (Virtual private networks)

Category 23.D VPNs (Virtual private networks)

2007-04-20 DHS Daily OSIR; Network World http://www.networkworld.com/news/2007/042007-nortel-vpn-router-flaw.html

NORTEL WARNS OF THREE VPN ROUTER PRODUCT FLAWS.

Nortel last week warned of several backdoors, and other flaws, in its VPN and secure routing products that could allow unauthorized remote access to an enterprise network. User accounts used for diagnostics on Nortel VPN routers (formerly known as Contivity) could be used to gain access to a corporate VPN. In another potential vulnerability, unauthorized remote users could also gain administrative access to a VPN router through a Web interface. A third vulnerability could result in someone cracking users' VPN passwords. Nortel says it has issued software that fixes these flaws. Product versions affected include all Nortel VPN router models -- 1000, 2000, 3000, 4000 and 5000.

24.1 Windows 9x/Me/NT/2K/XP/CE

Category 24.1 Windows 9x/Me/NT/2K/XP/CE

2006-02-06 DHS Daily OSIR; http://computerworld.co.nz/news.nsf/scrt/AFAC1C3187BF9027CC25710900773FD8

CHINA ATTACKS UK PARLIAMENT USING WINDOWS SECURITY HOLE.

Chinese hackers attacked the UK Parliament in January, the government's e-mail filtering company, MessageLabs, has confirmed. The attack, which occurred on January 2, attempted to exploit the Windows Meta File (WMF) vulnerability to hijack the PCs of more than 70 named individuals. E-mails were sent to staff with an attachment that contained the WMF-exploiting Setabortproc Trojan. Anyone opening this attachment would have enabled attackers to browse files and possibly install a key-logging program to attempt the theft of passwords. None of the e-mails got through to the intended targets, MessageLabs says, but the UK authorities were alerted. MessageLabs said the e-mails had been traced to servers in China's Guangdong Province, hence the suspicion that the latest attack was part of a more general campaign of electronic subversion. This is not the first time the UK Government has come under Trojan attack from China. Last summer, the National Infrastructure Security Coordination Center (NISCC) reported that UK government departments had been hit by a wave of Trojans originating in China.

Category 24.1 Windows 9x/Me/NT/2K/XP/CE

2007-02-14 DHS Daily OSIR; InformationWeek http://www.informationweek.com/showArticle.jhtml

MICROSOFT ISSUES WARNING ON DAYLIGHT-SAVINGS TIME SOFTWARE FLAW.

Microsoft is warning customers that the switch to early daylight savings time this year isn't accounted for in a number of its products, including Windows XP, and that users will need to update their software to avoid potential problems. U.S. daylight savings time will start on March 11, this year -- three weeks earlier than usual. The change was authorized by the U.S. Energy Policy Act of 2005, but Microsoft says its Y2K-like implications mean computer users need to parry like its 1999. "Unless certain updates are applied to your computer, it is possible that the time zone settings for your computer's system clock may be incorrect during this four week period," the software maker said in a statement issued Tuesday, February 13. That could lead to all kinds of problems, from calendaring applications not working properly to key, automated processes not taking place on time. Microsoft said the fix is already built into Windows Vista and Office 2007, but that earlier operating systems and applications could be hit by the problem. As of Tuesday, the company had released an update for Windows XP SP2 users via its Automatic Updates service.
Microsoft statement: http://support.microsoft.com/gp/dst_homeuser#affected

Category 24.1 Windows 9x/Me/NT/2K/XP/CE

2007-04-03 DHS Daily OSIR; US-CERT http://www.us-cert.gov/current/current_activity.html#ms07017

TECHNICAL CYBER SECURITY ALERT TA07-093A: MICROSOFT UPDATE FOR WINDOWS ANIMATED CURSOR VULNERABILITY.

Microsoft has released Security Bulletin MS07-017 to correct vulnerabilities in the way that Microsoft Windows handles image files. This update includes a fix for the animated cursor ANI header stack buffer overflow vulnerability (VU#191609). Applying these updates will mitigate the vulnerability described in Technical Cyber Security Alert TA07-089. The impact of exploiting that vulnerability is that a remote, unauthenticated attacker could execute arbitrary code or cause a denial-of-service condition. MS07-017: http://www.microsoft.com/technet/security/bulletin/ms07-017.mspx
US-CERT Vulnerability Note VU#191609: http://www.kb.cert.org/vuls/id/191609 US-CERT Technical Cyber Security Alert TA07-089A:
http://www.us-cert.gov/cas/techalerts/TA07-089A.html

Category 24.1 Windows 9x/Me/NT/2K/XP/CE

2007-04-04 DHS Daily OSIR; CNET News
http://news.com.com/Windows+cursor+patch+causing+trouble/2100-1002_3-6173413.html

WINDOWS CURSOR PATCH CAUSING TROUBLE.

Installing Microsoft's Tuesday, April 3, patch for a "critical" Windows vulnerability is causing trouble for some users. Microsoft broke with its monthly patch cycle to repair a bug in the way Windows handles animated cursors. Cybercrooks had been using the hole since last week to attack Windows PCs. But the fix is not compatible with software that runs audio and networking components from Realtek Semiconductor, some Windows users have found. An additional update is available from Microsoft to remedy the problem, according to the company's Website. Microsoft is not
aware of networking issues, a representative said.

Category 24.1 Windows 9x/Me/NT/2K/XP/CE

2007-04-09 DHS Daily OSIR; ComputerWorld
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9015923&intsrc=hm_list

MORE PROBLEMS POP UP WITH MICROSOFT'S ANI PATCH.

Microsoft Corp. has acknowledged several new problems with the emergency patch it released last week to quash the Windows animated cursor file (ANI) bug and has updated a hotfix that it's telling some Windows XP SP2 users to download and install. The first problem with the MS07-017 update, the series of seven patches released last Tuesday, April 3, that among other things fixed the ANI flaw, was known to Microsoft before it posted the security bulletin. In fact, a hotfix to correct a flaw in the Realtek HD Audio Control Panel was published simultaneously with MS07-017. A glance at the Microsoft support forums that day and the next, however, showed that many Realtek users were unaware of the hotfix and were frustrated by the error messages they saw after installing the security update. Last Friday, Microsoft refreshed the hotfix to include three more third-party applications that won't start and may throw up an error message that states, "The system DLL user32.dll was relocated in memory. The application will not run properly." The applications are ElsterFormular, a German value-added tax calculator; TUGZip, a free compression utility; and CD-Tag, a $19 CD ripper.

Category 24.1 Windows 9x/Me/NT/2K/XP/CE

2007-04-10 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/07/04/10/HNexploitaniflaw_1 .html

OVER 2,000 SITES EXPLOIT .ANI SECURITY FLAW.

More than 2,000 unique Websites have been rigged to exploit the animated cursor security flaw in Microsoft's software, according to security vendor Websense Inc. Those Websites are either hosting exploit code or are redirecting Internet users to sites with bad code, Websense's blog reported Monday, April 9. The number of Websites engineered to exploit the problem has jumped considerably since the vulnerability was publicly disclosed by Microsoft on March 29. It will likely continue to rise until patches are applied across corporate and consumer PCs, said Ross Paul, senior product manager for Websense. Hackers are hoping to catch some of the millions of unpatched machines.

Websense blog: http://www.websense.com/securitylabs/blog/blog.php?BlogID=122

24.2 Windows VISTA

Category 24.2 Windows VISTA

2006-08-16 EDUPAGE;
ZDNet http://news.zdnet.com/2100-1009_22-6106039.html

MS SECURITY UPDATE NEEDS AN UPDATE

Microsoft acknowledged that a patch issued earlier this month for significant flaws in its operating system has led to new problems for some users. Computers that installed the August patch on Windows 2000 or Windows XP machines with Service Pack 1 and Internet Explorer 6 are experiencing browser crashes when they visit Web sites that use HTTP 1.1 and compression. Fred Dunn, a systems administrator at the University of Texas Health Science Center at San Antonio, said that at his institution, computers with the patch are crashing when users access pages in PeopleSoft applications. The workaround, he said, is to disable the compression in the PeopleSoft applications, which slows performance considerably. Microsoft said that on August 22 it would issue a new patch to replace the patch that is causing these problems.

Category 24.2 Windows VISTA

2006-10-04 EDUPAGE; ZDNet http://news.zdnet.com/2100-1009_22-6122462.html

WINDOWS VISTA ANTIPIRACY TECHNOLOGY LOCKS PCS

Microsoft has embedded antipiracy technology in Windows Vista that locks a PC if the operating system isn't activated using a legitimate product registration key within 30 days of installation. The system will run with reduced functionality until activated. The technology is part of Microsoft's new Software Protection Platform and will be part of future versions of all Microsoft products, said Cori Hartje, director of Microsoft's Windows Genuine Software Initiative. Scheduled for wide availability in January, Vista is the successor to Windows XP.

Category 24.2 Windows VISTA

2006-10-20 DHS Daily OSIR; CNET News
http://news.com.com/Gartner+Vista+antitrust+tweaks+to+take+years/2100-1016_3-6128157.html

GARTNER: VISTA ANTI-TRUST TWEAKS TO TAKE YEARS.

Anti-trust related changes to security in Windows Vista 64-bit will take years to complete and will cause compatibility trouble in the interim, according to Gartner. Users of security technologies such as host intrusion-prevention systems (HIPS) should postpone buying 64-bit versions of Vista, Gartner analyst Neil MacDonald wrote in a research note published on Wednesday, October 18. MacDonald also noted that many integrated security products today include HIPS functionality. "Recognize that many of these products will not deliver full functionality using 64-bit Vista," MacDonald wrote. "Do not plan for initial use of 64-bit Vista if you are using incompatible products for which no suitable alternative exists." People should ask their security vendor for Vista compatibility guarantees, he suggested. MacDonald's research note:
http://www.gartner.com/DisplayDocument?doc_cd=144225

Category 24.2 Windows VISTA

2006-10-27 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2167387/security-vendor-circumvents

SECURITY VENDOR CIRCUMVENTS WINDOWS VISTA'S PATCHGUARD.

Security researchers with Authentium have found a way to circumvent the Patchguard security technology that Microsoft has built into the 64-bit version of its forthcoming Windows Vista operating system. Over the past months the Patchguard technology has been subject of a fierce
debate between security vendors and Microsoft because it prevents some anti-virus software from functioning. Authentium's technology allows an application to effectively disable Patchguard. In a blog posting the company argued that providing kernel access to third party Websites will enable future security innovations.

Category 24.2 Windows VISTA

2007-01-10 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/07/01/10/HNnsamadevistasecure_1.html

NSA HELPED MICROSOFT MAKE VISTA SECURE.

The U.S. agency best known for eavesdropping on telephone calls had a hand in the development of Microsoft's Vista operating system, Microsoft confirmed Tuesday, January 9. The National Security Agency (NSA) stepped in to help Microsoft develop a configuration of its next-generation operating system that would meet Department of Defense requirements, said NSA spokesperson Ken White. This is not the first time the secretive agency has been brought in to consult with private industry on operating system security, White said, but it is the first time the NSA has worked with a vendor prior to the release of an operating system. By getting involved early in the process, the NSA helped Microsoft ensure that it was delivering a product that was both secure and compatible with existing government software, he said. Still, the NSA's involvement in Vista raises red flags for some. Part of this concern may stem from the NSA's reported historical interest in gaining "back-door" access to encrypted data produced by products from U.S. computer companies like Microsoft.

Category 24.2 Windows VISTA

2007-01-23 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2086703,00.asp

COMPATIBILITY CONCERNS HINDER VISTA UPGRADES.

Microsoft's new operating system may be the most eagerly anticipated release of the past 10 years, but concerns over compatibility, bugs and security are keeping many IT professionals from doing so soon, according to the survey released Tuesday, January 23, by Cambridge, MA-based Bit9, a provider of desktop lockdown solutions. Only 68 percent of IT pros reported that they'd be upgrading to Vista in 2007, though very few had made immediate plans. Of those who had expressed their intention to shift to the new operating system, 58 percent said they'd be waiting six months to one year after the launch to do so, while but 10 percent planned to roll out the upgrade in the next six months. Research Brief (registration required): http://www.bit9.com/files/Bit9_Vista_Survey_Research_Brief_vf.pdf

Category 24.2 Windows VISTA

2007-01-25 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/07/01/25/HNpiratedvista_1.html

HALF OF PIRATED VISTA IS MALWARE.

About half of the downloads claiming to be free versions of Microsoft's Vista operating system are actually malicious Trojan horse software, security vendor DriveSentry warned Thursday, January 25. With Vista's consumer launch just days away, hackers have been bombarding discussion boards with offers of "cracked" versions of Windows Vista, which are typically being distributed on peer-to-peer networks, said John Lynch, vice president of sales and marketing for DriveSentry. These posts offer downloads of the operating system that skip Vista's activation process, created by Microsoft to prevent users from running illegal copies. Users who fall for the scam can end up with some pretty nasty problems, according to Lynch. DriveSentry researchers have found malicious key-logging software and spyware on about half of the downloads it has examined recently, he said.

Category 24.2 Windows VISTA

2007-02-01 DHS Daily OSIR; InfoWorld
http://www.infoworld.com/article/07/02/01/HNvistaspeechbug_1 .html

VISTA HOLE OPENS DOOR TO SHOUT HACKING.

The honeymoon ended early for Microsoft's Vista operating system, after word spread Wednesday, January 31, about a flaw that could allow remote attackers to take advantage of the new operating system's speech recognition feature. Microsoft researchers are investigating the reports of a vulnerability that could allow an attacker to use the speech recognition feature to run malicious programs on Vista systems using prerecorded verbal commands. The potential security hole was discovered after an online discussion prompted blogger George Ou to try out a speech-based hack. Ou reported on ZD Net on Tuesday that he was able to access the Vista Start menu and, conceivably, run programs using voice commands played over the system's speakers. The speech recognition flaw is novel and notable for being the first publicized hole in the new operating system since the public launch of Vista on Tuesday. The impact of the flaw, however, is expected to be small. Microsoft recommends that users who are concerned about having their computer shout-hacked disable the speaker or microphone, turn off the speech recognition feature, or shut down Windows Media Player if they encounter a file that tries to execute voice commands on their system.

Category 24.2 Windows VISTA

2007-05-10 DHS Daily OSIR; Computerworld http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9019118&intsrc=hm_list

HACKERS HIJACK WINDOWS UPDATE'S DOWNLOADER.

Hackers are using the file transfer component used by Windows Update to sneak malware past firewalls, Symantec researchers said Thursday, May 10. The Background Intelligent Transfer Service (BITS) is used by Microsoft Corp.'s operating systems to deliver patches via Windows Update. BITS, which debuted in Windows XP and is baked into Windows Server 2003 and Windows Vista, is an asynchronous file transfer service with automatic throttling--so downloads don't impact other network chores. It automatically resumes if the connection is broken. Although BITS powers the downloads delivered by Microsoft's Windows Update service, Oliver Friedrichs, director of Symantec's security response group, said that there was no risk to the service itself. "There's no evidence to suspect that Windows Update can be compromised. If it has a weakness, someone would have found it by now. Microsoft was unable to immediately respond to questions about unauthorized BITS use.

Category 24.2 Windows VISTA

2007-05-16 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2131595,00.asp

RESEARCHER REVEALS TWO-STEP VISTA UAC HACK.

A Web application developer has uncovered a two-step process for exploiting Windows Vista's User Account Control (UAC), essentially by having a Trojan piggyback on what could be a legitimate download. Robert Paveza, a senior Web application developer with Terralever, published details of the vulnerability in a paper titled, "User-Prompted Elevation of Unintended Code in Windows Vista." Paveza said in the paper that the vulnerability uses a two-part attack vector against a default Vista installation. The first step requires that malware called a proxy infection tool be downloaded and run without elevation. That software can behave as the victim expects it to while it sets up a second malicious payload in the background.
White paper: http://www.robpaveza.net/VistaUACExploit/UACExploitWhitepaper.pdf

Category 24.2 Windows VISTA

2007-05-21 DHS Daily OSIR; ComputerWorld http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9020262

OFFICE 2007 LEFT UNPROTECTED IN UPDATE SNAFU.

Office 2007 users running Windows Vista may not have realized that their systems had not received several of this month's patches, Microsoft Corp. said last week when it acknowledged that its security update services had failed to deploy the fixes. "We have updated the detection logic for the May 8th security and non-security updates for Office 2007," said Mark Griesi, a program manager with the Microsoft Security Response Center (MSRC), in an entry on the team's blog. "In some cases, the original detection logic may not have offered the updates or the updates may not have been installed successfully on systems running Windows Vista," Griesi added. Only Vista users with Office 2007 on their hard drives who rely on Microsoft Update or Windows Server Update Services for patches were affected, Microsoft said. The updates that may not have been deployed two weeks ago included ones for Excel 2007 and Office 2007 in general.
MSRC Blog: http://blogs.technet.com/msrc/archive/2007/05/17/new-detecti on-logic-for-may-8th-office-2007-updates.aspx

24.3 UNIX flavors

Category 24.3 UNIX flavors

2006-05-02 DHS Daily OSIR; http://www.securiteam.com/unixfocus/5LP050KIKW.html

MULTIPLE VULNERABILITIES IN LINUX-BASED CISCO PRODUCTS.

A vulnerability in the CiscoWorks WLSE "show" CLI application allows execution of arbitrary code as the root user. Analysis: The Cisco shell presents the administrator with a restricted set of commands which includes a "show" application. The "show" application has several vulnerabilities which allow an attacker to "break out" of the shell and execute commands (including /bin/sh) as the root user. A cross site scripting flaw exists in: /wlse/configure/archive/archiveApplyDisplay.jsp with the "displayMsg" parameter. This can be used to steal the JSP session cookie, therefore giving a targeted attacker admin level access to the system. Once the attacker has admin Web GUI access to the system via the XSS, they can then change the admin password or create a new admin user (without requiring the admin password). Affected software: Cisco Wireless Lan Solution Engine (WLSE); Cisco Hosting Solution Engine (HSE); Cisco Ethernet Subscriber Solution Engine (ESSE); Cisco User Registration Tool (URT); CiscoWorks2000 Service Management Solution (SMS); Cisco Vlan Policy Server (VPS); Cisco Management Engine (ME1100 Series); CiscoWorks Service Level Manager (SLM). Solution: Cisco has released patches for the vulnerabilities. Cisco Security Advisory: http://www.cisco.com/warp/public/707/cisco-sa-20060419-wlse. shtml Cisco Security Response: http://www.cisco.com/warp/public/707/cisco-sr-20060419-priv. shtml

Category 24.3 UNIX flavors

2006-05-02 DHS Daily OSIR; http://www.eweek.com/article2/0,1895,1956652,00.asp

DEPARTMENT OF HOMELAND SECURITY AUDIT FLAGS 'CRITICAL' LINUX BUG.

An open-source security audit program funded by the U.S. Department of Homeland Security has flagged a critical vulnerability in the X Window System which is used in Unix and Linux systems. Coverity, the San Francisco-based company managing the project under a $1.25 million grant, described the flaw as the "biggest security vulnerability" found in the X Window System code since 2000. Coverity Chief Technical Officer Ben Chelf said the flaw resulted from a missing parenthesis on a small piece of the program that checked the ID of the user. It could be exploited to allow local users to execute code with root privileges, giving them the ability to overwrite system files or initiate denial-of-service attacks.

Category 24.3 UNIX flavors

2006-07-17 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/06/07/17/HNhackerslearnfrom opensource_1.html

HACKERS LEARN FROM OPEN SOURCE.

Hackers are taking a page from the open-source playbook, using the same techniques that made Linux and Apache successes to improve their malicious software, according to McAfee Inc. Nowhere is this more apparent than within the growing families of "bot" software. Unlike viruses of the past, bots tend to be written by a group of authors, who often collaborate by using the same tools and techniques as open source developers, said Dave Marcus, security research and communications manager with McAfee's Avert Labs. The current generation of bot software has grown to the point where open-source software development tools make a natural fit. With hundreds of source files now being managed, developers of the Agobot family of malware, for example, are using the open-source Concurrent Versions System software to manage their project.

24.4 TCP/IP, HTTP, IMS (IP Multimedia System)

Category 24.4 TCP/IP, HTTP, IMS (IP Multimedia System)

2006-04-06 DHS Daily OSIR; http://secunia.com/advisories/19553/

CISCO OPTICAL NETWORKING SYSTEM 15000 SERIES MULTIPLE VULNERABILITIES.

Some vulnerabilities have been reported in Cisco Optical Networking System 15000 Series, which can be exploited by malicious people to cause a denial-of-service (DoS) or compromise a vulnerable management system. Multiple services are vulnerable to ACK DoS attacks where an invalid response is sent instead of the final ACK packet during the 3-way handshake. This can be exploited to cause the control cards to exhaust memory resources, not respond to further connections, or reset by establishing multiple of these connections. Successful exploitation requires that IP is configured on the LAN interface (enabled by default). For more information please see source advisory. Solution: Updated versions are available -- see patch matrix in vendor advisory: http://www.cisco.com/warp/public/707/cisco-sa-20060405-ons.s html Also update to Cisco Transport Controller version 4.1.0 or later.

24.6 Wireless (WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax)

Category 24.6 Wireless (WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax)

2006-01-16 DHS Daily OSIR; http://www.vnunet.com/vnunet/news/2148609/microsoft-wi-flaw-found

WINDOWS 2000/XP FALL THROUGH WI-FI FLAW

Hackers have exposed details of a previously undocumented flaw in Microsoft's handling of Wi-Fi which affects users of Windows 2000 and XP. The vulnerability was detailed at the Shmoocon hackers conference in Washington, DC, by self-confessed hacker Mark Loveless, (a.k.a. Simple Nomad), a senior security researcher for Vernier Threat Labs. Loveless explained that the issue centers on the way in which the operating systems look for wireless networks during start-up. When a Wi-Fi equipped laptop starts up using Windows 2000 or XP it immediately starts scanning for wireless networks. If none is found it sets up an ad hoc link using the name of the last wireless network accessed. If a hacker was aware of the last used network ID, for example knowing the name of a corporate Wi-Fi network address, it could be used to establish a direct local link with the Windows PC offering access to all local drives. However, the problem only arises if the target machine is not running a firewall. One of the changes in Windows XP SP2 turns the built-in firewall on by default.

Category 24.6 Wireless (WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax)

2006-02-22 DHS Daily OSIR; http://news.zdnet.co.uk/internet/security/0,39020375,3925373 0,00.htm

SECURITY FEARS OVER LONDON'S BLANKET WI-FI.

Security company McAfee on Tuesday, February 21, raised security concerns over the London's plan to install a Wi-Fi network throughout the Square Mile. The system will be constructed by The Cloud, and should give most of the city's workers wireless access within six months. However, McAfee has raised concerns about the security implications of the project. "Our big concern is that most people care more about connectivity than security. Always-on broadband makes it easier for hackers to find and target people. There is also a knowledge gap -- most people aren't that savvy when it comes to this technology," said Sal Viveros, security expert at McAfee. McAfee recommended that companies prepare themselves for always-on wireless access by learning about the techniques that hackers are using to target susceptible mobile employees, as London is a tempting target for hackers.

Category 24.6 Wireless (WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax)

2006-09-14 DHS Daily OSIR; Times West Virginian
http://www.timeswv.com/local/local_story_257002229.html

WIMAX: POTENTIAL SOLUTION TO INTEROPERABILITY IN A MOUNTAINOUS TERRAIN.

Lack of "interoperability" among first responders using separate communications networks is an issue that officials at the West Virginia High Technology Consortium Foundation (WVHTC) hope to address with cutting-edge wireless technology called WiMAX, or Worldwide Interoperability for Microwave Access. The WiMAX system has a special use in the mountainous and rural terrain of a state such as West Virginia, said David Ramsburg. "I think it can be used in both environments," said Ramsburg, the project manager for the wireless initiative. "We do have a unique situation that's not going to be addressed by large carriers. We are addressing rural areas first because we're dealing with a couple of issues here: topology and sparse population." And WiMax, Ramsburg believes, is the technology that will allow emergency responders to bridge those areas of challenge. The WVHTC is in the first phase of a $1.6 million, three-phase study to develop the technology and apply it in a pilot program.

Category 24.6 Wireless (WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax)

2006-10-04 EDUPAGE; Red Herring
http://www.redherring.com/Article.aspx?a=18946&hed=Nokia+Stakes+Short-Range+Claims

NOKIA'S WIBREE CHALLENGES BLUETOOTH

Finnish cell-phone maker Nokia has introduced Wibree technology, which ties low-power devices such as sensors into a personal network that also includes Bluetooth-connected devices such as cell phones. According to Michael Foley, executive director of the Bluetooth Special Interest Group, "Wibree consists of a small extension to a standard Bluetooth radio." Nokia, however, insists that Wibree is not offered as an extension to Bluetooth but as a separate technology designed to prompt demand in areas such as personal fitness and toys where low-power devices monitor things such as heart rate or the movement of a toy car.

Category 24.6 Wireless (WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax)

2006-10-23 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/06/10/23/HNcitywifi_1.html

CITY WI-FI COVERAGE PUT TO THE TEST.

Numerous cities around the world, and some rural areas, are building or exploring wireless networks that can deliver fast Internet access everywhere. Even when they don't pay to build the networks, municipalities invest political capital in the promise of connectivity everywhere. Now, a consulting company has launched an independent testing service and is offering to check on the performance of Wi-Fi networks. The service is becoming available as municipal wireless is projected to grow quickly over the next few years. Using a notebook PC with a Global Positioning System and custom software, the consulting company can gather performance data every 100 feet across the advertised service area. Parameters include coverage, data throughput, delay, packet loss and loss of entire files. The company has already tested three networks and found widely varying performances.

Category 24.6 Wireless (WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax)

2007-01-02 DHS Daily OSIR; New York Times
http://www.nytimes.com/2007/01/02/technology/02avis.html

ROLLING WI-FI HOTSPOT TO BE OFFERED IN RENTAL CARS.

Try connecting to a high-speed wireless network from a car, and you are pretty much limited to one method: rigging your laptop computer with a special modem and subscribing to a costly, and sometimes temperamental, wireless service. But a start-up wireless technology company based in San Francisco is expected to announce this week that it has reached an agreement with a rental car company to provide a rolling Wi-Fi hotspot to customers by March. For $10.95 a day, the rental car company will issue motorists a notebook-size portable device that plugs into a car's power supply and delivers a high-speed Internet connection. A mobile Wi-Fi hotspot that lets laptops and personal digital assistants link to the Internet without the benefit of wires represents an important step toward what technology experts call the "connected car." Users of these new Wi-Fi hotspots still must contend with technological limitations, like bandwidth restrictions and, for vehicles with too few auxiliary power outlets for all passengers who want to be online at the same time, battery consumption.

Category 24.6 Wireless (WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax)

2007-01-04 DHS Daily OSIR; Reuters
http://www.nytimes.com/2007/01/04/technology/04bluetooth.html

THREE CELL PHONE MAKERS ARE SUED OVER BLUETOOTH TECHNOLOGY.

A United States research institute has sued three cell phone makers, accusing them of violating a patent for Bluetooth technology. The Washington Research Foundation, which markets technology from universities and other nonprofit research institutions in Washington State, is seeking damages from Nokia, Samsung Electronics and Panasonic, owned by Matsushita, contending that the three companies were using a radio frequency receiver technology patented by a University of Washington scientist in 1999. The suit was filed December 21 in Federal District Court in Seattle. The claim appears to restrict itself to Bluetooth devices sold or used in the United States, which means any ruling will affect around 15 to 20 percent of total global sales of Bluetooth mobile phones and headsets in the near term, according to Neil Mawston, an analyst at the market research group Strategy Analytics. But Ben Wood, a consultant at CCS Insight, said the implications for the standard could be more serious if the foundation's claim was successful. "A standard which everyone assumes to be royalty-free is now at risk of becoming a chargeable element inside mobile phones and other devices," he said.

Category 24.6 Wireless (WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax)

2007-01-08 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/07/01/08/HNwifialliance_1.html

WI-FI BODY TO SIMPLIFY SECURITY.

The group that certifies Wi-Fi products aims to make more wireless LANs secure by taking some of the work out of locking them down. The Wi-Fi Alliance announced on Monday, January 8, at the International Consumer Electronics Show its Wi-Fi Protected Setup (WPS) specification, which lays out an easier process for setting up a secure wireless LAN. The group also revealed the first devices certified under WPS, though it will take a few more months for consumer products to reach store shelves. Wi-Fi security has greatly improved since home users first embraced wireless LANs a few years ago, but most consumers still don't use the available tools because they are too hard to set up, said Frank Hanzlik, managing director of the Wi-Fi Alliance. WPS cuts the number of steps required to secure a new network, he said.

Category 24.6 *Wireless (WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax)*

2007-01-09 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2172121/experts-warn-wimax-security

EXPERTS WARN OF WIMAX SECURITY HOLES.

Even before the much-hyped WiMax wide area wireless networking gets off the ground experts are warning of security issues affecting the technology. Analyst firm ABI Research noted that, contrary to many users' expectations, WiMax does have "a number of security vulnerabilities." "Early Wi-Fi consumers enjoyed a false sense of security until there were some well-publicized hacking exploits," said ABI vice president Stan Schatt. "The WiMax Forum has emphasized how much more secure WiMax is than early Wi-Fi. As a result, there may be WiMax customers who are similarly lulled into a false sense of security." Schatt warned that the flaws should begin to show themselves once the first big WiMax rollouts begin. Gaps in WiMax security fall into three categories: user terminals; intrusion detection; and connectivity service networks. User terminals will need encryption acceleration to handle AES processing demands. In addition, access service networks at the edge of WiMax networks offer the ideal place for vendors to add intrusion detection and protection software and hardware.

Category 24.6 *Wireless (WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax)*

2007-03-03 DHS Daily OSIR; CNET News.com http://news.com.com/Your+Wi-Fi+can+tell+people+a+lot+about+you/2100-7355_3-6163666.html

YOUR WI-FI CAN TELL PEOPLE A LOT ABOUT YOU.

Simply booting up a Wi-Fi-enabled laptop can tell people sniffing wireless network traffic a lot about your computer--and about you. Soon after a computer powers up, it starts looking for wireless networks and network services. Even if the wireless hardware is then shut-off, a snoop may already have caught interesting data. Much more information can be plucked out of the air if the computer is connected to an access point, in particular an access point without security. There are many tools that let anyone listen in on wireless network traffic. These tools can capture information such as usernames and passwords for e-mail accounts and instant message tools as well as data entered into unsecured Websites. People who have the option of using a Virtual Private Network when connected to a wireless network should use it to establish a more secure connection, experts suggest. Also, on home routers WPA, or Wi-Fi Protected Access, offers improved security over the cracked WEP, or Wired Equivalent Privacy.

Category 24.6 *Wireless (WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax)*

2007-04-04 DHS Daily OSIR; IDG News Service http://www.infoworld.com/article/07/04/04/HNdontusewep_1.html

RESEARCHERS HAVE DISCOVERED A FASTER WAY TO CRACK THE WI-FI SECURITY PROTOCOL.

Three German security researchers have discovered a faster way to crack the Wi-Fi security protocol WEP (Wired Equivalent Privacy). They plan to demonstrate their findings at a security conference in Hamburg this weekend. It takes just 3 seconds to extract a 104-bit WEP key from intercepted data using a 1.7GHz Pentium M processor. The necessary data can be captured in less than a minute, and the attack requires so much less computing power than previous attacks that it could even be performed in real time by someone walking through an office. "We think this can even be done with some PDAs or mobile phones, if they are equipped with wireless LAN hardware," said Erik Tews, a researcher in the computer science department at Darmstadt University of Technology in Darmstadt, Germany. Paper: http://eprint.iacr.org/2007/120.pdf

Category 24.6 *Wireless (WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax)*

2007-05-16 DHS Daily OSIR; Associated Press http://news.yahoo.com/s/ap/20070516/ap_on_hi_te/wi_fi_alliance;_ylt=AvIaUxryih5orNPkYrIjm8QjtBAF

NEXT GEN OF WI-FI IS PLANNED FOR SUMMER.

The next generation of wireless Internet products certified by the Wi-Fi Alliance is expected to hit shelves this summer, even though a final standard for the technology isn't due for another year, the industry group says. The Wi-Fi Alliance was announcing Wednesday, May 16, that it will begin certifying wireless routers, networking cards, microchips and other so-called "Draft N" products in June. The products, which take their name from the upcoming 802.11n technical standard, are expected to reach retail stores shortly thereafter.

24.7 SWDR (Software-defined radio)

Category 24.7 SWDR (Software-defined radio)

2006-03-08 INNOVATION (Scientific American 20 Feb 2006)<http://www.sciam.com/article.cfm?chanID=sa006&colID=1&articleID=000C7B72-2374-13F6-A37483414B7F0000>

COGNITIVE RADIO

Wouldn't it be nice if your radio were smart enough to switch to a different frequency when it hit a patch of interference? Even better, such built-in intelligence could prove a lifesaver for emergency cell phone communications. Engineers are developing adaptive software that enables radios, cell phones and other wireless communications devices to reconfigure their communications functions on the fly, locating and linking to any locally available unused radio spectrum as needed. As envisioned, cognitive radio technology will "learn" what to do based on prior experience, so that if you lose the signal every time you cross a bridge on your morning commute, the unit would build an internal database that defines how it could best operate in that place at that time of day.

Experts say that if cognitive radio catches on, it could alleviate the current overcrowding in some of the more popular spectrum bands.

Category 24.7 SWDR (Software-defined radio)

2006-10-04 INNOVATION (BBC News 27 Sep 2006) <http://news.bbc.co.uk/2/hi/technology/5382086.stm>

TAKING ON THE WIRELESS 'TOWER OF BABEL'

Scientists at European space firm EADS-Astrium are working on what has been dubbed "Tower of Babel" technology -- software that can converge different wireless gadgets into a single mobile device. Researchers say Software Defined Radio (SDR) technology would enable a plethora of wireless devices operating on different standards with different software to communicate with one another, regardless of protocols. EADS-Astrium engineer Francis Kinsella puts it this way: "If you were to go on a hill-walking trip, you might have a walkie-talkie to talk to friends who are not far away, a mobile in case of emergency, GPS, a Bluetooth connection and even a laptop or PDA with a wireless LAN connection. Every single one of these things is a radio, and they are all slightly different.

But in the future, with Software Defined Radio, all you need is one thing that can do the job of all these devices." The first applications are slated for the military, but Kinsella predicts that there could be "an explosion in the next five to 10 years for SDR."

Category 24.7 SWDR (Software-defined radio)

2007-02-14 INNOVATION (Portable Design Jan 2007) <http://pd.pennnet.com/display_article/281218/21/ARTCL/none/none/Cognitive-rad ios-solve-a-host-of-problems/>

COGNITIVE RADIO = SMARTER CELL PHONES

Advances in software-defined radio (SDR) are making it possible to add new features such as machine learning, vision and natural language processing to what is called "cognitive radio," a term coined by Joe Mitola of MITRE Corp. Unlike SDRs, cognitive radios are aware of their location and spectrum use, and can change frequency, power level, transmission mode and modulation characteristics in response to changing conditions or "learned" owner preferences. The result will be cell phones capable of knowing where they are and automatically switching bands to log onto the nearest cellular network and negotiating a roaming agreement if necessary. For instance, upon landing in Europe, a phone could switch from CDMA to GSM technology, log onto the free WiFi network at the airport, and direct the user to the rental car desk. Upon request, it will even be able to find a nice, mid-priced Italian restaurant in the area and make reservations. In addition to learning from its user, a cognitive radio will also be able to learn from other cognitive radios in the area – for instance learning the calling frequencies and protocols for emergency services in a new city, just in case they're needed. So the big question is, at what point is your cell phone smarter than you?

24.8 MAC OS

Category 24.8 MAC OS

2006-01-26 DHS Daily OSIR; http://www.eweek.com/article2/0,1895,1915923,00.asp

APPLE'S SWITCH TO INTEL COULD ALLOW OS X EXPLOITS.

The recent move by Apple Computer to begin shipping Macintosh computers that use microprocessors from Intel could open the door to more attacks against computers running the company's OS X operating system, security experts warn. The change could put more pressure on Apple to build security features into OS X. In an e-mail statement, the company said that the security technologies and processes that have made Mac OS X secure for PowerPC remain the same for Intel-based Macs. However, using the Intel x86 platform pulls Macintosh systems onto the same platform used by Microsoft's Windows computers, a prime target of the hacking community for years. "Attackers have been focused on the [Intel] x86 for over a decade. Macintosh will have a lot more exposure than when it was on PowerPC," said Oliver Friedrichs, a senior manager at Symantec Corp. Security Response. There are many more malicious hackers who understand the x86 architecture in-depth than understand the PowerPC. And attackers have access to hundreds of documents and examples of how to exploit common vulnerabilities on x86, whereas exploits for PowerPC are far fewer, Friedrichs said.

Category 24.8 MAC OS

2006-03-07 DHS Daily OSIR; http://news.com.com/Mac+OS+X+patch+faces+scrutiny/2100-1002_ 3-6046588.html?tag=cd.top

MAC OS X PATCH FACES SCRUTINY.

An Apple Computer patch released last Wednesday, March 1, that doesn't completely fix a high-profile Mac OS X flaw, leaving a toehold for cyber attacks, experts said. The update added a function called "download validation" to the Safari Web browser, Apple Mail client, and iChat instant messaging tool. The function warns people that a download could be malicious when they click on the link. Before that change, clicking on a link could have resulted in the automatic execution of code on a Mac. But Apple failed to address a key part of the problem; the fix should be at a lower, operating system level, experts said. It is now still possible for hackers to construct a file that appears to be a safe file type, such as an image or movie, but is actually an application, they said.

Category 24.8 MAC OS

2006-04-06 DHS Daily OSIR; http://www.techweb.com/wire/security/184429499

MAC USERS MAY MEET WINDOWS THREATS.

Users installing Windows XP on Intel-based Macs face some special security issues, a security expert said Thursday. By applying Apple Computer's just-released Boot Camp, Mac owners can now create a dual-boot system that runs either Mac OS X or Windows XP. It's the latter that worries Ken Dunham, the director of the rapid response team at security intelligence firm iDefense. "When a Mac is booted into Windows, it can be attacked by the same [exploits] that threaten any Windows PC," said Dunham. "If you're running an unpatched version of Windows XP on any box, it'll be hacked pretty quickly." But it's not the vulnerability of Windows that concerns Dunham; it's the fact that the Mac will have multiple operating systems on its hard drive. Typically, argued Dunham, people are less diligent about updating their secondary system.

Category 24.8 MAC OS

2006-05-12 DHS Daily OSIR; http://www.uscert.gov/cas/techalerts/TA06-132A.html

US-CERT TECHNICAL CYBER SECURITY ALERT TA06-132A: APPLE MAC PRODUCTS AFFECTED BY MULTIPLE VULNERABILITIES.

Apple has released Security Update 2006-003 to correct multiple vulnerabilities affecting Mac OS X, Mac OS X Server, Safari Web browser, Mail, and other products. The most serious of these vulnerabilities may allow a remote attacker to execute arbitrary code. Impacts of other vulnerabilities include bypassing security restrictions and denial of service. Systems affected: Apple Mac OS X version 10.3.9 (Panther) and version 10.4.6 (Tiger); Apple Mac OS X Server version 10.3.9 and version 10.4.6; Apple Safari Web browser; Apple Mail. Previous versions of Mac OS X may also be affected. Please see Apple Security Update 2006-003 for further information. Apple Security Update 2006-003 resolves a number of vulnerabilities affecting Mac OS X, OS X Server, Safari Web browser, Mail, and other products. Further details are available in the individual US-CERT Vulnerability Notes: VULNERABILITY#519473: http://www.kb.cert.org/vuls/id/519473 Solution: Install Apple Security Update 2006-003: http://docs.info.apple.com/article.html?artnum=303737 This and other updates are available via Apple Update: http://docs.info.apple.com/article.html?artnum=303737 For additional protection, disable the option to "Open 'safe' files after downloading," as specified in "Securing Your Web Browser": http://www.us-cert.gov/reading_room/securing_browser/#sgeneral

Category 24.8 MAC OS

2006-06-08 EDUPAGE; New York Times (registration req'd)
http://www.nytimes.com/2006/06/09/technology/08cnd-apple.html

ITUNES IN TROUBLE IN EUROPE

Government regulators in several European countries are taking Apple to court over the way its iTunes music service functions. Norwegian officials have said that Apple's user agreement violates the country's law and that the inability to play iTunes songs on non-Apple devices likely also is illegal in Norway. Specifically at issue are parts of Apple's user agreement that give the company the right to change the terms without notice and that free Apple from any liability for viruses or other harm caused by iTunes downloads. Bjorn Erik Thon, director of the Consumer Ombudsman's Office of Norway, said his office would hear Apple's counterargument concerning whether iTunes songs should be playable on non-Apple equipment, but he added that he expects the office to rule against Apple.

Thon rejected an earlier claim by Apple that limiting the songs to Apple devices discourages copyright violations. If consumers cannot play songs they have bought, said Thon, "they will get a download of it free from Napster," increasing piracy.

Government officials in Sweden and Denmark are expected to follow Norway's lead in these affairs, and Britain reportedly also shares the same concerns.

Category 24.8 MAC OS

2006-06-14 EDUPAGE; CNET http://news.com.com/2100-1047_3-6083590.html
<http://www.educause.edu/email/edupage/ep061406/track.asp?id=story_2>

IPOD UNDER SCRUTINY FROM ITC

According to Creative Technology, the U.S. International Trade Commission (ITC) will investigate whether the extremely popular iPod device infringes on a patent held by Creative. Creative, based in Singapore, and its U.S. Subsidiary have filed two lawsuits alleging that the iPod infringes on a user-interface patent Creative holds for its own portable music devices. Creative is seeking a permanent cease-and-desist order from the courts against Apple Computer. The ITC, which reviews some patent disputes, will assign the case to an administrative law judge. After that judge makes a recommendation on the matter, the ITC will decide whether to proceed. The process typically takes between 12 and 15 months.

Category 24.8 MAC OS

2006-06-27 DHS Daily OSIR; CRN http://www.crn.com/sections/breakingnews/breakingnews.jhtml

APPLE FIXES VULNERABILITIES IN OS X UPDATE.

Apple Tuesday, June 27, released Mac OS X version 10.4.7, which fixes several security vulnerabilities that at least one security vendor rated as serious. Although the issues don't affect OS X versions prior to 10.4., and no exploits have been reported, Symantec assigned its highest severity rating -- 10 out of 10 -- to the vulnerabilities in an advisory issued Tuesday afternoon to subscribers of its DeepSight Threat Management System.

Category 24.8 MAC OS

2006-07-06 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,1985712,00.asp

NEW MAC OS FEATURE RAISES PRIVACY CONCERNS.

Some Apple users are wondering if their privacy is being compromised after installing an updated version of the company's Mac OS X --Version 10.4.7 --that aims to help authenticate desktop widgets. Apple's Dashboard Advisory, another security feature in the recent update, was designed to ensure that the widgets users download are legitimate and authorized by the company that created them. The debate about Mac OS comes at a sensitive time as IT vendors' efforts to track online computing activity, particularly without giving warnings, are raising users' ire and triggering legal action. John Pescatore, an analyst with market research firm Gartner, said these types of issues come at a time when there is a growing debate about balancing end users' security and privacy concerns. Pescatore said the best option for software companies is to ensure that they clearly explain every feature to customers and offer people the option to opt out. "If you sneak it in, it's automatically wrong," Pescatore said on July 6.

Category *24.8* *MAC OS*

2006-08-21 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2162657/hackers-let-apple-hook-macbook

HACKERS CLEAR APPLE OVER MACBOOK ATTACK.

Security researchers who demonstrated a so-called vulnerability in an Apple MacBook at the Black Hat conference in Las Vegas have cleared Apple's name in security circles. David Maynor and Jon Ellch, who work for security firm SecureWorks, performed a 60-second hack on a MacBook earlier this month to demonstrate a vulnerability in the device drivers of several wireless cards, including what was thought to be Apple's. Although the news was widely reported as an attack on Apple's wireless drivers, the researchers have since posted a disclaimer revealing that the attack was performed via third-party software not shipped with the MacBook.

Category *24.8* *MAC OS*

2007-01-06 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2079624,00.asp

MAC OS X DEVELOPERS WATCH MONTH OF APPLE BUGS.

Developers of applications for Apple's Mac OS X have been watching the Month of Apple Bugs (MOAB) project closely, and are generally in favor of the project's goal of uncovering OS flaws. But they, and security companies, have questions about the MOAB group's method, which involves making their findings public immediately, instead of first alerting Apple Computer. "In the long term, this project is making OS X more secure," said Gus Mueller, a developer who sells his software through his company Flying Meat. "However, in the short term, these bugs, once shown, can be used destructively," he added. "I think the correct way to handle the exploits would have been to inform Apple, and give them something like four to six weeks to get a fix out," Mueller said.

24.9 Peer-to-peer networking

Category 24.9 Peer-to-peer networking

2006-11-29 EDUPAGE; San Jose Mercury News
http://www.siliconvalley.com/mld/siliconvalley/16122678.htm

BITTORRENT DEALS WITH STUDIOS TO OFFER VIDEO ONLINE

BitTorrent has made deals with Paramount, MTV Networks, 20th Century Fox, and smaller studios to permit its users to purchase or rent movies and buy TV shows when the new video service begins in February 2007. The company signed a similar agreement with Warner Brothers earlier this year. Initially, customers will be able to play the video downloads only on their computers, but the company plans to support downloads to portable devices in the future.

25.1 Remote control, RATs, reprogramming, auto-updates

Category 25.1 Remote control, RATs, reprogramming, auto-updates

2006-04-15 RISKS; Daily Telegraph http://tinyurl.com/e6668

RISKS OF DRIVE-BY-WIRE SYSTEMS FOR AUTOMOBILES

In March 2006, British motorist was trapped in his BMW at speeds of 130 mph for 26 minutes when his electronic accelarator linkage jammed at maximum throttle. He called police on his mobile phone and miraculously avoided crashing into any other cars on the heavily-travelled motorway during his terrifying trip up the A1 highway. He flipped the car at a roundabout but walked away uninjured.

Don Norman commented in RISKS,

>Seems that stuck throttles were a continual event with old, mechanical throttles. The electronic throttles have received numerous complaints, but all of the ones I could find were about "unintended acceleration". Doing a web search for "electronic throttle accident" (without the quotes) is quite revealing.

I still don't know enough about this class of potential accidents to offer definitive comment. But from what I can tell, automobile incidents will replace aircraft ones for the RISKS community. The more things change, …

Example:

The National Highway Transportation Safety Administration is investigating complaints that some Toyota Motor Corp. cars may suddenly accelerate or surge, causing one car to strike a pedestrian. The 2002 and 2003 Toyota Camry, Camry Solara and Lexus ES300 vehicles all come equipped with an electronic throttle control system, which the NHTSA said uses sensors to determine how much throttle is being applied.

The NHTSA said 30 crashes have been attributed to the problem, with four accidents resulting in five injuries. The crashes "varied from minor to significant and may have involved other vehicles and/or building structures." The preliminary investigation is the first step in the investigative process. The NHTSA will contact Toyota to ask for documents pertaining to the issue, and could upgrade the investigation to an engineering analysis. More than 1 million Toyotas are covered by this investigation, according to the agency.

Toyota officials could not immediately be reached for comment.<

25.2 Jamming

Category 25.2 Jamming

2006-10-05 DHS Daily OSIR; Reuters http://today.reuters.com/news/articlenews.aspx?type=topNews&storyid=2006-10-05T164730Z_01_N02361333_RTRUKOC_0_US-ARMS-SPACE.xml

CHINA JAMMING TEST SPARKS U.S. SATELLITE CONCERNS.

China has beamed a ground-based laser at U.S. spy satellites over its territory, a U.S. agency said, in an action that exposed the potential vulnerability of space systems that provide crucial data to American troops and consumers around the world. The Department of Defense remains tight-lipped about details, including which satellite was involved or when it occurred. The Pentagon's National Reconnaissance Office Director Donald Kerr acknowledged the incident two weeks ago, first reported by Defense News, but said it did not materially damage the U.S. satellite's ability to collect information. The issue looms large, given that U.S. military operations have rapidly grown more reliant on satellite data for everything from targeting bombs to relaying communications to spying on enemy nations. Critical U.S. space assets include a constellation of 30 Global Positioning Satellites that help target bombs and find enemy locations. This system is also widely used in commercial applications, ranging from car navigation systems to automatic teller machines. The Pentagon also depends on communications satellites that relay sensitive messages to battlefield commanders, and satellites that track weather in critical areas so U.S. troops can plan their missions.

Category 25.2 Jamming

2007-03-09 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article97887-03-09-07-Web

ARMY CAN NOW JAM IEDS WITHOUT DISRUPTING COMMUNICATIONS.

With the help of the Navy, the Army is now able to operate improvised explosive device (IED) jammers in Iraq without disrupting its communications equipment, according to a senior Army officer. IED jammers, such as the Counter Radio-Controlled Improvised Explosive Device Electronic Warfare systems, can cause the loss of all communications from co-located or nearby tactical radio systems, Naval Sea Systems Command said. The radio systems also can render the jammers ineffective. Until recently, soldiers in Iraq were turning off the jammers to communicate, said Gen. William Wallace, head of the Army's Training and Doctrine Command. But on his recent trip to the Middle East, Wallace heard no complaints about IED jammers, he said. The Navy experts taught Army soldiers how to remove conflicts from the frequency spectrum so that IED jammers and communications equipment can be used simultaneously in the same environment, Wallace said. IEDs remain the single greatest cause of casualties to U.S. forces in Iraq. The Department of Defense has asked for $4 billion in funding in its fiscal 2008 budget and $2.4 billion in its fiscal 2007 supplemental budget to counter the devices.

25.3 RFI, HERF, EMP/T

Category 25.3 *RFI, HERF, EMP/T*

2006-01-26 DHS Daily OSIR; NewScientist http://space.newscientist.com/article/dn11033-mysterious-source-jams-satellite-communications.html

MYSTERIOUS SOURCE JAMS SATELLITE COMMUNICATIONS.

Paris-based satellite company Eutelsat is investigating "unidentified interference" with its satellite broadcast services that temporarily knocked out several television and radio stations. The company declined to say whether it thought the interference was accidental or deliberate. The problem began Tuesday afternoon, January 23, blocking several European, Middle East and northeast African radio and television stations, as well as Agence France-Presse's news service. All transferred their satellite transmissions to another frequency to resume operations. Theresa Hitchens of the Center for Defense Information think-tank in Washington, DC, says there have been cases of deliberate satellite jamming in the past, but it is hard to see what motivation there would be in this instance. "It's really puzzling to me," she said. "If it was accidental, why would they be so secretive about saying what the source was and if it's deliberate, you've got to wonder why -- it just seems to me to be an odd target..." she says.

Category 25.3 *RFI, HERF, EMP/T*

2006-04-20 RISKS; Chaos Computer Club https://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN)

RFID ZAPPERS

The Chaos Computer Club of Germany had a discussion of RFID Zappers at its 22nd Chaos Communication Congress in December 2005 in Berlin. Al Mac provided a summary:

…[S]ome hobbyist has come up with what it takes for a paranoid person to obliterate any RFID tags that might be on consumer merchandise, or where not expected or wanted….

I imagine that there will be a consumer market for this.

People who want one but do not have the personal what it takes to build stuff in their garage with assurance the contraption works right, and that they not injure themselves before getting it completed. Call this a niche industry that will attract a lot of imitators. To be profitable it needs mass production like on a circuit board assembly line.

* Then the next market needed will be some way to assure purchasers that the RFID Zapper that THEY got really works.
* Then the next society development will be that objects where RFID was inserted for purposes of identification, like in ID cards, Passports etc. Will malfunction because someone had used the RFID Zapper on them, rendering those people's ID unusable for the intended purposes.
* Then stores, and other institutions, will have to institute rules that people are not allowed to enter their premises carrying an RFID Zapper, so as to prevent unauthorized usage on the store merchandise.
* Then the next result might be that RFID Zappers will get declared to be illegal … although I expect this will be a few years away … the effort to illegalze RFID Zappers may get a lot more attention from the general public than the usual illegalization of technology tools.

There have been several problems with RFID deployment so far.
* There is the mass public panic over conspiracy theories, leading to a ton of Urban Legends, of which there is a glimmer of validity at the fringes. There are in fact some risks of abuse, but they are relatively small risks compared to the frenzy of claims out there.
* There's recent threads on the notion that el cheapo implementation can lead to security holes, where RFID is no exception to that risk, such as susceptibility to malware.
* Spread of the RFID Zapper into society and its effects will become problem area # 3.

Al Mac also pointed to the CAUTION section, which he described as" = ROFL." That section follows, idiosyncratic spelling and all.

>Caution

(This part of this article probably will be longer than the equivalent part in the german article, since english-speaking peoble seem to be more concerned with safety matters and less careful with electric devices ;-)

* Poldi kindly informed us, that having a RFID-Zapper with you when checking in to a plane might cause trouble or even get you arrested (he almost was). RFID-Zappers are basically some kind of pocket-EMP. Although we doubt that it has the capacity to cause any trouble aboard an airplane, we seriously recommend against testing it, for reasons of your own health as well as that of others.

* RFID-Zappers don't comply with the FCC-rules.

* Modifying a single-use-camera into a RFID-Zapper isn't completely free of risks. If the capacitor is still charged fully or partly, you might catch yourself an electric shock. If you are a healthy, young person, this is probably only going to hurt a lot, but if you should have any kind of problems with your heart and/or circulation, you definetly want to properly decharge the capacitor first. If you use a bigger capacitor, the risk increases.

* Soldering irons are known to be unpleasantly hot at the tip.

* We also recommend against using the RFID-Zapper on RFID-Tags found within electrical devices, for these are likely to suffer damage too. You also shouldn't use RFID-Zappers too near to electric devices, especially if they are expensive. You also shouldn't use it near any magnetic data storage, like floppy disc, MCs, hard discs, credit cards, streamer-cartridges and so on. And don't try it near your grandpa's pacemaker or other sensitive medical equipment either!

* We don't think that the RFID-Zapper is a strong source of what is known in Germany as Elektrosmog, which means some kind of smog caused by electromagnetic fields. But if you are concerned about it, you might want to be careful. Unfortunately we can't tell you wether wearing a hat of aluminium helps or not.

* The RFID-Zapper might cause you to feel armed against companies or governments trying to compromise your privacy. You might even experience euphoria, especially when destroying RFID-Tags. This could lead to dangerous behavior, like speaking your mind, using freedom of speech, fighting for your rights, all of which are bound to ultimately lead to the communist world revolution ;-)
* Shoplifting: No. This tool was not constructed as a burgular tool and is not to be used as. Besides, shops do not use RFID-Chips for eletronic theft prevention. However, it may be considered as such as a result of unknowledge.<

Category 25.3 RFI, HERF, EMP/T

2007-03-07 DHS Daily OSIR; Government Technology
http://www.govtech.net/news/news.php?id=104292

CONFLICTING SIGNALS CAN CONFUSE RESCUE ROBOTS.

Prototypes and commercial models of urban search and rescue robots will soon begin to work rubble piles across the country. Too many of these lifesaving robots, however, could be too much of a good thing, according to researchers at the National Institute of Standards and Technology (NIST), who report that the radio transmissions of multiple robots can interfere with each other and degrade search and rescue performance. The NIST report lists a number of ways to improve urban search and rescue wireless communications. Options, some of which are currently being investigated by robot manufacturers, include changes in frequency coordination, transmission protocols, power output, access priority, and using relay transformers to increase the range of wireless transmissions. The researchers also suggest establishing new access schemes or software-defined radios that allow interoperable communications.
Report: http://www.nist.gov/public_affairs/techbeat/tb2007_0301.htm#robots

26.1 Spyware, Web bugs & cookies

Category 26.1 Spyware, Web bugs & cookies

2006-01-05 EDUPAGE; http://www.internetnews.com/bus-news/article.php/3575421

FTC WINS SETTLEMENT FOR BOGUS ANTISPYWARE SCHEME

The operators of two supposed antispyware products agreed to pay nearly $2 million to settle complaints by the Federal Trade Commission (FTC) that the products amounted to nothing more than a scam. Last year, the FTC charged the operators of Spykiller and Spyware Assassin with running similar schemes to defraud consumers. According to the FTC, both companies used pop-up ads and e-mail to draw consumers to the companies' Web sites, where users could supposedly receive free scans of their machines. After the scans reported spyware, which frequently did not exist, users were offered a spyware-removal service for around $30-40. The removal also did not do what was advertised, said the FTC. In addition, many of the e-mail messages violated provisions of the CAN-SPAM Act. The makers of Spyware Assassin agreed to pay $76,000, which represents the amount the FTC spent on its investigation. Makers of Spykiller will pay $1.9 million.

Category 26.1 Spyware, Web bugs & cookies

2006-01-13 Effector Online; BoingBoing
http://www.boingboing.net/2006/01/11/steve_jobs_apple_dis.html

ITUNES "PHONE HOME" FEATURE PART OF DANGEROUS DATA COLLECTION TREND.

This week at MacWorld, Apple unveiled version 6.0.2 of iTunes, which it simply claimed "includes stability and performance improvements over iTunes 6.0.1." Among these so- called improvements is the Apple iTunes MiniStore--a localized "recommendation" engine that would look at what you listen to and then suggest additional songs and artists you might like. The MiniStore arrives turned on by default without asking a user's permission first. However, as news reports have revealed this week, it appears that the MiniStore also automatically transmits your listening information over the Internet back to the Apple Mothership. What Apple does with this information is unknown, although Apple has represented that it is not collecting data on its users--yet. Nor has Apple disclosed the steps it takes to prevent disclosure or leakage of the information to third parties. Ironically, this news comes on the heels of the recent Sony BMG DRM fiasco, a part of which included an undisclosed "phone home" feature of its own. While the Apple MiniStore isn't a rootkit DRM, it is part of a dangerous trend EFF has been witnessing in the digital music space market. When companies like Apple and Sony BMG start adjusting or installing software to micro-monitor our personal and private actions, even under the rubric of convenience, it is just one short stop down the road toward attempting to condition and control our behavior. All it takes is an enforcement protocol to turn recommendations into restrictions overnight. If companies like Apple are truly about user empowerment, they must watch this trend closely and remain on the right side of it. Allowing users to upload information voluntarily and expressly with adequate privacy protections is pro-user; surreptitiously siphoning it into a remote database without any privacy guarantees is not. It's time for Apple to pick a side of the line and walk it. Note: You can turn off the Apple MiniStore by hitting Shift- Command-M, or choose Edit: Hide MiniStore. EFF recommends that iTunes users do so until Apple at least comes clean about its MiniStore data practices.
More from Macworld: http://www.macworld.com/weblogs/editors/2006/01/ministore/
More from BoingBoing: http://www.boingboing.net/2006/01/11/steve_jobs_apple_dis.html

Category 26.1 Spyware, Web bugs & cookies

2006-02-06 DHS Daily OSIR; http://www.securityfocus.com/brief/128

STUDY: SPYWARE REMAINS RAMPANT AS WINAMP EXPLOITED.

A new study by the University of Washington finds that one in twenty executables on the Internet contain spyware. The study, which sampled more than 20 million Internet addresses, also found other disturbing trends. Among them: one in 62 Internet domains contains "drive-by download attacks," which try to force spyware onto the user's computer simply by visiting the Website. The problems for Web surfers primarily affect Microsoft's Internet Explorer browser but exist to a lesser extent for other browsers as well.

University of Washington study: http://www.cs.washington.edu/homes/gribble/papers/spycrawler.pdf

Category 26.1 Spyware, Web bugs & cookies

2006-03-17 DHS Daily OSIR; http://www.infoworld.com/article/06/03/17/76590_HNspycar_1.html

NEW SPYCAR SOFTWARE WILL TEST ANTISPYWARE.

With security experts warning of "rogue" antispyware products that sometimes do more harm than good, two security researchers have decided to take matters into their own hands. They're working on a new software product, called Spycar, that will test the effectiveness of antispyware products. Spycar will contain about 25 small programs, each of which engages in the kind of nasty behavior normally associated with spyware. The software will then undo all of the changes it has made after the testing has been completed. Spycar will be available free of charge in May. More information will be made available on the http://www.intelguardians.com Website at that time.

Category 26.1 Spyware, Web bugs & cookies

2006-03-20 DHS Daily OSIR; http://www.infoworld.com/article/06/03/20/76629_HNspywarepan el_1.html

PANEL EXPLORES ROOTS OF SPYWARE, ADWARE.

Following the money trail behind the flood of spyware and adware on the Internet poses some sticky questions around liability, said a panel of spyware experts at a workshop in New York City Friday, March 17. Legal experts, government officials and technology professionals gathered at New York University School of Law to discuss the causes of and solutions to unwanted software programs that track Internet users' behavior. One panelist suggested that companies advertising online should develop more thorough policies to control where their ads go on the Internet.

Category 26.1 Spyware, Web bugs & cookies

2006-03-20 DHS Daily OSIR; http://www.infoworld.com/article/06/03/20/76595_HNbadware_1. html

TOUGH WEEK AHEAD FOR 'BADWARE' COMPANIES.

The fight against invasive software will take a step forward this week as the Center for Democracy and Technology (CDT) and the Google-backed Stopbadware Coalition will release two separate reports that state the names of undesirable software programs and the advertisers who help fund them. On Monday, March 20, the CDT will publish its report on the major advertisers who are behind so-called "adware" software. Two days later, the Stopbadware Coalition is set to release its first report, which will name several software programs to its Badware Watch List.

Category 26.1 Spyware, Web bugs & cookies

2006-03-21 DHS Daily OSIR; http://www.eweek.com/article2/0,1895,1940747,00.asp

SPYWARE TRAIL LEADS TO KAZAA, BIG ADVERTISERS.

The StopBadware.org coalition, funded by Google, has listed the Kazaa file-sharing application at the top of a list of noxious software programs that present a threat to business and consumer users. The coalition, which counts Sun Microsystems and Lenovo among its sponsors, will recommend in its inaugural Badware Report that users stay away from Kazaa and three other programs that can be combined with Trojans and bots for use in data theft attacks. Adware and spyware programs that come bundled with peer-to-peer applications present a huge security risk to corporate networks, and StopBadware.org says Kazaa's claim to be spyware-free cannot be trusted. In addition to Kazaa, StopBadware.org said computer users should stay away SpyAxe, a rogue anti-spyware program; MediaPipe, a download manager that offers access to media content; and Waterfalls 3, a screensaver utility. StopBadware.org Report: http://www.stopbadware.org/pdfs/badwarev1r3.pdf

Category 26.1 Spyware, Web bugs & cookies

2006-03-24 DHS Daily OSIR; http://www.eweek.com/article2/0,1895,1942497,00.asp

DO-IT-YOURSELF SPYWARE KIT SELLS FOR $20.

A do-it-yourself malware creation kit is being hawked on a Russian Website for less than $20, according to security researchers tracking the seedier side of the Internet. Virus hunters at SophosLabs discovered the spyware kit, called WebAttacker, on a Website run by self-professed spyware and adware developers. The WebAttacker kit includes scripts that simplify the task of infecting computers and spam-sending techniques to lure victims to specially rigged Websites.

Category 26.1 Spyware, Web bugs & cookies

2006-04-07 DHS Daily OSIR; http://www.theregister.co.uk/2006/04/07/unspypc/

WARNING OVER ROGUE ANTI-SPYWARE APPLICATION.

A rogue anti-spyware application is falsely identifying popular security products and file system tools as spyware. Security firm SurfControl advises not to use the application, UnSpyPC. False-positive reporting is hardly unknown across many supposed anti-spyware applications, as SurfControl notes, but this case is particularly severe since UnSpyPC could disable critical security and business applications.

Category 26.1 Spyware, Web bugs & cookies

2006-05-16 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,1963097,00.asp

RESEARCHERS WARN OF FAKE ANTI-SPYWARE

The latest report issued by Finjan's Malicious Code Research Center highlights the growth of several emerging breeds of cyber-attack, including the increasing popularity of so-called "ransomware" and viruses that are being spread via fake anti-spyware applications. The anti-virus software maker's research arm said in its Web Security Trends Report, issued on May 16, that the growth of "rogue anti-spyware" and the emergence of hackers looking to hold stolen corporate data up for ransom are two of the fastest growing trends in the security threat landscape. Virus rootkits continue to pose one of the most prevalent and challenging obstacles for IT administrators to overcome, according to the study. In these attacks, hackers disguise the malware in programs advertised online as free anti-spyware applications. Once downloaded onto a user's computer, the applications may deliver their own payloads of malicious code or expose affected machines to subsequent attacks. In some cases, the false anti-spyware tools even run fake computer security scans that claim to find existing spyware programs on infected devices. The software then directs the computer's user to a Website where the user is encouraged to purchase a full version of the free application already on the PC.

To download report, follow link and click on “Security Trends Report”:
http://www.finjan.com/Content.aspx?id=827#SecurityTrendsReport

Category 26.1 Spyware, Web bugs & cookies

2006-06-13 DHS Daily OSIR; TechSpot http://www.techspot.com/news/21899-spyware-attacks-tripled-last-year.html

SPYWARE ATTACKS TRIPLED IN 2005

New research conducted by security company Aladdin's Content Security Response Team finds that the amount of spyware detected on the Internet is booming. The construction of spyware and Trojans now dominates malware production, with malware authors shifting their attention away from traditional computer viruses. Aladdin's report found that the number of malicious threats rose from 1,083 in 2004 to 3,389 in 2005. This represents a massive increase of more than 213 percent. Trojans grew from 1,455 in 2004 to 3,521 in 2005, which is a 142 percent rise. Shimon Gruper, vice president of technologies for the Aladdin eSafe Business Unit believes that this represents a fundamental shift for many criminals away from traditional crimes and into computer crime.

Aladdin eSafe CSRT 2005 Malicious Code Report: The Big Threats Shift -
http://www.aladdin.com/news/2006/eSafe/CSRT_Report.asp

Category 26.1 Spyware, Web bugs & cookies

2006-08-24 DHS Daily OSIR; Techworld http://www.techworld.com/news/index.cfm?newsID=6707&printerfriendly=1

UK TOPS SPYWARE INFECTION CHARTS.

The UK has the highest spyware infection rate of any European country, security vendor Webroot has said in its quarterly State of Spyware report. The report, based on an international survey of enterprise and consumer PCs, found that spyware infections are again on the rise after a lull last year. Said Webroot chief executive C. David Moll, "Spyware is a financially motivated threat and as long as there is a dollar to be had, cyber criminals will do everything possible to steal it." The UK took over from Ireland at the top of the spyware charts for the second quarter of 2006, with an average of 30.5 pieces of spyware per PC. Ireland followed with 30.3 spies per PC, Lithuania with 29.3and Latvia with 26.5. The worldwide average was 24.5 spies per PC. While Webroot and others say the targeting of English-language countries is a big factor upping the infection rate, the U.S. scored lower than the UK with an average of 30 spies per PC.

Category *26.1* *Spyware, Web bugs & cookies*

2006-09-06 DHS Daily OSIR; Federal Trade Commission http://www.ftc.gov/opa/2006/09/enternet.htm

FTC SHUTS DOWN SPYWARE OPERATION.

An operation that placed spyware on consumers' computers in violation of federal laws will give up more than $2 million to settle Federal Trade Commission (FTC) charges. The FTC said Wednesday, September 6, that it has obtained a settlement order against Enternet Media Inc., Conspy & Co. Inc., Lida Rohbani, Nima Hakimi, and Baback Hakimi, all based in California. The defendents distributed software called Search Miracle, Miracle Search, EM Toolbar, EliteBar, and Elite Toolbar. According to the FTC's complaint, the Websites of the defendants and their affiliates caused "installation boxes" to pop up on consumers' computer screens. In one variation of the scheme, the boxes offered a variety of "freeware," including music files, cell phone ring tones, photographs, wallpaper, and song lyrics. In another, the boxes warned that consumers' Internet browsers were defective, and offered free browser upgrades or security patches. Consumers who downloaded the supposed freeware or security upgrades did not receive what they were promised; instead, their computers were infected with spyware that interferes with the functioning of the computer and is difficult for consumers to uninstall or remove.

Category *26.1* *Spyware, Web bugs & cookies*

2006-10-09 DHS Daily OSIR; Daily Mail (UK) http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=409289&in_page_id=1770

HOME COMPUTERS TARGETED BY HACKERS 50 TIMES A DAY.

Home PCs could be under attack from hackers over 50 times a night, suggests a BBC News Website experiment. The BBC News Website team set up a 'honeypot' PC -- a computer that looks like a normal PC online but records everything that's done to it -- in order to find out the dangers facing Web users. Every single time the 'honeypot' was put online it was attacked. In one of the busiest nights of malicious online activity, the computer was attacked 53 times. The results: one hijack attempt that would have handed over control of the machine to a hacker; two "port scans" which look for weak spots in Windows software -- reconnaissance by hackers seeking new victims; eleven attacks by the 'Blaster' worm -- success would have rendered the machine unusable; three attacks by the 'Slammer' worm -- success would have left machine crippled and prone to crashing; 36 fake security announcements for fake security software posing as warnings, which could leave a PC clogged with spyware. Over the course of the whole experiment, on average at least one attack an hour came from a dangerous computer bug with the ability to cripple an unprotected PC.

Category *26.1* *Spyware, Web bugs & cookies*

2006-10-11 DHS Daily OSIR; USA TODAY http://news.yahoo.com/s/usatoday/20061012/tc_usatoday/cybercrimeflourishesinonlinehackerforums;_ylt=AjXO89GuCYldzVhBWj97Z8IjtBAF;_ylu=X3oDMTA0cDJlYmhvBHNlYwM

CYBERCRIME FLOURISHES WITH ONLINE HACKERS.

Cybercrime forums gird a criminal economy that robs U.S. businesses of $67.2 billion a year, according to an FBI projection. Over the past two years, U.S. consumers lost more than $8 billion to viruses, spyware and online fraud schemes, Consumer Reports says. In 2004, a crackdown by the FBI and U.S. Secret Service briefly disrupted growth of the forums. But they soon regrouped, more robust than ever. Today, they are maturing -- and consolidating -- just like any other fast-rising business sector, security experts and law enforcement officials say. Security firms CardCops and RSA Security, EMC, and volunteer watchdog group Shadowserver observed the forced mergers, as well, and compiled dozens of takeover-related screen shots. Forum leaders have become increasingly selective about accepting new members. "Vouching" for new members is now the norm, requiring a member in good standing to extend an invitation to new recruits. Veteran vendors and buyers typically do business in multiple forums simultaneously, in case any particular forum shuts down. Some forums have become known for their specialties, such as offering free research tools to do things such as confirming the validity of a stolen credit card number or learning about security weaknesses at specific banks.

Category 26.1 Spyware, Web bugs & cookies

2006-10-13 DHS Daily OSIR; Washington Post http://www.washingtonpost.com/wp-dyn/content/article/2006/10/12/AR2006101201744.html

HACKERS STEPPING UP PACE OF MICROSOFT EXPLOITS.

The cat-and-mouse game that Microsoft Corp. and hackers have been playing for years escalated last week, just as the software giant was addressing some of the biggest problems facing computer users. On Tuesday, October 10, the company released a record 26 security fixes for the Windows operating system and the widely used Office programs such as Word, Excel and Outlook. Thursday, October 12, hackers pounced again, posting on the Internet information about vulnerabilities in PowerPoint 2003, one of the Office programs widely used by business customers and increasingly used by students. Microsoft, whose products are the largest targets of hackers because its products are used on most computer systems, issues software updates to protect users' computers from the viruses, worms and spyware that are spread through their products via e-mail attachments and the Web. But because those patches are released on a regular schedule -- the second Tuesday of each month -- the people who expose and exploit the vulnerabilities in the programs tend to wait until a day or so after the monthly release to reveal other vulnerabilities they have discovered.

26.2 Adware & scumware

Category *26.2* *Adware & scumware*

2006-04-11 DHS Daily OSIR; http://www.it-observer.com/news/6058/web_rebates_steals_confidential_personal_information/

WEB REBATES SCUMWARE/SPYWARE A SECURITY RISK FOR COMPUTER USERS.

Security experts at MicroWorld Technologies are stating that a new variant of the "WebRebates" program, "Win32.WebRebates.s," is a serious security risk for computer users. WebRebates claims to offer rebates and discounts when purchasing items on Internet, however it's found to be a Spyware, Adware and a security hazard in many ways. This program monitors browser activity and other operations on your PC. It also pesters your computer with annoying pop-ups, apart from clogging your mailbox with spam. WebRebates comes bundled with many software utilities. Once installed, it tries to get additional malware from a series of Websites.

Category *26.2* *Adware & scumware*

2006-08-18 DHS Daily OSIR; IDG News Service http://www.infoworld.com/article/06/08/18/HNaoladware_1.html

AOL SECURITY TOOLS RAISE ADWARE QUESTIONS.

Just days after posting details of searches made by hundreds of thousands of subscribers, AOL is in hot water again with consumer advocates. This time the issue is with the company's Active Virus Shield anti-virus software, released last week. The software's licensing agreement authorizes AOL to gather and share data on how the software is being used and permits AOL and its affiliates to send e-mail to users. Although security experts say that the Active Virus Shield does not behave in a malicious fashion or serve up unwanted ads, some are concerned that the product's end user license agreement (EULA) would allow AOL to send spam or serve up adware at some point in the future. "If it actually does any of the things stated in the EULA, we would actually flag it as spyware," said Christina Olson, a project manager with Stopbadware.org.

Category *26.2* *Adware & scumware*

2006-09-03 DHS Daily OSIR; BBC http://news.bbc.co.uk/1/hi/technology/5310114.stm

"ADWARE" ATTACK ON PRIVACY TOOL.

Software that claimed to provide increased privacy while surfing the Web has been criticized by computer experts and the blogging community. The application Browzar has been branded "adware" by many because it directs Web searches to online adverts. When a user searches using the Browzar search engine or the search box, many of the results are for sponsored links or adverts. The paid-for sponsored links are generated by a program known as "Overture," which is used by many search engines and sites. But many of these sites keep sponsored links separate from search results. Browzar does not.

26.3 Keystroke loggers

Category 26.3 Keystroke loggers

2006-02-08 http://www.theregister.co.uk/2006/02/08/france_keylogs_losses/

RUSSIAN KEYLOGGERS HIT BANK CUSTOMERS: FRENCH BANKS LOSE €1M

John Oates wrote in _The Register_:

"Russian scammers used key logging Trojans to steal more than a €1m from French people accessing online bank accounts. The Trojans were sent by email but were not activated until people accessed their online bank accounts. Then the Trojan forwarded on user names and passwords to the crooks. The thieves then used the details to transfer funds to third party *mule* accounts. The worst individual loss was €40,000. French police were told in November 2004 and the scam lasted 11 months. Arrests have been made in Moscow and St Petersburg and several *Ukrainian masterminds* have also had their collars felt."

Mr Oates pointed to an article in The Guardian at
< http://www.guardian.co.uk/france/story/0,,1703777,00.html >
by Kim Willsher with more details.

Category 26.3 Keystroke loggers

2006-05-15 DHS Daily OSIR;
http://www.techweb.com/article/printableArticle.jhtml?articleID=187203291

KEYLOGGERS, SPYWARE CONTINUE TO STRIKE ENTERPRISES.

Nearly one in five enterprises have had workers' PCs infected with keyloggers, the worst kind of spyware, a survey released Monday, May 15 said. Keyloggers are a type of spyware, and are used to record keystrokes (and sometimes mouse movements as well) to capture information such as usernames and passwords. They're often planted on consumers' PCs by identity thieves, but are becoming a corporate problem, too. The poll, conducted by Harris Interactive for San Diego-based security vendor Websense, found that 17 percent of IT administrators said that one or more employees had launched a keylogger on their network. In last year's survey, only 12 percent of administrators had acknowledged that keyloggers infected their domains. Bots are also a major problem for corporations, as they are for consumers, the survey showed. Just over a third of administrators (34 percent) were confident that they could keep bots from infecting workers' PCs when those machines weren't connected to the company's network, while almost one in five (19 percent) said that they have had employees' work desktops or laptops hit by a bot.

Category 26.3 Keystroke loggers

2006-08-10 DHS Daily OSIR; Silicon
http://www.silicon.com/financialservices/0,3800010364,39161320,00.htm

SECURITY EXPERTS DOWNPLAY HSBC'S ONLINE BANKING FLAW.

Security professionals have questioned reports of a "serious flaw" in HSBC's online banking system. Researchers at Cardiff University claim to have discovered the flaw which, according to The Guardian, over two years left 3.1 million customers exposed due to a defect in how people access their online accounts. The vulnerability, which was not detailed in the researchers' report, relies on a hacker using a keystroke logger. Graham Cluley, senior technology consultant for antivirus company Sophos, said: "Unless Cardiff gives some more information, it's a non-story -- there's no meat on this." To access HSBC's banking Website, users are required to enter an alpha-numeric password, a date of birth then a PIN. Cardiff University claims that any account can be broken into within nine attempts of hacking the Website, though first the hackers would need to plant a keystroke logger on the victim's PC. Cluley added: "They could gather [PIN] digits in up to nine attempts but it doesn't seem a very effective way of doing this."

Category 26.3 Keystroke loggers

2006-08-10 EDUPAGE; BBC http://news.bbc.co.uk/2/hi/business/4778351.stm

UNIVERSITY RESEARCHERS FIND HOLE IN HSBC BANK

Researchers at the School of Computer Science at Cardiff University showed that with the help of keylogging software, they were able to access HSBC bank accounts in nine attempts. Although security experts agree that no system is completely secure, the announcement prompted some to call for tighter security at the financial institution. Michael Panhallurick of the Risk Advisory Group said, "Nine attempts suggests that HSBC's system is not robust enough." A spokesperson from HSBC said that the problem does not present "a viable route for fraudsters." Online thieves, he said, would be better off spending their efforts elsewhere rather than gaining access to individual accounts. Still, officials from HSBC said they would review their security procedures in light of the announcement.

Category 26.3 Keystroke loggers

2007-01-15 DHS Daily OSIR; eChannel Line (Canada)
http://www.echannelline.com/canada/story.cfm?item=DLY011507-5

KEYLOGGING UP 250 PERCENT IN TWO YEARS.

A new white paper from McAfee Inc's Avert Labs highlights the latest computer and online identity theft trends, and features major increases in keyloggers and phishing scams. Entitled "Identity Theft," the report notes that keyloggers increased by 250 percent between January 2004 and May 2006 while phishing alerts tracked by the Anti-Phishing Working Group multiplied 100-fold over the same period of time. Dave Marcus of McAfee Avert Labs said the increase in keyloggers is due to financial institutions being the biggest targets for malware writers. While keylogging and phishing are done by different people, Marcus said at the end of the day the rise in both is because their target is the same. The report noted that organized crime, petty criminals and terrorists are the groups most likely to conduct online identity theft attacks. Marcus said that what attracts these organizations is the sense of anonymity and the fact that there is very low-risk when it comes to identity theft. White paper: http://www.mcafee.com/us/local_content/white_papers/wp_id_th eft_en.pdf

Category 26.3 Keystroke loggers

2007-05-10 DHS Daily OSIR; CNET News
http://news.com.com/Cybercrooks+add+QuickTime%2C+WinZip+flaws+to+arsenal/2100-1002_3-6182981.html

CYBERCROOKS ADD QUICKTIME, WINZIP FLAWS TO ARSENAL.

Cybercrooks are trying to breach PCs through previously unexploited security holes in QuickTime and WinZip, security firm Symantec warned on Thursday, May 10. The attacks involve malicious Websites rigged with multiple exploits, Symantec said. The sites appear to be that of a trusted financial institution, but instead attempt to silently install keystroke-logging software, according to Symantec. Links to the sites are likely advertised in spam, it said. Symantec discovered the attacks when one of the PCs that it uses as bait was breached earlier this week. "This compromise was especially interesting, because the site made use of a QuickTime vulnerability discovered in January 2007 and a WinZip vulnerability discovered in November 2006," Symantec said. "Before our analysis, it was not known that these issues were being exploited in the wild." In addition to the QuickTime and WinZip flaws, the miscreants tried to breach the Symantec system via a pair of holes in Microsoft software, Symantec said. Fixes for all the vulnerabilities are available.

26.4 Cell/mobile phones tracking, eavesdropping & cameras

Category 26.4 Cell/mobile phones tracking, eavesdropping & cameras

2006-02-05 EDUPAGE; http://news.com.com/2100-1039_3-6035317.html

CELL PHONES AS TRACKING TOOLS

Companies that use cell phones to track people have seen significant increases in business in the past few years. In Britain, firms such as Followus and Verilocation frequently work with employers who want to keep tabs on staff, despite concerns that the service infringes on individuals' civil rights. Kevin Brown of Followus noted that his company's service requires the consent of those being tracked. Users must agree to having their cell phones tracked, and periodic messages are sent randomly to users reminding them that their movements are being followed. Officials at Verilocation pointed to such events as the bombings in London last summer as times when being able to locate all of your employees is highly valuable. Experts on business processes said being able to track employees can allow companies to provide better service to customers by, for example, letting them know exactly where a technician is and when he will arrive at a customer's home. Officials from Liberty, a civil rights group, were unconvinced, saying that employees' rights in the workplace have been eroded and that there is a significant risk that businesses will misuse tracking data.

Category 26.4 Cell/mobile phones tracking, eavesdropping & cameras

2006-03-29 DHS Daily OSIR; http://news.com.com/Spy+program+snoops+on+cell+phones/2100-1029_3-6055760.html?tag=nefd.top

SPY PROGRAM SNOOPS ON CELL PHONES.

New software, called FlexiSpy, released in March by Bangkok, Thailand-based Vervata, hides on cell phones and captures call logs and text messages. It is being sold as a way to monitor kids and spouses. The data captured is sent to Vervata's servers and is accessible to customers via a special Website. Security company F-Secure has labeled the software a Trojan. "This application installs itself without any kind of indication as to what it is," Jarno Niemela wrote on the Finnish antivirus maker's corporate blog Wednesday, March 29. In addition, FlexiSpy could be used by miscreants as part of malicious software that targets phones, Niemela wrote.

Category 26.4 Cell/mobile phones tracking, eavesdropping & cameras

2006-05-24 EDUPAGE; CBS News
http://www.cbsnews.com/stories/2006/05/24/tech/main1653702.shtml

CAMPUS LANDLINES GIVING WAY TO CELL PHONES

A growing number of colleges and universities are questioning their ongoing investments in providing landline phone services to students. Indeed, some institutions have decided to discontinue landlines altogether. Morrisville State College, for example, no longer offers landline service in dorms. While some universities rely on students to provide their own cell phones, the University of Cincinnati is working with a local phone company to provide free cell phones to all students. Frederick Siff, vice president and CIO at the university, noted that cell-phone technology makes them more attractive for a range of tasks than laptops. "Students don't carry laptops around constantly," he said, "but they always have their cell phones." Officials at other schools expressed concerns about eliminating landline service or limiting it to a few house phones in dorms. Although money spent on landlines could be reinvested elsewhere, some said that safety issues make a strong case for keeping wired phone service.

Category 26.4 Cell/mobile phones tracking, eavesdropping & cameras

2006-07-05 DHS Daily OSIR; Times-Picayune (LA) http://www.nola.com/news/t-p/frontpage/index.ssf?/base/news-6/1152079275187350.xml&coll=1

NATION'S 911 SYSTEMS: DUE FOR AN OVERHAUL.

While Louisiana's Statewide Interoperable Communication System Executive Committee is making progress setting up new radio communications for state and local rescue teams, it has not discussed how the public could send text or e-mail messages for emergencies. Michael Abiatti, chairman of the committee, said he is trying to figure out how it could be done. A new system to receive the messages would need the components, capacity and know-how among operators to make it work. The National Emergency Number Association has launched an effort called Next Generation E911 to examine the shortcomings of response mechanisms to emergency messages from cell phones by text message, automobile satellite-link radio systems, the Internet and voice phone systems over the Internet. "While the existing 911 system has been a success story for more than 30 years, it has been stretched to its limit as technology advances," according to an association report. "Unfortunately, the current 911 system was never intended to receive calls and data from these new and emerging technologies. As a result, it is being asked to perform functions it was not designed to handle. In short, the nation's 911 systems are in need of a significant overhaul."

Category 26.4 Cell/mobile phones tracking, eavesdropping & cameras

2006-07-13 EDUPAGE; New York Times (registration req'd) http://www.nytimes.com/2006/07/13/nyregion/13cnd-cellphone.html

SQUABBLE OVER CELL PHONES IN SCHOOL GOES TO COURT

Parents of public school kids in New York City have filed a lawsuit to overturn a ban on cell phones in schools. The ban, which was originally put in place in 1988 and concerned primarily pagers, was not widely enforced until recently, when schools added X-ray machines to help keep schools safe. Under the ban, cell phones can be confiscated and only returned to parents, who must go to the school to pick them up. Parents objected, saying cell phones represent a safety issue for kids and that the chancellor of schools overstepped his authority in banning the devices. School officials said students use cell phones for cheating, making drug deals, taking photos in locker rooms, and other inappropriate activities. The parents hoping to overturn the ban are looking to a case from the early 1990s in which the courts ruled that the school system went beyond its authority in distributing condoms to students. The argument, which the court accepted, was that such activity is properly under the purview of parents, not the school. Opponents of the cell phone ban contend that having a cell phone is similarly the decision of parents rather than school administrators.

Category 26.4 Cell/mobile phones tracking, eavesdropping & cameras

2006-08-24 DHS Daily OSIR; University of California-Davis http://www.news.ucdavis.edu/search/news_detail.lasso?id=7855

STEALTH ATTACK DRAINS CELL PHONE BATTERIES.

Cell phones that can send or receive multimedia files could be targeted by an attack that stealthily drains their batteries, leaving cellular communications networks useless, according to computer security researchers at University of California (UC)-Davis. Hao Chen, assistant professor of computer science at UC Davis, and graduate students Denys Ma and Radmilo Racic, found that the Multimedia Messaging Service protocol can be used to send packets of junk data to a cell phone. Every time the phone receives one of these packets, it "wakes up" from standby mode, but quickly discards the junk packet without ringing or alerting the user. Deprived of sleep by repeated pulses of junk data, the phone's batteries run down up to 20 times faster than in regular use.

Category 26.4 Cell/mobile phones tracking, eavesdropping & cameras

2006-10-02 DHS Daily OSIR; Reuters http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9003788&intsrc=news_ts_head

SCREAMING CELL PHONES AIM TO CUT DOWN THEFTS.

A new phone security system may work to halt a spiraling rise in phone theft in the UK. The system sets off a high pitch scream, permanently locks the handset and wipes all data if reported stolen. The Remote XT technology, designed to make phones unusable and therefore worthless if they are stolen, works by installing software onto the operating system of the device that can be activated via a call to a call center once users realize their phone has been stolen or lost. The phone is then remotely disabled, all the data held on it is wiped and a high-pitched screech is triggered. According to UK government statistics, mobile phone theft has risen 190 percent in recent years, with one third of all UK robberies now solely involving mobile phones. The software currently works only on "smart phones" that run operating systems such as Symbian or Windows Mobile. But it is expected to be suitable for the majority of phones within two years.

Category 26.4 Cell/mobile phones tracking, eavesdropping & cameras

2006-12-01 Cnet News.com http://news.com.com/2100-1029_3-6140191.html

FBI USES REMOTE ACTIVATION OF CELL-PHONE MICROPHONES FOR SURVEILLANCE

In December 2006, Declan McCullagh and Anne Broache reported on c|net News.com that ruling by US District Judge Lewis Kaplan revealed the use of remote activation of mobile-phone microphones in an investigation of the Genovese organized-crime family. The surveillance technique "functioned whether the phone was powered on or off" according to the Judge and the reporters noted that "Some handsets can't be fully powered down without removing the battery; for instance, some Nokia models will wake up when turned off if an alarm is set." Security experts quoted in the article said that some phones had been rigged with small microphones and transmitters but that others were susceptible to software downloads that allowed remote control of the microsphones. "Because modern handsets are miniature computers, downloaded software could modify the usual interface that always displays when a call is in progress. The spyware could then place a call to the FBI and activate the microphone--all without the owner knowing it happened." The authors noted that criminal hackers have also used this feature and cited the case of a Trojan Horse that activated webcams.

Category 26.4 Cell/mobile phones tracking, eavesdropping & cameras

2007-01-11 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article97333-01-11-07-Web

NAVY NEXT-GENERATION E-WARFARE TARGETS CELLULAR SPECTRUM.

The Office of Naval Research (ONR) has asked industry to help develop next-generation electronic warfare technologies that will extend the Navy's e-warfare dominance over a broader range of spectrum, including frequency bands used by cell phone companies, FM radio and TV stations. ONR said it also wants to develop the capability to detect, locate, track and counter radio frequency emitters beyond the traditional scope of Navy and Marine Corps e-warfare systems. Both services operate EA6B Prowler aircraft that fly e-warfare missions to support all military services. The goal of e-warfare is to control the electromagnetic spectrum by exploiting, disrupting or denying enemy use while ensuring that friendly forces can use it, ONR said.

Category 26.4 Cell/mobile phones tracking, eavesdropping & cameras

2007-04-17 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2115133,00.asp

WIRELESS PROBLEMS PLAYED PART IN CHAOS AT VIRGINIA TECH.

The inability of students and others at Virginia Tech in Blacksburg, VA, to make cell phone calls during the April 16 shooting tragedy added to the chaos surrounding the events of the day. Many students reported being unable to gain access to the wireless phone system either to place a voice call or to send text messages. The reason appeared to be due to a massive increase in wireless call volume, according to carriers serving the Virginia Tech campus. Verizon Wireless spokesperson John Johnson acknowledged that for awhile during the heaviest call volumes on April 16, some calls did not go through. "We did see some call blocking," Johnson said. "We did also see some heavy text message traffic." Cingular/AT&T's Mark Siegel said that his company also saw very heavy call volumes, but saw no call blocking. "We had no problems with text messaging," Siegel noted. "It's a great alternative in these situations." Part of the problem, notes Verizon's Johnson, is that wireless companies have to build their networks to handle the demand that they anticipate. "We are engineered to handle heavy call volume there [Blacksburg]. But of course you can't engineer for a tragedy on this scale," he said.

Category 26.4 Cell/mobile phones tracking, eavesdropping & cameras

2007-04-24 DHS Daily OSIR; Associated Press
http://news.yahoo.com/s/ap/cell_phones911;_ylt=AiDD_TVK2WCgcKBpP3MhfKwjtBAF

RESCUERS OFTEN CAN'T FIND 911 CALLERS.

A new report by a public safety group throws into question the ability of police and firefighters to locate people through their cell phones when they dial 911 in an emergency. The study is believed to be the first independent evaluation of wireless location technology and sends a clear message: Do not assume rescuers will know where you are if you call 911 from a cell phone. The report was commissioned by the Association of Public Safety Communications Officials International, a group that has long been concerned about the limitations of the technology and the public's unrealistic expectations of what it can deliver. The Associated Press was given an advance copy of the study, which will be officially released in May. While the report pointed out the generally poor performance of the wireless industry in locating 911 callers, it also pointed out a need for 911 call centers to work closely with providers and the importance of public education. A new generation of telephone customers is being raised without using land-based telephone lines. But they still expect rescuers to be able to find them.

26.6 RFID tags

Category 26.6 RFID tags

2006-03-15 DHS Daily OSIR; http://www.nytimes.com/2006/03/15/technology/15tag.html?ex=1300078800&en=24f421ff24864376&ei=5090&partner=rssuserland&em c=rss

STUDY SAYS CHIPS IN ID TAGS ARE VULNERABLE TO VIRUSES.

A group of European computer researchers have demonstrated that it is possible to insert a software virus into radio frequency identification tags (RFIDs), part of a microchip-based tracking technology in growing use in commercial and security applications. In a paper entitled, "Is Your Cat Infected With a Computer Virus?," to be presented Wednesday, March 15, at an academic computing conference in Pisa, Italy, the researchers plan to demonstrate how it is possible to infect a tiny portion of memory in the chip, which can hold as little as 128 characters of information. Until now, most computer security experts have discounted the possibility of using RFID chips to spread a computer virus because of the tiny amount of memory on the chips. Ultimately, by their research, they have introduced a series of worrisome prospects, including the ability of terrorists and smugglers to evade airport luggage scanning systems that will use RFID tags in the future.

Category 26.6 RFID tags

2006-04-26 INNOVATION (SciTech Today 14 Apr 2006) <http://www.sci-tech-today.com/story.xhtml?story_id=10300AQR2C8F>

SMARTBALL

The use of RFID (radio frequency identification) tags is by now well-established in shipping, retailing, and other business applications that have requirements to track the precise location of parcels or inventory. Well, why not apply the same technology to the officiating of football, soccer and other sports? Last year the world's governing soccer authority experimented with a specially made ball from Adidas that contained an RFID chip. The RFID tag in the "smartball" sends a signal to antennas arranged around the field, and a computer, after determining the exact location, sends the information to a wrist-worn device that can tell a referee if a goal was scored or a ball went out of bounds. The system needs to be given further testing, but it will surely be used by the NFL one of these days.

Category 26.6 RFID tags

2007-01-10 INNOVATION (Information Week 1 Jan 2007) <http://www.informationweek.com/shared/printableArticle.jhtml?articleID=196800208>

TOP TECH TRENDS OF 2007

Radio-frequency identification is one of several promising technologies expected to make a splash in the technology mainstream in 2007. As more vendors join Wal-Mart and the Defense Department in using RFID to track everything from pill bottles to palettes to people, enterprises are developing back-end, supply-chain, and inventory systems that can deliver real productivity benefits. Other rising stars: Web applications, which continue to change the way enterprise software is deployed. Software-as-a-service (SaaS), mashups, RSS feeds, Wikis, blogs, social networking sites, group chat rooms -- the Web services movement is producing more robust enterprise-class applications, which can be deployed in a fraction of the time that more traditional apps demanded. One typical application: Overlay the location of your current sales leads on Google Maps for a visual depiction of where to deploy your sales force. Finally, expect a rise in "virtual servers." The concept is simple: take a single server, divvy it up into separate "virtual" machines, each with its own memory, virtual hardware, drive images and other resources. It's not new: IBM has been doing this on mainframes for 30 years, and blade servers have been around for five years. What is new is that the power of a VM can now be delivered to the PC platform. And that trend is accelerating, now that Microsoft and EMC are literally giving away their VM server software and pre-configured VMs, making setup even easier.

Category 26.6 RFID tags

2007-04-30 DHS Daily OSIR; Government Computer News
http://www.gcn.com/online/vol1_no1/43601-1.html

NIST ISSUES RFID GUIDELINES.

The National Institute of Standards and Technology (NIST) last week issued guidelines and a set of best practices for the use of radio frequency technology by federal agencies, as well as private corporations. NIST said entities deploying RFID technologies need to consider any security or privacy risks that could arise and should minimize those risks by following a list of best practices developed for RFID users. The guidelines focus specifically on the use of RFID technologies for asset management, tracking, matching and process and supply chain control. While RFID offers the potential for organizations to improve their logistics, reduce expenses and increase safety, it also entails the risk of eavesdropping and unauthorized use, according to NIST, an organization within the Commerce Department. Guidelines for Securing Radio Frequency Identification Systems: http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_R FID-2007.pdf

26.7 Cameras (real-world)

Category 26.7 Cameras (real-world)

2006-06-17 DHS Daily OSIR; Agence France-Presse
http://www.breitbart.com/news/2006/06/17/060617210138.lttks67y.html

POLICE LAUNCH EYE-IN-THE-SKY TECHNOLOGY ABOVE LOS ANGELES.

The Los Angeles County Sheriff's Department is testing an unmanned aerial vehicle above Los Angeles. Police say the drone, called the SkySeer, will be able to accomplish tasks too dangerous for officers and free up helicopters for other missions. "This technology could be used to find missing children, search for lost hikers, or survey a fire zone," said Commander Sid Heal, head of the Technology Exploration Project of the Los Angeles County Sheriff's Department. The drone comes equipped with low-light and infrared capabilities and can fly at speeds up to 30 miles per hour for 70 minutes. A small camera capable of tilt and pan operations is fixed to the underside of the drone which sends the video directly to a laptop command station.

Though the SkySeer is not capable of spying into windows just yet, for some a future of nearly invisible eyes in the sky is an unsettling introduction of science fiction into daily life. "A helicopter can be seen and heard, and one can make behavior choices based on that," said Beth Givens of the Privacy Rights Clearinghouse. "Do we really want to live in a society where our backyard barbeques will be open to police scrutiny?" But police say that such privacy concerns are unwarranted because surveillance is already ubiquitous. "You shouldn't be worried about being spied on by your government," said Heal. "These days you can't go anywhere without a camera watching you whether you're in a grocery store or walking down the street."

Category 26.7 Cameras (real-world)

2006-07-05 DHS Daily OSIR; Associated Press
http://www.leesvilledailyleader.com/articles/2006/07/05/news /news3.txt

VOTES THIS WEEK ON CAMERAS IN ALEXANDRIA STORES, RAPIDES SCHOOLS.

Surveillance cameras could be required at convenience stores in Alexandria, LA, and installed in as many as 20 Rapides Parish schools under proposals up for votes this week. Police and the Northern and Central Louisiana Interfaith Group have lobbied the Alexandria City Council for a law mandating working cameras, recording equipment, and other safety measures in convenience stores. And, on Thursday, July 6, the Rapides Parish School Board will consider a resolution about matching a $400,000 federal grant for video cameras and other security equipment at as many as 20 schools. Superintendent Gary Jones said the cameras are not for discipline but to monitor the schools' outside areas and hallways, a guard against after-hours vandalism and thefts, and to watch who is coming and going and whether they belong on the schools' campuses.

Category 26.7 Cameras (real-world)

2006-08-08 DHS Daily OSIR; Register (UK)
http://www.theregister.co.uk/2006/08/08/mobile_bank_mugging/

CAMERA PHONES LINKED TO SOUTH AFRICAN BANK THEFT MUGGINGS.

South African muggers are using camera phones to capture pictures of potential victims in banks before their accomplices stalk and rob them, according to reports. The ruse is helping street thieves in the Walmer district of Port Elizabeth to target well-heeled victims, according to police spokesperson Captain Verna Brink. "This way the person is not actually followed out of the bank, and there is very little suspicion aroused," Brink said, the Herald reports. Local police are urging banks to prohibit the use of camera phones on their premises. Theft of a different sort -- fears over the use of camera phones to help low-level scammers make a clean getaway or to help thieves to case premises in preparation for armed robberies -- has prompted a number of U.S. banks to prohibit the use of mobiles on their premises. First National Bank branches in Chicago has joined with banks in Citizens Bank of Northern California and Indiana-based Citizens Financial Bank in banning the technology. Banks in Mexico City began banning mobiles in May as part of attempts to foil armed robberies, the Chicago Tribune reports.

Category 26.7 Cameras (real-world)

2006-09-14 DHS Daily OSIR; Enterprise (MA)
http://enterprise.southofboston.com/articles/2006/09/05/news/news/news03.txt

SECURITY ALERT AT THE LIBRARY.

Librarians are concerned as a growing number of the homeless in the cities seek refuge, and some sex offenders seek victims in the library stacks. In Taunton, MA, 10 surveillance cameras are set to be installed inside the library after staff noticed an increase in people -- including Level 3 sex offenders -- loitering, doing drugs or trying to steal in the past two years. In Brockton, MA, private security officers as well as cameras keep watch at the library and branches. And some public libraries in smaller communities have panic alarms installed in case of trouble. In Pennsylvania, a bill was filed calling for sex offenders and sexually violent predators to notify a staff member every time they go into a library. "The library is a public place. It is not all that different than the mall," said Susan Hildreth, president of the Public Library Association. "Many people don't understand or don't recognize that the public library is the last free institution in our society that is open to anyone." Lt. John Crowley, chief of detectives in Brockton, said people may be lulled into a false sense of security at the library. "There are people with problems everywhere, including the library," he said.

Category 26.7 Cameras (real-world)

2006-10-02 DHS Daily OSIR; NBC4 (Washington, DC) http://www.nbc4.com/news/9985252/detail.html

SURVEILLANCE CAMERAS NOT LIVING UP TO EXPECTATIONS.

Many Washington, DC, police said they had hoped that installing dozens of new surveillance cameras across the city would assist them in cracking down on crime, but the system does not appear to be working as planned. It was a very violent weekend across the DC area, with 11 people shot, four of them fatally. One of the shootings in the District was caught on one of the new cameras, but police said so far, the cameras have not been much help in any other case. The incident remains under investigation. Community members said the shooting happened within yards of the cameras, which were of little deterrent. In some places trees limit what
cameras see. The surveillance program has been in effect for about a month, but police said there has yet to be prosecution involving evidence used from the cameras. The cameras, which focus on public space only, are "passively monitored" by the Metropolitan Police Department, meaning that officers generally do not watch the camera feeds in real time. The 48 surveillance cameras have been installed in communities that are considered high-crime areas throughout the city.

Category 26.7 Cameras (real-world)

2007-02-28 INNOVATION (AP/Wired 25 Feb 2007)
<http://hosted.ap.org/dynamic/stories/S/SMART_SURVEILLANCE?SITE=WIRE&SECTION=HOME&TEMPLATE=DEFAULT>

SMARTER SURVEILLANCE

Researchers at the University of Maryland are working on intelligent surveillance systems that could transform cameras from passive observers to "eyes with brains" that can detect suspicious behavior and potentially prevent crime before it occurs. The intelligent systems use computer algorithms to interpret what the camera is recording, and can be programmed to look for things like unattended bags or people walking around in restricted areas. U. of Md. engineering professor Rama Chellappa is heading up a team of graduate students working on systems that can identify a person's unique gait or analyze from the way they walk or their actions whether they're a potential threat. Intelligent surveillance technology is used by Marines in Iraq and by the subway system in Barcelona, according to ObjectVideo, a surveillance software firm, but industry officials emphasize that human input is still essential to the process. After all, even intelligent surveillance systems can't see what's in your backpack or under your jacket -- yet. "That is an eventual goal, but we're not there yet," says Chellappa.

26.8 GPS, GPS tracking & satellite imagery

Category 26.8 GPS, GPS tracking & satellite imagery

2006-10-10 DHS Daily OSIR; Washington Technology http://www.washingtontechnology.com/news/1_1/daily_news/2947 7-1.html

SPACE POLICY TOUTS SATELLITE IMAGERY FOR HOMELAND SECURITY.

The White House published an ambitious, new national space policy Friday, October 6, that lays out goals for exploration and addresses the government's need to enhance homeland security by collecting intelligence imagery within the United States using high-resolution government satellites. The policy supports human and robotic exploration of space and a robust science and technology base for national security. It charges the national intelligence director with responsibilities to implement intelligence goals for the collection, processing, analysis and dissemination of national intelligence related to space.
U.S. National Space Policy (unclassified version):
http://www.ostp.gov/html/US%20National%20Space%20Policy.pdf

Category 26.8 GPS, GPS tracking & satellite imagery

2007-04-16 DHS Daily OSIR; Government Computer News http://www.gcn.com/print/26_08/43512-1.html

SOLAR FLARE PUTS GPS OFF THE AIR.

Mysteriously, on December 6, 2006, Global Positioning System (GPS) devices suddenly malfunctioned across large swaths of the planet. The cause was an intense burst of radio energy, called a solar flare, emitting from the sun's surface. Although the event temporarily knocked out many GPS receivers, no airplanes fell from the sky, and no ships lost their way at sea. But the event nonetheless generated concern among scientists. Although they were aware that radio bursts generated by solar flares could affect GPS equipment, they were surprised that this large an event occurred during a period of relatively low solar-flare activity and that its impact was as strong as it was. "It's more serious than we thought. We didn't think this was going to happen until the next solar maximum, which is about 2011," said Paul Kintner Jr., professor of electrical and computer engineering at Cornell University. "We've been monitoring solar flares for four years. [The Dec. 6 event] suggests that monitoring has been inaccurate. And we don't have a good historical basis for predicting what's going to happen, so we're concerned." The radio bursts don't actually damage equipment but only interfere with transmissions between GPS satellites and receivers.

Category 26.8 GPS, GPS tracking & satellite imagery

2007-04-16 DHS Daily OSIR; WRAL-TV (NC) http://www.wral.com/news/local/story/1275366/

NORTH CAROLINA FIRST RESPONDERS GET HIGH-TECH UPGRADE.

Wake County, NC, emergency dispatchers handle 851,000 calls a year. In almost every case, they make split-second decisions on whom to send where. Monday, April 16, the county was showing off a high-tech tool that will modernize the way emergency units are dispatched and perhaps save lives. It's obvious that the closest help is the best help to send to an emergency. To do that, however, you have to know who's closest. That's what Wake County's new Automatic Vehicle Location system does. Ambulances, sheriff's cruisers, even crime-scene investigators' cars are now fitted with Global Positioning System (GPS) satellite transceivers. With just a click of the computer mouse, 911 operators can pinpoint the location of emergency vehicles. The nearest unit -- not the nearest fire or ambulance station -- gets the call.

27.1 Vulnerability assessment & penetration testing

Category 27.1 Vulnerability assessment & penetration testing

2006-04-24 DHS Daily OSIR; http://www.informationweek.com/news/showArticle.jhtml?articleID=186700539

HACKER'S TOOLKIT ATTACKS UNPATCHED COMPUTERS.

A dirt-cheap, do-it-yourself hacking kit sold by a Russian Website is being used by more than 1,000 malicious Websites, a security company said Monday, April 24. Those sites have confiscated hundreds of thousands of computers using the "smartbomb" kit, which sniffs for seven unpatched vulnerabilities in Internet Explorer and Firefox, then attacks the easiest-to-exploit weakness. For $15 to $20, hackers can buy the "Web Attacker Toolkit," said San Diego-based Websense in an online alert. The tool, which uses a point-and-click interface, can be planted on malicious sites -- or on previously-compromised computers -- to ambush unsuspecting users. "It puts a bunch of code on a site that not only detects what browser the victim is running, but then selects one of seven different vulnerabilities to exploit, depending on how well-patched the browser is," said Dan Hubbard, senior director of security and research at Websense. Websense Informational Alert: Web attacker sites increase: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =472

Category 27.1 Vulnerability assessment & penetration testing

2006-07-05 DHS Daily OSIR; ZDNET News http://news.zdnet.com/2100-1009_22-6090825.html

HP TO HACK CUSTOMERS' NETWORKS.

Hewlett-Packard (HP) is taking a cue from hackers to help protect corporate systems. The company plans to launch a penetration-testing service for businesses in October that will use the same techniques as hackers to gain access to its customers' machines. However, the exploit code it will use will be controlled and will not propagate itself as a worm would, HP said on Tuesday, July 4. The HP Active Countermeasures (HPAC) service will use a single server and between eight and 10 scanning clients per 250,000 connected devices. Each of the clients will be given a range of Internet Protocol addresses to scan, and will move through the range scanning for particular flaws.

Category 27.1 Vulnerability assessment & penetration testing

2006-09-03 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2011679,00.asp

SANDIA'S RED TEAMS: ON THE HUNT FOR SECURITY HOLES.

The Sandia National Laboratories' Red Teams' job is to anticipate cyber-terrorism, create contingency plans that assume the worst and ultimately thwart a pending attack by plugging existing holes. Michael Skroch, leader of the Red Teams, said utilities and government agencies are increasingly at risk as they replace custom IT systems created in the 1950s and 1960s with less expensive, off-the-shelf Windows and Unix systems that, incidentally, are easier marks for hackers. The older systems were secure because they weren't well known and had limited contact with other systems. Thus, "It's clear that the threat and risk level has never been higher for cyber-security," Skroch said. The Red Teams provide independent assessments of information, communication and critical infrastructure to identify vulnerabilities, improve system design and help decision makers increase system security.

27.3 Intrusion detection systems

Category 27.3 Intrusion detection systems

2006-03-02 DHS Daily OSIR; http://www.forbes.com/entrepreneurs/feeds/ap/2006/03/02/ap2564113.html

ISRAELI SOFTWARE COMPANY FACES U.S. PROBE.

Days after the Bush administration approved a ports deal involving the United Arab Emirates, the same review panel privately notified an Israeli software company it faced a rare, full-blown investigation over its plans to buy a smaller U.S. rival. The company was told U.S. officials feared the transaction could endanger some of the government's most sensitive computer systems. The objections by the Federal Bureau of Investigations and Pentagon were partly over specialized intrusion detection software known as "Snort," which guards some classified U.S. military and intelligence computers. Snort's author is a senior executive at Sourcefire Inc. based in Columbia, MD, which would be sold to publicly traded Check Point Software Technologies Ltd. in Ramat Gan, Israel.

Category 27.3 Intrusion detection systems

2006-06-01 DHS Daily OSIR; Security Focus http://www.securityfocus.com/bid/18200/discuss

SNORT URICONTENT RULES DETECTION EVASION VULNERABILITY.

Snort is reportedly prone to a vulnerability that may allow malicious packets to bypass detection.

Analysis: A successful attack can allow attackers to bypass intrusion detection and to carry out attacks against computers protected by Snort.

Vulnerable: Snort Project Snort 2.4.4; Snort Project Snort 2.4.3; Snort Project Snort 2.4.2; Snort Project Snort 2.4.1; Snort Project Snort 2.4.0.

Solution: Currently, Security Focus is not aware of any official vendor-supplied patches for this issue.

For more information: http://www.securityfocus.com/bid/18200/references

Category 27.3 Intrusion detection systems

2006-07-19 DHS Daily OSIR; Security Focus http://www.securityfocus.com/bid/19071/references

CISCO SECURITY MONITORING ANALYSIS AND RESPONSE SYSTEM MULTIPLE VULNERABILITIES.

Cisco Security Monitoring, Analysis and Response System (CS-MARS) is prone to multiple vulnerabilities. Analysis: To include privilege-escalation, arbitrary command-execution, and information-disclosure issues. An attacker could exploit these issues to retrieve potentially sensitive information and possibly execute arbitrary commands with Super User privileges. This may facilitate a remote compromise of affected computers. Vulnerable: Cisco CS-MARS 4.1.5; Cisco CS-MARS 4.1.3; Cisco CS-MARS 4.1.2; Cisco CS-MARS 4.1. Solution: Fixes are available. Refer to the Cisco advisory for details: http://www.securityfocus.com/bid/19071/references

27.4 Firewalls & other perimeter defenses

Category 27.4 Firewalls & other perimeter defenses

2006-03-09 DHS Daily OSIR; http://www.securiteam.com/windowsntfocus/5IP012KI0K.html

EIGHTEEN WAYS TO ESCALATE PRIVILEGES IN ZONE LABS ZONEALARM SECURITY SUITE.

A locally exploitable security vulnerability in Zone Labs ZoneAlarm Security Suite allows normal users to elevate their privileges. Analysis: Instead of using the full path to the DLL during the load process only the name of the DLL is used. This causes several instances of Windows PATH trolling where Windows tries to locate the DLL in the directories listed in its PATH environment variable on behalf of the vsmon.exe process. This PATH trolling is what makes the vsmon.exe process vulnerable to several privilege escalation techniques. Vulnerable product: Zone Labs ZoneAlarm Security Suite build 6.1.744.000. Patches/Workarounds: The vendor was notified several times but there was no response.

Category 27.4 Firewalls & other perimeter defenses

2006-03-13 DHS Daily OSIR; http://www.frsirt.com/english/advisories/2006/0947

ZONEALARM TRUEVECTOR SERVICE LOCAL PRIVILEGE ESCALATION VULNERABILITY

A vulnerability has been identified in ZoneAlarm, which could be exploited by malicious users to obtain elevated privileges. Analysis: The error in the TrueVector service ("VSMON.exe") that loads certain Dynamically Linked Libraries (DLL) in an insecure manner, which could be exploited by local attackers to execute arbitrary commands with SYSTEM privileges by placing a malicious DLL in a specific directory. Affected product: ZoneAlarm versions 6.x. Solution: The FrSIRT is not aware of any official supplied patch for this issue.

Category 27.4 Firewalls & other perimeter defenses

2006-08-15 DHS Daily OSIR; Computer World http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9002482

CISCO CAN'T REPRODUCE BLACK HAT FLAW.

Cisco Systems Inc. has been unable to reproduce a security flaw reported in its PIX firewall appliance earlier this month, the networking company said Tuesday, August 15. The alleged vulnerability was discovered by Hendrik Scholz, a developer with Freenet Cityline GmbH, who discussed it during an August 2 presentation at the Black Hat USA conference in Las Vegas. Scholz claimed that if someone sent the PIX device a specially crafted Session Initiation Protocol message, the firewall would then allow attackers to send traffic to any device on the network. "We've had engineers both within the business unit and within our PSIRT organization looking into this," said John Noh, a Cisco spokesperson. "We have not been able to replicate what he claims he has discovered."

Category 27.4 Firewalls & other perimeter defenses

2006-08-23 DHS Daily OSIR; Cisco http://www.cisco.com/warp/public/707/cisco-sa-20060823-firewall.shtml

CISCO SECURITY ADVISORY: UNINTENTIONAL PASSWORD MODIFICATION IN CISCO FIREWALL PRODUCTS.

Certain versions of the software for the Cisco PIX 500 Series Security Appliances, the Cisco ASA 5500 Series Adaptive Security Appliances (ASA), and the Firewall Services Module (FWSM) are affected by a software bug that may cause the EXEC password, passwords of locally defined usernames, and the enable password in the startup configuration to be changed without user intervention. Unauthorized users can take advantage of this bug to try to gain access to a device that has been reloaded after passwords in its startup configuration have been changed. In addition, authorized users can be locked out and lose the ability to manage the affected device. Cisco has made free software available to address this issue for affected customers. Affected products: Cisco PIX 500 Series Security Appliances, the Cisco ASA 5500 Series Adaptive Security Appliances, and the Firewall Services Module (FWSM) for the Cisco Catalyst 6500 Switches and Cisco 7600 Series Routers are impacted if they are running an affected software version. Solution: Refer to source to obtain fixes and workarounds.

27.6 Honeynets

Category 27.6 Honeynets

2006-11-20 DHS Daily OSIR; Tech Web http://www.techweb.com/wire/software/194700014

HACKERS USE VIRTUAL MACHINE DETECTION TO FOIL RESEARCHERS.

Hackers are adding virtual machine detection to their worms and Trojans to stymie analysis by anti-virus labs, a security research expert said Sunday, November 19. The tactic is designed to thwart researchers who use virtualization software, notably that made by VMware, to quickly and safely test the impact of malicious code. "Three out of 12 malware specimens recently captured in our honeypot refused to run in VMware," said Lenny Zeltser, an analyst at SANS Institute's Internet Storm Center in an online note Sunday. Malware writers use a variety of techniques to detect virtualization, including sniffing out the presence of VMware-specific processes and hardware characteristics, said Zeltser.

27.7 Anti-malware

Category 27.7 Anti-malware

2006-02-01 EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4669304.stm

FIVE COMPANIES COOPERATE AGAINST SPYWARE

A group of computer security companies is cooperating on an initiative to help consumers combat the growing problem of spyware, which is estimated to be increasing by 50 to 100 percent per year. ICSA Labs, McAfee, Symantec, Thompson Cyber Security Labs, and Trend Micro will initially offer tools that will help users identify spyware on their systems and effectively remove it. That effort will involve developing a common naming scheme for malicious programs and a coordination of various removal tools. Later, the five members of the group will work on tools that can help users avoid spyware in the first place. A related effort called Stop Badware was announced recently by Google, Sun Microsystems, the Berkman Center for Internet and Society, and the Oxford Internet Institute.

Category 27.7 Anti-malware

2006-03-06 DHS Daily OSIR; http://www.smh.com.au/news/breaking/new-safety-net-for-web-surfers/2006/03/06/1141493583941.html

NEW SAFETY NET FOR WEB SURFERS.

A fresh approach to "safe surfing" has been dreamt up by a group of Massachusetts Institute of Technology engineers involved in a crusade to make the Internet a safer place for their friends and families. The result of their labors is a product called SiteAdvisor which labels particular Websites with a color-coded security rating to help users identify those that might contain spyware, spam, viruses, and online scams. The millions of Websites on the Internet are trawled using sophisticated computer "robots" that can intelligently analyze the safety of a given destination. The tool then presents its findings alongside search engines such as Google, Yahoo! or MSN and labels results as either green, yellow or red. SiteAdvisor: http://www.siteadvisor.com/preview/

Category 27.7 Anti-malware

2006-03-13 DHS Daily OSIR; http://www.computerworld.com/securitytopics/security/story/0,10801,109525,00.html?SKC=security-109525

MCAFEE ANTIVIRUS UPDATE WREAKS HAVOC.

A faulty antivirus update from McAfee Inc. that mistakenly identified hundreds of programs as a Windows virus has resulted in some companies accidentally deleting significant amounts of data from affected computers. The McAfee update (DAT 4715) released on Friday, March 10, was designed to protect computers against the W95/CTX virus. But because of a programming error, the update also incorrectly identified, renamed and quarantined hundreds of legitimate executables. For companies that had configured their McAfee antivirus program to automatically delete bad files, the error resulted in the loss of hundreds, and in some cases even thousands, of files on systems in which the update had been installed, said Johannes Ullrich, chief technology officer at the SANS Internet Storm Center in Bethesda, MD. McAfee released a new patch (DAT 4716) updating the earlier one, five hours later.

Category 27.7 Anti-malware

2006-03-14 RISKS; news.com http://tinyurl.com/jtaht

McAFEE ANTIVIRUS ATTACKS SYSTEM FILES & MICROSOFT OFFICE

According to McAfee spokesperson Joe Telafici, speaking to CNET News.com writer Joris Evers, >At about 1 p.m. PST [on March 10, 2006] we started getting reports that people were seeing an unusual number of W95/CTX infections in their environment," Telafici said. "Files that we did identify would probably be deleted or quarantined, depending on your settings."< Evers continued, "McAfee's antivirus software detected Excel.exe and Graph.exe, two Microsoft Office components, as well as other software, including AdobeUpdateManager.exe, an application installed alongside Adobe products that deals with software updates, Telafici said. . . . The problem occurred with virus definition file 4715, which was released at about 10:45 a.m. on Friday as part of McAfee's daily update cycle. The repaired, emergency-definition file 4716 was pushed out at about 3:30 p.m."

[MK adds: Hmm, many people have been arguing for years that MS products are malware. . . .]

Category 27.7 Anti-malware

2006-03-15 INNOVATION (Eweek 2 Mar 2006) <http://www.eweek.com/article2/0,1895,1933210,00.asp>

ATTACK ON THE ZOMBIES

A team of high-profile security experts has launched a search-and-disable mission, aimed at taking out the command-and-control infrastructure that directs a large network of zombie drone machines, or bots, that have been hijacked by hackers. The compromised machines, which are used for spamming, denial-of-service attacks and malware installation, are controlled by a "botmaster" via an IRC (Inter Relay Chat) server installed illegally on a broadband educational or corporate network. "If that command-and-control is disabled, all the machines in that botnet become useless to the botmaster. It's an important part of dealing with this problem," says Israeli CERT manager Gadi Evron. Over the past year, the team has operated covertly through invitation-only e-mail lists, but Evron has now launched a public, open mailing list to solicit the public's assistance in tracking down botnet servers. "The vetted lists will still do the bulk of the work, but we needed a public place to involve a wider audience," says Evron, who admits security experts are always stuck working in a catch-up mode. "Anything you do that kills the problem right now has one direct result. The bad guys go back to the drawing board and plan a more sophisticated mode of attack… It's all about return on investment… If you can change the economics by making it more dangerous and difficult for [the bad guys] to control the botnets, that's the only to try to get ahead of game."
(Eweek 2 Mar 2006) <http://www.eweek.com/article2/0,1895,1933210,00.asp>

Category 27.7 Anti-malware

2006-08-07 DHS Daily OSIR; CNET News http://news.com.com/AOL+offers+free+antivirus+software/2100-7355_3-6102917.html?tag=nefd.top

AOL OFFERS FREE ANTIVIRUS SOFTWARE.

AOL has introduced free antivirus software that is likely to become the highest-profile alternative to security software you pay for. Active Virus Shield offers basic protection against viruses, spyware and other malicious software, AOL said in a statement Monday, August 7. The product is available to all Internet users, not just to subscribers to AOL's Internet access service. The protective tool is being delivered in partnership with Kaspersky Lab, a well-respected Russian antivirus software maker.

Category 27.7 Anti-malware

2006-08-23 DHS Daily OSIR; IDG News Service http://www.networkworld.com/news/2006/082306-sophos-offers-free-rootkit-detection.html

SOPHOS OFFERS FREE ROOTKIT DETECTION TOOL.

Sophos has released a free tool to help PC users root out rootkits. Called Sophos Anti-Rootkit, the software will detect and remove both known and unknown rootkits, and it will also warn system administrators if removing the software might harm operating system integrity. Sophos Anti-Rootkit can be downloaded here: http://www.sophos.com/products/free-tools/sophos-anti-rootkit.html

Category 27.7 Anti-malware

2007-01-03 INNOVATION (Tech News World 21 Dec 2006) <http://www.technewsworld.com/story/9wcTtXAPIbrQOv/Solid-State-PCs-Computings-Next-Horizon.xhtml>

SOLID-STATE PCs: VIRUS KILLERS?

Solid-state PCs, which are already under development in Asia and South America, do not have a hard drive, and the operating system will be burned onto a chip, making malware manipulations and viruses problems of the past. These devices are entirely feasible to develop, say experts, although there still are issues with booting from Flash RAM (random access memory). "Solid-state PCs are a natural progression of existing technology," says Ken Steinberg of Savant Protection, which has been experimenting with improving operating system security for such devices. A trend toward this new type of PC is being driven, in part, by security worries and a push toward Unix/Linux operating systems. Today's operating systems are vulnerable to viruses and other intrusions because they live on a device that permits write-only access, Steinberg says. The core component in the Windows OS is not locked down, but Linux's can be, making it the OS of choice for solid-state computers. In fact, it is already possible to produce a solid-state PC that uses Linux, but a Windows version will take another two or three years. The computer industry is also on the verge of seeing solid-state replacements for the aging spinning hard drive technology, said consultant Robert Hoffer. "The time is right to move forward with Flash RAM storage because spindle drive capacity is at the end of its possibilities for greater storage."

Category 27.7 Anti-malware

2007-02-12 DHS Daily OSIR; InformationWeek http://www.informationweek.com/showArticle.jhtml

PENN STATE RESEARCHERS DEVELOP NEW WORM-STOPPING TECHNOLOGY.

Researchers at Penn State University say they have developed anti-malware technology that can identify and contain worms in milliseconds rather than minutes -- greatly limiting how far they spread and how much damage they cause. The new technology focuses on analyzing packet rate and frequency of connections, rather than signature or pattern identification, according to a release from Penn State. "A lot of worms need to spread quickly in order to do the most damage, so our software looks for anomalies in the rate and diversity of connection requests going out of hosts," said Peng Liu, associate professor of information sciences and technology at Penn State and lead researcher on the system. Penn State researchers assert that because many security technologies focus on signature or pattern identification for blocking worms, they cannot respond to new attacks fast enough, allowing worms to exploit network vulnerabilities.

Category 27.7 Anti-malware

2007-05-16 INNOVATION (New Scientist 5 May 2007) <http://www.newscientisttech.com/channel/tech/mg19426026.000-web-browsers-are-new-frontline-in-internet-war.html>

BOTWARE MIGRATES TO THE WEB

Bot malware -- malicious software that installs itself unbeknownst to a computer owner, allowing the machine to be controlled by a "botmaster" for nefarious activities like spewing spam -- is migrating to Web sites. "We still see a tremendous amount of bot propagation via e-mail, but the Web has overtaken it in the past year," says one security expert. As savvy users became wary of e-mail attachments from unknown senders, spammers switched to "drive-by" downloads from innocent Web sites corrupted to exploit browser vulnerabilities.

And although antivirus software often detects the malware, the bots fight back by disabling it. Most users would never know their computer had been infected unless their browser starts crashing or they're inundated with pop-up ads, says Google security specialist Niels Provos.

And Web site owners would be equally oblivious because the malware is typically camouflaged
-- for instance, tucked into the JavaScript program used to create the site. Security experts are fighting back with a system called "herd computing" that links multiple online computers into a sort of a "neighborhood-watch" network. Members of the herd monitor the health of their computers as they navigate the Net and warn others away from fraudulent or malicious sites. Members can then decide for themselves whether to visit a site. Jonathan Zittrain, who heads up the herding project, likens the concept to "giving the Internet a nervous system."

27.8 Anti-phishing

Category 27.8 Anti-phishing

2006-06-28 DHS Daily OSIR; TechWeb http://www.techweb.com/wire/security/189601692

NEW ANTI-PHISHING SUITE UNVEILED.

On Monday, June 26, Symantec announced an online transaction safety suite scheduled to release for Windows and the Mac OS X operating system this fall. Norton Confidential, which will enter beta testing sometime this summer, will include anti-phishing blacklists and heuristic-based detectors; what Symantec calls "crimeware protection, essentially keylogger and screen-grabbing Trojan horse sniffers; additional site authentication cues; and password encryption." Symantec didn't provide a release date for Confidential but said that the beta would be available "shortly."

Product Overview: http://www.symantec.com/home_homeoffice/products/overview.jsp?pcid=ts&pvid=nco

Product Review: http://www.pcworld.com/article/id,128067/article.html

Category 27.8 Anti-phishing

2006-08-07 EDUPAGE; BBC http://news.bbc.co.uk/2/hi/technology/5251742.stm

GOOGLE DEBUTS WEB SITE WARNINGS

Google has debuted a new service that warns users who click links to visit sites that have been identified by the Stop Badware coalition, itself a project of Google, Lenovo, and Sun Microsystems. The coalition was founded to help address the problems of spyware and other malicious software by helping users know which sites have distributed such software. Users of Google's search engine who try to access a site on Stop Badware's list are shown a warning that the site they want to visit has been flagged as potentially dangerous, though users are not prevented from going to that site. The warning messages are expected to become more detailed over time, including specific information about exactly how the site tries to install malicious software. A product called Scandoo, from company ScanSafe, performs a similar function for users of Google or MSN.

Category 27.8 Anti-phishing

2006-09-13 INNOVATION (Carnegie Mellon press release 31 Aug 2006) <http://www.cmu.edu/PR/releases06/060831_phishing.html>

PHOOLPROOF PHISHING PREVENTION

Phishing expeditions are on the rise, luring users to conduct financial transactions on fraudulent Web sites where their personal information is then exploited. Researchers at Carnegie Mellon's CyLab have come up with technology designed to thwart such attacks even when users make mistakes. "Essentially, our research indicates that Internet users do not always make correct security decisions, so our new system helps them make the right decision and protects them even if they manage to make a wrong decision," says CMU engineering professor Adrian Perrig. The innovative security system activates mutual authentication between a Web site and the user by making the user's cell phone part of the process. "The mobile device acts like an electronic assistant, storing a secure bookmark and a cryptographic key for each of the user's online accounts," says Perrig. Because the key is separate from the computer used to access the Web, the system also serves to protect against keyloggers and other malicious software that might be lurking on a user's hard drive.

Category 27.8 Anti-phishing

2006-11-13 DHS Daily OSIR; CNET News http://news.com.com/With+IE+7%2C+green+means+go+for+legit+sites/2100-1029_3-6134647.html

WITH IE 7, GREEN MEANS GO FOR LEGITIMATE SITES.

Starting early next year, the address bar in Internet Explorer 7 will turn green when surfing to a legitimate Website -- but only in some cases, not all. The colored address bar is designed to be a sign that a specific site can be trusted, giving people the green light to carry out transactions there. It is a weapon in the fight against phishing scams, which use fraudulent Websites. The idea is among the draft guidelines created by the CA Browser Forum, an organization that issues certificates for Websites and major browser makers. Last week, Microsoft decided to adopt that draft version for IE 7, released last month. It plans to add the functionality in January. Initially, only corporations will be able to get the online trust indicator -- a rule that shuts out smaller businesses. A primary concern is to help the targets of online scams, said Markellos Diorinos of Microsoft. There is broad agreement in the industry that Web browsers need a better way to identify trusted sites than the familiar yellow padlock icon which was designed to show that traffic with a Website is encrypted and that a third party certification authority has identified the site.

Category 27.8 Anti-phishing

2007-02-12 DHS Daily OSIR; SecurityFocus http://www.securityfocus.com/brief/431

PAYPAL OFFERS SECURITY KEY.

Online payment firm PayPal announced that the company will offer a hardware key fob to users as an additional way of securing their accounts. The PayPal Security Key generates a new six-digit number every 30 seconds and displays the number when a button is pressed. Users that pay $5, a fee that is waived for business customers, will receive a key that they can then register to their account. The company made the announcement last week at the RSA Security Conference, saying that the offering in the United States is a "public beta." The security key is the latest measure by the company to help lock down its users, Michael Barrett, chief information security officer for the subsidiary of eBay, told SecurityFocus. PayPal and eBay generally top the list of brands targeted by phishing attacks.

Category 27.8 Anti-phishing

2007-05-21 DHS Daily OSIR; Computerworld Australia http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9020062&intsrc=hm_list

XML FORMAT FOR ANTIPHISHING INFO TO GO LIVE IN JULY.

A common format to electronically report fraudulent activities will be fully operational by July 2007. Anti-Phishing Working Group (APWG) secretary general, Peter Cassidy, said a structured data model is necessary to improve incident reporting, share information and allow forensic searches and investigations. Cassidy said the first base specification was submitted in June 2005 and the Incident Object Description Exchange Format (IODEF) XML Schema with e-crime relevant extensions will be a recognized IETF standard in about six weeks. He said reporting will be automated with greater ease using a standard schema. "For example, a Korean CERT (Computer Emergency Response Team) reporting an incident can send it to a French bank," he said. Cassidy said the APWG first started collecting data in October 2003. To date, he said 2.5 million records of attacks and 13,500 URLs are added to the database every month. Cassidy said the block list is updated every five minutes and is a 10MB file used as a historical
archive, most commonly used by browser developers. URLs are sent by banks, institutions, retailers, CERTs and volunteer organizations.

Category 27.8 Anti-phishing

2007-05-23 DHS Daily OSIR; CNET News
http://news.com.com/Promising+antispam+technique+gets+nod/2100-1029_3-6185904.html

PROMISING ANTISPAM TECHNIQUE GETS NOD.

An Internet standards body gave preliminary approval on Tuesday, May 23, to a powerful technology designed to detect and block fake e-mail messages. Yahoo, Cisco Systems, Sendmail and PGP Corporation are behind the push for DomainKeys, which the companies said in a joint statement will provide "businesses with heightened brand protection by providing message authentication, verification and traceability to help determine whether a message is legitimate." The draft standard that the Internet Engineering Task Force adopted is more promising than most other anti-spam and antiphishing technologies because it harnesses the power of cryptographically secure digital signatures to thwart online miscreants. DomainKeys works by embedding a digital signature in the headers of an outgoing e-mail message. If the cryptographically secure signature checks out, the message can be delivered as usual. Otherwise, it can be flagged as spam. In the long run, DomainKeys is more promising than existing antispam and antiphishing technologies, which rely on techniques like assembling a "blacklist" of known fraudsters or detecting such messages by trying to identify common characteristics. But the DomainKeys approach does suffer from one serious, short-term problem: it's only effective if both the sender and recipient's mail systems are upgraded to support the standard.

Category 27.8 Anti-phishing

2007-05-25 DHS Daily OSIR; Register (UK)
http://www.channelregister.co.uk/2007/05/25/strange_spoofing_technique/

STRANGE SPOOFING TECHNIQUE EVADES ANTIPHISHING FILTERS.

Newly published screen shots demonstrate a powerful phishing technique that's able to spoof eBay, PayPal and other top Web destinations without triggering antiphishing filters in IE 7 or Norton 360. Plenty of other PayPal users are experiencing the same ruse, according to search engine results. UK resident Matty Hall, after attempting to log in to a PayPal page that both IE and Norton had given a clean bill of health, was prompted for his date of birth, social security number, credit card details and other sensitive information. The message included poor grammar and awkward syntax. The scam method isn't limited to PayPal. Hall has supplied screen shots of something similar happening when he used IE to log on to his online account at HSBC, and he says he also experiences variations on that theme when trying to access Barklays and eBay. Roger Thompson, who tracks Web exploits for Exploit Prevention Labs, guesses those experiencing this attack have inadvertently installed an html injector. That means the victims' browsers are, in fact, visiting the PayPal Website or other intended URL, but that a dll file that attaches itself to IE is managing to read and modify the html while in transit.

27.9 Anti-spyware

Category 27.9 Anti-spyware

2006-01-30 DHS Daily OSIR; http://www.theregister.co.uk/2006/01/30/spyware_testing/

SECURITY VENDORS OPEN ANOTHER FRONT AGAINST SPYWARE.

The three biggest anti-virus vendors have teamed up with testing labs to develop standards for spyware detection. Trend Micro, Symantec and McAfee are joining forces with ICSA Labs and Thompson Cyber Security Labs in a bid to standardize methods for sharing spyware samples and testing anti-spyware products and services. The effort is aimed at curtailing a possible source of user confusion before it becomes a problem, as well as driving up standards for detection across the anti-spyware industry. Spyware testing, modeled on schemes the anti-virus industry has been running for years, will also make it easier to compare the efficacy of various anti-spyware products, at least in theory. The group's anti-spyware testing methodology and best practices can be viewed at Spywaretesting.org. The initiative is one of a number of cross industry efforts aimed at coordinating the fight against spyware -- the invasive programs that track user's surfing habits or, in the worst cases, steal their personal information, such as credit card or Social Security numbers. Spywaretesting Website: http://www.spywaretesting.org/metadot/index.pl

Category 27.9 Anti-spyware

2006-08-04 DHS Daily OSIR; Government Computer News
http://www.gcn.com/online/vol1_no1/41559-1.html?topic=security

THE BATTLE LINES ARE DRAWN IN THE WAR ON SPYWARE.

The good news from the war on spyware is that there seems to be less support for organizations engaging in questionable behavior such as installing adware on the computers of unsuspecting users. But the bad news is that as the gray hats are being weeded out of the industry, the real bad guys are being left with the field to themselves. "We're seeing a lot more cases of keystroke loggers," said Ari Schwartz, deputy director of the Center for Democracy and Technology, during last week's Black Hat Briefings in Las Vegas. Although the application of criminal law has put a damper on the adware industry, what remains are those who are using tools like keyloggers to steal passwords, account information and other valuable data. These threats are not likely to disappear soon.

Category 27.9 Anti-spyware

2006-10-24 DHS Daily OSIR; CNET News http://news.com.com/Microsofts+free+anti-spyware+hits+market/2100-1029_3-6128978.html

MICROSOFT'S FREE ANTI-SPYWARE HITS THE MARKET.

Microsoft announced on Tuesday, October 24, the general release of its free anti-spyware program, a move that significantly steps up the software maker's competitive challenge in the security industry. Windows Defender anti-spyware is now available in English to Windows XP users, with other languages set for delivery in coming weeks. Windows Defender will also be bundled with Windows Vista, Microsoft's next-generation operating system, when it is released in January. Windows Defender anti-spyware:
http://www.microsoft.com/athome/security/spyware/software/default.mspx

Category 27.9 Anti-spyware

2007-04-25 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2188549/rogue-apps-dominating

ROGUE SOFTWARE FLOODS ANTI-SPYWARE MARKET.

Malware writers are flooding the market with rogue anti-spyware applications in an attempt to steer consumers away from genuine security software and make money from selling bogus applications. Download service Snapfiles said that the rogue applications outnumber genuine software by a factor of four to one. Snapfiles hosts free and trial applications for consumers to download, and claims to reject any software that fails to deliver the promised functionality or causes harm to a system. Download site Tucows confirmed the figure, saying that it too rejects about four-fifths of the anti-spyware programs it receives from developers. Rogue anti-spyware programs present themselves as legitimate security solutions, but have no intention of ridding a user's system of malware. Instead, the application scares the user with false test results, fails to get rid of existing spyware infections, and in some cases even infects the system with additional pieces of spyware and adware.

27.A Anti-spam

Category 27.A Anti-spam

2006-05-15 Effector Online http://www.eff.org/news/archives/2006_05. php#004653

AOL STARTS PAY-TO-SEND EMAIL SHAKEDOWN "CERTIFIED MAIL" ALLOWS MASS MAILERS TO BYPASS SPAM FILTERS.

San Francisco - AOL has quietly flipped the switch on its "certified mail" service, delivering pay-to-send email to some of its millions of customers. The Goodmail CertifiedEmail service allows large mass- emailers to pay a fee to bypass AOL's spam filters and get guaranteed delivery directly into AOL customers' inboxes. The Electronic Frontier Foundation (EFF) believes the pay- to-send model could leave nonprofits, small businesses, and other groups with increasingly unreliable service. "Many groups suffer from what the Wall Street Journal called 'spam filters gone wild,' and their email never reaches many on their mailing lists," said EFF Activism Coordinator Danny O'Brien. "With AOL's system in place, AOL will be taking money from big companies to skip those filters entirely. If ISPs can make money for a premium service that evades their malfunctioning filters, we worry that they won't fix those filters for groups who do not pay." While the creators of "certified mail" claim that their programs help customers recognize legitimate worthy causes and vital banking mail in their inbox, the first pay-to-send mailing spotted by EFF was a promotion for Overstock.com. Overstock has every right to reach customers who signed up for its mailing list, but just because corporations have the money to pay for email delivery doesn't make that mail more important than any other noncommercial mail. "We already know what commercial, paidfor mass mail is, but we don't call it certified mail. We call it junk mail," said O'Brien. "Why should paying ISPs for delivery let some companies gain special access to your inbox?" EFF and hundreds of other groups have joined together in the DearAOL.com coalition, which formed to urge AOL and other ISPs to reject pay-to-send schemes. However, in a pointed example of how ISP control of your inbox can go wrong, last month AOL silently started dropping email that even mentioned DearAOL.com. After EFF publicized the problem, AOL quickly rectified the situation.
For more on the DearAOL.com Coalition: http://www.dearaol.com
For more on AOL's CertifiedEmail launch: http://www.dearaol.com/blog
For this release: http://www.eff.org/news/archives/2006_05. php#004653

Category 27.A Anti-spam

2006-11-14 DHS Daily OSIR; Register (UK) http://www.theregister.co.uk/2006/11/14/spamhaus_worst_spammer_list/

THE WORLD'S MOST PROLIFIC SPAMMERS.

Spamhaus has published a revised list of the world's 10 worst spammers. The top 10 are: 1) Alex Blood; 2) Leo Kuvayev; 3) Michael Lindsay; 4) Ruslan Ibraqimov; 5) Amichai Inbar; 6) Pavka; 7) Vincent Chan; 8) Alexey Panov; 9) Yambo Financials; 10) Jeffrey Peters. For further detail: http://www.spamhaus.org/statistics/spammers.lasso

---

Category 27.A Anti-spam

2007-04-18 INNOVATION (Washington Post 10 Apr 2007) < http://www.washingtonpost.com/wp-dyn/content/article/2007/04/10/AR2007041000479.html

STALLING TACTIC STYMIES SPAMMERS

Spammers hate to wait, so Canadian firm MailChannels is capitalizing on their impatience in a new approach toward stemming the tide of unwanted e-mail. By forcing e-mail programs to slow down their digital handshake -- the exchange of information required before Internet servers will handle the recipients' incoming mail -- MailChannels has found that many spammers just decide to give up and move on to more promising pastures. The program, called Traffic Control, allows e-mail administrators to extend the handshake time -- normally around 2 seconds -- to anywhere between 10 seconds to a couple of minutes. MailChannels founder Ken Simpson says that unlike legitimate senders, 90% of spammers give up after 10 seconds of being "on hold." "Even after eight minutes, 60% of legitimate e-mail senders are still hanging on trying to get their message delivered. This is the technique spammers are really only going to get hurt by, because if we just build a better spam filter, the spammers will respond by increasing the amount of junk mail they're blasting out. But if you throttle them, there really is nothing they can do except persist like legitimate senders, but if they do that then the economics of spamming goes out the window," says Simpson. To get around the prospect of a legitimate e-mail traffic jam, Traffic Control offers an additional feature that helps e-mail servers perform more efficiently. Spam researcher Bill Stearns says the volume of spam that is filtered out by this technique is impressive, and that unlike conventional filters, spammers can't just circumvent the barricade. "It's going to take a long time before a technique like this becomes useless."

27.B Multifunction packages

Category 27.B Multifunction packages

2006-05-31 EDUPAGE; BBC http://news.bbc.co.uk/2/hi/technology/5032832.stm

MICROSOFT ENTERS SECURITY MARKET WITH ONECARE

Microsoft is set to begin offering its OneCare security service, a single package that includes antivirus, antispyware, and firewall protections. Announced nearly three years ago, the OneCare service includes advice on how to avoid computer threats and tools to help users recover from security incidents that can occur. According to Microsoft, as many as 70 percent of personal computers are either unprotected or use outdated tools to protect themselves from computer threats. Symantec and McAfee, two leading vendors of security products, are reportedly working on new products that integrate several kinds of computer protection into a single package, as OneCare does. Microsoft said it will not build OneCare into its Windows operating system.

Category 27.B Multifunction packages

2006-06-07 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,1970575,00.asp

SINGLE AGENT DESKTOP SECURITY COMES OF AGE.

Microsoft's impending move into the business PC security market is accelerating the development and adoption of so-called single agent desktop defense applications, according to many industry watchers. While the launch of the software giant's OneCare PC management service during the last week in May 2006 has already pushed rival security software makers to create their own bundled offerings for the home market, experts say that Microsoft's move into the enterprise security sector is similarly accelerating the development of centralized enterprise PC defense applications. Microsoft has already distributed a beta version of Microsoft Client Protection, a new security product that aims to help protect business desktops, laptops and file servers from a range of threats including viruses, spyware and rootkits, among other things. While single agent desktop security products are nothing new, the impending emergence of Microsoft Client Protection and demands from customers for integrated, easier-to-manage PC applications is driving traditional security software vendors to promote the tools more aggressively. Enterprise customer buying patterns, along with the demand for integrated security applications, are finally driving adoption of the technology.

Category 27.B Multifunction packages

2006-07-17 EDUPAGE;
CNET http://news.com.com/2100-1029_3-6094932.html

AOL INTRODUCES SECURITY TOOLS

AOL is set to release a test version of a security package that the company will offer to anyone, not just AOL customers. The company currently offers security applications to subscribers, including a firewall and antivirus and antispyware tools. The new offering, known as Total Care, will be a comprehensive package, with components coming from various third parties. Firewall, antivirus, and antispyware tools come from McAfee; Iolo Technologies provides tools for PC performance, and backup tools come from FarStone Technology. Following Microsoft's launch of Windows Live OneCare in May, leading makers of security products pledged to offer similar one-stop products that should serve all of a user's needs. According to Gartner, growing numbers of consumers are looking to their ISPs to provide security solutions rather than buying tools from other vendors. The firm said that last year, 14 percent of computer security sales were from ISPs, compared to just 5 percent the year before.

28.3 Heat, fires, explosions

Category 28.3 Heat, fires, explosions

2006-07-10 DHS Daily OSIR; New York Times
http://www.iht.com/articles/2006/07/10/business/dell.php

DELL'S EXPLODING COMPUTER AND OTHER IMAGE PROBLEMS.

A Dell notebook computer burst into flames last month in Osaka, Japan. Photos of the flaming and smoking notebook were posted on a technology news Website called the Inquirer on June 21. Two days later, Cindy Shaw, a securities analyst with Moors & Cabot, notified her clients about the publicity. Last Thursday, July 6, citing reports of a second smoking laptop, this one in Pennsylvania, she advised them that "should this story also hit the mainstream press, we believe there is headline risk and potentially negative demand ramifications for Dell." Dell said its engineers examined and tested what remained of the flaming notebook computer for several days to find the source of the problem. They concluded that the fire was caused by a faulty lithium ion battery cell. Dell said that it found no pattern of battery failure and that the Pennsylvania incident publicized by the Inquirer Website was caused by a chip problem and not batteries.

Photos of the Osaka, Japan, incident: http://theinquirer.net/default.aspx?article=32550

[2006-08-15]
DELL RECALLS 4 MILLION SONY LITHIUM-ION PORTABLE-COMPUTER BATTERIES

Dell issued a recall order of 4.1 Li-ion batteries manufactured by Sony for its laptop computers. The company was responding to a growing number of reports of batteries burning or exploding and pictures being osted on the Web by victims [MK adds: and pranksters?]. According to an article by Louisa Hearn in the Sydney Morning Herald, the worldwide recall would cost Dell and Sony over U$300M. The batteries in question were sold or replaced between 1 April 2004 and 18 July 2006. Details of the recall were posted at http://www.dellbatteryprogram.com .
[http://www.smh.com.au/news/biztech/dell-recalls-4-million-batteries/2006/08/15/1155407776670.html]

Category 28.3 Heat, fires, explosions

2006-08-14 DHS Daily OSIR; CNET News
http://news.com.com/Dell+to+recall+over+4+million+batteries/2100-1044_3-6105486.html

DELL TO RECALL FOUR MILLION BATTERIES.

Dell and the U.S. Consumer Product Safety Commission recalled 4.1 million notebook batteries on Tuesday, August 15. The recall affects certain Inspiron, Latitude and Precision mobile workstations and XPS units shipped between April 2004 and July 18, 2006. Sony manufactured the batteries that are being recalled. Dell has so far received six reports of overheating units that caused property damage, but no injuries. Customers can determine if they need a new battery at: https://www.dellbatteryprogram.com/Default.aspx

Category 28.3 Heat, fires, explosions

2006-10-23 DHS Daily OSIR; USA TODAY http://www.usatoday.com/tech/news/2006-10-23-battery-usat_x.htm

SONY RECALLS 3.5 MILLION MORE BATTERIES.

Sony and the Consumer Product Safety Commission said late Monday, October 23, that the company will recall nearly 3.5 million additional laptop computer batteries because of fire risks. The new recall involvesnumerous models of batteries in some Sony, Gateway, Toshiba and Fujitsu laptops. Consumers can check their PC-maker's Website or cpsc.gov. The new recall comes as buyers have returned only a small percentage of the 7 million Sony laptop batteries already recalled, data from computer-makers and analysts suggest.

Category 28.3 Heat, fires, explosions

2007-01-19 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2173035/nokia-cleared-exploding-phone

NOKIA CLEARED IN EXPLODING PHONE CASE.

A man thought to have been the victim of an exploding mobile phone has left investigators baffled after engineers examined the device and gave it the all clear. Luis Picaso, 59, is in a critical condition with 50 percent second- and third-degree burns to his upper body, back, right arm and right leg after being found in his hotel room in Vallejo, CA. The cause of the fire was assumed to be his mobile phone, which was still in his pocket where the fire started. But engineers from Nokia have flown to California to examine the 2125i handset and gave it the all clear and were even able to switch it on. While there have been instances of mobile phones overheating and catching fire, the usual culprit is third-party batteries with faulty power management controllers.

Category 28.3 Heat, fires, explosions

2007-03-01 DHS Daily OSIR; IDG News Service http://www.infoworld.com/article/07/03/01/HNlenovorecallsbat teries_1.html

LENOVO RECALLS 205,000 NOTEBOOK BATTERIES.

Months after joining other PC vendors in a massive recall of faulty notebook batteries, Lenovo Group has found a different problem with some models, and will recall 205,000 notebook batteries worldwide, the company said Thursday, March 1. Lenovo made the move after four customers complained their batteries overheated after they had dropped or hit the notebooks. The defect caused minor eye irritation for one user, and damaged the property and computers of the others, according to the U.S. Consumer Product Safety Commission. The recall affects the nine-cell, extended-life version of a battery pack manufactured by Sanyo Electric, of Japan.

Category 28.3 Heat, fires, explosions

2007-03-02 DHS Daily OSIR; Reuters http://www.eweek.com/article2/0,1895,2099929,00.asp

SANYO TO SHARE BATTERY RECALL COST WITH LENOVO.

Troubled Japanese electronics maker Sanyo Electric Co. said on Friday, March 2, it would shoulder with China's Lenovo Group the cost of recalling 205,000 Sanyo-made laptop battery packs that can overheat. The ThinkPad battery recall comes during an investigation of loss-making Sanyo by Japan's securities watchdog the Securities Exchange and Surveillance Commission. The lithium-ion extended-life battery packs, jointly designed by Lenovo and Sanyo and tested by Lenovo, can overheat and spark if dropped hard on to the ground, the two companies said.

Category 28.3 Heat, fires, explosions

2007-04-25 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2122185,00.asp

ACER JOINS SONY BATTERY PACK RECALL.

Nine months following those first voluntary recalls of Sony-made notebook battery packs, Acer will recall some 27,000 notebooks that also contained those same lithium-ion batteries. Acer announced the recall Wednesday, April 25. The 27,000 notebooks recalled by Acer were all sold in the United States between May 2004 and November 2006. The models that came with faulty packs included the company's TravelMate notebooks with model numbers 321x, 242x, 330x, 561x, C20x, 422x, 467x and 320x. The recall also involves some models in the company's Aspire line, including the 980x, 556x, 930x, 941x, 560x and 567x.

28.4 Distraction

Category 28.4 Distraction

2006-02-10 http://www.straightdope.com/columns/060210.html

IS CELL PHONE USE IN CARS REALLY DANGEROUS

Dear Cecil:

Last year my town made it illegal to use a "hands-on" cell phone while driving--hands-free phones are still OK. Since laws here tend to get passed on the basis of what will look good in the newspapers, I'm wondering: How dangerous is cell phone use in cars really? You see drivers all the time drinking coffee, putting on makeup, chatting with passengers, etc. As distractions go, the only obvious difference with cell phones is that they're relatively new and thus a target for legislative busybodies and the easily alarmed--there was all that noise a while back about cell phones causing brain cancer. What's the Straight Dope, Cecil? For that matter, what's up with cell phones and cancer? --Fritz R., Chicago

Cecil replies:

Wish I could tell you it was all crap, compañero, but uh-uh. Accumulating evidence suggests gabbing on the phone while driving is definitely dangerous, probably more so than other distractions. What's more, hands-free phones don't solve the problem. What gets you into trouble, it seems, isn't so much fumbling with the phone (though that doesn't help) as the apparent fact that driving and conducting a conversation at the same time consumes more mental processing power than most people can spare. A few data points:

* Cell phones are involved in a lot of crashes. Best evidence: investigations of actual incidents. One study of 456 accidents in Australia requiring a hospital visit (McEvoy et al, BMJ, 2005) found that in nine percent of cases (40 crashes) the driver had been talking on a cell phone during the ten minutes prior to the accident, based on phone records. The authors conclude, "A person using a mobile phone when driving is four times more likely to have a crash that will result in hospital attendance." A 1997 study of 699 accidents in Toronto (Redelmeier and Tibshirani, New England Journal of Medicine) came to a comparable conclusion.

In another study, researchers at the Virginia Tech Transportation Institute installed cameras, sensors, and data recording equipment in 100 cars, then watched what happened over the ensuing 12 to 13 months. They recorded 69 crashes, 761 near crashes, and 8,295 lesser close calls. Of driver distractions that may have contributed to these incidents, use of cell phones was by far the most common, occurring in close to 700 cases. The distant runner-up was passenger-related activities, presumably including conversation, with fewer than 400 instances. Of the cell-phone-related distractions, 87 involved dialing a handheld phone and 466 talking or listening.

* Hands-free phones don't help much. Although laws restricting cell phone use in cars typically make an exception for the hands-free variety, numerous studies show such phones aren't markedly safer. Dialing does make you take your eyes off the road, but as suggested above most cell-phone-related accidents seem to happen while the driver is merely conversing.

* Drivers using cell phones have slower reaction times and miss important visual cues. Studies using driving simulators have found that drivers brake slower, fail to see pedestrians and traffic signals, and otherwise pay less attention to the road while on the phone. Some experts compare driving while phoning to driving while drunk, but a study by folks at the University of Utah (Strayer et al, 2004) suggests that in certain respects drunks actually do better behind the wheel than phone users--they seem to stay closer to the speed limit and brake faster in response to braking vehicles ahead. All in all, there's solid evidence that talking on the phone is among the more dangerous things you can do while driving.

Other cell phone risks quickly noted:

* Do cell phones cause cancer? Most studies say no, but some holdouts still argue the point--and they're not all crackpots, either. One difficulty: digital phones, the most popular type, have been in common use for less than ten years, too short a time for long-term health effects to show up.

* Do cell phones cause other bad things? One never knows. A Hungarian study last fall was ominously entitled "Is There a Relationship Between Cell Phone Use and Semen Quality?" (Answer: maybe, and if so it ain't good.) I've also got a couple reports here of tendinitis and such due to excess sending of text messages.

On the bright side, cell phone interference with medical devices seems to have diminished, due in part to replacement of analog phones by digital ones. Finally, news of a cell-phone-abetted breakthrough in medical diagnosis: UK doctors report that a patient claimed to have "small bumps" in a delicate spot, but by the time he showed up at the clinic the bumps had subsided. "Fortunately, the patient had taken . . . Both a still and a video of his penis" using his cell phone. "The images were very clear and there was no doubt this man had had an outbreak of genital herpes." Ain't progress great?

--CECIL ADAMS

Category 28.4 Distraction

2006-02-10 The Straight Dope http://www.straightdope.com/columns/060210.html

DON'T DRIVE WHILE USING CELL PHONES

Cecil Adams, author of the popular "THE STRAIGHT DOPE" column, summarized the case against driving while talking on cell phones as follows:

Accumulating evidence suggests gabbing on the phone while driving is definitely dangerous, probably more so than other distractions. What's more, hands-free phones don't solve the problem. What gets you into trouble, it seems, isn't so much fumbling with the phone (though that doesn't help) as the apparent fact that driving and conducting a conversation at the same time consumes more mental processing power than most people can spare. A few data points:

Cell phones are involved in a lot of crashes. Best evidence: investigations of actual incidents. One study of 456 accidents in Australia requiring a hospital visit (McEvoy et al, BMJ, 2005) found that in nine percent of cases (40 crashes) the driver had been talking on a cell phone during the ten minutes prior to the accident, based on phone records. The authors conclude, "A person using a mobile phone when driving is four times more likely to have a crash that will result in hospital attendance." A 1997 study of 699 accidents in Toronto (Redelmeier and Tibshirani, New England Journal of Medicine) came to a comparable conclusion.

In another study, researchers at the Virginia Tech Transportation Institute installed cameras, sensors, and data recording equipment in 100 cars, then watched what happened over the ensuing 12 to 13 months. They recorded 69 crashes, 761 near crashes, and 8,295 lesser close calls. Of driver distractions that may have contributed to these incidents, use of cell phones was by far the most common, occurring in close to 700 cases. The distant runner-up was passenger-related activities, presumably including conversation, with fewer than 400 instances. Of the cell-phone-related distractions, 87 involved dialing a handheld phone and 466 talking or listening.

Hands-free phones don't help much. Although laws restricting cell phone use in cars typically make an exception for the hands-free variety, numerous studies show such phones aren't markedly safer. Dialing does make you take your eyes off the road, but as suggested above most cell-phone-related accidents seem to happen while the driver is merely conversing.

Drivers using cell phones have slower reaction times and miss important visual cues. Studies using driving simulators have found that drivers brake slower, fail to see pedestrians and traffic signals, and otherwise pay less attention to the road while on the phone. Some experts compare driving while phoning to driving while drunk, but a study by folks at the University of Utah (Strayer et al, 2004) suggests that in certain respects drunks actually do better behind the wheel than phone users--they seem to stay closer to the speed limit and brake faster in response to braking vehicles ahead. All in all, there's solid evidence that talking on the phone is among the more dangerous things you can do while driving.

. . . .

Category 28.4 Distraction

2007-03-21 INNOVATION (Wall Street Journal 14 Mar 2007) <http://online.wsj.com/article/SB117382745468236048.html>

THE NEW DWI -- DRIVING WHILE TEXTING

Forget DWI. The new traffic-safety issue is DWT -- Driving While Texting. Lawmakers around the country are wrestling with this latest "distracted driving" issue, as electronic devices become an ever more integral part of people's lives. In the last few years a number of states have outlawed the use of handheld cell phones while driving, and 38 states are currently debating bills that would regulate their use while behind the wheel. But few driver distractions are as potentially life-threatening as attempting to read and type messages while weaving through traffic. "I don't think you'd find anyone who would say that trying to text and drive is not reckless behavior," says a spokesman for CTIA -- the Wireless Association, an industry lobby group. The behavior seems particularly prevalent among younger drivers: A study conducted by Nationwide found that while 19% of all drivers own up to text messaging while driving, in the 18-27 age group it's 37%. Meanwhile, a study by the state of Washington in 2006 blamed "driver distractions" for 7.5% of the 50,000 reported accidents in the first nine months of that year, with "operating a handheld communications device," including texting, coming in fifth.

29.1 Addiction, games & violence

Category 29.1 Addiction, games & violence

2006-01-31 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2173816/online-criminals-aim-online

CYBER-CROOKS TAKE AIM AT ONLINE GAMES.

Cyber-criminals are increasingly targeting online games in an effort to rob players of virtual assets and sell them on auction Websites. Trend Micro identified more than 3,600 spyware attacks last year designed to gather log-in and password information for online games such as Second Life, Lineage, and World of Warcraft. The password stealers are often spread through spam messages where they are presented as virtual goods or popular media content such as music or movie files. The thieves can then auction off virtual currencies and accessories such as clothing and weapons.

Category 29.1 Addiction, games & violence

2006-10-18 EDUPAGE; BBC http://news.bbc.co.uk/2/hi/technology/6062980.stm

STUDY SHOWS EVIDENCE OF WEB ADDICTION

A study conducted by researchers at Stanford University indicates considerable and rising rates of Internet addiction among U.S. users. The study, which asked more than 2,500 people about their Web habits, found that almost 14 percent said it was difficult to be offline for more than a few days. Eight percent said they use the Internet as a means to escape the real world, and a similar portion admitted to hiding their Web habits from their partners. Researchers said these kinds of behaviors are not unlike those exhibited by people with problems such as alcoholism. According to the study, the profile of a typical user who has problems with Internet addiction is a single, college-educated, white male who spends more than 30 hours per week using the Internet for "non-essential" purposes. Elias Aboujaoude, one of the researchers in the study, said that it is important to remind ourselves that despite all the benefits of technology, "it creates real problems for a subset of people." Indeed, six percent of the respondents said their addiction had adversely affected their relationships with other people.

29.3 Digital divide, Internet access

Category 29.3 Digital divide, Internet access

2006-04-26 EDUPAGE; http://news.com.com/2100-1034_3-6065240.html

DIGITAL DIVIDE SHRINKING

According to a study conducted by IBM and "The Economist" magazine, although the digital divide remains considerable for some countries, the gaps are shrinking. The study assessed both availability and use of technology in 68 countries and assigned each an "e-readiness" score on a scale of 1 to 10. The gap from the top of the list (Denmark, 9.00) to the bottom (Azerbaijan, 2.92) is indeed significant, but in certain regions of China and India, connectivity rivals that of developed nations, according to Peter Korsten, European director at IBM's Institute for Business Value. The study noted that nearly every country's score improved from last year but that countries nearer the bottom of the list saw greater gains than those in the upper tiers, indicating a shrinking digital divide overall. Beyond the issue of connectivity lies the question of what efforts each country makes to use technology. As Korsten said, "It's up to governments to take advantage with education and other initiatives."

Category 29.3 Digital divide, Internet access

2006-09-05 EDUPAGE; CNET http://news.com.com/2100-7351_3-6112569.html

CONSORTIUM ANNOUNCES FREE WI-FI FOR SILICON VALLEY

A group of companies calling itself Silicon Valley Metro Connect has announced a vast Wi-Fi network covering large portions of Silicon Valley. The network will be the result of a solicitation from the San Mateo County Telecommunications Authority, an agency representing cities and counties in Silicon Valley. The agency selected Metro Connect's bid for the project, though the deal allows cities to work with other contractors. Metro Connect includes IBM, Cisco Systems, Azulstar Networks, and the nonprofit SeaKay. The network, which is expected to begin operating as early as next year, will offer speeds of up to 1 Mbps for free or higher speeds for a fee. Nearly 2.5 million residents of an area covering 1,500 square miles will be able to access the network outside, though they will need to purchase boosters to use the signal inside homes or offices.

Category 29.3 Digital divide, Internet access

2006-09-05 EDUPAGE; San Jose Mercury News
http://www.siliconvalley.com/mld/siliconvalley/15444856.htm

DIGITAL DIVIDE REMAINS FOR STUDENTS

According to new data from the National Center for Education Statistics, despite an overall increase in computer usage among students, minorities continue to trail in their levels of Internet access. The data, gathered from a 2003 survey, indicate that while two-thirds of white students use the Internet, just 47 percent of black students and 44 percent of Hispanic students do so. Due to increasing computer access at schools, the gaps are lower during the school day. At home, however, 54 percent of white students have Internet access, compared to 27 percent of black and 26 percent of Hispanic students. Mark Lloyd, senior fellow at the Center for American Progress, expressed strong concern about the persistence of the digital divide. "This creates incredible barriers for minorities," he said, "[narrowing] their ability to even think about the kind of work they can be doing."

Category 29.3 Digital divide, Internet access

2006-11-06 EDUPAGE; New York Times (registration req'd)
http://www.nytimes.com/2006/11/06/technology/06ecom.html

CASE EXPECTED TO CLARIFY ONLINE ACCESSIBILITY REQUIREMENTS

A lawsuit filed against Target is expected to establish an important ruling concerning the level of access Web site operators are required to provide to users with disabilities. Specifically, the suit alleges that Target's Web site failed to make its site accessible to screen readers, which help visually impaired users read and navigate online. The Americans with Disabilities Act, which was enacted in 1990, sufficiently predates the Web that it provides little guidance on what access retailers are required to offer online. Jane Jarrow, president of Disability Access Information and Support, said that the online education sector is at particularly high risk for discovering that it has unmet legal obligations for users with disabilities. Many online programs rely heavily on chat rooms, a technology that does not accommodate screen readers well, leaving blind and visually impaired students at a significant disadvantage in their efforts to complete coursework online. A recently changed federal regulation allows online programs to qualify for federal financial aid, but institutions that seek to take advantage of this program must meet the terms of the Rehabilitation Act of 1973, which stipulates that Web sites must be accessible to all users to qualify for federal aid.

Category 29.3 Digital divide, Internet access

2007-01-23 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/07/01/23/HNchinainternetgrows_1.html

CHINA INTERNET MARKET GROWS TO 137 MILLION USERS.

China added another 14 million Internet users in 2006, retaining its status as the world's second largest Internet market with 137 million total users, the China Internet Network Information Center announced Tuesday, January 23. Of those, 90.7 million access the Internet using a broadband connection, a 15 percent jump over 2005, although total broadband use held steady at two-thirds of the Internet population. Also, 17 million users now access the Internet primarily via a wireless device.

29.4 Online & electronic voting

Category 29.4 Online & electronic voting

2006-01-19 http://www.computerworld.com/printthis/2006/0,4814,107881,00.html

E-VOTING SYSTEMS TESTER SEES 'PARTICULARLY BAD' SECURITY ISSUES

Herbert Thompson tested Diebold AccuVote optical scanning equipment used for vote-counting in Leon County, FL. Marc Songini interviewed Dr Thompson for an article in Computerworld and discussed the issues. Dr Thompson and his colleagues were able to alter voting results by tampering with the device's memory card. The results could twist the vote-count to favor a preselected candidate. Diebold officials strongly criticized the test methodology, saying that the memory cards were normally sealed precisely to prevent such tampering and that the tests were equivalent to complaining about poor security by deliberately disabling protection and then complaining about security breaches. They also complained that the tests themselves may have violated the terms of Diebold's licensing agreements and intellectual property rights.

Category 29.4 Online & electronic voting

2006-03-31 RISKS; Wisconsin State Journal http://tinyurl.com/napdn

E-VOTING SOFTWARE GLITCHES RUINS UNIVERSITY ELECTION

Computer problems caused the University of Wisconsin-Madison Student Council to throw out online votes cast this week for campus offices, but retained votes cast for two referendums on the same ballot. The cause of the problem may have been a "little-used, multiple-name tool has worked in prior elections but may have been corrupted by a database upgrade several months ago." The main risk appears to be the lack of testing of the voting system prior to the vote (along with no testing after a major software upgrade).

The parallels with the world of voting machines are obvious: the voting system needs to be tested and certified BEFORE voting occurs.

[Abstract by Dana Freiburger]

Category 29.4 Online & electronic voting

2006-06-27 EDUPAGE;
http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1439&Itemid=26

REPORT CALLS E-VOTING TOOLS INSECURE

A report issued by the Brennan Center Task Force on Voting System Security claims that all three of the most commonly used e-voting systems in the United States are vulnerable to fraud but that problems with the systems can be addressed. The task force, which is an effort of the Brennan Center for Justice at New York University Law School, conducted what it called the most comprehensive study of e-voting machines, which will reportedly be used by 80 percent of U.S. voters in November's election. Officials from the task force said they hope the report will encourage state and federal officials to require vendors to address the problems. "We know how to reduce the risks," said Michael Waldman, executive director of the Brennan Center, "and the solutions are within reach." Rep. Rush Holt (D-N.J.) has introduced a bill that would increase the security of e-voting systems.

Category 29.4 Online & electronic voting

2006-09-14 DHS Daily OSIR; Security Focus http://www.securityfocus.com/brief/302

PRINCETON RESEARCHERS DEMONSTRATE DIEBOLD VIRUS.

Researchers at Princeton University have demonstrated major security holes in U.S. electronic voting machines made by Diebold that make vote-stealing viruses a reality. The Diebold AccuVote-TS and TSx systems are the mostly widely deployed voting systems in the United States. The Princeton study was summarized in four main points. First, they found that malicious software, likely in the form of a virus, would be capable of "steal[ing] votes with little if any risk of attention." Second, the study concluded that anyone with physical access to a voting machine, or a memory card that would later be inserted into the machine, could easily install malicious software. Third, the Princeton researchers demonstrated a proof-of-concept virus that manipulates voting results, both on screen and in printed format, stealing votes and potentially rigging a U.S. election. Finally, the paper concludes that the only feasible remedy to such major security concerns is through replacing the voting machines themselves, along with changes to electoral procedures in the U.S. -- noting that software changes alone would be insufficient to patch the Diebold design flaws. Princeton University report: http://itpolicy.princeton.edu/voting/ts-paper.pdf

Category 29.4 Online & electronic voting

2006-10-10 http://www.brennancenter.org/dynamic/subpages/download_file_38150.pdf

THE MACHINERY OF DEMOCRACY: VOTING SYSTEM SECURITY, ACCESSIBILITY, USABILITY, AND COST

On October 10, 2006, the Brennan Center for Justice released The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost. The report is the final product of the first comprehensive, empirical analysis of electronic voting systems in the United States. It comes after nearly two years of study with many of the nation's leading academics, election officials, economists, and security, usability and accessibility experts.

Up until this point, there has been surprisingly little empirical study of voting systems in the areas of security, accessibility, usability, and cost. The result is that jurisdictions make purchasing decisions and adopt laws and procedures that have little to do with their overall goals.

The Brennan Center analysis finds that there is not yet any perfect voting system or set of procedures. One system might be more affordable, but less accessible to members of the disabled community; certain election procedures might make the systems easier to use, but they compromise security.

Election officials and community members should be aware of the trade-offs when choosing one voting system or set of procedures over another, and they should know how to improve the system they choose.

Included in the report is an executive summary of the Brennan Center's June 2006 analysis of voting system security and the August 2006 analysis of voting system usability, as well as analyses of voting system accessibility and cost….

[From the Brennan Center description of the report at < http://www.brennancenter.org/stack_detail.asp?key=97&subkey=38150&proj_key=76 >

Category 29.4 Online & electronic voting

2006-11-14 Effector Online http://www.eff.org/deeplinks/archives/004996.php

E-VOTING PROBLEMS IN TIGHT FLORIDA RACE.

According to vote tallies, more than one in eight voters did not select a candidate in Sarasota County, Florida's Congressional race. Seems fishy, no? Sadly, problems with electronic voting machines may be responsible for the undervote, and, in a race separated by a mere 373 votes, design flaws might be the difference maker. Voters in that county chose last week to scrap the machines in favor of paper ballots by 2008, but that can't remove the shadow evoting machines cast over this election.
For our initial report on this race: http://www.eff.org/deeplinks/archives/004993.php
For the Orlando Sentinel's recent update on the race: http://www.orlandosentinel.com/news/local/state/orl-voterprobs1206nov12

Of course, Sarasota isn't the only close race impacted by e- voting machines. Down over 7,000 votes to Democratic challenger Jim Webb, Virginia Senator George Allen conceded the race without a recount, but the fact remains that a full and thorough recount wasn't even possible. The majority of Virginia counties use touchscreen voting machines, and most of those counties use machines that do not generate voter- verified paper ballots. Instead of creating anything truly useful for officials to recount, the machines simply reproduce data that is already in memory, in effect reprinting the results rather than recounting ballots in any meaningful sense.

Read more about e-voting in Virginia: http://www.eff.org/deeplinks/archives/004996.php

Category 29.4 Online & electronic voting

2006-11-15 Effector Online http://www.eff.org/Activism/E-voting/

ELECTRONIC VOTING MACHINE HEADACHES SHUT OUT CITIZENS. DELAYS MEAN LONG LINES FOR VOTERS IN FLORIDA, UTAH, AND OTHER STATES.

San Francisco - Problems with electronic voting machine failures kept some polls from opening, created long lines, and left many voters puzzled about whether their votes were counted in Tuesday's high stakes election. The Electronic Frontier Foundation (EFF) joined a nationwide team of technology lawyers and other experts staffing nationwide call centers and legal command posts on Election Day. The volunteers chronicled election problems, assisted voters, and worked with election officials to pull malfunctioning machines wherever possible. By 8:00 pm ET on Tuesday, over 17,000 incidents, including machine related problems, had been reported to the Election Protection Coalition's 866-OUR-VOTE hotline. The types of machine problems reported to EFF volunteers were wide-ranging in both size and scope. Polls opened late for machine-related reasons in polling places throughout the country, including Ohio, Florida, Georgia, Virginia, Utah, Indiana, Illinois, Tennessee, and California. In Broward County, Florida, voting machines failed to start up at one polling place, leaving some citizens unable to cast votes for hours. EFF and the Election Protection Coalition sought to keep the polling place open late to accommodate voters frustrated by the delays, but the officials refused. In Utah County, Utah, more than 100 precincts opened one to two hours late on Tuesday due to problems with machines. Both county and state election officials refused to keep polling stations open longer to make up for the lost time, and a judge also turned down a voter's plea for extended hours brought by EFF. "If election officials insist on depending on this unreliable technology, they should be prepared to react appropriately when things go wrong," said EFF Legal Director Cindy Cohn. "Voters should not have to bear the brunt of this poor planning. We are very disappointed that the court did not recognize that." "Jumping vote" problems -- touchscreen machines displaying selections not intended by voters -- once again appeared across the country and across machine models. Some voters again encountered difficulty making or changing selections on touchscreen machines, resulting in long lines and frustrated voters leaving polling places. Optical scan machines also broke down in many places, most prominently in Cook County, Illinois, but also in Los Angeles, California, also leading to long delays for voters. The national monitoring campaign was developed after many states hastily implemented flawed electronic voting machines and related election procedures. Twenty-three states still do not require a paper record of all votes, despite the demonstrated technical failures of e-voting machines in the 2004 presidential election. In addition, most of these machines use "black box" software that hasn't been publicly reviewed for security. But poorly designed systems are not the only problem. Most election workers remain woefully under-trained regarding potential e-voting problems. Vendor technicians frequently have unsupervised access to voting equipment, and local election officials routinely deny attempts to examine e- voting audit data. Along with supporting local election reform, EFF has helped Congressional Rep. Rush Holt's Voter Confidence and Increased Accessibility Act garner immense, bipartisan support. "Voters deserve these practical election reforms -- not long lines and unverifiable results," said EFF Staff Attorney Matt Zimmerman.
For the latest election news: http://www.eff.org/deeplinks/archives/cat_evoting.php
For more on EFF's e-voting efforts: http://www.eff.org/Activism/E-voting/

Category 29.4 Online & electronic voting

2006-12-11 EDUPAGE; Internet News http://www.internetnews.com/bus-news/article.php/3648376

E-VOTING CHANGES DON'T SATISFY ALL

Despite a number of changes to the oversight of electronic voting machines, critics argue that the systems remain open to bugs and mischief. In January, a voluntary program approved by the Election Assistance Commission (EAC) will go into effect that covers testing and certification. Under that program, the National Institute of Standards and Technology will identify independent testing authorities (ITAs) it deems appropriate for testing electronic voting systems. Critics said that because the developers of e-voting systems will choose and pay ITAs, those organizations will be beholden to the voting system company, not to the government or to the voters. Deforest Soaries, former chairman of the EAC, said that such a conflict compromises the integrity of the program. A spokesperson from the EAC noted that the agency does not have authority to manage testing programs for e-voting systems, and he noted that developers of such systems that do not participate in the voluntary program risk being decertified by the EAC.

Category *29.4* *Online & electronic voting*

2007-01-04 DHS Daily OSIR; New York Times
http://www.nytimes.com/2007/01/04/washington/04voting.html

U.S. BARS LAB FROM TESTING ELECTRONIC VOTING.

A laboratory that has tested most of the nation's electronic voting systems has been temporarily barred from approving new machines after federal officials found that it was not following its quality-control procedures and could not document that it was conducting all the required tests. The company, Ciber Inc. of Greenwood Village, CO, has also come under fire from analysts hired by New York State over its plans to test new voting machines for the state. New York could eventually spend $200 million to replace its aging lever devices. Experts on voting systems say the Ciber problems underscore longstanding worries about lax inspections in the secretive world of voting-machine testing. The action by the federal Election Assistance Commission seems certain to fan growing concerns about the reliability and security of the devices. Ciber, the largest tester of the nation's voting machine software, says it is fixing its problems and expects to gain certification soon. Experts say the deficiencies of the laboratory suggest that crucial features like the vote-counting software and security against hacking may not have been thoroughly tested on many machines now in use.

Category *29.4* *Online & electronic voting*

2007-02-06 Effector Online http://www.eff.org/deeplinks/archives/005105.php

FLORIDA GOVERNOR WANTS TO DUMP E-VOTING MACHINES.

Florida Governor Charlie Crist says his state should dump the touch-screen voting systems that were installed after the disputed 2000 presidential race in favor of more reliable optical-scanning machines. Voters would mark up a paper ballot and be able to verify their vote on the spot with a paper receipt. "You go to an ATM machine, you get some kind of a record. You go to the gas station, you get a record. If there's a need for a recount, it's important to have something to count," said Crist. The governor plans to ask the Florida legislature for $20 million to replace the touch-screen machines. The current machines provide no paper backup and have been plagued by irregularities and scandal in recent elections. EFF and a coalition of voting integrity groups, representing Sarasota County voters, have filed suit in state court in Tallahassee asking for a re-vote in Florida's 13th congressional district. In a high-profile battle over former Rep. Katherine Harris' seat, the result was decided by 363 votes, yet over 18,000 ballots cast on Sarasota County's e-voting machines registered no vote in the race, an exceptional anomaly in the State.
For this post and related links: http://www.eff.org/deeplinks/archives/005105.php

Category *29.4* *Online & electronic voting*

2007-02-16 DHS Daily OSIR; InformationWeek
http://www.informationweek.com/shared/printableArticle.jhtml?articleID=197006847

PRINCETON PROFESSOR FINDS NO HARDWARE SECURITY IN E-VOTING MACHINE.

A Princeton University computer science professor who bought several Sequoia electronic voting machines off the Internet claims he found no hardware security to prevent someone from accessing the technology that controls the vote counting. Andrew Appel said Friday, February 16, there was nothing in the five Sequoia AVC Advantage machines he bought for $82 that would stop him from reaching the read-only memory (ROM) chips that hold the program instructions for counting votes. The chips were not soldered to the circuit boards, and could be easily removed with a screwdriver and replaced with other chips. Therefore, a person who had access to a machine chip could reverse engineer the program instructions and then write his own instructions on a ROM chip available from any computer equipment retailer, according to Appel. If that person had access to a machine in a voting station, he could easily open the computer, pop out the original chip from its socket, and press in the new one. Sequoia, which says it has managed thousands of electronic elections for 14 years in 16 states, said the professor's analysis was incorrect because the machines bought off the Internet are not in a voting station, where election officials implement their own security measures to prevent machine tampering.

Category 29.4 Online & electronic voting

2007-05-16 Effector Online http://action.eff.org/site/Advocacy?id=109

ELECTRONIC VOTING REFORM BILL HEADED TO HOUSE FLOOR

A bipartisan bill requiring paper trails for electronic voting machines just cleared a major hurdle and could be taken up by the House of Representatives next week. . . . E-voting machines have wreaked havoc and undermined confidence in our election system. Despite demonstrated technical failures -- including the loss of thousands of votes -- nearly half of all states still do not require a voter-verified paper ballot. Most of the voting machines in operation today haven't been sufficiently reviewed for security, and pollworkers frequently do not receive adequate training to deal with machine problems. Along with requiring machines to produce a voter-verified paper ballot, H.R. 811 mandates random audits, the mandatory availability of voting machine computer code for review by experts and litigants, and many other critical reforms. The House Administration Committee passed the bill last week and approved amendments that further improve it, including a requirement that voters be allowed to use paper ballots upon request and a more robust ban on connecting voting equipment to the Internet. For over three years, EFF has been helping Rep. Rush Holt move this legislation forward, and support from individuals like you has been crucial in garnering an astounding 215 cosponsors. Hundreds of activists joined EFF for Washington, D.C., lobby days in 2005 and 2006, and thousands of letter have poured in to Congress. . . .
Advocacy page: http://action.eff.org/site/Advocacy?id=109

29.7 Social networks

Category 29.7 *Social networks*

2006-02-01 INNOVATION (Reuters/CNet News.com 28 Jan 2006) <http://news.com.com/Online+service+makes+matches+in+the+sky/2100-1038_3-6032505.html>

SOCIAL NETWORKING AT 30,000 FEET

New York-based AirTroductions provides a way for like-minded passengers to find each other and so they can chat during the flight. Travelers register online and create a profile listing their interests. When they book a flight, they can post their itineraries on the site and the registry provides information on their profiles to other AirTroductions passengers on that flight. The registry is free, but it costs $5 to make contact with another passenger. And while the concept was originally conceived as a social networking tool, some users acknowledge that what they are really looking for potential dating partners. Randy Petersen, editor of InsideFlyer magazine, says the system's biggest obstacle is that most frequent flyers put a lot of thought into their seat assignments and won't want to switch to something less comfortable. "A frequent flyer would never give up an upgrade to first class to go back and sit in coach next to someone you may want to throw out of the plane in the first hour," he notes.

Category 29.7 *Social networks*

2006-05-03 INNOVATION (BBC News 2 May 2006) <http://news.bbc.co.uk/2/hi/technology/4953620.stm>

CASH CARD TAPS VIRTUAL FUNDS

The developers of Project Entropia, an online role-playing game, are blurring the lines between virtual and reality with their real world cash card that allows players to convert virtual dollars into hard currency at any cash machine in the world. "We're bridging the gap between virtual reality and reality right now," says Entropia founder Jan Welter. The Entropia economy works by allowing gamers to exchange real currency for Project Entropia Dollars (PEDs) and back again into real money. Gamers accumulate PEDs through their online efforts to acquire and sell goods, buildings and land. For instance, a gamer may assume the role of a hunter who traps virtual animals for their furs and then trades them for weapons. MindArk, maker of Entropia, makes its money by periodically "repairing" all the tools that characters need to survive and prosper. Last year, $165 million passed through the game, and the founders of the online Universe expect that number to more than double this year. "It is incredible to now think that is possible to manufacture and sell a virtual item one minute and then go out and buy real dinner the next minute, with the same funds," says one player, who owns a virtual space resort in the game.

Category 29.7 *Social networks*

2006-05-22 DHS Daily OSIR; Chicago Sun-Times http://www.suntimes.com/output/news/cst-nws-myspace22.html

SCAMS BEGIN TO TARGET USERS OF MYSPACE

The Website MySpace.com has rocketed to second place in worldwide popularity, with an estimated 78 million users. But the site also has brought concerns about teens meeting strangers online. And now there's a new worry: a "phishing" scam that experts say could compromise teens' -- or their parents' -- financial information. As with other phishing scams, the MySpace scam tricks people into going to a copycat page and signing on. Once the user gets on the site, their computer can be infected with software that can later capture keystrokes typed while visiting legitimate banking or shopping sites, said Hiep Dang, director of threat research for Aluria Software.

Category 29.7 *Social networks*

2006-05-25 DHS Daily OSIR; TechWeb http://internetweek.cmp.com/news/188500411

NEW YORK TEEN PAIR CHARGED IN MYSPACE EXTORTION PLOT.

Two New York men were arrested in Los Angeles and charged with trying to extort $150,000 from the popular social networking site MySpace.com, prosecutors announced Wednesday, May 24. The two men allegedly hacked MySpace by exploiting a service vulnerability that let them steal users' personal information. MySpace discovered the intrusion, and notified the joint local and federal task force in Los Angeles. During the investigation, the pair supposedly threatened to release new exploit code unless MySpace came up with $150,000. The two New Yorkers traveled to California Friday, May 19, to meet with MySpace employees, but were met instead by undercover agents from the U.S. Secret Service and the Los Angeles district attorney's office, who arrested them in the sting. Extortion isn't unusual in cyber crime, but it's typically connected with threats to launch a denial-of-service attack against a company's Website. This is one of the first known cases where hackers allegedly threatened to develop exploit code.

Category 29.7 Social networks

2006-06-09 EDUPAGE; Inside Higher Ed http://www.insidehighered.com/news/2006/06/09/blog

PENN TAKES NEW APPROACH WITH BLOGS

Beginning this fall, all incoming students in the College of Arts and Sciences at the University of Pennsylvania will keep blogs of their academic interests and development. Unlike typical blogs, the Penn blogs will not be public. Access is limited to the student, the student's advisor, and, under certain circumstances, authorized university officials. Penn has a long-standing practice of requiring students to complete questionnaires to help guide their academic careers, and the popularity of online forums such as Facebook prompted university officials to introduce the blog format for the questions.

Students will be required to make a small number of entries. Beyond that, they can keep the blog as current as they choose. The blog entries will be part of a student's academic record and cannot be changed later. The introduction of the blogs follows a pilot program last year involving 300 freshmen.

Category 29.7 Social networks

2006-07-19 INNOVATION (Knowledge@Wharton 14 Jun 2006)
<http://knowledge.wharton.upenn.edu/index.cfm?fa=viewArticle&id=1500>

REAPING THE BENEFITS OF SOCIAL NETWORKS

Social networking, in the form of MySpace or Friendster, has gone mainstream among younger Internet users, but the data that social networks reveal has also captured the attention of academics, consultants and corporations seeking insight into how companies operate, how employees interact, and how employee relationships and social networks can be used to improve productivity and channel knowledge dissemination. Wharton management professor Lori Rosenkopf says social network analysis "will give you a sense of whether actual work flow and communication match what you hope to achieve. Maybe there are bottlenecks where one person is managing all interactions. If you expect two groups to work together closely, and you don't see them doing this, you might want to create liaison roles or other relationships to make information flow better." Networks can also reveal what are known as "cosmopolitans" -- the employees who serve as hubs to information flow within a company. "Often you find that people you might not even think of as very valuable turn out to be important links in the structure of the organization," says University of Chicago professor Valery Yakubovich. Rosenkopf notes that companies are just now becoming aware of the benefits of social network analysis: "Some firms are doing interesting things, but in many cases the idea hasn't hit its stride yet. The top leaders of Fortune 100 companies haven't been exposed to it in a major way. They may be aware of things like small worlds and 'The Tipping Point.' It's not yet reached the point where companies are using these ideas for business process reengineering. But I do think it's coming."

Category 29.7 Social networks

2006-07-21 DHS Daily OSIR; Newsfactor Magazine
http://www.newsfactor.com/story.xhtml?story_id=11100AT9AXG3

MYSPACE BANNER AD INFECTS MILLION USERS.

A banner advertisement posted on the MySpace Website may have infected more than one million users with adware, according to security firm iDefense. The advertisement was included in user profiles on MySpace and could have been operating for about one week. The deckoutyourdeck.com advertisement exploited a flaw in the way Microsoft's Internet Explorer (IE) browser handles Windows Metafile image files. Users running unpatched versions of IE would never have realized that the banner ad had silently installed programs that generate pop-up ads on their system.

Category 29.7 Social networks

2006-07-31 EDUPAGE; BBC http://news.bbc.co.uk/2/hi/technology/5230506.stm

U.S. LEGISLATORS MOVE TO BAN SOCIAL NETWORKING SITES

A bill introduced by Rep. Michael Fitzpatrick (R-Pa.) that aims to restrict social networking Web sites in schools and libraries passed the U.S. House of Representatives by a vote of 410-15. The Deleting Online Predators Act (DOPA) would require organizations that receive funds under the federal E-Rate program to install Internet filters that would block access to sites such as Facebook and MySpace. The FCC would be responsible for defining what sites would be covered by the law. According to the American Library Association (ALA), about two-thirds of U.S. libraries would be subject to the law. Supporters of the legislation said that children who use such Web sites become targets of sexual predators. Opponents of the law said it is overly broad and would prevent computer users from accessing a number of unrelated sites, such as Amazon, blogs, wikis, and even news sites. Leslie Burger, president of the ALA, said, "DOPA is redundant and unnecessary legislation," noting that the Children's Internet Protection Act already requires institutions to block Web content considered harmful to children. The bill now goes to the Senate.

Category 29.7 Social networks

2006-08-10 EDUPAGE; The Register
http://www.theregister.com/2006/08/10/social_sites_breed_malware/

REPORT POINTS TO MALWARE IN SOCIAL NETWORKS

A recent monthly report from Internet security firm ScanSafe calls attention to the rising incidence of malware on social networking sites. According to the report, as many as 1 in 600 profile pages contained sypware, adware, or other malicious software. Social networking sites have become extremely popular with children and college students, and Eldar Tuvey, chief executive and cofounder of ScanSafe, said his company's report points to another risk users face. "[B]eyond unsafe contact with harmful adults, these sites are an emerging and potentially ripe threat vector that can expose children to harmful software," he said. The report noted that some sites, including Facebook and LinkedIn, have fewer malware pages than sites without restrictions on who can join. ScanSafe noted that in addition to social networking traffic from teens, use of the sites has also grown to represent about 1 percent of Internet usage in the workplace, potentially exposing corporate networks and users as well.

Category 29.7 Social networks

2006-08-30 EDUPAGE; Chronicle of Higher Education (sub. req'd)
http://chronicle.com/daily/2006/08/2006083001t.htm

HARVARD OFFERS VIRTUAL CLASS IN SECOND LIFE

This fall, Harvard Law School professor Charles Nesson will coteach a course on argument with his daughter, Harvard Extension School instructor Rebecca Nesson, that will take place in the Second Life virtual world. In Second Life, users create avatars that they control, using them to move around the virtual environment and interact with others and with the virtual physical space. A number of other colleges and universities have used Second Life as a component of certain courses. For this new course at Harvard, Nesson and Nesson will teach students--entirely through the virtual environment--how to use blogs, wikis, podcasts, and other electronic tools to make effective arguments. The class, which is open to the public through Harvard's extension school, will take place in an online replica of the university's Ames Courtroom. Rebecca Nesson will hold office hours in Second Life; Charles Nesson's office hours will be in his actual office.

Category 29.7 Social networks

2006-09-08 EDUPAGE; Wall Street Journal (sub. Req'd)
http://online.wsj.com/article/SB115767827826257155.html

FACEBOOK RESPONDS TO USER OUTCRY

An outcry over new features on the social networking site Facebook has prompted the company to add new privacy measures to the site just days after the new features debuted. Earlier this week, Facebook users could take advantage of new tools that work like news feeds, notifying those who sign up for the feeds when users update their profiles. Despite Facebook's mission of connecting users and allowing individuals to post information about themselves on the Web, hundreds of thousands of the site's nine million registered users reportedly complained that the feeds violated their privacy. With the most recent changes, users have the option of controlling which information is included in the feeds. The company said it would later implement the ability to prevent any personal information from being shared through the feeds.

Category 29.7 Social networks

2006-09-12 EDUPAGE; New York Times
http://www.nytimes.com/2006/09/12/technology/12online.html

FACEBOOK OPENS THE GATES

Social networking site Facebook has announced plans to open the site to anyone, a fundamental change from how the site has functioned since it started operating two years ago. Initially, the site was restricted to individuals affiliated with participating college and university campuses. Since then, access was opened to high school students, with some restrictions, and to employees of certain corporations. According to Mark Zuckerberg, founder and chief executive of Facebook, the new change is to accommodate the growing number of individuals who want to join but might not be able to. As students graduate and enter the workforce, he said, some of their colleagues might want to participate but not have a necessary affiliation with their alma mater. Observers noted that until now, one of Facebook's attractions was its exclusivity compared to sites such as MySpace. Zuckerberg pointed out that Facebook users will still have a high degree of control over the information in their profiles and who is allowed to access that information.

Category 29.7 Social networks

2006-09-25 EDUPAGE; ZDNet http://news.zdnet.com/2100-9595_22-6118975.html

MYSPACE WORKS TO EDUCATE PARENTS

Operators of the social networking site MySpace are partnering with several organizations to help educate users of the site--many of whom are minors--and their parents about appropriate ways to protect kids online. MySpace has become wildly popular with the teen crowd and, as a result, with some online predators. Working with Seventeen magazine, the National School Boards Association, and the National Association of Independent Schools, MySpace will write and publish a guide to safe usage of online networking tools. The guide will be available on the MySpace home page and will be distributed to students in grades 7 through 12 at about 55,000 schools. Atoosa Rubenstein, Seventeen's editor in chief, commented that parents bear responsibility for teaching their kids safe habits. "My mom was the person who told me not to walk down the dark alley by myself," she said, "not the person who created the dark alley."

Category 29.7 Social networks

2006-10-30 EDUPAGE; Red Herring http://www.redherring.com/Article.aspx?a=19451

MYSPACE TO IMPLEMENT COPYRIGHT CONTROLS

Social networking site MySpace will begin using software from Gracenote, which will allow it to identify copyrighted music that users have uploaded to the site. The MusicID audio-fingerprinting technology and Global Media Database will also allow the site to block users who try to upload copyrighted music. If a user continues to try to upload copyrighted music, that user's MySpace account will be deleted. Chris DeWolfe, CEO of MySpace, said, "MySpace is staunchly committed to protecting artists' rights." Sites such as MySpace and YouTube have come under increasing pressure to take action against users who include media content without authorization.

Category 29.7 Social networks

2006-11-08 DHS Daily OSIR; CNET News http://www.usatoday.com/tech/products/cnet/2006-11-08-adware-myspace_x.htm

ADWARE MAY BE LURKING IN VIDEO ON MYSPACE.

Several MySpace pages offer what appear to be YouTube videos that trigger installation of adware when played, Websense Security Labs has warned. The explicit videos can be found on a number of user pages on the MySpace social networking Website, Websense said Monday, November 6. They look like You Tube video, but are in fact hosted on a copycat "Yootube.info" Website, Websense said. That Website was still online as of Tuesday evening. "When users click on the video, they are directed to a copy of the video," Websense said. People are then redirected to the Windows Media Player, which will pop up a license agreement with installation of an adware program called Zango Cash, it said. "Assuming that users have accepted the agreement, the video downloads and attempts to install setup.exe from Zango Cash," Websense said.

Category 29.7 Social networks

2006-12-03 EDUPAGE; CNET http://news.com.com/2100-1043_3-6140298.html

TAXES LOOM FOR ONLINE ASSETS

At the fourth annual State of Play/Terra Nova symposium, a panel discussion on the tax implications of real assets in virtual worlds offered attendees a clear message: paying taxes on such assets is just a matter of time. One panelist, Bryan Camp, tax professor at the Texas Tech University School of Law, noted that existing law is sufficiently broadly defined that revenue from activities in a virtual world, such as Second Life or World of Warcraft, is already subject to taxes, despite there being no mechanism to track or collect such taxes. William LaPiana, a wills, trusts, and estates professor at New York Law School, made similar comments, saying that estates above a certain threshold are subject to tax, and that includes virtual assets that are part of those estates. Dan Miller, a senior economist with the Joint Economic Committee of the U.S. Congress, said, "[T]he question is when, not if, Congress and IRS start paying attention to these issues." That committee is expected to release a report next year outlining the government's approach to the issues of taxation on events and assets held in virtual worlds.

Category 29.7 Social networks

2006-12-06 EDUPAGE; New York Times (registration req'd)
http://www.nytimes.com/2006/12/06/technology/06myspace.html

MYSPACE TO SCREEN FOR SEX OFFENDERS

Social networking site MySpace said it is developing tools that will compare data for its 135 million members to published lists of sex offenders. A total of 46 states publish such lists, which include 550,000 registered sex offenders. MySpace's new tool will cross-reference names of users registered to use its site with names on those lists. The tool will also seek to identify matches using date of birth, height, weight, and ZIP code. MySpace staff will review matches to try to determine whether they are accurate; if so, those users will not be permitted to use the site and may be referred to law enforcement officials. Ernie Allen, president of the National Center for Missing and Exploited Children, welcomed the announcement, saying, "It's not a panacea, but it makes a whole lot of sense."

Category 29.7 Social networks

2007-01-22 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/07/01/22/HNmyspacesuesspamking_1.html

MYSPACE FILES LAW SUIT AGAINST SPAM KING.

MySpace.com has filed a lawsuit against the self-proclaimed "Spam King" for allegedly blasting the portal with spam through the use of compromised user accounts, the Website said on Monday, January 22. MySpace also seeks a permanent injunction to bar Scott Richter, who has fought with Microsoft and the state of New York over spam, and his affiliates from using the popular social networking site. Richter runs Optinrealbig.com, an e-mail marketing company based in Westminster, CO. MySpace, which is owned by News Corp., also accused Richter of running afoul of the federal CAN-SPAM act and California's anti-spam law. The suit was filed Friday in U.S. District Court in Los Angeles. MySpace users can send "bulletins" -- a few lines of text -- to blocks of users who are in their circle of friends. That distribution power has made MySpace a frequent target for spammers, who can reach up to thousands of users if they have the log-in and password for a single account.

Category 29.7 Social networks

2007-04-11 Effector Online http://www.eff.org/deeplinks/archives/005190.php

MYTH V. FACT: IS MYSPACE SAFE FOR KIDS?

Does the increased use of social networking sites by children lead to increased risk? Concern about online predators and pornography has led some politicians and law enforcement officials to call for unreasonable restrictions on public access to these sites. But is the perception of increased risk accurate? How much of the public discussion of these trends is myth, and how much is fact? Two recent studies suggest that many fears are overblown. The Crimes Against Children Research Center at the University of New Hampshire recently released a study that found that unwanted online solicitations are down from 19% in 1999 to 13% today -- a decline that is taking place despite the rising popularity of social networking sites. Of the unwanted solicitations that were received, a significant number (43%) came from other minors, not from adults. A separate study of MySpace by Dr. Larry D. Rosen at Cal State found that only 7% of those teens interviewed were ever approached by anyone on MySpace with a sexual intent. Nearly all of them simply ignored the person and blocked him from their page. But in the face of this tempered analysis, legislators are still pushing for unreasonable restrictions. The Deleting Online Predators Act (DOPA), which has been re-introduced in the House and Senate, would cut funding to public schools and libraries unless they block access to social networking sites. Meanwhile, some state Attorneys General have been pushing for stricter age verification that will in all likelihood have little or no effect. Adam Thierer, a senior fellow at the Progress and Freedom Foundation, says that attempts to block all social networking sites are likewise unworkable and undesirable, since under the current definition, sites as useful and diverse as Wikipedia, CBSNews, and Flickr would fall into that category. Age verification is another unworkable solution, according to Thierer. As he points out in a recent paper, all the existing methods for verifying age are unreliable and easily circumvented. The danger with age verification solutions is that they may lead parents to a false sense of security. The solution, says Thierer, is not stricter controls, but the same things that have helped defend children in the offline world: education, effective law enforcement, and healthy adult supervision.
For this post and related links: http://www.eff.org/deeplinks/archives/005190.php

Category 29.7 Social networks

2007-04-16 Effector Online

A WIN FOR KIDS' FREE SPEECH RIGHTS

A ruling in the Indiana Court of Appeals last week gave a middle school student her free speech rights back. The girl, who is called "A.B." in the court record, had posted comments on a MySpace page criticizing her school's policy on body piercings. The post was full of expletives, which a judge ruled ""obscene" despite the lack of any sexual content. The girl was found to be a "delinquent child" and was put on probation for nine months. However, the girl appealed the ruling, arguing that her post was protected political speech. A three-judge panel agreed: "While we have little regard for A.B.'s use of vulgar epithets, we conclude that her overall message constitutes political speech." The judges threw out the "delinquent child" finding, holding that the lower court's conclusion "contravened her right to speak." A lot of media coverage focuses on the perceived dangers for kids on the Internet. But, expletives or not, this case shows how students use the web to discuss issues of importance to them. It's heartening that judges like these see the importance as well.
For this post and related links: http://www.eff.org/deeplinks/archives/005198.php

Category 29.7 Social networks

2007-04-25 INNOVATION (The Economist 4 Apr 2007) <
http://economist.com/business/displaystory.cfm?story_id=8960555>

SOCIAL NETWORKING IN THE OFFICE

Social networking, which cut its teeth in consumer sites such as MySpace, is finding a role in the corporate setting. For instance, Visible Path uses a combination of e-mail traffic, calendars and diary entries to identify relationships between people both inside and outside a company. One obvious application is to promote sales leads -- a sales person can use the service to determine who within her company has the closest links to a hot prospect, and request an introduction. Another new offering from IBM, Lotus Connections, allows workers to post detailed profiles of themselves, team up on projects and share bookmarks. One beta testing site is using it to pair inexperienced members of its customer-service operation with engineers to teach them the ropes.

Category 29.7 Social networks

2007-05-14 DHS Daily OSIR; Telegraph (UK)
http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/05/14/nfraud14.xml

ONLINE COMMUNITIES FACE MONEY-LAUNDERING.

Anti-Fraud experts are calling on the UK government to start regulating virtual online communities amid fears that criminals and terrorists could use them to launder money. The Fraud Advisory Panel (FAP) issued a report warning that participants in online communities such as Second Life could transfer large amounts of money with little risk of detection. Second Life, which has 6.2 million users, was created by Linden Lab, a U.S. company. Players use "Linden dollars" which are converted from real currencies. Experts claim there are few checks to ensure whether these transfers are legitimate. Potential criminals can hide behind the computer characters they create, making identification difficult. FAP members believe gangs could use Second Life for credit card fraud, identity theft and tax evasion. David Naylor of Field Fisher Waterhouse, the first major law firm to set up in Second Life, said Linden dollars were being exchanged for real currencies on Second Life and eBay using credit cards and PayPal accounts. "From the point of view of money laundering it's like operating an unregulated currency exchange," he said.

Category 29.7 Social networks

2007-05-23 INNOVATION (Silicon.com 15 May 2007)
<http://www.silicon.com/retailandleisure/0,3800011842,39167128,00.htm>

LEGAL TROUBLES IN SECOND LIFE

Planning on doing business in Second Life? Maybe you should consult a lawyer first. These virtual worlds may contain legal minefields to navigate. After all, commerce is one of the fundamental building blocks of Second Life. Players can create, buy and sell goods, and the money they make (in Linden dollars, the currency of Second Life) can be turned into real-world cash. Like real-world currencies, the exact value depends on the current exchange rate. The legal issues you might encounter are as varied as the avatars and buildings you come across as you traverse the virtual landscape. Lawyers say transactions like buying, selling and even employing staff in a virtual world may have real-world legal implications. Other issues such as gambling in virtual casinos and offering financial services through virtual banks can raise even more regulatory issues. And, of course, whenever you have people -- or avatars -- making money, then you have the taxman interested too. Throw in additional concerns, such as competition, intellectual property exploitation and infringement, and there's little wonder the lawyers are getting interested. Considering all that, it’s no surprise that law firms are moving into Second Life. How long before courts and prisons go virtual, too?

31.1 Surveys, studies

Category 31.1 Surveys, studies

2006-01-10 DHS Daily OSIR; http://news.com.com/Study+Instant-messaging+attacks+rose+in+2005/2100-7349_3-6025226.html?tag=cd.top

INSTANT MESSAGING ATTACKS ROSE IN 2005

Security attacks over instant-messaging (IM) networks became more prevalent in 2005, according to a new study. Microsoft's MSN network experienced the largest number of IM security incidents in both 2004 and 2005, while year-on-year incident growth rates were largest on AOL's AIM network, according to the report, published Monday, January 9, by IM security vendor FaceTime Communications. In 2005, MSN had a 57 percent share of the attacks, AOL had 37 percent and Yahoo had six percent, FaceTime said in its "Impact report: Analysis of IM & P2P Threats in 2005." While the incidence rate of attacks over IM is still low compared with e-mail-borne attacks, the rate appears to be increasing rapidly. There were 778 incidents recorded in the fourth quarter of last year compared with 59 in the first quarter, according to the report. Worms and rootkits were at the heart of the main incidents in 2005, said Chris Boyd, security research manager at FaceTime who also warned of the growing danger of cross-network attacks. FaceTime said that exploits can jump networks through IM "consolidation" applications, such as Trillian or Gaim, which let people combine contacts from multiple IM networks on one list. FaceTime's report is available by request: http://www.facetime.com/forms/impact_report2005.aspx

Category 31.1 Surveys, studies

2006-01-11 DHS Daily OSIR; http://searchsecurity.techtarget.com/originalContent/0,28914 2,sid14_gci1157706,00.html

FEDERAL BUREAU OF INVESTIGATION SAYS ATTACKS SUCCEEDING DESPITE SECURITY INVESTMENTS

Despite investing in a variety of security technologies, enterprises continue to suffer network attacks at the hands of malware writers and inside operatives, according to an annual Federal Bureau of Investigation (FBI) report released Wednesday, January 11. The 2005 FBI Computer Crime Survey was taken by 2,066 organizations in Iowa, Nebraska, New York, and Texas late last spring, which survey organizers deemed a good sample of enterprises nationwide. The report is designed to "gain an accurate understanding" of computer security incidents experienced "by the full spectrum of sizes and types of organizations within the United States," the FBI said. The 23-question survey is not the same as the CSI/FBI Computer Crime and Security Survey. The survey addressed such issues as the computer security technologies enterprises used, what kinds of security incidents they've suffered and what actions they've taken. Among the findings: 1) Security software and hardware failed to prevent more than 5,000 incidents among those surveyed; 2) A common point of frustration came from the nonstop barrage of viruses, Trojans, worms and spyware; 3) Use of antivirus, antispyware, firewalls and antispam software is almost universal among those who responded. But the software apparently did little to stop malicious insiders. FBI 2005 Computer Crime Survey: http://www.fbi.gov/publications/ccs2005.pdf

Category 31.1 Surveys, studies

2006-01-11 DHS Daily OSIR; http://www.channelregister.co.uk/2006/01/11/it_spending_shrinks/

EUROPEAN IT SPENDING SHRINKING

IT spending across Europe is under even more pressure and budgets will grow by just 1.6 percent in 2006, compared to 2.9 percent last year. Researchers from Forrester found that more than half of European firms plan to reduce IT budgets this year. The main priority across Europe is for spending on security, anti-virus and host intrusion detection. For IT services price pressure is the main concern, with nearly half of European firms saying that cutting costs is an important or critical priority for the year ahead. Miguel Angel Mendez, associate analyst at Forrester Research, said the caution on IT spending was at odds with people's more optimistic view of their own industries -- 60 percent of respondents expect the coming year to be good or okay for their industries. The feeling in the United Kingdom seems slightly more optimistic -- British firms expect to increase IT spending by 2.3 percent, but only 20 percent of this will go on new developments. Big technology brands such as Cisco, HP, IBM, Microsoft, SAP and Oracle get the lion's share of purchasing preferences.

Category 31.1 Surveys, studies

2006-01-16 DHS Daily OSIR; http://www.net-security.org/press.php?id=3761

NUMBER OF "CLASSIC" VIRUSES DROPPED DRAMATICALLY IN 2005

According to data released by PandaLabs, less than one percent of the new threats detected in 2005 were viruses, whereas threats like Trojans and worms still had a significant presence compared to the previous year. “Viruses, described as threats that add their code to other executable files in order to carry out their malicious actions, have reached rock bottom this year,” explains Luis Corrons, director of PandaLabs. “The aim of creators of this type of threat is usually fame. However, legislation against computer crime in many countries worldwide has led to a dramatic drop in the number of new specimens of this type. Now, almost nobody runs the risk if it does not lead to financial gain.” Of the new threats detected by PandaLabs in 2005, 42 percent were Trojans, 26 percent were bots, 11 percent were backdoor Trojans, eight percent were dialers, six percent were worms and three percent were types of adware/spyware.

Category 31.1 Surveys, studies

2006-01-23 EDUPAGE; http://news.bbc.co.uk/2/hi/business/4637226.stm

U.K. CALLS ON BANKS TO INCREASE ONLINE SECURITY

The Financial Services Authority (FSA), a financial watchdog organization in Britain, has called on the country's banks to increase online security. According to the FSA, losses to online banking fraud tripled in the first half of 2005 compared to a year earlier. A study conducted by the FSA revealed that half of online banking customers are concerned about security and that three-quarters would stop banking online if they are forced to bear the costs of fraud. The group acknowledged that part of the responsibility lies with consumers, who need to understand the risks and the steps they can take to minimize them. Banks, however, must do more to increase security and to educate users, said the FSA. Some banks are piloting projects aimed at increasing online security. Lloyds TSB issued 30,000 electronic security devices that users must have to access their accounts. The devices generate new ID codes every 30 seconds and must be used in tandem with existing security measures.

Category 31.1 Surveys, studies

2006-01-30 EDUPAGE; http://online.wsj.com/article/SB113858617249559658.html

NUMBER OF ID THEFTS DROPS, COSTS RISE

According to a new report from Javelin Strategy and Research and the Better Business Bureau, the number of individuals victimized by identity theft has fallen in recent years, but the amount of money lost to such malfeasance is climbing. Researchers found that about 8.9 million people suffered identity theft last year, compared to 9.3 million the year before. In 2003, the Federal Trade Commission estimated that identity thieves successfully targeted 10.1 million individuals. Experts said the decline in the number of victims indicates heightened awareness and better tools to combat identity crimes. Even as the number of victims has dropped, the total losses to such crimes has risen from $53.2 billion in 2003 to $56.6 billion last year. "Criminals are building up more expertise," said James Van Dyke, founder and principal analyst of Javelin, "and they have to soak victims for more money."

Category 31.1 Surveys, studies

2006-02-03 DHS Daily OSIR; http://www.techweb.com/wire/security/178601917

REPORT: ISP FILTERS FORCING DECLINE IN SPAM.

ISP filters are largely responsible for a decline in e-mail spam, which is expected to continue declining through 2010, according to a report released Friday, February 3, by Jupiter Research. Jupiter said the average e-mail consumer received 3,253 spams in 2005, but that number will drop to 1,640 in 2010. The company forecasts that the volume of spam messages per consumer will decrease by 13 percent a year until 2010. "The next five years will see a more organized e-mail marketing arena," said David Schatsky, senior vice president of research, in a statement.

Category 31.1 Surveys, studies

2006-02-24 DHS Daily OSIR; http://news.com.com/Is+your+cell+phone+due+for+an+antivirus+shot/2100-7349_3-6042745.html

SECURITY EXPERTS: THREATS TO CELL PHONES ARE LIKELY TO INCREASE.

Programs that fight viruses have become a necessary evil on Windows PCs. Now the antivirus industry is turning its attention to mobile phones -- but it's running into reluctance from cell service providers, who aren't so sure that the handset is the best place to handle security. Verizon Wireless doesn't see a need for its customers to install antivirus software on cell phones. "At this point, that is absolutely not required by individual customers," spokesperson Jeffrey Nelson said. But makers of security software are eager to get their products onto handsets, a huge potential market. About 812 million mobile terminals -- such as cell phones and smart phones -- were sold in 2005, according to market researcher Gartner. That compares with an estimated 219 million PCs in the same period. The market research firm expects annual mobile device shipments to exceed one billion units for the first time in 2008. While the number of threats to cell phones is low, security experts and analysts agree that situation is likely to change. Gartner suggests a widespread attack could surface by the end of next year.

Category 31.1 Surveys, studies

2006-02-27 DHS Daily OSIR; http://www.computerworld.com/printthis/2004/0,4814,109007,00.html

BREACHES PUSH COMPANIES TO IMPROVE INTERNAL SAFEGUARDS; SECURITY MANAGERS SHIFT FOCUS TO PREVENTING ACCIDENTAL DATA LEAKS.

After spending years implementing controls to protect network perimeters from external threats, companies are now guarding against internal data lapses, according to attendees at RSA Conference 2006 this month. Driving the trend are concerns about accidental data leaks or thefts resulting from internal miscues, a rash of recent data breaches caused by the mishandling of information, and regulations that require companies to exercise greater control over data they handle. "Even up to last year, there was a huge focus on strengthening the perimeter to make sure the hacker from outside didn't get in," said Stuart McIrvine of IBM. "Everyone was concerned about malware penetrating the perimeter." More recently, though, "there's been a big shift in focus to what's going on inside the enterprise," McIrvine said. Gene Fredriksen of Raymond James Financial Inc. said "Traditional information security has been very good at protecting structured data." But now, he added, there's a whole class of unstructured data in spreadsheets, Web forms, and other formats.

Category 31.1 Surveys, studies

2006-03-07 DHS Daily OSIR; http://today.reuters.com/news/articlenews.aspx?type=technologyNews&storyid=2006-03-07T061445Z_01_N06313562_RTRUKOC_0_US- SYMANTEC-SECURITY.xml

REPORT: CYBER CRIMINALS STEPPING UP TARGETED ATTACKS.

Cyber criminals are stepping up smaller, more targeted attacks as they seek to avoid detection and reap bigger profits by stealing personal and financial information, according to a report issued on Monday, March 6. Symantec Corp.'s Internet Security Threat report said during the second half of 2005, attackers continued to move away from broad attacks seeking to breach firewalls and routers and are now taking aim at the desktop and Web applications. The latest report said threats such as viruses, worms and Trojans that can unearth confidential information from a user's computer rose to 80 percent of the top 50 malicious software code threats from 74 percent in the previous six months.

Category 31.1 Surveys, studies

2006-03-08 EDUPAGE; http://news.yahoo.com/s/nf/20060308/tc_nf/41987

ATTACKS ON THE RISE, WITH MORE MONEY AT RISK

In a new report, computer security firm Symantec says the number of Internet attacks is rising and that the motive for such attacks is increasingly money. The report is based on data gathered from 40,000 security devices from around the world and covers Internet mischief ranging from spam and adware to network attacks and phishing scams. Although many hackers formerly plied their trade merely to demonstrate what they could do, Internet scams such as phishing are designed to put money into the hands of online thieves. Symantec noted that the tools used to launch Internet attacks are becoming very sophisticated, and the report also highlights the fact that many networks remain poorly protected despite simple means to increase security against such threats. Javier Santoyo, development manager at Symantec Security Response, said, "Just letting users know about configuration management and maybe installing heuristics-based solutions on desktops goes a long way."

Category 31.1 Surveys, studies

2006-03-16 DHS Daily OSIR; http://www.theregister.co.uk/2006/03/16/ibm_cybercrime_survey/

CYBERCRIME COSTS BUSINESSES MORE THAN PHYSICAL CRIME.

Cybercrime is more costly to businesses than physical crime, according to a recent IBM survey of 600 U.S. businesses. Lost revenue, wasted staff time dealing with IT security attacks and damage to customer goodwill were rated as a bigger problem than conventional crime by 57 percent of firms in the healthcare, financial, retail and manufacturing industries. Of the respondents in the U.S. finance industry, 71 percent were the most concerned about the threat of cybercrime. According to the IBM survey, 83 percent of U.S. organizations believe they have safeguarded themselves against organized cybercrime but most concentrated on upgrading virus software, improving firewall defenses and implementing patch management systems. IBM said these procedures are a necessary first step but fail to go far enough.

Category 31.1 Surveys, studies

2006-03-17 EDUPAGE; http://news.com.com/2100-7350_3-6050875.html

SURVEY HINTS AT CYBERCRIME LOSSES

A recent survey conducted by IBM of CIOs in manufacturing, financial, health-care, and retail industries shows the growing threat of cybercrime on organizational resources. Of the 600 U.S. CIOs in the survey, 57 percent said cybercrime costs their companies more than conventional crime. About 75 percent said the threat from cybercrime comes in part from within their companies. Moreover, 84 percent said hackers are increasingly part of organized crime, not simply individuals working alone. Results from international CIOs in the survey closely followed those of the U.S. companies for most measures, but they diverged on several key points. Among U.S. CIOs, 83 percent said they were prepared to face the threats of cybercriminals, compared to just 53 percent of internationals.

Category 31.1 Surveys, studies

2006-03-23 EDUPAGE; http://chronicle.com/daily/2006/03/2006032301t.htm

SURVEY SUGGESTS WIDESPREAD PRIVACY VIOLATIONS

A study conducted by Bentley College and software company Watchfire indicates that nearly three-quarters of colleges and universities in California fail to comply with a state law concerning the collection and use of personal information. The California Online Privacy Protection Act of 2003 requires organizations that collect such information online to clearly post privacy policies on their home pages and on every page from which personal information is collected. According to the study, which examined the Web sites of 236 institutions, only 28 percent had privacy policies linked from their home pages. Moreover, every one of the 236 institutional Web sites had at least one page that collects personal data without encrypting it. Mary Culnan, management professor at Bentley and author of the report, said she hopes these results serve "as a wake-up call to students, alumni, and prospective students."

Category 31.1 Surveys, studies

2006-04-03 EDUPAGE; http://news.zdnet.com/2100-1009_22-6057000.html

PROBING WHY PHISHING REMAINS SUCCESSFUL

A new paper published by three academics tries to explain why, after all the press about phishing scams, so many computer users continue to fall for them. "Why Phishing Works," written by Rachna Dhamija of Harvard University and Marti Hearst and J. D. Tygar of the University of California at Berkeley, points out that despite a general awareness of phishing rackets, most users are unable to discern the difference between a legitimate Web site and one spoofed to look like the site of a bank or other financial institution. In one exercise, the researchers created a fake bank site that fooled 91 percent of subjects participating in the experiment. Similarly, 77 percent misidentified a legitimate E*Trade e-mail as fraudulent. Experts attribute some of the problem to ignorance and some to users' not taking simple precautions, such as looking closely at the address bar of Web pages. Bernhard Otupal, a crime intelligence officer for high-tech crime at Interpol, noted that in one recent phishing scam, a number of users went to a site pretending to be that of a prominent bank and entered personal information even though they were not even customers of that bank.

Category 31.1 Surveys, studies

2006-04-03 EDUPAGE; http://www.pcworld.com/news/article/0,aid,125291,00.asp

REPORT ESTIMATES EXTENT OF IDENTITY THEFT

According to data from the National Crime Victimization Survey, which is conducted by the U.S. Department of Justice, identity theft affected an estimated 3.6 million households--with losses totaling $3.2 billion--in the first six months of 2004. The survey contacts a random sample of 42,000 households every six months and follows them for three years. The new data are from the first instance of the survey to specifically address identity theft. The most common types of theft were from unauthorized use of credit cards. Households with annual incomes of more than $75,000 and those headed by individuals between 18 and 24 years old were more likely to suffer identity theft, though the survey did not investigate the possible reasons behind these trends.

Category 31.1 Surveys, studies

2006-04-04 EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4875142.stm

FILE SHARING COSTS BRITISH MUSIC INDUSTRY NEARLY $2 BILLION

The British Phonographic Industry (BPI) estimates that illegal file sharing has cost nearly $2 billion (U.S.) over the past three years, and the International Federation of the Phonographic Industry (IFPI) has filed lawsuits against another 2,000 individuals suspected of file trading in 10 countries. The targets of the new lawsuits are said to be uploaders, those who make copyrighted music available to others for download. The lawsuits are extending to countries such as Portugal, which had not previously been included in such suits. In previous lawsuits, those found guilty of infringement or who settled with the IFPI paid several thousand dollars in fines. The IFPI also pointed out that parents are responsible for the actions of their children and can be made to pay damages on their behalf. Despite the legal action against file sharers and the emergence of legal online music services, data from research firm XTN indicate that in the United Kingdom, illegal downloading has risen 3 percent since September, now representing 28 percent of all music downloads.

Category 31.1 Surveys, studies

2006-04-12 INNOVATION (InformationWeek 27 Mar 2006)
<http://www.informationweek.com/story/showArticle.jhtml?articleID=183702594>

THE UNSEEN COSTS OF MALWARE

A study of 2 million consumer PCs by anti-spyware vendor Webroot found that spyware infected 81% of them last year. Although that percentage was down from 91% in 2004, the average spyware count on each machine climbed in 2005 to 25 instances; in addition, there were more Trojan horses than before. Spyware also is growing in seriousness and complexity, with the embedded code being used to steal funds and data, and adware slows PCs and clogs networks with the traffic it generates. The bad guys specialize in such skills as writing malicious code, placing spyware on PCs, creating false IDs and ATM cards from stolen information, and selling stolen identities. The damage wrought by all this mischief goes beyond the harm felt by the direct victims. Princeton University computer scientist and public affairs professor Edward Felton knows that there are tools on the Web that could help with his hobby of music editing; however, because of the malicious code out on the Internet, he says, "I'm less prone to try new software. I'm more careful of what Web sites I go to. I spend time trying to protect myself." Since he and others like him now shy away from doing business with small companies and from using software from sites they don't know, the result is many lost opportunities both for individual software users and for the companies they would otherwise patronize.

Category 31.1 Surveys, studies

2006-04-18 DHS Daily OSIR; http://news.bbc.co.uk/2/hi/technology/4907588.stm

FIRMS SLOW TO FIX SECURITY FLAWS.

Hackers are getting a helping hand from firms taking too long to fix software vulnerabilities, research shows. A study carried out for security firm McAfee found that 19 percent of companies take more than a week to apply software patches to close vulnerabilities. A further 27 percent said it took two days to apply fixes for software loopholes. Across Europe, the French took the longest to apply patches. It took 27 percent of French firms a week to fix loopholes and a further 39 percent had them applied in 48 hours.

Category 31.1 Surveys, studies

2006-04-24 DHS Daily OSIR; http://www.infoworld.com/article/reuters/2006-04-25_L2447182 0.html

PASSWORD OVERLOAD HITTING FIRMS' IT SECURITY: STUDY.

Security breaches from computer viruses, spyware, hacker attacks and theft of equipment are costing British business an estimated $18 billion a year, according to a survey on Tuesday, April 25. The loss is 50 percent higher than the level calculated two years ago, said the study by consultancy PricewaterhouseCoopers for the Department of Trade and Industry. One area of concern for security, the study warned, was the increasing number of user IDs and passwords employees were having to remember. Virtually every UK company uses anti-virus software, but a quarter of businesses are not protected against the newer threat of spyware. In addition, one in five corporate wireless networks is completely unprotected.

Category 31.1 Surveys, studies

2006-04-25 EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4939386.stm

STUDY SAYS BUSINESSES MAKING PROGRESS AGAINST HACKERS

A survey conducted by PricewaterhouseCoopers for the Department of Trade and Industry indicates that British businesses are making strides in their efforts to thwart computer attacks. Overall, the number of U.K. businesses to suffer computer incidents dropped from 74 percent in 2004 to 62 percent in 2005, according to the Information Security Breaches survey. By far the largest drop was seen in computer viruses, which fell by one-third, while other sorts of attacks and accidental data loss stayed relatively steady, said Chris Potter, who led the survey. He noted that the reduction of incidents follows an increase in security spending in the business sector, which now spends between 4 and 5 percent of technology budgets on security, compared to just 3 percent in 2004. Still, said Potter, many businesses, particularly smaller ones, continue to leave themselves vulnerable to computer attacks. In fact, the survey showed that the number of computer incidents affecting small businesses has risen by 50 percent since 2004.

Category 31.1 Surveys, studies

2006-06-07 EDUPAGE; ZDNet http://news.zdnet.co.uk/internet/0,39020369,39273076,00.htm

STUDY REPORTS ON EMPLOYERS MONITORING EMPLOYEE E-MAIL

A new study conducted by Forrester Research for e-mail security firm Proofpoint indicates that more than one-third of U.S. and British companies read employees' outgoing e-mail. A similar proportion of U.S. companies also said that inappropriate disclosure of information had damaged their businesses within the past 12 months. Exposure of financial or other personal data for clients was the most common concern of businesses worried about the content of outgoing e-mail.

Other concerns included compliance issues and the need to keep business information confidential. The survey also indicated that at nearly one-third of the companies surveyed, an employee had been terminated within the past 12 months for violating e-mail policies.

Category 31.1 *Surveys, studies*

2006-06-13 DHS Daily OSIR; Deloitte
http://www.deloitte.com/dtt/cda/doc/content/us_fsi_150606globalsecuritysurvey(1).pdf

SECURITY BREACHES RISE AT FINANCIAL FIRMS.

More than three-quarters of the world's biggest banks and financial firms suffered an external security attack in the past year and half experienced an internal breach, the 2006 Global Security Survey from advisory firm Deloitte said Tuesday, June 13. Approximately 78 percent of big financial institutions reported a security breach from outside the organization in the past year, up from 26 percent the previous year. More than half of the external attacks were attributed to phishing and pharming. Mike Maddison of Deloitte said the scale and nature of the problem indicated a more serious threat had emerged. The survey of senior security officers at the world's top 100 financial firms said 49 percent of the institutions had experienced at least one internal breach of security in the last year, up from 35 percent a year earlier. Insider fraud and leakage of customer data were cited as the most common internal breaches.

* * *

Key Findings of the Survey (excerpts)

1. Sophistication of attacks and proliferation of vulnerabilities continues to dominate attention.
There continues to be an exponential increase in the sophistication of threats and their potential impact across an organization. When asked to rate the intensity of perceived threats over the next twelve months, 53% of respondents chose phishing and pharming while 51% chose viruses, spyware, trojans and worms. While internal threats continue to rise over previous years (employee misconduct – 20%, internal financial fraud – 19%) organizations appear to be more concerned with threats from the outside, since, in their minds, they bring a higher degree of publicity and damage to reputation.

2. Identity theft – the crime of the 21st Century.
Identity theft is emerging as one of the crimes of the 21st century. It involves the deliberate stealing of another person's identifying information for criminal purposes. According to this year's survey, identity theft and account fraud are two priorities that Financial Institutions (FI) (58%) will likely be focusing on this year. To battle these ever-increasing threats, Fis around the globe will be looking to identify and implement solutions in the areas of data privacy and information management. The rash of high-profile data security breaches in 2005, supported by the survey respondents' admissions that 18% of them have experienced some form of data leakage, has exposed deeply rooted and long-term problems in the way Fis have been managing their sensitive customer data. Identity theft is typically associated with credit card and mail fraud. But new methods, such as spear-phishing (targeted and convincing email attacks) are constantly emerging. High-tech versions include the use of phishing and pharming (persuading people to disclose sensitive information through phony emails and web sites), malicious spyware and hacking to obtain information. Organizations also have to recognize that identity theft is not just about the technology. Low-tech forms consist of laptop, mobile device theft or social engineering techniques, such as posing as a call-centre employee or sending a fake email to obtain personal identifying information. Often the security of information is compromised by human behavior, whereby the individuals who have been entrusted with managing personal information lack adequate security qualifications, leading to an increase in release of confidential, personal identification information. Organizations that are custodians of information are struggling with how they can do a better job of securing and protecting what many would refer to as the "crown jewels" of an organization. Although some organizations have made great strides, particularly in areas such as showing consumers how to protect themselves, many fall far short in other areas, such as revoking access on a timely basis so that former employees and contractors are unable to access and abuse sensitive information.

3. Planning for the unimaginable.
This year, survey respondents reported hardware and software failures as the number one cause of downtime for critical business systems (70%). The ability to continue to function after a major disruption is essential for all organizations – and doubly so for those whose services include providing real-time financial information to their customers. For the first year in the history of this survey, disaster recovery business continuity management is one of the top five priorities for respondents (49%). Even though only 24% of respondents indicate that some form of cost of continuity services has been included as part of the information security budget, it is clear that the information security function is now a key role within the organization. Survey respondents identify viruses (9%), human error (43%) and malicious acts (3%), as some of the causes of serious business interruption that they have experienced.

4. Phishing and pharming lead to Government intervention.
The sophistication of the attacks on today's web applications continues to increase. The threat that respondents most anticipated over the coming year was phishing/pharming (53%), a finding no doubt bolstered by the fact that 51% of respondents have themselves experienced some form of a breach due to phishing/ pharming. As a reaction to this increase, in June 2005, the Federal Deposit Insurance Corporation (FDIC) in the USA stated that financial institutions should implement some form of multi-factor authentication or layered security to protect customer data. This was later supported by The US Federal Financial Institutions Examination Council's (FFIEC), a federal inter-agency council responsible for the examination of US financial institutions. Their guidance entitled "Authentication in an Internet Banking Environment" determined that a User ID and password combination is no longer sufficient to combat increasing threats. In October, 2005, the council released a guideline endorsing twofactor authentication for web banking that is to be adopted by December 2006 citing that single factor

authentication alone is inadequate for high-risk transactions such as access to customer information or the movement of funds.

5. The value of measuring performance.
According to the survey, the challenge lies with the fact that many financial institutions still do not measure the effectiveness of their information security controls – and one cannot prove what one does not measure. While reporting and measurement were identified as one of the top five security initiatives in 2005 (62%), the topic did not make the top five this year. It is difficult to determine whether those who indicated that it was a priority last year achieved their goal, or whether they simply gave up in frustration. In 2006, respondents who indicate that reporting and measurement is a top priority fell to 36%, while the number who indicate that they measure success with their information security programs fell from 34% in 2005 to 23% in 2006. This year, 29% of respondents indicate that they have attempted to define a set of Key Performance Indicators (KPIs) that executives could use to assess and improve their information security programs. Another 30% indicate that this is in progress. However, another 26% of respondents are still struggling with how to define and measure the success of their programs.

6. Convergence is not here yet.
High-level examination shows that corporate and logical security share fundamentally similar internal structures and processes and, therefore, appear to be ripe for convergence. But closer examination reveals the many disparities and challenges. The difficulties do not appear to stem from a lack of rationale but rather from the cultural and structural elements of organizational architecture. Of this year's respondents, only 12% have an individual who is both the Corporate Security Officer and the Chief Information Security Officer. Of the organizations that have separate individuals in each position, 25% of them have a reporting structure that sees both individuals reporting to the same executive. Herein lies the problem: perception and reporting within the organization are major cultural hurdles. Other potential barriers to convergence include issues such as competencies, whereby physical security employees are viewed as either highly specialized in a niche type activity or as not having the same levels of education, training and continual education typically found on the logical side. The result is that there are major differences in areas such as compensation, another disparity that exacerbates barriers and tension between the two groups.

Category 31.1 Surveys, studies

2006-06-20 DHS Daily OSIR; TechWeb http://www.techweb.com/wire/security/189501126

AT&T STUDY FINDS COMPANIES AREN'T PREPARED FOR DISASTERS.

AT&T Inc.'s fifth-annual Business Continuity Survey released Tuesday, June 20, which polled about 1,000 CIOs and IT executives at U.S. companies with more than $10 million in annual revenue, reveals that 28 percent do not have adequate plans in place to cope with natural or other disasters. Nearly 30 percent of executives who participated in the survey said their company has suffered from a disaster. Eighty-one percent of executives said cyber security is part of their overall business plan for interruptions in 2006, up from 75 percent in 2005. Eight out of 10 companies have revised plans in the past 12 months, including 48 percent that say they've been updated in the past six months. Of those companies with plans in place, 40 percent say they have not tested their plan in the past year.

AT&T's study: http://www.sbc.com/Common/files/pdf/biz_cont_full_report.pdf

Category 31.1 Surveys, studies

2006-06-20 eWeek: http://www.eweek.com/article2/0,1895,1979225,00.asp

SECURITY SPENDING SLOWS IN 2006

It may seem counterintuitive, but a survey by Merrill Lynch suggests that enterprises will slow additional spending on new IT security measures in the second half of the year. In March, chief information security officers said that they planned to increase spending by 11.4 percent during the next 12 to 18 months. The more recent survey said that the hike will be only 2.9 percent. The portion of respondents who spend less than 5 percent of their budget on security products increased from 40 percent to 56 percent in the responses, which were gathered at the end of May. The reduced spending can at least in part be explained by the inclusion of security features in hardware and in Windows Vista, the story says. Among other conclusions is that the influence of CISOs continues to grow in the enterprise. [Abstract from IT Business Edge]

Category 31.1 *Surveys, studies*

2006-07-13 DHS Daily OSIR; Search Security
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1199280,00.html

CSI/FBI SURVEY: DATA BREACHES STILL BEING SWEPT UNDER THE RUG.

On the surface, the results of the 11th annual CSI/FBI Computer Crime and Security Survey are positive, with fewer companies reporting financial loss from data breaches compared to last year. But a majority of companies are still reluctant to report security breaches to law enforcement, suggesting that the survey isn't capturing the full extent of the problem. The Computer Security Institute (CSI) and the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad released its 2006 report Thursday, July 13, after surveying 616 computer security practitioners in U.S. corporations, government agencies, financial and medical institutions and universities. The average loss reported by respondents was $167,713, an 18 percent decrease over last year's average loss of $203,606. CSI/FBI Survey: http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml

Category 31.1 *Surveys, studies*

2006-08-16 DHS Daily OSIR; Computer World
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9002493&taxonomyId=17

SURVEY: 81 PERCENT OF U.S. FIRMS LOST LAPTOPS WITH SENSITIVE DATA IN THE PAST YEAR.

Loss of confidential data -- including intellectual property, business documents, customer data and employee records -- is a pervasive problem among U.S. companies, according to a survey released Tuesday, August 15 by Ponemon Institute. Eighty-one percent of companies surveyed reported the loss of one or more laptops containing sensitive information during the past 12 months. One of the main reasons corporate data security breaches occur is because companies don't know where their sensitive or confidential business information resides within the network or enterprise systems, said Larry Ponemon of the Ponemon Institute. "This lack of knowledge, coupled with insufficient controls over data stores, can pose a serious threat for both business and governmental organizations," Ponemon said. "Moreover, the danger doesn't stop at the network, but includes employees' and contractors' laptop computers and other portable storage devices." Survey: http://www.vontu.com/uploadedFiles/global/Ponemon-Vontu_US_S urvey-Data_at-Risk.pdf

Category 31.1 *Surveys, studies*

2006-09-12 EDUPAGE; PRNewswire http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/02-08-2005/0002986646&EDATE=

SURVEY FINDS INSIDER SECURITY BREACHES NOT REPORTED

Results of a recent survey indicate that at U.S. corporations, a considerable portion of IT security breaches are not reported. Nearly 80 percent of the respondents to the survey, which was conducted by Ponemon Institute, said that an insider-related breach has not been reported.

Of the 163 companies surveyed, seventy-five percent reported a serious security breach had occurred within the past twelve months. The survey also revealed the most common types of data security breaches. The majority of data breaches involved the loss of confidential business information, followed closely by the loss of personal customer information. The survey reports that of the top data security breaches:

* 39% involved confidential business information
* 27% involved personal information about customers
* 14% involved intellectual property including software source code
* 10% involved personal information about employees.

More than 61 percent of the respondents said careless or untrained employees and contractors cause accidental data leaks "frequently" or "very frequently"; 48 percent said deliberate violations of IT security occur "frequently" or "very frequently." The top reasons cited for insider breaches were lack of resources (93 percent) and lack of leadership (80 percent). Thirty-one percent said no single person at their organization has oversight for insider threats.

Category 31.1 Surveys, studies

2006-10-10 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article96412-10-10-06-Web

MOST CAMPUSES REPORT SECURITY BREACHES.

The majority of higher education managers experienced at least one information technology security incident last year and one-third reported a data loss or theft. Those are among the findings of the second annual Higher Education IT Security Report Card, which CDW-Government released this week. The report is based on a survey of 182 higher education IT directors and managers nationwide. Fifty-eight percent of those respondents reported at least one security incident last year. In addition to the 33 percent reporting data loss or theft, 9 percent of the IT managers encountered data loss or theft of student personal information. Managers cited lack of funding and insufficient staff resources as the biggest barriers to improving campus security.

Category 31.1 Surveys, studies

2006-10-10 DHS Daily OSIR; Information Week
http://www.informationweek.com/security/showArticle.jhtml?articleID=193105716

TELEWORKERS KNOW AND IGNORE SECURITY RISKS, STUDY SAYS.

The majority of telecommuters are aware of the security dangers that go along with using mobile devices and remotely logging onto their employers' networks, yet their behavior for the most part contradicts this awareness, according to a study issued Monday, October 9, by Cisco Systems and research firm InsightExpress. Of 1,000 teleworkers contacted across 10 countries, more than one of every five allows friends, family members, or other non-employees to use his/her work computer to access the Internet. About one-third of the teleworkers admitted using work computers for personal computing, while nearly half of the respondents indicate that they download personal files onto their work devices. One of every four remote workers surveyed indicated he or she opens unknown e-mails when using work devices. Despite this behavior, don't expect companies to corral their remote workers anytime soon. Telecommuting and remote access are "an unstoppable force, so we have to build security for it," says Bob Gleichauf, CTO of Cisco's security business unit. This means security has to be taken out of the hands of end users as much as possible. Security in the future has to be "security out of the box, building security into processes and technologies," he added.

Category 31.1 Surveys, studies

2006-10-17 DHS Daily OSIR; Reuters
http://news.com.com/Study+Workers+often+jot+down+passwords/2100-1029_3-6126924.html

STUDY: WORKERS OFTEN JOT DOWN PASSWORDS.

One in three people write down computer passwords, undermining their security, and companies should look to more advanced methods, including biometrics, to ensure their systems are safe, a new study shows. A study released on Tuesday, October 17, by global research firms Nucleus Research and KnowledgeStorm found companies' attempts to tighten IT security by regularly changing passwords and making them more complex by adding numbers as well as letters had no impact on security. Staff still had a tendency to jot down passwords either on a piece of paper or in a text file on a PC or mobile device. The study, which surveyed 325 U.S. employees, found that a single sign-on system is just as effective as more complex schemes and that user education on the importance of proper password protection did not deter employees from their lax habits. Study: http://www.nucleusresearch.com/research/g68.pdf

Category 31.1 Surveys, studies

2006-10-24 DHS Daily OSIR; Washington Post http://www.washingtonpost.com/wp-dyn/content/article/2006/10/23/AR2006102301257_pf.html

HACKERS ZERO IN ON ONLINE STOCK ACCOUNTS.

Hackers have been breaking into customer accounts at large online brokerages in the U.S. and making unauthorized trades worth millions of dollars as part of a fast-growing new form of online fraud under investigation by federal authorities. E-Trade Financial Corp. said last week that "concerted rings" in Eastern Europe and Thailand caused their customers $18 million in losses in the third quarter alone. TD Ameritrade also has suffered losses from customer account fraud. "It is an industry problem," spokesperson Katrina Becker said. Federal regulators say that the fraud is fed by the rising use of the Internet for personal finance and the easy availability of snooping software that allows hackers to steal personal account information. More than 10 million people have bought or sold investments online in the United States in the last few months, according to Gartner Inc. The scams typically begin with a hacker obtaining customer passwords and user names. One way is by placing keystroke-monitoring software on any public computer. Hackers wait until anyone types in the Web address of an online broker, and then watch the next several dozen keystrokes, which are likely to include someone's password and login name.

Category 31.1 Surveys, studies

2006-10-25 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1759,2037326,00.asp

STUDY: TECHNOLOGY NOT AN IT SECURITY SOLUTION.

Management support of security policies is the most important element in effectively securing organizations' infrastructure, according to the third annual Global Information Security Workforce Study, conducted by analyst firm IDC and sponsored by the (ISC)². The list of imperative ingredients for a secure infrastructure also included having users follow security policy, having qualified security staff, and software and hardware solutions. Responses came from more than 4,000 information security professionals in over 100 countries. Technology as an enabler, but not the solution, for implementing a sound security strategy was an ongoing theme in the results. Processes and people were also highlighted in responses; these are areas which have been traditionally overlooked in favor of trusting hardware and software to solve security problems. The study, released Wednesday, October 25, found that increasingly, responsibility for security information assets is shifting from the chief information officer to other senior managers, and in many cases, outside IT altogether to chief financial and chief risk officers and legal and compliance departments. Global Information Security Workforce Study (registration required): https://www.isc2.org/cgi-bin/request_wfstudy_public.cgi

Category 31.1 Surveys, studies

2006-11-01 http://redtape.msnbc.com/2006/11/us_near_the_bot.html

US NEAR BOTTOM IN PRIVACY STUDY

The privacy watchdog groups Privacy International (UK) and the Electronic Privacy Information Center (US) published their annual evaluation of the state of privacy in 36 nations including the European Union on the 1st of November 2006. Argentina, Austria, Belgium, Canada, Germany and New Zealand ranked at the top in protection of citizen privacy. Australia, China, Malaysia, Russia, UK & the US were in the worst-protected category.

Category 31.1 Surveys, studies

2006-11-01 DHS Daily OSIR; Associated Press http://www.nasdaq.com/aspxcontent/NewsStory.aspx?cpath=20061031%5cACQDJON200610311911DOWJONESDJONLINE000948.htm

STUDY: ONE IN FOUR SAY FINANCIAL, PERSONAL INFORMATION STOLEN.

More than one in four Americans say their financial or personal information has been stolen, sometimes by someone they knew, according to a survey released Tuesday, October 31. The study done for Experian, the credit rating agency, found that about 19 percent of consumers report that financial information, including a bank or credit card number, has been misused. About 14 percent say they've had personal information such as a Social Security number or birth certificate taken. The survey, conducted by The Gallup Organization, also found that some consumers were more likely to be victimized than others. Among the prime targets were college graduates, those with annual household income of $75,000 or more, people residing in the West, and Americans between the age of 30 and 49. The study also found that about one-fifth of those who suffered the theft of financial or personal data knew the person who stole their information.

Category 31.1 Surveys, studies

2007-01-15 DHS Daily OSIR; Finextra (UK) http://finextra.com/fullstory.asp?id=16370

PUMP-AND-DUMP STOCK PHISHING SPAM UP 400 PERCENT IN 2006.

Pump and dump penny stock e-mail phishing scams rose by a massive 400 percent in 2006 according to data from digital security firm SonicWall. Last year both U.S. and Canadian regulators warned online investors of the so-called pump-and-dump stock schemes. Gleb Budman of SonicWall, says: "Online theft has become more sophisticated, more "stealthy" and more universal: rather than targeting large organizations, scammers are making substantial profits by focusing on individuals." The SonicWall data also shows a 64 percent increase in the numbers of definite phishing e-mails. The top ten institutions whose names were spoofed by e-mail spammers were all banks. Phishing attempts are becoming more ingenious and scammers are also sending more spam messages for each attack, says SonicWall.

Category 31.1 Surveys, studies

2007-01-22 DHS Daily OSIR; Sophos
http://www.sophos.com/pressoffice/news/articles/2007/01/secrep2007.html

U.S. IS WORST FOR MALWARE HOSTING AND SPAM-RELAYING: REPORT.

Sophos has published its Security Threat Report 2007, examining the threat landscape over the previous twelve months, and predicting malware and spam developments during 2007. The report reveals that the U.S. hosts more than one third of the Websites containing malicious code identified during 2006, as well as relaying more spam than any other nation. The Sophos Security Threat Report 2007 examines in detail the top ten malware threats of the last year, and also confirms that malware authors are continuing to turn their backs on large-scale attacks in favor of more focused strikes against computer users. Microsoft Windows continues to be the primary target for hackers, with Internet criminals increasingly manufacturing downloading Trojan horses rather than mass-mailing worms to do their dirty work for them.
Report (registration required): http://www.sophos.com/security/whitepapers/sophos-security-threats-2007_wsrus

Category 31.1 Surveys, studies

2007-01-26 DHS Daily OSIR; Finenxtra (UK) http://finextra.com/fullstory.asp?id=16432

CUSTOMERS WANT STRONGER AUTHENTICATION FOR WEB BANKING, SAYS RSA.

An overwhelming majority of consumers would willingly ditch password protection in favor of stronger authentication technology for online banking, according to a global poll published by RSA security. The survey of nearly 1,700 customers in eight countries also found that 82 percent want banks and brokerages to monitor online and telephone banking transactions for suspicious activity -- similar to the way that credit card transactions are monitored. Furthermore, 91 percent are willing use a new authentication method, beyond the standard username-and-password procedure, if their banks decided to offer stronger security. Over two third of respondents (69 percent) say banks should replace the standard username-and-password log-in procedure with stronger authentication. More than half (58 percent) also want banks to ramp up telephone banking authentication. But consumers are divided on the kind of stronger authentication they want. Nearly three quarters (73 percent) voted for "risk-based" authentication, which involves a behind-the-scenes assessment of the user's identity based on factors including log-on location, IP address and transaction behavior. Around 40 percent said they would like to use a hardware token for authentication, while 56 percent opted for image-based authentication. RSA Study: http://finextra.com/finextra-downloads/newsdocs/RSAauth.pdf

Category 31.1 Surveys, studies

2007-02-05 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/07/02/05/HNbanksecuritystudy_1.html

STUDY: USERS IGNORE BANK SECURITY FEATURES.

Users of online banking sites tend to bypass critical clues that the integrity of those sites may have been compromised, according to the working draft of a study released on Sunday, February 4, by researchers at Harvard University and the Massachusetts Institute of Technology. The study, which will be formally released in May at the IEEE Symposium on Security and Privacy in Oakland, CA, underscores how new technologies and warnings can't completely protect Internet users. For the first test, HTTPS indicators were removed from the address bar along with the lock that appears in the bottom right corner of Internet Explorer 6. Although the absence of HTTPS indicators should be a warning, all 67 participants continued with their transactions, the study found. The researchers then conducted a test where the site-authentication image was removed along with the HTTPS indicators. Only two of 60 people chose not to log in when the image was removed. In the last test, researchers replaced a password-entry page with a warning page from Internet Explorer 7 Beta 3. The page advises of a problem with the security certificate of the chosen Website. Despite the warning, 30 of 57 users entered their passwords.

Category 31.1 Surveys, studies

2007-02-06 DHS Daily OSIR; Computer World
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9010540&intsrc=hm_list

STUDY: WEAK PASSWORDS REALLY DO HELP HACKERS.

Left online for 24 days to see how hackers would attack them, four Linux computers with weak passwords were hit by some 270,000 intrusion attempts -- about one attempt every 39 seconds, according to a study conducted by a researcher at the University of Maryland. Among the key findings: Weak passwords really do make hackers' jobs much easier. The study also found that improved selection of usernames and associated passwords can make a big difference in whether attackers get into someone's computer. The study was led by Michel Cukier, an
assistant professor of mechanical engineering and an affiliate of the university's Clark School Center for Risk and Reliability and Institute for Systems Research. His goal was to look at how hackers behave when they attack computer systems -- and what they do once they gain access. Using software tools that help hackers guess usernames and passwords, the study logged the most common words hackers tried to use to log into the systems. Cukier and two graduate students found that most attacks were conducted by hackers using dictionary scripts, which run through lists of common usernames and passwords in attempts to break into a computer.

Category 31.1 Surveys, studies

2007-03-21 DHS Daily OSIR; Associated Press
http://www.accessnorthga.com/news/ap_newfullstory.asp?ID=89500

STUDY: U.S. CITIES UNPREPARED FOR NUCLEAR ATTACK.

The largest U.S. cities are catastrophically unprepared for a nuclear attack and the widespread medicalemergencies that would result, according to a new study from the University of Georgia. The three-year study paints a horrifying picture. Millions dead. Hundreds of thousands more wounded with burns and radiation poisoning. The most critical hospital infrastructure in downtowns destroyed and outlying medical facilities unable to cope with the mass burn injuries. "It would be hard for me to see how we'll make it more than 10 years without a nuclear weapon being detonated on American soil," said Cham Dallas, center director and study co-author. The study looks at four cities -- Atlanta, New York City, Chicago, and Washington, DC -- and simulates the impact a 20 kiloton and a 550 kiloton nuclear detonation would have. The study calls for states to stock thousands of mobile hospital beds in rural areas and make plans for fast transport of the equipment. It also calls for the storage of medical records away from city centers so that they could be accessed if the hospital is destroyed. Cities also should buy geographic information system devices that pinpoint where toxic chemical or radioactive agents have been released.

Category 31.1 Surveys, studies

2007-03-29 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article98089-03-29-07-Web

SUCCESSFUL CYBERATTACKS AGAINST DOD DROP.

The number of successful cyberattacks against the Department of Defense (DoD) networks and information systems declined from about 130 in January 2005 to about 40 in January 2007, Air Force Lt. Gen. Charles Croom, director of the Defense Information Systems Agency, told a House Armed Services Committee subcommittee hearing March 28. In testimony to the House Terrorism, Unconventional Threats and Capabilities Subcommittee, Croom said the decline in successful attacks occurred at the same time DoD deterred increasingly larger numbers of attacks and probes against its information systems. The number of cyber incidents grew from 16,000 in 2004 to 23,000 in 2005 and 30,000 in 2006, he said, in addition to cyberscans running about four times that number each year. Hearing information: http://www.house.gov/hasc/hearing_information.shtml Transcript: http://armedservices.house.gov/pdfs/TUTC032807/Croom_Testimo ny032807.pdf

Category 31.1 Surveys, studies

2007-03-31 DHS Daily OSIR; San Francisco Chronicle http://sfgate.com/cgi-bin/article.cgi?file=/c/a/2007/03/31/M NGSCOVGGI1.DTL

U.S. INTERNET FRAUD AT ALL-TIME HIGH.

Americans lost a record amount to Internet fraud schemes last year, and the notorious "Nigerian 419" scam is blamed for the largest individual losses. A government report on 2006 Internet crimes also records the sudden emergence of extortionists who use e-mail to deliver ominous threats that grave consequences await unless money is sent. The new federal statistics show that Americans reported losing an all-time high of $198.4 million to Internet fraud in 2006, up 8 percent from 2005 levels of $183 million and 191 percent from 2004 levels of $68 million. Law enforcement
officials believe that actual losses are higher -- many victims don't report the crimes because they are embarrassed or afraid to do so. Of the Internet criminals who could be traced to their location, 61 percent resided inside the United States, followed by criminals based in the United Kingdom at 16 percent. Nigeria-based criminals were next at 6 percent. The FBI has received about 159 complaints since the scam emerged, said John Hambrick, the top FBI official at the Internet Crime Complaint Center. The FBI has received no reports of money loss or murder threats that were carried out, he said in an interview. Report: http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf

Category 31.1 Surveys, studies

2007-04-11 DHS Daily OSIR; InformationWeek http://www.informationweek.com/security/showArticle.jhtml

SECURITY BREACHES COST $90 TO $305 PER LOST RECORD.

While security breaches can cost a company dearly when it comes to a marred public image and a loss in customer confidence, the actual financial costs can be staggering. The average security breach can cost a company between $90 and $305 per lost record, according to a new study from Forrester Research. The research firm surveyed 28 companies that had some type of data breach. "After calculating the expenses of legal fees, call centers, lost employee productivity, regulatory fines, stock plummets, and customer losses, it can be dizzying, if not impossible, to come up with a true number," wrote senior analyst Khalid Kark in the report. A recent Forrester survey found that 25% of respondents do not know, or do not know how to determine, the cost of data security breaches. Kark said the majority of organizations will incur a wide array of associated costs, sometimes significant enough to even put them out of business. Report Excerpt: http://www.forrester.com/Research/Document/Excerpt/0,7211,42 082,00.html

31.2 Audits, GAO reports

Category 31.2 Audits, GAO reports

2006-01-31 DHS Daily OSIR; Government Accountability Office
http://www.gao.gov/new.items/d07310.pdf

GAO-07-310: HIGH-RISK SERIES: AN UPDATE (SPECIAL REPORT).

The Government Accountability Office's (GAO) audits and evaluations identify federal programs and operations that, in some cases, are high risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement. In recent years, GAO also has identified high-risk areas to focus on the need for broad-based transformations to address major economy, efficiency, or effectiveness challenges. Since 1990, GAO has periodically reported on government operations it has designated as high risk. In this 2007 update for the 110th Congress, GAO presents the status of high-risk areas identified in 2005 and new high-risk areas warranting attention by Congress and the executive branch. Lasting solutions to high-risk problems offer the potential to save billions of dollars, dramatically improve service to the public, strengthen confidence and trust in the performance and accountability of the U.S. government, and ensure the ability of government to deliver on its promises. This report contains GAO's views on what remains to be done to bring about lasting solutions for each high-risk area. Perseverance by the executive branch in implementing GAO's recommended solutions and continued oversight and action by Congress are both essential to achieving and sustaining progress Highlights: http://www.gao.gov/highlights/d07310high.pdf

Category 31.2 Audits, GAO reports

2006-01-31 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/07/01/31/HNlowcybergrades_1 .html

U.S. GOVERNMENT DOES POORLY IN CYBERSECURITY.

The Cyber Security Industry Alliance (CSIA) has given the U.S. government D grades on its cybersecurity efforts in 2006, and renewed its call for the Congress to pass a comprehensive data protection law in 2007. The CSIA, a trade group representing cybersecurity vendors, gave the U.S. government D grades in three areas: security of sensitive information, security and reliability of critical infrastructure, and federal government information assurance. In addition to a comprehensive data protection bill, CSIA called for the U.S. government to strengthen the power of agency chief information officers and called on agencies to increase testing of cybersecurity controls. Report:
https://www.csialliance.org/resources/pdfs/CSIA_06Report_07A genda_US_Govt.pdf

Category 31.2 Audits, GAO reports

2006-03-23 DHS Daily OSIR; http://www.gao.gov/highlights/d06328high.pdf Source:
http://www.gao.gov/cgi-bin/getrpt?GAO-06-328

GAO-06-328: INFORMATION SECURITY: CONTINUED PROGRESS NEEDED TO STRENGTHEN CONTROLS AT THE INTERNAL REVENUE SERVICE (REPORT).

The Internal Revenue Service (IRS) has a demanding responsibility in collecting taxes, processing tax returns, and enforcing the nation's tax laws. It relies extensively on computerized systems to support its financial and mission-related operations. Effective information security controls are essential for ensuring that information is adequately protected from inadvertent or deliberate misuse, disruption, or destruction. As part of its audit of IRS's fiscal year 2005 financial statements, the Government Accountability Office (GAO) assessed (1) the status of IRS's actions to correct or mitigate previously reported information security weaknesses at two sites and (2) whether controls over key financial and tax processing systems located at the facilities are effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer data. GAO recommends that the IRS Commissioner take several actions to fully implement an information security program. In commenting on a draft of this report, IRS concurred with our recommendations.

Category 31.2 Audits, GAO reports

2006-04-17 DHS Daily OSIR; US Government Accountability Office
http://www.gao.gov/cgi−bin/getrpt?GAO−06−383

DHS SHOULD TAKE STEPS TO ENCOURAGE MORE WIDESPREAD USE OF ITS PROGRAM TO PROTECT AND SHARE CRITICAL INFRASTRUCTURE INFORMATION (REPORT GAO−06−383)

A wide array of cyber and physical assets is critical to America's national security, economic wellbeing, and public health and safety. Information related to threats, vulnerabilities, incidents, and security techniques is instrumental to guarding these critical infrastructures against attacks and mitigating the impact of attacks that may occur. The ability to share security−related information can unify the efforts of federal, state, and local government as well as the private sector, as appropriate, in preventing and minimizing terrorist attacks. The Critical Infrastructure Information Act of 2002 was enacted to encourage nonfederal entities to voluntarily share critical infrastructure information and established protections for it. The Department of Homeland Security (DHS) has a lead role in implementing the act. The Government Accountability Office (GAO) was asked to determine (1) the status of DHS's efforts to implement the act and (2) the challenges it faces in carrying out the act. GAO is recommending that the Secretary of Homeland Security, among other things, better define DHS's and other federal agencies' critical infrastructure information needs, and explain how DHS and the other agencies will use the information received from the private sector. In oral comments on a draft of this report, DHS concurred with our findings and recommendations.

Highlights: http://www.gao.gov/highlights/d06383high.pdf

Category 31.2 Audits, GAO reports

2006-05-03 DHS Daily OSIR; Council on Foreign Relations
http://www.cfr.org/publication/10570/us_government_failing_to_mobilize_private_sector_in_homeland_security_efforts_warns _council_special_report.html

REPORT: GOVERNMENT FAILING TO MOBILIZE PRIVATE SECTOR IN HOMELAND SECURITY EFFORTS.

A special report by the Council on Foreign Relations begins by laying out the policy dilemma in detail, offers a recent history of the security role of the private sector, highlights specific problems that have kept the public-private relationship from maturing, and offers a series of principles for a more productive relationship. It concludes with a series of specific recommendations -- some will be the work of Congress, others the purview of the administration, still others the responsibility of the private sector -- to secure the homeland better. Among its conclusions, it states that to make America more secure, the federal government urgently needs to provide better leadership on homeland security issues and become an active partner with the private sector on target protection, preparedness, response, and recovery. Report: http://www.cfr.org/publication/10457/

Category 31.2 Audits, GAO reports

2006-05-24 DHS Daily OSIR; Government Computer News
http://www.gcn.com/online/vol1_no1/40857-1.html

NIST PUBLISHES DRAFT REPORT ON PIV CARD.

The National Institute of Standards (NIST) has released a draft report detailing requirements and specifications for smart cards and readers that agencies can use when purchasing products to meet upcoming Homeland Security Presidential Directive 12 deadlines. The report offers interoperability standards and performance-based requirements for Personal Identity Verification (PIV) systems consistent with mandates under Federal Information Processing Standard 201-1.

NIST Special Publication 800-96: http://csrc.nist.gov/publications/drafts/800-96/Draft-ipd-sp 800-96-052306.pdf

Category 31.2 Audits, GAO reports

2006-05-31 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-06-498

GAO-06-498: HOMELAND DEFENSE: NATIONAL GUARD BUREAU NEEDS TO CLARIFY CIVIL SUPPORT TEAMS' MISSION AND ADDRESS MANAGEMENT CHALLENGES (REPORT).

To prepare for potential attacks in the United States involving weapons of mass destruction (WMD), Congress approved the development of National Guard Civil Support Teams (CST) tasked to identify chemical, biological, radiological, nuclear, or high-yield explosive weapons; assess consequences; advise civil authorities on response measures; and assist with requests for additional support. Thus far, 36 of the 55 approved teams have been fully certified to conduct their mission. The National Guard Bureau (NGB) is in the process of establishing, certifying, and planning for the long-term sustainment of the CSTs. The Government Accountability Office (GAO) was asked to address the extent to which (1) the CSTs are ready to conduct their mission and (2) effective administrative mechanisms are in place for the CSTs. To ensure the sustainment of CSTs, the Secretary of Defense should work with NGB and the Secretaries of the Army and of the Air Force to clarify the types of non-WMD response efforts that belong in the CST mission; develop guidance to address CST management challenges; and develop guidance and work with state adjutants general to clarify administrative oversight and support structures for CSTs. The Department of Defense generally agreed with GAO's recommendations. Highlights: http://www.gao.gov/highlights/d06498high.pdf

Category 31.2 Audits, GAO reports

2006-05-31 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-06-612

GAO-06-612: HOMELAND SECURITY: GUIDANCE AND STANDARDS ARE NEEDED FOR MEASURING THE EFFECTIVENESS OF AGENCIES' FACILITY PROTECTION EFFORTS (REPORT).

The protection of U.S. federal facilities has become an important concern due to the ongoing threat of terrorism. The General Services Administration (GSA), U.S. Postal Service (USPS), and the Departments of Veterans Affairs (VA) and Interior(Interior) hold the most domestic, nonmilitary property. Additionally, the Department of Homeland Security (DHS) is responsible for the protection of GSA facilities. DHS chairs the Interagency Security Committee (ISC), which is tasked with coordinating federal agencies' facility protection efforts. The need to better protect federal facilities, as well as federal budget constraints, have prompted the need for these agencies to measure the performance of their facility protection efforts. The Government Accountability Office's (GAO) objectives were (1) to identify examples of performance measures for facility protection being used by selected organizations outside of the federal government; and (2) to determine the status of U.S. federal agencies' efforts to develop and use performance measures as a part of their facility protection programs. GAO is recommending that the Secretary of DHS direct ISC to establish guidance and standards for measuring performance in federal government facility protection. DHS agreed with the findings and recommendations in this report. Highlights: http://www.gao.gov/highlights/d06612high.pdf

Category 31.2 Audits, GAO reports

2006-06-09 DHS Daily OSIR; U.S. Newswire http://releases.usnewswire.com/GetRelease.asp?id=67279

JCAHO STUDY ON EMERGENCY PREPAREDNESS PUBLISHED.

A new study from the Joint Commission on Accreditation of Healthcare Organizations finds that community-based preparation for and response to disasters will require more effective communication and planning among hospitals, public health agencies and community first responders than currently exist. The study, "Integrating Hospitals into Community Emergency Preparedness Planning," also found that national benchmarks are needed to measure and promote emergency preparedness planning. The study is the first large-scale national assessment of how closely hospitals and their communities are collaborating and planning together for natural or other disasters. Recent natural disasters and terrorist attacks have underscored the need for health care facilities to integrate their activities with community-based emergency preparedness efforts.

Study: http://www.annals.org/cgi/content/full/144/11/799

Category 31.2 Audits, GAO reports

2006-06-14 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-06-693R

GAO-06-693R: DOD PERSONNEL CLEARANCES

Questions and Answers for the Record Following the Second in a Series of Hearings on Fixing the Security Clearance Process (Correspondence). In this report, the Government Accountability Office addresses three questions posed by the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia. The Government Accountability Office (GAO) will continue to assess and monitor the Department of Defense's (DoD) personnel security clearance program, including DoD's progress in meeting the goals and objectives outlined in the governmentwide plan. At this time, GAO has no ongoing or future work that would assess whether the federal intelligence community is meeting the goals and objectives of the government's plan. GAO is currently reviewing the timeliness and completeness of DoD's and the Office of Personnel Management's processes used to determine whether industry personnel are eligible to hold a Top Secret clearance. GAO will report that information to the subcommittee this fall.

Category 31.2 Audits, GAO reports

2006-06-14 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-06-864T

GAO-06-864T: AVIATION SECURITY: MANAGEMENT CHALLENGES REMAIN FOR THE TRANSPORTATION SECURITY ADMINISTRATION'S SECURE FLIGHT PROGRAM (TESTIMONY).

After the events of September 11, 2001, the Transportation Security Administration (TSA) assumed the function of passenger prescreening —or the matching of passenger information against terrorist watch lists to identify persons who should undergo additional security scrutiny—for domestic flights, which is currently performed by the air carriers. To do so, TSA has been developing Secure Flight. This testimony covers TSA's progress and challenges in (1) developing, managing, and overseeing Secure Flight; (2) coordinating with key stakeholders critical to program operations; (3) addressing key factors that will impact system effectiveness; and (4) minimizing impacts on passenger privacy and protecting passenger rights. A prior Government Accountability Office (GAO) report recommended that the Department of Homeland Security (DHS) direct TSA to take several actions to manage risks associated with Secure Flight's development, including finalizing system requirements, test plans, privacy and redress requirements, and program cost estimates, and establishing plans to obtain data needed to operate the system. DHS generally concurred with GAO's recommendations, but has not yet completed the actions it planned to take. TSA's re-baselining effort is reassessing program goals, requirements, and capabilities.

Highlights: http://www.gao.gov/highlights/d06864thigh.pdf

Category 31.2 Audits, GAO reports

2006-06-14 DHS Daily OSIR; Government Accountability Office
http://www.gao.gov/highlights/d06866thigh.pdf

GAO-06-866: LEADERSHIP NEEDED TO ADDRESS INFORMATION SECURITY WEAKNESSES AND PRIVACY ISSUES (TESTIMONY).

Linda D. Koontz, Director, Information Management Issues
Gregory C. Wilshusen, Director, Information Security Issues
Government Accountability Office of the United States
Testimony before the Committee on Veterans' Affairs, House of Representatives
June 14, 2006

Highlights of Testimony (p. 2 of Report)

For many years, significant concerns have been raised about VA's information security—particularly its lack of a robust information security program, which is vital to avoiding the compromise of government information, including sensitive personal information. Both GAO and the department's inspector general have reported recurring weaknesses in such areas as access controls, physical security, and segregation of incompatible duties. The department has taken steps to address these weaknesses, but these have not been sufficient to establish a comprehensive information security program. For example, it is still developing plans to complete a security incident response program to monitor suspicious activity and cyber alerts, events, and incidents. Without an established and implemented security program, the department will continue to have major challenges in protecting its information and information systems from security breaches such as the one it recently experienced.

In addition to establishing robust security programs, agencies can take a number of actions to help guard against the possibility that databases of personally identifiable information are inadvertently compromised. A key step is to develop a privacy impact assessment—an analysis of how personal information is collected, stored, shared, and managed—whenever information technology is used to process personal information. In addition, agencies can take more specific practical measures aimed at preventing data breaches, including limiting the collection of personal information, limiting the time that such data are retained, limiting access to personal information and training personnel accordingly, and considering the use of technological controls such as encryption when data need to be stored on portable devices.

When data breaches do occur, notification of those affected and/or the public has clear benefits, allowing people the opportunity to protect themselves from identity theft. Although existing laws do not require agencies to notify the public of data breaches, such notification is consistent with agencies' responsibility to inform individuals about how their information is being accessed and used, and it promotes accountability for privacy protection. That said, care is needed in defining appropriate criteria for triggering notification. Notices should be coordinated with law enforcement to avoid impeding ongoing investigations, and in order to be effective, notices should be easy to understand. Because of the possible adverse impact of a compromise of personal information, it is critical that people fully understand the threat and their options for addressing it. Strong leadership, sustained management commitment and effort, disciplined processes, and consistent oversight will be needed for VA to address its persistent, long-standing control weaknesses.

Full report: http://www.gao.gov/cgi-bin/getrpt?GAO-06-866T

Category 31.2 Audits, GAO reports

2006-06-16 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-06-672

GAO-06-672: INTERNET INFRASTRUCTURE: DHS FACES CHALLENGES IN DEVELOPING A JOINT PUBLIC/PRIVATE RECOVERY PLAN (REPORT).

Since the early 1990s, growth in the use of the Internet has revolutionized the way that our nation communicates and conducts business. While the Internet was originally developed by the Department of Defense, the vast majority of its infrastructure is currently owned and operated by the private sector. Federal policy recognizes the need to prepare for debilitating Internet disruptions and tasks the Department of Homeland Security (DHS) with developing an integrated public/private plan for Internet recovery. The Government Accountability Office (GAO) was asked to (1) identify examples of major disruptions to the Internet, (2) identify the primary laws and regulations governing recovery of the Internet in the event of a major disruption, (3) evaluate DHS plans for facilitating recovery from Internet disruptions, and (4) assess challenges to such efforts. GAO is suggesting that Congress consider clarifying the legal framework guiding Internet recovery. GAO is also making recommendations to the Secretary of the Department of Homeland Security to strengthen the department's ability to serve as a focal point for helping to recover from Internet disruptions by completing key plans and activities and addressing challenges. In written comments, DHS agreed with GAO's recommendations. Highlights: http://www.gao.gov/highlights/d06672high.pdf

Category 31.2 Audits, GAO reports

2006-06-20 DHS Daily OSIR; GAO http://www.gao.gov/cgi-bin/getrpt?GAO-06-897T

GAO-06-897T: INFORMATION SECURITY: LEADERSHIP NEEDED TO ADDRESS WEAKNESSES AND PRIVACY ISSUES AT VETERANS AFFAIRS (TESTIMONY).

The recent information security breach at the Department of Veterans Affairs (VA), in which personal data on millions of veterans were compromised, has highlighted the importance of the department's security weaknesses, as well as the ability of federal agencies to protect personal information. Robust federal security programs are critically important to properly protect this information and the privacy of individuals. The Government Accountability Office (GAO) was asked to testify on VA's information security program, ways that agencies can prevent improper disclosures of personal information, and issues concerning notifications of privacy breaches. In preparing this testimony, GAO drew on its previous reports and testimonies, as well as on expert opinion provided in congressional testimony and other sources. To ensure that security and privacy issues are adequately addressed, GAO has made recommendations previously to VA and other agencies on implementing federal privacy and security laws. In addition, GAO has previously testified that in considering security breach notification legislation, the Congress should consider setting specific reporting requirements for agencies.

Highlights: http://www.gao.gov/highlights/d06897thigh.pdf

Category 31.2 Audits, GAO reports

2006-06-22 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-06-905T

GAO-06-905T: INFORMATION TECHNOLOGY: VA AND DOD FACE CHALLENGES IN COMPLETING KEY EFFORTS (REPORT).

The Department of Veterans Affairs (VA) is engaged in an ongoing effort to share electronic medical information with the Department of Defense (DoD), which is important in helping to ensure high-quality health care for active duty military personnel and veterans. Also important, in the face of current military responses to national and foreign crises, is ensuring effective and efficient delivery of veterans' benefits, which is the focus of VA's development of the Veterans Service Network (VETSNET), a modernized system to support benefits payment processes. The Government Accountability Office (GAO) is testifying on (1) VA's efforts to exchange medical information with DoD, including both near-term initiatives involving existing systems and the longer term program to exchange data between the departments' new health information systems, and (2) VA's ongoing project to develop VETSNET. To develop this testimony, GAO relied on its previous work and followed up on agency actions to respond to GAO recommendations. GAO has previously made numerous recommendations on these topics, including that VA and DoD develop an integrated project plan to guide their efforts to share patient health data, and that VA develop an integrated project plan for VETSNET.

Highlights: http://www.gao.gov/highlights/d06905thigh.pdf

Category 31.2 Audits, GAO reports

2006-06-30 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-06-706

GAO-06-706: MANAGING SENSITIVE INFORMATION: DOD CAN MORE EFFECTIVELY REDUCE THE RISK OF CLASSIFICATION ERRORS (REPORT).

Misclassification of national security information impedes effective information sharing, can provide adversaries with information to harm the United States and its allies, and incurs millions of dollars in avoidable administrative costs. As requested, the Government Accountability Office (GAO) examined (1) whether the implementation of the Department of Defense's (DoD) information security management program, effectively minimizes the risk of misclassification; (2) the extent to which DoD personnel follow established procedures for classifying information, to include correctly marking classified information; (3) the reliability of DoD's annual estimate of its number of classification decisions; and (4) the likelihood of DoD's meeting automatic declassification deadlines. To reduce the risk of misclassification and improve DoD's information security operations, GAO is recommending six actions, including several to increase program oversight and accountability. In reviewing a draft of this report, DoD concurred with GAO's recommendations. DoD also provided technical comments, which GAO have included as appropriate. Highlights: http://www.gao.gov/highlights/d06706high.pdf

Category 31.2 Audits, GAO reports

2006-07-05 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-06-939T

GAO-06-939T: BORDER SECURITY: INVESTIGATORS TRANSPORTED RADIOACTIVE SOURCES ACROSS OUR NATION'S BORDERS AT TWO LOCATIONS (TESTIMONY).

Given today's unprecedented terrorism threat environment and the resulting widespread congressional and public interest in the security of the nation's borders, the Government Accountability Office (GAO) conducted an investigation testing whether radioactive sources could be smuggled across U.S. borders. Most travelers enter the United States through the nation's 154 land border ports of entry. Department of Homeland Security U.S. Customs and Border Protection (CBP) inspectors at ports of entry are responsible for theprimary inspection of travelers to determine their admissibility into the United States and to enforce laws related to preventing the entry of contraband, such as drugs and weapons of mass destruction. GAO's testimony provides the results of undercover tests made by its investigators to determine whether monitors at U.S. ports of entry detect radioactive sources in vehicles attempting to enter the United States. GAO also provides observations regarding the procedures that CBP inspectors followed during its investigation. GAO has also issued a report on the results of this investigation (GAO-06-545R). Highlights: http://www.gao.gov/highlights/d06939thigh.pdf

Category 31.2 Audits, GAO reports

2006-07-18 DHS Daily OSIR;
Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-06-885T

GAO-06-885T: GLOBAL WAR ON TERRORISM: OBSERVATIONS ON FUNDING, COSTS, AND FUTURE COMMITMENTS (TESTIMONY).

After the terrorist attacks of September 11, 2001, the President announced a Global War on Terrorism (GWOT), requiring the collective instruments of the entire federal government to counter the threat of terrorism. Ongoing military and diplomatic operations overseas, especially in Iraq and Afghanistan, constitute a key part of GWOT. These operations involve a wide variety of activities such as combating insurgents, civil affairs, capacity building, infrastructure reconstruction, and training military forces of other nations. The U.S. has reported substantial costs to date for GWOT related activities and can expect to incur significant costs for an unspecified time in the future, requiring decision makers to consider difficult trade-offs as the nation faces increasing long-range fiscal challenges. The Government Accountability Office (GAO) has issued several reports on current and future financial commitments required to support GWOT military operations, as well as diplomatic efforts to stabilize and rebuild Iraq. This testimony discusses (1) the funding Congress has appropriated to the Department of Defense (DOD) and other U.S. government agencies for GWOT-related military operations and reconstruction activities since 2001; (2) costs reported for these operations and activities and the reliability of DOD's reported costs, and (3) issues with estimating future U.S. financial commitments associated with continued involvement in GWOT. Highlights: http://www.gao.gov/highlights/d06885thigh.pdf

Category 31.2 Audits, GAO reports

2006-08-01 DHS Daily OSIR; National Defense
http://www.nationaldefensemagazine.org/issues/2006/august/DisjointedDefenseim.htm

DISJOINTED DEFENSE SIMULATION PROGRAMS PROMPT REORGANIZATION.

The increasing demand for virtual training and war gaming has prompted the Department of Defense to reorganize how it manages modeling and simulation. Ongoing efforts to integrate disparate modeling and simulation work reflect growing pressures on the armed services to collaborate more closely in weapon systems procurement, research and development, officials said. "We need to do things better and we need to make a collaborative effort across the community," said Fred Hartman, deputy director of readiness and training policy and programs in the office of the deputy under secretary of defense for personnel and readiness. The Pentagon's modeling and simulation office was directed seven years ago to show the benefits of "cross-service and cross-community" cooperation, said Hartman. To attain "common and cross-cutting" tools, data and services, the office is transitioning to a modeling and simulation coordination office that will support six communities: training, analysis, acquisitions, testing, planning and experimentation.

Category 31.2 *Audits, GAO reports*

2006-08-02 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-06-976T

GAO-06-976T: BORDER SECURITY: CONTINUED WEAKNESSES IN SCREENING ENTRANTS INTO THE UNITED STATES (TESTIMONY).

Agents successfully entered the United States using fictitious driver's licenses and other bogus documentation through nine land ports of entry on the northern and southern borders. CBP officers never questioned the authenticity of the counterfeit documents presented at any of the nine crossings. On three occasions -- in California, Texas, and Arizona -- agents crossed the border on foot. At two of these locations -- Texas and Arizona -- CBP allowed the agents entry into the United States without asking for or inspecting any identification documents. The results of this current work indicate that (1) CBP officers at the nine land border crossings tested did not detect the counterfeit identification we used and (2) people who enter the United States via land crossings are not always asked to present identification. Furthermore, periodic tests since 2002 clearly show that CBP officers are unable to effectively identify counterfeit driver's licenses, birth certificates, and other documents. This vulnerability potentially allows terrorists or others involved in criminal activity to pass freely into the United States from Canada or Mexico with little or no chance of being detected.

Category 31.2 *Audits, GAO reports*

2006-09-06 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-06-618

GAO-06-618: CATASTROPHIC DISASTERS: ENHANCED LEADERSHIP, CAPABILITIES, AND ACCOUNTABILITY CONTROLS WILL IMPROVE THE EFFECTIVENESS OF THE NATION'S PREPAREDNESS, RESPONSE, AND RECOVERY SYSTEM (REPORT).

Hurricane Katrina was the largest, most destructive natural disaster in our nation's history. The problems experienced in responding to Katrina resulted in a number of investigations -- by congressional committees, the White House Homeland Security Council, and others -- regarding the preparations for and response to Katrina. The Government Accountability Office (GAO) assisted the congressional investigations and, under the Comptroller General's authority, initiated a number of Katrina-related reviews. In March 2006 testimony, GAO provided its preliminary observations to Congress. The purpose of this report is to summarize what went well and why, what did not go well and why, and what changes are needed to improve the nation's readiness to respond to a catastrophic disaster; and to identify selected issues associated with the Gulf Coast's recovery. This report is based on GAO's prior work on catastrophic disasters, including Hurricane Andrew in 1992, the over 30 GAO reports completed to date on Hurricanes Katrina and Rita, ongoing GAO work, and other Hurricane Katrina reviews and lessons learned. This report includes six recommendations to the Secretary of the Department of Homeland Security (DHS) with which DHS generally agreed, describing actions taken to implement them. Highlights: http://www.gao.gov/highlights/d06618high.pdf

Category 31.2 *Audits, GAO reports*

2006-09-07 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-06-423

GAO-06-423: OFFSHORING: U.S. SEMICONDUCTOR AND SOFTWARE INDUSTRIES INCREASINGLY PRODUCE IN CHINA AND INDIA (REPORT).

Much attention has focused on offshoring of information technology (IT) services overseas. "Offshoring" of services generally refers to an organization's purchase from other countries of services such as software programming that it previously produced or purchased domestically. IT manufacturing, notably semiconductor manufacturing, has a longer history of offshoring of manufacturing operations. Under the Comptroller General's authority to conduct evaluations on his own initiative, the Government Accountability Office (GAO) addressed the following questions: (1) How has offshoring in semiconductor manufacturing and software services developed over time? (2)What factors enabled the expansion of offshoring in these industries? (3) As these industries have become more global, what have been the trends in their U.S.-based activities? GAO makes no recommendations in this report. GAO provided copies of our draft report to the Departments of State and Commerce. The Department of State did not provide comments; the Department of Commerce agreed with GAO's findings. Highlights: http://www.gao.gov/highlights/d06423high.pdf

Category 31.2 Audits, GAO reports

2006-09-20 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-06-1091T

GAO-06-1091T: AVIATION SAFETY: FAA'S SAFETY EFFORTS GENERALLY STRONG BUT FACE CHALLENGES (TESTIMONY).

The U.S. commercial aviation industry has had an extraordinary safety record in recent years. However, expected increases in air-traffic—including the introduction of new vehicles into the national airspace, such as unmanned vehicles and very light jets—and human resource issues, present challenges that have the potential to strain the existing safety oversight system. The Government Accountability Office's (GAO) testimony focuses on these questions: (1) How is the Federal Aviation Administration (FAA) ensuring that the areas of highest safety risk are addressed? (2) How is FAA ensuring that its staff maintain the skills and knowledge to consistently carry out the agency's oversight programs? and (3) What are the key safety challenges facing FAA? This statement is based on our recent reports on FAA's inspection oversight programs, industry partnership programs, and enforcement and training programs. It is also based on interviews with FAA and relevant industry officials. To help FAA fully realize the benefits of its safety oversight system, GAO has made several recommendations to address the weaknesses identified in GAO's reviews. Although FAA has begun addressing the recommendations, many have not been fully implemented. Highlights: http://www.gao.gov/highlights/d061091thigh.pdf

Category 31.2 Audits, GAO reports

2006-09-29 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-06-1031

GAO-06-1031: TERRORIST WATCH LIST SCREENING: EFFORTS TO HELP REDUCE ADVERSE EFFECTS ON THE PUBLIC (REPORT).

A consolidated watch list managed by the FBI's Terrorist Screening Center (TSC) contains the names of known or suspected terrorists, both international and domestic. Various agencies whose missions require screening for links to terrorism use watch list records. For example, U.S. Customs and Border Protection screens travelers at ports of entry. Because screening is based on names, it can result in misidentifications when persons not on the list have a name that resembles one on the list. Also, some names may be mistakenly included on the watch list. In either case, individuals can be negatively affected and may express concerns or seek agency action, or redress, to prevent future occurrences. This report addresses: (1) the extent to which the numbers of misidentified persons are known and how they could be affected, (2) the major reasons misidentifications occur and the actions agencies are taking to reduce them or minimize their effects, and (3) the opportunities for redress available to individuals with watch list-related concerns. In conducting work at TSC and the principal federal agencies that use watch list data, the Government Accountability Office (GAO) reviewed standard operating procedures and other relevant documentation and interviewed responsible officials. GAO makes no recommendations at this time because the agencies have ongoing initiatives to improve data quality, reduce the number of misidentifications or mitigate their effects, and enhance redress efforts. Highlights: http://www.gao.gov/highlights/d061031high.pdf

Category 31.2 Audits, GAO reports

2007-02-07 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-07-386T

GAO-07-386T: HOMELAND SECURITY: APPLYING RISK MANAGEMENT PRINCIPLES TO GUIDE FEDERAL INVESTMENTS (TESTIMONY).

Since the terrorist attacks of September 11, 2001, and the subsequent creation of the Department of Homeland Security (DHS), the federal government has provided DHS with more than $130 billion in budget authority to make investments in homeland security. However, as the Government Accountability Office (GAO) has reported, this federal financial assistance has not been guided by a clear risk-based strategic plan that fully applies risk management principles. This testimony discusses the extent to which DHS has taken steps to apply risk management principles to target federal funding for homeland security investments (1) in making grant allocations, (2) in funding transportation and port security enhancements, (3) in other DHS mission areas, and (4) at a strategic level across DHS. This testimony summarizes previous GAO work in these areas. GAO has made numerous recommendations over the past four years aimed at enhancing DHS's use of risk management principles to guide homeland security investments in, for example, promoting all-hazards capabilities for catastrophic disasters, assessing customs and immigration systems for immigration enforcement, determining the potential for cyber attacks, and conducting modal transportation security research and
development efforts.
Highlights: http://www.gao.gov/highlights/d07386thigh.pdf

Category 31.2 Audits, GAO reports

2007-02-07 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-07-381R

GAO-07-381R: HOMELAND SECURITY GRANTS: OBSERVATIONS ON PROCESS DHS USED TO ALLOCATE FUNDS TO SELECTED URBAN AREAS (CORRESPONDENCE).

The results of the Urban Areas Security Initiative (UASI) eligibility and funding allocations in fiscal year 2006 raised congressional questions and concerns about Department of Homeland Security's (DHS) methods in making UASI determinations. Several congressional members requested that the Government Accountability Office (GAO) examine aspects of DHS's UASI funding process, and the fiscal year 2007 DHS Appropriations Act directed GAO to examine the validity, relevance, reliability, timeliness, and availability of the risk factors (including threat, vulnerability, and consequence) used by the Secretary of Homeland Security for the purpose of allocating discretionary grants. On November 17, 2006, GAO responded to the mandate and the request by briefing congressional staff on the results of this review. GAO specifically examined (1) DHS's method of estimating relative risk of terrorism in fiscal year 2006; (2) DHS's process for assessing the effectiveness of the various risk mitigation investments submitted in UASI applications; (3) how DHS used estimated relative risk scores and assessments of effectiveness to allocate UASI grant funds in fiscal year 2006; and (4) what changes, if any, DHS plans to make in its UASI award determination process for fiscal year 2007. This letter and the accompanying appendices transmit the information provided during those briefings.

Category 31.2 Audits, GAO reports

2007-03-01 DHS Daily OSIR; National Defense http://www.nationaldefensemagazine.org/issues/2007/March/Def enseDept.htm

DOD NEEDS MORE TECHNICAL EXPERTISE.

Despite decades of acquisition reforms, major military procurement programs continue to experience cost growth and technology readiness problems. These challenges could be solved to a large extent if the Department of Defense (DoD) put more emphasis on the early phases of the development process, says the Pentagon's chief weapon tester. Often the wrong decisions are made because the government lacks enough technical expertise to oversee complex programs, says Charles McQueary, director of operational test and evaluation at the DoD. "You need top notch engineering capability in the government. Unfortunately, the government has lost quite a bit of its systems engineering capabilities, and when you lose these capabilities, you tend to do too much designing without an adequate knowledge of the tradeoffs." Before they enter production, major weapon systems undergo "developmental testing" and later they move to "operational testing." Program officials also tend to identify problems when the systems reach the operational testing phase. At that point, it becomes much more expensive to change the design. "Developmental testing is the place to find problems. Operational testing should be the period of confirmation, not a period of discovery," McQueary says.

Category 31.2 Audits, GAO reports

2007-04-12 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-07-681T

GAO-07-681T: TRANSPORTATION SECURITY: TSA HAS MADE PROGRESS IN IMPLEMENTING THE TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL PROGRAM, BUT CHALLENGES REMAIN (TESTIMONY).

The Transportation Security Administration (TSA) is developing the Transportation Worker Identification Credential (TWIC) to ensure that only workers that do not pose a terrorist threat are allowed to enter secure areas of the nation's transportation facilities. This testimony is based primarily on the Government Accountability Office's (GAO) December 2004 and September 2006 reports on the TWIC program and interviews with TSA and port officials conducted in March and April 2007 to obtain updates on the TWIC program. Specifically, this testimony addresses (1) the progress TSA has made since September 2006 in implementing the TWIC program; and (2) some of the remaining challenges that TSA and the maritime industry must overcome to ensure the successful implementation of the TWIC program. GAO has previously recommended that TSA develop a comprehensive plan for managing the TWIC program, conduct additional testing of the TWIC program to ensure that all key components work effectively, strengthen contract planning and oversight practices, and develop a plan for communicating and coordinating with stakeholders. TSA agreed with these recommendations. Highlights: http://www.gao.gov/highlights/d07681thigh.pdf

Category 31.2 Audits, GAO reports

2007-04-16 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-07-634

GAO-07-634: AVIATION SECURITY: RISK, EXPERIENCE, AND CUSTOMER CONCERNS DRIVE CHANGES TO AIRLINE PASSENGER SCREENING PROCEDURES, BUT EVALUATION AND DOCUMENTATION OF PROPOSED CHANGES COULD BE IMPROVED (REPORT).

The Transportation Security Administration's (TSA) most visible layer of commercial aviation security is the screening of airline passengers at airport checkpoints, where travelers and their carry-on items are screened for explosives and other dangerous items by transportation security officers (TSO). Several revisions made to checkpoint screening procedures have been scrutinized and questioned by the traveling public and Congress in recent years. For this review, the Government Accountability Office (GAO) evaluated (1) TSA's decisions to modify passenger screening procedures between April 2005 and December 2005 and in response to the alleged August 2006 liquid explosives terrorist plot, and (2) how TSA monitored TSO compliance with passenger screening procedures. To conduct this work, GAO reviewed TSA documents, interviewed TSA officials and aviation security experts, and visited 25 airports of varying sizes and locations. In the March 2007 report that contained sensitive security information, GAO recommended, and the Department of Homeland Security concurred, that TSA develop sound methods to assess whether proposed screening changes would achieve their intended purpose and generate complete documentation on proposed screening changes that are deemed significant. Highlights: http://www.gao.gov/highlights/d07634high.pdf

Category 31.2 Audits, GAO reports

2007-04-19 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-07-596T

GAO-07-596T: INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE: PRELIMINARY OBSERVATIONS ON DOD'S APPROACH TO MANAGING REQUIREMENTS FOR NEW SYSTEMS, EXISTING ASSETS, AND SYSTEMS DEVELOPMENT (TESTIMONY).

As operations overseas continue, the Department of Defense (DoD) is experiencing a growing demand for intelligence, surveillance, and reconnaissance (ISR) assets to provide valuable information in support of military operations. While the 2006 Quadrennial Review emphasized the need for the ISR community to improve the integration and management of ISR assets, DoD plans to make significant investments in ISR capabilities for the future. Congress has been interested in DoD's approach for managing and integrating existing assets while acquiring new systems. This testimony addresses preliminary observations based on the Government Accountability Office's (GAO) ongoing work regarding (1) the status of DoD initiatives intended to improve the management and integration of ISR requirements and challenges DoD faces in implementing its initiatives, (2) DoD's approach to managing current ISR assets to support military operations, and (3) the status of selected ISR programs in development and the potential for synergies between them. GAO's ongoing work included document review, interviews with officials at relevant organizations, observations of some U.S. Central Command operations, and review of 13 airborne ISR development programs. Highlights: http://www.gao.gov/highlights/d07596thigh.pdf

Category 31.2 Audits, GAO reports

2007-05-15 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-07-835T

GAO-07-835T: HOMELAND SECURITY: OBSERVATIONS ON DHS AND FEMA EFFORTS TO PREPARE FOR AND RESPOND TO MAJOR AND CATASTROPHIC DISASTERS AND ADDRESS RELATED RECOMMENDATIONS AND LEGISLATION.

As a new hurricane season approaches, the Federal Emergency Management Agency (FEMA) within the Department of Homeland Security (DHS) faces the simultaneous challenges of preparing for the season and implementing the reorganization and other provisions of the Post-Katrina Emergency Management Reform Act of 2006. The Act stipulates major changes to FEMA intended to enhance its preparedness for and response to catastrophic and major disasters. As the Government Accountability Office (GAO) has reported, FEMA and DHS face continued challenges, including clearly defining leadership roles and responsibilities, developing necessary disaster response capabilities, and establishing accountability systems to provide effective services while protecting against waste, fraud, and abuse. This testimony (1) summarizes GAO's findings on these challenges and FEMA's and DHS's efforts to address them; and (2) discusses several disaster management issues for continued congressional attention. This testimony includes no new recommendations, but identifies issues to which Congress, FEMA, and DHS may wish to give continued attention so that FEMA may fulfill the requirements of the Post-Katrina Reform Act. These issues are based on the findings and recommendations of more than 30 Katrina-related GAO reports. Highlights: http://www.gao.gov/highlights/d07835thigh.pdf

Category 31.2 Audits, GAO reports

2007-05-16 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-07-346

GAO-07-346: AVIATION SECURITY: EFFORTS TO STRENGTHEN INTERNATIONAL PASSENGER PRESCREENING ARE UNDER WAY, BUT PLANNING AND IMPLEMENTATION ISSUES REMAIN (REPORT).

Passenger prescreening—a process that includes matching passengers' identifying information against records extracted from the U.S. government terrorist watch list—is one of several security measures in place to help ensure the safety of commercial flights traveling to or from the United States. DHS has several efforts underway to strengthen international aviation passenger prescreening. This report focuses on certain elements of the passenger prescreening process as well as some of the actions that DHS is taking or has planned to strengthen prescreening procedures. This report is a limited version of the original November 2006 report as various agencies that we reviewed deemed some of the information in the original report to be security sensitive. The Government Accountability Office's (GAO) work included interviewing officials and assessing relevant documentation from federal agencies, U.S. and foreign air carriers, industry groups, and several foreign countries. GAO recommended in November 2006 that the Department of Homeland Security complete a strategic plan and develop an evaluation strategy for one of its prescreeningprograms, (2) take steps to ensure that international and domestic prescreening programs are aligned, and (3) ensure full compliance with applicable privacy laws. DHS generally concurred with these recommendations. Highlights: http://www.gao.gov/highlights/d07346high.pdf

Category 31.2 Audits, GAO reports

2007-05-17 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-07-842T

GAO-07-842T: DOD PERSONNEL CLEARANCES: DELAYS AND INADEQUATE DOCUMENTATION FOUND FOR INDUSTRY PERSONNEL (TESTIMONY).

Individuals working for the private industry are playing a larger role in national security work conducted by Department of Defense (DoD) and other federal agencies. As of May 2006, industry personnel held about 34 percent of DoD-maintained personnel security clearances. The damage that the unauthorized disclosure of classified information can cause to national security necessitates the prompt and careful consideration of who is granted a security clearance. Long-standing delays in determining clearance eligibility and other challenges led the Government Accountability Office (GAO) to designate the DoD personnel security clearance program as a high-risk area in January 2005 and again in GAO's January 2007 update of the high-risk areas. In February 2005, DoD transferred its security clearance investigations functions to the Office of Personnel Management (OPM) and now obtains almost all of its clearance investigations from OPM. The Office of Management and Budget is responsible for effective implementation of policy relating to determinations of eligibility for access to classified information. This testimony addresses the timeliness of the process and completeness of documentation used to determine eligibility of industry personnel for top secret clearances in January and February 2006. This statement relies primarily on GAO's September 2006 report (GAO-06-1070).
Highlights: http://www.gao.gov/highlights/d07842thigh.pdf

Category 31.2 Audits, GAO reports

2007-05-24 DHS Daily OSIR; Government Accountability Office http://www.gao.gov/cgi-bin/getrpt?GAO-07-461

GAO-07-461: DEFENSE INFRASTRUCTURE: ACTIONS NEEDED TO GUIDE DOD'S EFFORTS TO IDENTIFY, PRIORITIZE, AND ASSESS ITS CRITICAL INFRASTRUCTURE (REPORT).

The Department of Defense (DoD) relies on a network of DoD and non-DoD infrastructure assets in the United States and abroad so critical that its unavailability could hinder DoD's ability to project, support, and sustain its forces and operations worldwide. DoD established the Defense Critical Infrastructure Program (DCIP) to identify and assure the availability of mission-critical infrastructure. The Government Accountability Office (GAO) was asked to evaluate the extent to which DoD has (1) developed a comprehensive management plan to implement DCIP and (2) identified, prioritized, and assessed its critical infrastructure. GAO analyzed relevant DCIP documents and guidance and met with officials from more than 30 DoD organizations that have DCIP responsibilities, and with Department of Homeland Security (DHS) officials involved in protecting critical infrastructure. GAO recommends DoD take several actions to improve the efficiency and effectiveness of DCIP operations. Actions include developing a comprehensive management plan; issuing a chartering directive defining the relationship between the directorates responsible for DCIP and antiterrorism missions; and identifying non-DoD-owned critical infrastructure for DHS to consider in its assessments. DoD concurred with all of GAO's recommendations. Highlights: http://www.gao.gov/highlights/d07461high.pdf

31.3 Estimates, guesses, predictions, forecasts, recommendations, commentaries

Category 31.3 Estimates, guesses, predictions, forecasts, recommendations, commentaries

2006-01-19 EDUPAGE; http://news.com.com/2100-7349_3-6028946.html

PUTTING A PRICE ON CYBERCRIME

A study by the FBI estimates that yearly losses to computer crimes exceed $67 billion. The study is based on the results of a survey of more than 2,000 organizations, of which 90 percent reported having suffered some form of computer attack in the previous 12 months, and 64 percent said they suffered a financial loss due to those attacks. The average financial loss was $24,000 per company. In estimating total losses, the FBI multiplied the average loss by just 20 percent of U.S. organizations because survey results are often skewed when reporting problems. Even with the significant reduction in the number of affected businesses, the total estimate was an enormous amount of money, far exceeding the $1 billion in losses each year to telecommunications fraud. Because of the relatively large sample size, Bruce Verduyn of the FBI said he believes the estimate is more accurate than other studies that have attempted to quantify losses to cybercrime.

Category 31.3 Estimates, guesses, predictions, forecasts, recommendations, commentaries

2006-02-16 EDUPAGE; http://news.yahoo.com/s/nf/20060216/tc_nf/41677

PREDICTIONS OFFERED ON CYBERTHREATS

The Department of Homeland Security (DHS) and the National Cyber Security Alliance (NCSA) have issued a set of warnings about the kinds of cyberthreats the two organizations anticipate will be on the rise in 2006. Officials involved said the list of predictions is intended to raise awareness of computer threats in the hope that users will better protect themselves. "Arming consumers with a list of emerging threats is just the first step to educating consumers about the ever-evolving online security environment," said Ron Teixeira, executive director of the NCSA. The four areas identified in the list are instant-messaging viruses and worms, phishing, cell-phone and PDA viruses, and attacks on online brokerage accounts. Included with the warnings was acknowledgment that many computer crimes are not reported, complicating the task of tracking them. The agencies provided a number of strategies consumers can use to minimize their risks of being victimized.

Category 31.3 Estimates, guesses, predictions, forecasts, recommendations, commentaries

2006-04-05 http://www.gao.gov/docdblite/details.php?rptno=GAO-06-425

WEAKNESSES IN PROCEDURES AND PERFORMANCE MANAGEMENT HINDER JUNK FAX ENFORCEMENT

The Telephone Consumer Protection Act of 1991 prohibited invasive telemarketing practices, including the faxing of unsolicited advertisements, known as "junk faxes," to individual consumers and businesses. Junk faxes create costs for consumers (paper and toner) and disrupt their fax operations. The Junk Fax Prevention Act of 2005 clarified an established business relationship exemption, specified opt-out procedures for consumers, and requires the Federal Communications Commission (FCC)--the federal agency responsible for junk fax enforcement--to report annually to Congress on junk fax complaints and enforcement. The law also required GAO to report to Congress on FCC's enforcement of the junk fax laws. This report addresses (1) FCC's junk fax procedures and outcomes, (2) the strengths and weaknesses of FCC's procedures, and (3) FCC's junk fax management challenges.

FCC has procedures for receiving and acknowledging the rapidly increasing number of junk fax complaints, but the numbers of investigations and enforcement actions have generally remained the same. In 2000, FCC recorded about 2,200 junk fax complaints; in 2005, it recorded over 46,000. Using its procedures to review the complaints, FCC's Enforcement Bureau (EB) issued 261 citations (i.e., warnings) from 2000 through 2005. EB has ordered six companies to pay forfeitures for continuing to violate the junk fax rules after receiving a citation. The six forfeitures totaled over $6.9 million, none of which has been collected by the Department of Justice for various reasons. EB officials cited competing demands, resource constraints, and the rising sophistication of junk faxers in hiding their identities as hindrances to enforcement. An emphasis on customer service, an effort to document consumers' complaints, and an attempt to target enforcement resources efficiently are the strengths of FCC's procedures; however, inefficient data management, resulting in time-consuming manual data entry, data errors, and--most important--the exclusion of the majority of complaints from decisions about investigations and enforcement, are weaknesses. FCC's guidance to consumers does not provide them with all of the information they need to support FCC's enforcement efforts. FCC faces management challenges in carrying out its junk fax responsibilities. The commission has no clearly articulated long-term or annual goals for junk fax monitoring and enforcement, and it is not analyzing the junk fax data. Without analysis, FCC cannot explore the need for, or implement, changes to its rules, procedures, or consumer guidance that might help deter junk fax violations or give consumers a better understanding of the junk fax rules. Most important, without performance goals and measures and without analysis of complaint and enforcement data, it is not possible to explore the effectiveness of current enforcement measures.

Full report at < http://www.gao.gov/new.items/d06425.pdf >.

Category 31.3 Estimates, guesses, predictions, forecasts, recommendations, commentaries

2006-04-07 DHS Daily OSIR; http://www.computerworld.com/securitytopics/security/story/0,10801,110321,00.html

RESEARCHER: SECURITY RISKS IN WEB SERVICES LARGELY IGNORED.

In their rush to implement Web services, some companies may be exposing themselves to new security risks that they may not fully understand, a security researcher said on Thursday, April 6. During a presentation at the CanSecWest/Core06 Conference, researcher Alex Stamos outlined how a number of Web services technologies, including AJAX and the XQuery query language, could be exploited by hackers to attack systems. Stamos described an attack whereby a user could enter malicious code into a Web form and then get that code to run by calling up the company's customer service number and tricking a representative into inadvertently executing it. Stamos also showed how Web services requests could be used to conduct denial-of-service attacks.

Category 31.3 Estimates, guesses, predictions, forecasts, recommendations, commentaries

2006-04-13 DHS Daily OSIR; http://www.zdnet.com.au/news/software/soa/Boot_Camp_security_risk_is_just_hype_Gartner/0,2000061733,39251707,00.htm

BOOT CAMP SECURITY RISK IS JUST HYPE: GARTNER.

Any talk of Apple's Boot Camp software exposing the company's operating system to security risks is just hype and should be ignored, according to analyst firm Gartner. In a Garner advisory, research vice-president Michael Silver said: "The Mac software will be located on another partition within a different file system; thus, running Windows on a Mac will not expose the Mac software to more malware." However, if Boot Camp helps to increase the penetration of Apple's platform then OS X could attract the attention of cyber-criminals, he said.

Category 31.3 *Estimates, guesses, predictions, forecasts, recommendations, commentaries*

2006-04-20 DHS Daily OSIR; http://www.computerworld.com/softwaretopics/os/linux/story/0,10801,110710,00.html

LINUX DESKTOP GROWTH COULD SPUR NEW MALWARE ACTIVITY.

Besides Linux's low cost, its relative immunity from viruses, spyware, worms and other malware has long been one of the open-source operating system's key attractions to potential desktop users. But experts warn that could change if Linux begins to win a mass audience on the desktop, bringing in millions of users who are less proficient technically and less security-conscious than today's typical Linux user. The number of viruses that has so far targeted Linux remains small compared with the thousands of viruses and billions of dollars in estimated damage and lost productivity caused by Windows viruses. Some experts argue that because Linux, with its Unix heritage, was created from the ground up as a multi-user system with built-in access controls and privileges, it is fundamentally more secure than Windows. The relatively small number of Linux users spread among different versions of Linux has long hindered the growth of new software by creating a lower reward/effort ratio. That has also driven away virus creators, said Ed Metcalf, product marketing manager at McAfee Inc. Regardless, some Linux users, while reluctant to install antivirus software on client computers, are starting to take more safety measures.

Category 31.3 *Estimates, guesses, predictions, forecasts, recommendations, commentaries*

2006-04-25 DHS Daily OSIR; http://news.com.com/Mafia+insiders+infiltrating+firms%2C+U.K.+cops+warn/2100-7348_3-6064954.html?tag=cd.top

INSIDERS INFILTRATING FIRMS, UK CRIME AGENCY WARNS.

Employees are still one of the greatest threats to corporate security. Speaking Tuesday, April 25, at the Infosecurity 2006 conference in London, Tony Neate, e-crime liaison for the Serious Organized Crime Agency, said insider "plants" are causing significant damage to companies. "[Organized crime] has changed. You still have traditional organized crime, but now they have learned to compromise employees and contractors. [They are] new-age, maybe have computer degrees and are enterprising themselves," he added.

Category 31.3 *Estimates, guesses, predictions, forecasts, recommendations, commentaries*

2006-04-26 DHS Daily OSIR; http://www.fcw.com/article94201-04-26-06-Web

CHECKLIST OUTLINES NEW CYBERTHREATS.

The U.S. government and industry face many cyberthreats that, until now, have not received adequate attention, according to a new checklist outlining the threats. "We're talking about vulnerabilities where we can calculate the effects, and the effects are considerable," said Scott Borg, director and chief economist at the U.S. Cyber Consequences Unit. The unit's Cybersecurity Checklist looks at potential avenues for real-world cyberattacks and recommends ways to thwart them. The unit analyzed each of the 16 critical infrastructure sectors, Borg said. Many sectors say they follow international security standards but still have gaping security vulnerabilities, he said. Borg presented a draft version of the list at the GovSec conference in Washington, DC. The Department of Homeland Security has not yet approved the draft.

Category 31.3 *Estimates, guesses, predictions, forecasts, recommendations, commentaries*

2006-05-01 DHS Daily OSIR; http://www.techweb.com/headlines_week/showArticle.jhtml?articleId=187002202

SMARTER SPAM COULD MIMIC FRIENDS' MAIL.

The next generation of spam and phishing e-mails could fool both software filters and the most cautious people, Canadian researchers said Sunday, April 30, by mimicking the way friends and real companies write messages. John Aycock, an assistant professor of computer science at the University of Calgary, and his student, Nathan Friess, explained that tomorrow's criminals could plant malicious programs on compromised computers. Those programs would scan the e-mail in the zombie's inbox, mine it for information and writing patterns, then crank out realistic-looking replies to real messages.

Category 31.3 Estimates, guesses, predictions, forecasts, recommendations, commentaries

2006-05-14 DHS Daily OSIR; http://www.networkingpipeline.com/showArticle.jhtml?articleID=187202905

CYBER THREATS TO U.S. BUSINESS GROW MORE DANGEROUS.

Attacks on U.S. computer networks could escalate from mere inconveniences to disasters that ruin companies or even kill people, according to the head of a cyber-security unit working with the U.S. government. Scott Borg, director of the Cyber Consequences Unit, or CCU, a Department of Homeland Security advisory group, said increasing intelligence "chatter" was pointing to possible criminal or terrorist schemes to destroy physical infrastructure such as power grids. The CCU is considering how to prevent attacks beyond ubiquitous e-mail hoaxes or computer viruses, with concerns rising about plots to cause power blackouts, tamper with pharmaceutical products or reprogram machinery to build dangerously defective products. Borg's CCU, a small independent unit funded by Homeland Security, spends its time trying to imagine how technology could be used to cripple the United States. It also holds cyber-security exercises for U.S. corporations and investigates reports of attacks on computer systems. A major crisis could be triggered, for instance, by shutting down critical computer systems for as little as four days.

Category 31.3 Estimates, guesses, predictions, forecasts, recommendations, commentaries

2006-06-05 DHS Daily OSIR; Government Computer News
http://www.gcn.com/online/vol1_no1/40943-1.html

SPYWARE INFECTIONS SPREADING, SECURITY EXPERT SAYS.

Spyware programs are increasing in number and growing in sophistication to avoid detection, making it harder to guard against infections and more costly to repair their damage, according to a security expert. Gerhard Eschelbeck, chief technology officer for Webroot Software Inc. told the audience at Techno Security 2006 that through the first quarter of this year, his company has identified approximately 427,000 Websites that host spyware. In addition, “there are at least 10 variants for each spyware program identified,” Eschelbeck said, to make them stealthier and harder to detect.

Category 31.3 Estimates, guesses, predictions, forecasts, recommendations, commentaries

2006-06-13 DHS Daily OSIR; IDG News Service
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9001158

INTERNET PIONEERS WARN OF VOIP WIRETAP DANGER.

U.S. government efforts to require most voice-over-IP (VoIP) providers to permit law enforcement agencies to wiretap phone calls could introduce new security problems to the Internet, a group of Internet security experts said Tuesday, June 13. A Federal Communications Commission rule requiring providers to allow wiretapping by May 2007 would either require a massive re-engineering of the Internet or introduce broad cybersecurity risks, said authors of a new study released by the Information Technology Association of America (ITAA), an IT vendor trade group. In addition, the requirements would stall Internet innovations in the U.S. by adding hundreds of thousands of dollars in setup and maintenance costs to providers and potentially to other Internet applications that provide voice services, including instant messaging and online games, said the study.

ITAA study: http://www.itaa.org/news/docs/CALEAVOIPreport.pdf

[MK note: the authors of the report are as follows:

Steven Bellovin, Columbia University
Matt Blaze, University of Pennsylvania
Ernest Brickell, Intel Corporation
Clinton Brooks, NSA (retired)
Vinton Cerf, Google
Whitfield Diffie, Sun Microsystems
Susan Landau, Sun Microsystems
Jon Peterson, NeuStar
John Treichler, Applied Signal Technology]

Category 31.3 Estimates, guesses, predictions, forecasts, recommendations, commentaries

2006-08-03 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2161582/home-users-getting-wise-wi

HOME USERS GETTING WISE TO WI-FI SECURITY.

Home users are becoming increasingly aware of Wi-Fi security, a new study has found. Sixty percent of wireless network owners implement security on their equipment, according to research firm Jupiter Research. Home users are most worried about privacy issues from leaving their network open and they're also concerned about illicit use and bandwidth theft. Report is available for purchase at: http://www.jupiterresearch.com/bin/item.pl/research:concept/625/id=97415/

Category 31.3 Estimates, guesses, predictions, forecasts, recommendations, commentaries

2006-08-09 DHS Daily OSIR; CRN http://www.crn.com/showArticle.jhtml?articleID=191900748

RESEARCHER: HACKER SOPHISTICATION OUTPACING FORENSICS.

Speaking at the Black Hat conference in Las Vegas last week, Kevin Mandia, president of Mandiant, an Alexandria, VA-based security consultancy, said attackers are using increasingly sophisticated methods to evade detection and make life difficult for security incident response teams. The sophistication of hackers' tools is outpacing that of investigators' forensic tools, and one of the consequences is that incident response teams charged with investigating attacks on networks are taking between five and eight days to find malicious code, Mandia said. Although Windows security breaches make up the majority of security incidents, the kernel level rootkits Mandia has come across thus far have been Linux-based. Mandia said the main reason hackers aren't running kernel level rootkits is because they can make systems unstable, which could blow their cover. Other common indicators that a PC's security has been breached include the inability to execute a 'save as' command; continual termination of antivirus software; and Windows Task Manager closing immediately when a user executes a 'ctrl-alt-delete' command, according to Mandia.

Category 31.3 Estimates, guesses, predictions, forecasts, recommendations, commentaries

2007-04-10 DHS Daily OSIR; InfoWorld http://www.infoworld.com/article/07/04/10/HNmcafeereport_1.html?source=searchresult

MCAFEE: CYBER-CRIME WILL CONTINUE TO PAY.

The latest research report from McAfee's Avert Labs paints a frightening picture for enterprise IT administrators and end-users, predicting continued maturation of cyber-crime and the technological means being used to carry out external attacks. According to McAfee's semi-annual Sage journal, a roundup of the company's ongoing security research, everything from spam to spyware will become more dangerous over the course of 2007 as hackers look for new ways to exploit end users' machines in their quest for fast cash. As was the case in 2006, the drive for profits among hackers and malware code writers will dominate development of the threat landscape over the next 12 months, McAfee experts said. "The overall trend remains more attacks geared toward making money that make use of malware or support people making malware," said Dave Marcus, security research manager with Avert Labs. "What is surprising is the service and support that's going on around the malware industry; there are more sites selling custom Trojans with support contracts and attacks coded to target banks of the buyer's choice and more malware suppliers offering patches and variants to their users." McAfee's Sage Journal: http://www.mcafee.com/us/local_content/misc/sage_0407.pdf

Category 31.3 Estimates, guesses, predictions, forecasts, recommendations, commentaries

2007-04-26 DHS Daily OSIR; CNET News http://news.com.com/Schneier+questions+need+for+security+industry/2100-7355_3-6179500.html

SCHNEIER QUESTIONS NEED FOR SECURITY INDUSTRY.

Outspoken author and security guru Bruce Schneier has questioned the very existence of the security industry, suggesting it merely indicates the willingness of other technology companies to ship insecure software and hardware. Speaking this week at Infosecurity Europe 2007, a leading trade show for the security industry, Schneier said, "the fact this show even exists is a problem. You should not have to come to this show ever." "We shouldn't have to come and find a company to secure our e-mail. E-mail should already be secure. We shouldn't have to buy from somebody to secure our network or servers. Our networks and servers should already be secure." Schneier, chief technology officer at BT Counterpane, said his own company was bought by BT Group last year because the UK telecommunications giant realized the need for security to be part of any service, not an add-on at additional cost and inconvenience to the user. His words echoed those of Lord Broers, chair of the House of Lords science and technology committee, who suggested every company, from operating system and application vendors to ISPs, needs to take greater responsibility for the security of end users.

31.4 New technology with potential security vulnerabilities or implications

Category 31.4 New technology with potential security vulnerabilities or implications

2006-02-22 INNOVATION (Wired.com 14 Feb 2006)
<http://www.wired.com/news/technology/0,70190-0.html>

MAGNETIC CHIP TRUMPS MOORE'S LAW

Researchers at the University of Notre Dame have come up with a working prototype of a chip that uses nanoscale magnetic "islands" to juggle binary code rather than electrical transistors, making it impervious to the physical restrictions that threaten the end of Moore's Law. Because the chip has no wires, its device density and processing power may ultimately outshine those of transistor-based devices, while at the same time requiring less power. Computers using the chips would boot up almost instantly, and because the chip's memory is non-volatile, it would retain data during power interruptions. The magnetic architecture can be modified on the fly and its adaptability would make it very popular with manufacturers of special-purpose hardware, such as videogame consoles and medical diagnostic equipment.

Category 31.4 New technology with potential security vulnerabilities or implications

2006-03-29 INNOVATION (BBC News 24 Mar 2006)
<http://news.bbc.co.uk/2/hi/science/nature/4839088.stm>

BREAKTHROUGH NANO CIRCUIT

Researchers from IBM, the University of Florida and Columbia University have teamed up to produce the first computer circuit built on a single carbon nanotube, an advance they say could lead to faster computer chips. The announcement comes at a time when the standard silicon chip is rapidly reaching its physical limitations, signaling the eventual end of Moore's Law, which posits that the number of transistors on a chip will double every couple of years. At this stage, the circuit is not designed to be used in a computer chip, but scientists can use it to gauge the speed of such chips. Currently, it's much slower than its silicon counterparts, but researchers say with continued refinement, they hope to push speeds beyond those possible today.

Category 31.4 New technology with potential security vulnerabilities or implications

2006-04-19 INNOVATION (Electronic Design 30 March 2006)
<http://www.elecdesign.com/Articles/ArticleID/12203/12203.html>

WIRELESS SENSING AND THE CONNECTED WORLD

Imagine strolling through town and finding the goods and services you want just by consulting your PDA or smart phone, then walking into a store and making your purchase without a cashier or credit card. Seamless connectivity between people, objects, and events will someday create this ultra-intelligent environment, says Professor Dipankar Raychaudhuri, director of Rutgers' Wireless Information Network Laboratory (WINLAB).

Raychaudhuri says wireless sensor networks and pervasive computing will profoundly transform our everyday lives. Smart transportation systems will route vehicles around traffic jams in real time, and provide collision-avoidance feedback with augmented reality displays. They'll guide you to your parked car in a crowded parking garage. Your cell phone will play a vital role in many of these scenarios. You'll use your phone, for instance, to pay for food at the grocery store, eliminating the need to carry cash or credit cards. Motorola's M-Wallet cell phone is an indicator of how these capabilities will be incorporated into the designs of third-generation (3G) handheld devices. Looking ahead, wireless sensor techniques eventually will permit the seamless interconnection of the physical and virtual worlds. Wireless network technologies like WiMedia Ultra-Wideband (UWB) will let you do things like download an entire television show in just one minute.

Category 31.4 New technology with potential security vulnerabilities or implications

2006-04-27 DHS Daily OSIR; http://news.bbc.co.uk/2/hi/technology/4946512.stm

WARNINGS OVER USB MEMORY STICKS.

Smart phones, iPods and USB memory sticks are posing a real risk for businesses, warn security experts. Just over half of companies take no steps to secure data held on these devices, found a UK government-backed security survey. Figures from the Information Security Breaches Survey, which is backed by the Department of Trade and Industry, reveals how firms are struggling to control the growing use of USB flash memory sticks. Matt Fisher, spokesperson for Centennial Software, said USB sticks could also become an attack vector for viruses and other malicious programs largely because they are swapped between many different computers. Both the executive summary and the full results of the Information Security Breaches Survey, April 2006, can be found at: http://www.pwc.com/Extweb/pwcpublications.nsf/docid/F9843CD3 C8E0FB828025715A0058C63B

Category 31.4 New technology with potential security vulnerabilities or implications

2006-07-07 DHS Daily OSIR; Security Focus http://www.securityfocus.com/news/11399

RESEARCHERS LOOK TO PREDICT SOFTWARE FLAWS.

Using historical data, researchers at Colorado State University are attempting to build models that predict the number of flaws in a particular operating system or application. In an analysis to be presented at a secure computing conference in September, three researchers used monthly flaw tallies for the two most popular Web servers -- the Apache Foundation's Apache Web server and Microsoft's Internet Information Services server -- to test their models for predicting the number of vulnerabilities that will be found in a given code base. The goal is not to help software developers to create defect-free software -- which may be so unlikely as to be impossible -- but to give them the tools to determine where they need to concentrate their efforts, said Yashwant Malaiya, professor of computer science at Colorado State University and one of the authors of the paper on the analysis. The research could be another tool for developers in the fight to improve programmers' security savvy and reduce the number of flaws that open up consumers and companies to attack. While the number of vulnerabilities found in recent years leveled off, Web applications boosted the number of flaws found in 2005.

Category 31.4 New technology with potential security vulnerabilities or implications

2006-09-12 DHS Daily OSIR; Scotsman (United Kingdom)
http://news.scotsman.com/scitech.cfm?id=1344342006

ROBOTS HAILED AS SAFETY SOLUTION.

Tiny robots developed by Scottish scientists are set to improve the safety of airplanes, nuclear power plants, and oilrigs. Measuring just under four inches square, the devices use ultrasound, electrical currents, magnetic fields, and cameras to inspect structures for cracks, corrosion and leaks. Each battery-powered robot uses its own computer to process data and locate defects. This information is sent to a central computer for analysis.

Category 31.4 New technology with potential security vulnerabilities or implications

2006-09-18 DHS Daily OSIR; New York Times
http://www.nytimes.com/2006/09/18/technology/18chip.html

A CHIP THAT CAN TRANSFER DATA USING LASER LIGHT.

Researchers announced on Monday, September 18, that they have created a silicon-based chip that can produce laser beams. The advance will make it possible to use laser light rather than wires to send data between chips, removing the most significant bottleneck in computer design. As a result, chip makers may be able to put the high-speed data communications industry on the same curve of increased processing speed and diminishing costs -- the phenomenon known as Moore's law -- that has driven the computer industry for the last four decades. Commercializing the new technology may not happen before the end of the decade, but the prospect of being able to place hundreds or thousands of data-carrying light beams on standard industry chips is certain to shake up both the communications and computer industries. With the barrier removed, computer designers will be able to rethink computers, packing chips more densely both in home systems and in giant data centers. Moreover, the laser-silicon chips portend a vastly more powerful and less expensive national computing infrastructure.

Category 31.4 New technology with potential security vulnerabilities or implications

2006-09-26 DHS Daily OSIR; Federal Times http://federaltimes.com/index.php?S=2131748

SMART CAMERAS ASSUME LARGER ROLE IN HOMELAND SECURITY.

The future of facility security lies in rigging cameras that can be programmed to reliably search for suspicious people or vehicles and alert staff to potential dangers, says a security consultant overseeing an upgrade at the Port of Houston. James Black of TRC Solutions, said that the federal government, military, and industry are using video analytics at many -- but not all -- facilities. The technology can be programmed to watch for suspicious things, such as a truck parked in front of a building for a few minutes or a person walking into a restricted area, and then alert security officials. The technology is an improvement over simple motion detection devices that cannot tell a person from a deer, Black said, and it is much more reliable than having people watch banks of monitors looking for something out of the ordinary. Most people zone out after 15 minutes of watching static images and will miss subtle, but important, developments, he said. Once the system sounds an alert, a person can take a closer look and decide whether a response is needed or if it is nothing to worry about.

Category 31.4 New technology with potential security vulnerabilities or implications

2007-01-02 DHS Daily OSIR; Electric Light & Power http://uaelp.pennnet.com/display_article/281106/22/ARTCL/none/none/Robotic-crawler-detects-wear-in-power-lines/

ROBOTIC CRAWLER DETECTS WEAR IN POWER LINES.

Most power companies don't know the weak points in their electrical grids. And although lights get turned on after a storm, the long-term effects of hurricanes, landslides or windstorms lie unnoticed. Now a robot can roll along the miles of cable, performing a utilities' equivalent of check-ups. "This is the first robot built that can inspect power cables autonomously looking for incipient failures," says University of Washington (UW) assistant professor Alexander Mamishev. "It can find cables that may need repair, before they cause problems." The high-voltage lines that this robot monitors carry electricity from the distribution plant to the substations. UW's robot can pinpoint problem spots by using information from the surface of the cable to assess the condition of what's inside. The robot rides along the insulated distribution cable scanning for internal damage. It uses three sensors: a heat sensor that detects heat dissipation; an acoustic sensor that listens for partial electrical discharge; and a sensor that detects "water trees," filaments of water that have seeped into insulation. Engineers monitor the robot via wireless connection and watch through a video camera.

Category 31.4 New technology with potential security vulnerabilities or implications

2007-01-13 DHS Daily OSIR; IDG News Service http://www.computerworld.com/action/article.do?command=printArticleBasic&articleId=9008038

HACKERS LOOKING FORWARD TO IPHONE.

Within hours of Apple's iPhone unveiling on Tuesday, January 9, the iPhone was a hot topic on the Dailydave discussion list, a widely read forum on security research. Much of the discussion centered on the processor that Apple may have chosen to power its new device and what kind of assembly language "shellcode" might work on this chip. In an e-mail interview, one of the hackers behind the "Month of Apple Bugs" project, which is disclosing new Apple security vulnerabilities every day for the month of January, said he "would love to mess with" the iPhone. "If it's really going to run OS X, [the iPhone] will bring certain security implications, such as potential misuses of wireless connectivity facilities [and] deployment of malware in a larger scale," the hacker known as LMH wrote in an e-mail. Because the device could include a range of advanced computing features, such as Apple's Bonjour service-discovery protocol, it could provide many avenues of attack, according to LMH. "The possibilities of a worm for smartphones are something to worry about," he wrote. "Imagine Bonjour, and all the mess of features that OS X has, concentrated in a highly portable device which relies on wireless connectivity."

Category 31.4 New technology with potential security vulnerabilities or implications

2007-02-07 INNOVATION (Wired.com 29 Jan 2007) <http://www.wired.com/news/technology/medtech/0,72580-0.html>

YOUR THOUGHT IS ITS COMMAND

Researchers at the University of Zaragoza in Spain are working on a new brain-computer interface capable of translating thoughts into commands that could control a wheelchair's movements. Previous work in brain-computer interface has required users to have electrodes plugged directly into their brains, but the Spanish scientists hope to develop a small, mobile interface that works with EEGs (electroencephalogram electrodes) placed on the scalp. "We are planning to use non-invasive devices to record the rhythms from the surface of the skull," says researcher Javier Minguez. While EEG signals are not nearly as powerful as the ones derived from direct brain contact, advances in decoding algorithms produce patterns that are precise enough to control wheelchair movements such as turning and stopping. Two 800-MHZ Intel computers mounted on the wheelchair analyze the readings and send instructions to the wheels. While commands currently are limited to "turn left" or "turn right," Minguez says his team hopes eventually to use a combination of thought and mapping software to perform more complex tasks such as "Go to the kitchen." The first working prototype is expected in 2008 or early 2009.

Category 31.4 New technology with potential security vulnerabilities or implications

2007-03-01 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2099603,00.asp

BLACK HAT DEMONSTRATIONS SHATTER HARDWARE HACKING MYTHS.

At the Black Hat Briefings, two breakthrough hardware hacks were demonstrated. One shocker was Coseinc Senior Security Researcher Joanna Rutkowska's demonstration of a way to subvert system memory through software -- in essence, the shattering of the long-held belief that "going to hardware" to secure incident response is a security failsafe. Security professionals at the show called it the "attainment of the holy grail," particularly since the only way to fix the system's memory corruption is to reboot -- thus erasing all tracks of the subversion. It's a digital forensic team's worst nightmare. John Heasman from NGSS proved that rootkits can persist on a device -- on firmware -- rather than on disk, and can thus survive a machine being reimaged. These hacks are esoteric, but they're proving that much of what we thought of as hardware unassailability is pure folklore.

Category 31.4 New technology with potential security vulnerabilities or implications

2007-03-07 INNOVATION (NPR's Morning Edition 27 Feb 2007) <http://www.npr.org/templates/story/story.php?storyId=7615643&ft=1&f=1006>

NANOTECH GIVES COUNTERFEITERS A RUN FOR THEIR MONEY

A recent National Research Council study on currency predicts that counterfeiting is like to escalate sharply if the U.S. doesn't make radical changes to its paper money, thanks to the ubiquitous availability of inexpensive, high-quality printers that can reproduce any image, no matter how intricate. "The future is not going to be in more color, or more finely printed images," says Alan Goldstein, a molecular engineering professor at Alfred University. "The future is going to be in the materials from which the bill itself is made." Goldstein says by using nanotechnology to manipulate the molecules within a bill, engineers can make currency change its shape and/or texture. "Say you snap a dollar bill between your fingers and the edges become rigid. And then you pull on them and the edges become normal currency handled every day." Scientists could also make bills that are incredibly durable. "If you can cut it with a pair of scissors, then it's counterfeit," says Goldstein. Or nanotechnology could be used to make the images on a bill dynamic: if you pinched George Washington's cheek, for instance, he might wink or smile or even blush a deep pink. Goldstein notes that these possibilities are not wild fantasies -- they're already in use in medicine and the military, and within a decade the price will have dropped to the point where they can be used in everyday currency.

Category 31.4 New technology with potential security vulnerabilities or implications

2007-04-24 DHS Daily OSIR; Associated Press http://www.nytimes.com/aponline/technology/AP-Faster-Internet.html

RESEARCHERS BREAK INTERNET SPEED RECORDS.

A group of researchers led by the University of Tokyo has broken Internet speed records -- twice in two days. Operators of the high-speed Internet2 network announced Tuesday, April 24, that the researchers on December 30 sent data at 7.67 gigabits per second, using standard communications protocols. The next day, using modified protocols, the team broke the record again by sending data over the same 20,000-mile path at 9.08 Gbps.

Category 31.4 New technology with potential security vulnerabilities or implications

2007-05-02 INNOVATION (Popular Science Apr 2007) < http://www.popsci.com/popsci/science/0e54d952c97b1110vgnvcm1000004eecbccdrcrd.html >

HACKING THE HUMAN BRAIN

It's still in the primitive stage, but computers can now communicate with living brain cells. Ted Berger, head of USC's Center for Neural Engineering, says his chip's ability to converse with live cells is a dramatic first step toward an implantable machine that could restore memories in people with brain damage or help them make new ones. If Berger's grand vision plays out, remedying Alzheimer's Disease would be as simple as upgrading a bit of hardware. No more complicated drug regimens with their frustrating side effects. A surgeon simply implants a few computerized brain cells, and the problem is solved. So far, Berger's research team of neuroscientists, mathematicians, computer engineers and bioengineers has managed to reproduce only a minute amount of brain activity. Their chip models fewer than 12,000 neurons, compared with the 100 billion or so present in a human brain. Yet researchers within the field say that even this small number represents a stunning achievement in the field of neuro-engineering. "It's the type of science that can change the world," says a professor of brain sciences at Dartmouth College. Richard Granger says, "Replicating memory is going to happen in our lifetimes, and that puts us on the edge of being able to understand how thought arises from tissue -- in other words, to understand what consciousness really means."

Category 31.4 New technology with potential security vulnerabilities or implications

2007-05-30 INNOVATION (The Guardian 17 May 2007) <http://technology.guardian.co.uk/weekly/story/0,,2080840,00.html>

HOLOGRAPHIC STORAGE

The world's first holographic storage system is set to launch this fall, marketed under the Tapestry brand by InPhase Technologies. The 600GB write-once disc will be able to store the equivalent of 64 DVD movies, will cost about $180 and will require an $18,000 drive to read it. Marketing targets include banks, libraries, government agencies and businesses. InPhase CTO Kevin Curtis says, "Very large companies are showing the most interest, which is interesting, because large companies tend to be technology laggards. The amount of data they're getting through is becoming unmanageable." Industry consultant Bill Foster says holographic storage will have a difficult time supplanting more conventional tape technology, and suggests it has a better chance challenging another storage medium -- flash memory. "Holographic storage doesn't have to be on a disc -- it can also be on a solid state medium." But an IDC analyst says, "We believe the technology lends itself to both business and consumer applications. Almost every company involved in optical storage is also looking at holographics as a potential candidate for the next generation of optical disc." IDC predicts that by
2011 the holographics drive market will be around $200m globally.

32.1 Censorship in the USA

Category 32.1 Censorship in the USA

2006-02-01 EDUPAGE; http://www.internetnews.com/bus-news/article.php/3582016

MICROSOFT OUTLINES BLOG CENSORSHIP POLICY

Microsoft has announced details of a new policy on censoring the content of blogs maintained by its customers. According to the new policy, blog content will only be blocked to comply with local laws and with the terms of use of MSN Spaces, the company's blog application. In order to have content blocked, a local government must demonstrate that it violates local laws. Moreover, the content will only be blocked in areas where those laws apply; users in other parts of the world will still be able to see the content. In cases where content is blocked, users will be notified and told that the reason is a government restriction. Microsoft's announcement follows criticism of its decision to comply with requests of Chinese authorities to remove the blog content of an individual the government considered a threat. The announcement also comes on the heels of Google's plan to filter the content of its search results to comply with local laws in China. Both companies said their decisions are based on the belief that it is better to have a presence in countries like China, even if that requires limiting access to certain online content.

Category 32.1 Censorship in the USA

2006-03-31 Effector Online http://www.eff.org/bloggers/lg/faq-election.php

FEC PROTECTS BULK OF INTERNET SPEECH FROM CAMPAIGN FINANCE RULES.

On Monday, the Federal Election Commission voted unanimously to adopt new regulations that would leave Internet-related activities largely untouched by campaign finance rules. Monday's vote marked the culmination of a series of events put into motion in September 2004 when a federal district court ruled that the FEC couldn't categorically exempt the Internet from federal campaign finance rules and forced the agency to draw up new rules accordingly. The new rules are a big win for bloggers and other online speakers. When the proposed rules were first announced, bloggers across the spectrum raised concerns that the FEC might intrude too far, imposing burdensome record keeping regulations and potentially chilling online speakers who wanted to discuss political issues or coordinate volunteers. Frequently forgotten, however, was the fact that the FEC had expressed little interest in adopting any kind of Internet regulations in the first place. Indeed, the 2004 court ruling chastised the agency for shielding the Internet more than federal law allowed. The final rules should put most of the immediate free speech concerns of bloggers to rest. As the introduction to the final rules note, "These final rules therefore implement the regulatory requirements mandated by the Shays District decision by focusing exclusively on Internet advertising that is placed for a fee on another person's website." The FEC has interpreted campaign finance laws (and the admonition of the district court) extremely narrowly, limiting rules regarding spending limits and reporting requirements to instances where paid advertisements are placed on the Internet. Unless they take money in exchange for political advertisements, the bulk of online speakers will remain unaffected by the rule changes. The new regulations will go into effect in a little over a month. To read the regulations: http://www.fec.gov/agenda/2006/mtgdoc06-20.pdf
Read EFF's Election Law for Bloggers FAQ: http://www.eff.org/bloggers/lg/faq-election.php

Category 32.1 Censorship in the USA

2006-04-14 Effector Online http://eff.org/global/jurisdiction/viewfinder-amicus-final.pdf

EFF DEFENDS AMERICAN'S FREE SPEECH AGAINST FOREIGN COURT RULING.

Your online speech may be perfectly legal under our laws, but when can a US court be made to enforce a foreign law against you? Can the First Amendment be undermined by court decisions from nations that are less protective of free speech? That's the issue addressed in an amicus brief filed by EFF on Monday, arguing that the First Amendment blocks two French fashion design companies from enforcing a French court judgment in the U. S. In this case, Sarl Louis Feraud International v. Viewfinder Inc., the French companies had won a default judgment in France against Viewfinder Inc., an American company that maintains websites of photographs from fashion shows. The French designers claim that Viewfinder's posted photographs infringed rights in their dresses. The companies then tried to enforce the judgment in New York federal court, which rightly found that the French court judgment was "repugnant" to U.S. law and public policy because it would stifle Viewfinder's speech. Just because your online speech may be read in another country doesn't mean that country's law should bind you. Joined by ACLU and CDT, EFF supported the district court's decision and this week filed its brief opposing the French companies' appeal to the Second Circuit. Former EFF staff attorney Wendy Seltzer, now teaching at Brooklyn Law School, was counsel to EFF, ACLU and CDT on the brief.
For the brief: http://eff.org/global/jurisdiction/viewfinder-amicus-final.pdf

Category 32.1 Censorship in the USA

2006-11-29 Effector Online http://www.eff.org/news/archives/2006_11.php#005017

CALIFORNIA SUPREME COURT RULES IN FAVOR OF FREE SPEECH ON THE INTERNET.

San Francisco - In a victory for free speech on the Internet, the California Supreme Court ruled last week that no provider or user of an interactive computer service may be held liable for putting material on the Internet that was written by someone else. In doing so, the Court overruled an earlier decision by the Court of Appeal. This ruling affirms that blogs, websites, listservs, and ISPs like Yahoo!, as well as individuals like defendant Ilena Rosenthal, are protected under Section 230 of the federal Communications Decency Act (CDA), which explicitly states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." "By reaffirming that Congress intended to grant protection under Section 230 to those who provide a forum for the views of others, the Court has ensured that the Internet will remain a vibrant forum for debate and the free exchange of ideas," said Ann Brick, staff attorney at the ACLU of Northern California. "Any other ruling would have inevitably made speech on the Internet less free." The issue raised in Barrett v. Rosenthal was whether Section 230's protection applies to individuals who frequently use the Internet to pass on information obtained elsewhere, whether by forwarding an email written by someone else or, as was the case in Barrett, posting an email from someone else to a newsgroup. The ACLU-NC and the Electronic Frontier Foundation (EFF) filed an amicus brief in the California Supreme Court arguing that Section 230 means what it says and applies to "users" of interactive computer services as well as "providers." "Courts have consistently interpreted Section 230 to provide broad protections for the platforms upon which free speech has flourished online," said EFF Staff Attorney Kurt Opsahl. "By reversing the Court of Appeal, the California Supreme Court has brought California back in line with other jurisdictions and reaffirmed the critical rule that the soapbox is not liable for what the speaker has said.". . . . "The Supreme Court's opinion strengthens protection for speech on the Internet" said Mark Goldowitz, director of the California Anti-SLAPP Project and counsel for Rosenthal. "Justice Corrigan's opinion protects against the 'heckler's veto' chilling speech on the Internet."
For the full decision, see EFF's website at: http://www.eff.org/legal/cases/Barrett_v_Rosenthal/ruling.pdf
For this release: http://www.eff.org/news/archives/2006_11.php#005017

Category 32.1 Censorship in the USA

2007-02-06 Effector Online http://www.eff.org/news/archives/2007_01.php#005103

SURVEILLANCE OF SOLDIERS' BLOGS SPARKS LAWSUIT. DEFENSE DEPARTMENT WITHHOLDS RECORDS ABOUT ARMY BLOG MONITORING.

Program Washington, D.C. - The FLAG Project at the Electronic Frontier Foundation (EFF) filed suit against the Department of Defense last week, demanding expedited information on how the Army monitors soldiers' blogs. According to news reports, an Army unit called the Army Web Risk Assessment Cell (AWRAC) reviews hundreds of thousands of websites every month, notifying webmasters and bloggers when it sees information it finds inappropriate. Some bloggers have told reporters that they have cut back on their posts or shut down their sites altogether because of the activities of the AWRAC. EFF filed its suit after the Department of Defense and Army failed to respond to Freedom of Information Act (FOIA) requests about the blog monitoring program. "Soldiers should be free to blog their thoughts at this critical point in the national debate on the war in Iraq," said EFF Staff Attorney Marcia Hofmann. "If the Army is coloring or curtailing soldiers' published opinions, Americans need to know about that interference." EFF's suit demands records on how the AWRAC conducts its monitoring, as well as any orders to soldiers about revision or deletion of web posts. It also demands expedited processing, as the information is urgently needed by the public. "Of course, a military effort requires some level of secrecy. But the public has a right to know if the Army is silencing soldiers' opinions as well. That's why the Department of Defense must release information on how this program works without delay," Hofmann said. EFF's FLAG Project uses FOIA requests and litigation to expose the government's expanding use of technologies that invade privacy. Previous lawsuits have demanded information about the FBI's huge database of personal information and the Department of Homeland Security's program to assign secret "risk assessment" scores to American travelers.
For the FOIA complaint filed against the Department of Defense: http://www.eff.org/flag/awrac/awrac_complaint.pdf
For more on the FLAG Project: http://www.eff.org/flag/
For this release: http://www.eff.org/news/archives/2007_01.php#005103

Category 32.1 Censorship in the USA

2007-04-11 Effector Online http://www.eff.org/deeplinks/archives/005185.php

A BAD IDEA FROM UTAH: A BAN ON COMPARATIVE ADVERTISING

The Utah legislature has quietly passed a dangerous law allowing trademark owners to prevent their marks from being used as keywords to generate comparative ads. If this law takes effect, a company like Chevrolet couldn't purchase "sponsored link" space on the Google results page when a user types "Toyota" as part of a search query -- at least if the latter term is registered in Utah as an "electronic registration mark." As Martin Schwimmer notes, Utah's own general counsel warned the legislature that the law was likely to be found unconstitutional given the burden it would put on interstate commerce. To comply with the law, a search engine that received a search request would have to determine whether a user was located within Utah and, if so, check the search terms against Utah's registry of trademarks to prevent the unlawful triggering of advertising. The cost to search engines would be staggeringly high: "Literally millions of search requests from locations worldwide each day would be subject to verification of location." Aside from its constitutional flaws, the law is just bad public policy. It undermines the fundamental purpose of trademarks: to improve consumer access to accurate information about goods and services. Trademarks are just shorthand terms that designate the origin of a product. Comparative advertising uses those shorthand terms to provide more information about the trademarked product and competitive products. That's why comparative trademark use is clearly protected under federal trademark law. If it weren't, Pepsi wouldn't be able to tell consumers that more people think Pepsi tastes better than Coke, and Apple wouldn't be able to make fun of Microsoft on national television every night. The good news is that, given the constitutional problems, the law is likely to be challenged in court. But it's too bad the Utah legislature didn't heed its own counsel's advice and save Utah taxpayers the cost of defending this anti-consumer legislation.
For this post and related links: http://www.eff.org/deeplinks/archives/005185.php

Category 32.1 Censorship in the USA

2007-05-03 Effector Online http://www.eff.org/deeplinks/archives/005223.php

THE GREAT FIREWALL OF UTAH (AND BANNING OPEN WI-FI)

The Utah legislature has been considering a proposal that would require the state's ISPs to ensure that minors are unable to access explicit material on the Internet. The scheme would also make open wireless networks illegal (!) unless they are restricted to only allow connections on certain, censored, "community ports." Giving ISPs the responsibility and incentives to censor a particular subset of the web is precisely the same architecture that the Chinese Communist Party uses for their "Great Firewall of China." China uses it to filter news and political information as well as porn, but in neither case is it particularly effective. Users who are either knowledgeable or motivated quickly learn that there are easy ways around these filters. The absurd Utah proposal has been pushed by the CP80 Foundation, which pedals fantasies of a world where certain TCP ports (80, for instance) are free of any material that they consider "indecent." The group is fronted by SCO Chairman Ralph Yarro -- yes, the same SCO that went after IBM and others for allegedly using its code in Linux distributions. The chance that a state or even federal statute could (practically or constitutionally) prevent sexually explicit content from being transmitted through port 80 is approximately zero point zero zero zero percent. The chance that politicians could pass foolish laws that cause needless headaches and court battles for ISPs and users, however, is significantly higher.
For this post and related links: http://www.eff.org/deeplinks/archives/005223.php

32.2 Censorship outside the USA

Category 32.2 Censorship outside the USA

2006-01-06 EDUPAGE; http://www.nytimes.com/2006/01/06/technology/06blog.html

MICROSOFT AGREES TO CLOSE CHINESE BLOGGER'S SITE

Following a formal request from Chinese officials, Microsoft has shut down the blog of a high-profile Chinese journalist. China is well known for censoring public speech it considers critical of the government, and Microsoft's actions are not the first in which non-Chinese companies have complied with Chinese authorities. Officials from Microsoft noted that if their services are to be available in China, the company must comply with local laws. As Brooke Richardson, a group product manager for MSN said, "We think it's better to be there with our services than not be there." Last year Yahoo was faulted by some for cooperating with Chinese officials, and it too stated then that a requirement of continuing operation in the country is to conform to local laws and regulations. Rebecca MacKinnon, a fellow at the Berkman Center for Internet and Society at Harvard Law School, expressed concerns on her blog about Microsoft's action. "Can we be sure," she said, "they won't do the same thing in response to potentially illegal demands by an overzealous government agency in our own country?" New York Times, 6 January 2006 (registration req'd)

Category 32.2 Censorship outside the USA

2006-01-24 EDUPAGE; http://news.com.com/2100-1028_3-6030784.html

GOOGLE TO CENSOR SEARCH RESULTS IN CHINA

Google will launch search and news sites in China this week that will block access to information the Chinese government considers objectionable. Chinese officials have a long track record of censoring speech and ideas, and, according to Andrew McLaughlin, senior policy counsel for Google, the new sites "will comply with local Chinese laws and regulations." Search results from which content has been excluded will notify users that not all results are being displayed. Google said that the decision to offer its services even if they are censored reflects the belief that limited access to Internet resources is better than no access, which would be the alternative if Google did not comply with local legislation. "We must balance our commitments," said McLaughlin, "to satisfy the interest of users, expand access to information, and respond to local conditions." Reporters Without Borders, an organization that advocates for freedom of the press, was highly critical of the decision, saying, "The new Google version means that even if a human rights publication is not blocked by local firewalls, it has no chance of being read in China."

Category 32.2 Censorship outside the USA

2006-01-26 RISKS

COMPLEXITY OF SEARCH ENGINE COMPLIANCE WITH LOCAL LAWS

Lauren Weinstein, founder of People for Internet Responsibility < http://www.pfir.org >, wrote a thoughtful analysis of the problems search engine companies such as GOOGLE face in meeting conflicting standards in different nations. For example, GOOGLE recently cooperated with the Chinese government in blocking access to certain materials that frighten certain elements within that totalitarian regime; on the other hand, GOOGLE also refused to cooperate with US federal law enforcement requests for records of user searches because of privacy concerns. Weinstein wrote, "The situation highlights the minefield of issues that Google and other Internet companies now face, and the desperate need for proactive approaches to dealing with the ways that these technologies affect individuals and society."

He also pointed to initiatives in the US Congress that would have significant implications for international relations: "Congressman Tim Ryan has announced a hearing of the Congressional Human Rights Caucus (16 Feb is the date that I've heard) to explore the potential drafting of laws that would limit or otherwise control U.S.-based Internet companies from complying with the censorship demands of foreign countries. Emotions were clearly exasperated by Google's launching of the 'dot-cn' Chinese version of Google search that blocks links as per Chinese government directives, though Google is not alone in this regard among U.S.-based Internet companies."

For a streaming video of a one hour lecture by Lauren Weingstin touching on these issues and other of interest, see < http://neon.vortex.com/lauren-google-2006-01-24.asx >.

Category 32.2 Censorship outside the USA

2006-02-03 DHS Daily OSIR; http://www.csmonitor.com/2006/0203/p06s02-woeu.html

INTERNET JIHAD: TACKLING TERROR ON THE WEB.

Nearly 18 months ago, Babar Ahmad, a British citizen, was arrested on an extradition request to the U.S. Charged with running Websites hosted in the U.S. that promoted and supported Islamic militancy, Ahmad remains in British custody. He has appealed the extradition order and Britain's High Court will hear the case on Monday, February 20. The proceedings will test the ability of Western governments to put on trial Islamic radicals who use the Internet as a key recruiting and organizational tool. But while the U.S. government pursues those who operate Websites that allegedly encourage terrorism, some argue that the authorities should instead concentrate on shutting down the sites themselves as soon as possible to limit their impact. Ahmad's case illustrates how seriously the U.S. is taking such Websites. His extradition warrant accuses him -- among other things -- of helping to run azzam.com, one of the earliest and most high profile English-language pro-jihad Websites, which for a time was run by an Internet Service Provider (ISP) headquartered in Connecticut. A federal grand jury in the U.S. indicted Ahmad in October 2004 on four charges. If found guilty, he faces life imprisonment.

Category 32.2 Censorship outside the USA

2006-02-08 EDUPAGE; http://chronicle.com/daily/2006/02/2006020801t.htm

THAILAND BLOCKS YALE PRESS WEB SITE

Internet users in Thailand will not be able to access the Yale University Press Web site following the government's response to a biography that presents an unflattering image of the country's king, Bhumibol Adulyadej. Thai officials in the Ministry of Information and Communications Technology frequently block access to online materials that include adult or violent content, criticism of the Thai royal family, information about the country's national security, or allegedly false advertising. The book, written by journalist Paul M. Handley, who reported from Thailand for 13 years, will be released by the Yale University Press in July. It is also expected to be banned in the country. Although Handley refused to comment specifically on the government's decision to censor the press's Web site, saying that the book will speak for itself, Yale issued a statement defending the book and the author.

Category 32.2 Censorship outside the USA

2006-02-14 DHS Daily OSIR; http://www.techweb.com/wire/ebiz/180201737

U.S. STATE DEPARTMENT LAUNCHES INTERNET FREEDOM TASK FORCE.

The U.S. State Department on Tuesday, February 14, established a task force to investigate the problems posed to the Internet by repressive regimes, a move that followed a call for help by Google Inc., Microsoft Corp. and Yahoo Inc., which have been criticized for censoring information in China. The task force would consider how the use of technology to restrict access to political content has impacted U.S. companies. The panel would also investigate the use of technology to track and repress dissidents and efforts to modify Internet governance structures in order to restrict the free flow of information. The task force is expected to draw upon the department's expertise in international communications policy, human rights, democracy, business advocacy, corporate responsibility and relevant countries and regions, Shiner said. Besides working with U.S. companies and non-governmental agencies, such as human rights groups, the task force will seek help from the European Union and other governments facing similar problems with Internet censorship.

Category 32.2 Censorship outside the USA

2006-04-12 EDUPAGE; http://online.wsj.com/article/SB114484852659023945.html

GOOGLE REBUFFS CRITICS, EXPANDS CHINESE RESEARCH CENTER

Responding to critics of Google's decision to filter certain content to Chinese users, CEO Eric Schmidt reiterated the company's position that it is better to have a presence in China with some restrictions than not to be there at all. Other Internet companies operating in China face the same restrictions as Google--preventing access to sites the government deems objectionable--and Schmidt said Google has not received any complaints from Chinese users. Noting that one-fifth of the world's population lives in China and that many of them are or will be Internet users, Schmidt said Google would comply with applicable local laws and would expand its research operation in the country. The company currently employs about 30 engineers in its R&D facility in Beijing and plans to increase that number to 100. Schmidt also said Google is working with Chinese libraries to include their books in its Book Search program, which is scanning millions of books for online access.

Category 32.2 Censorship outside the USA

2006-05-09 EDUPAGE; http://www.nytimes.com/2006/05/09/world/asia/09internet.html

CHINESE STUDENTS POLICE INTERNET

In China, a government initiative known as "Let the Winds of a Civilized Internet Blow" aims to ensure that online content conforms to government expectations. Students at some Chinese universities are a key part of the effort. At Shanghai Normal University, 500 students serve as Internet monitors, participating in online discussions and trying to steer conversations away from topics considered objectionable. Unknown to most of the other students on campus, the monitors also report some content to campus officials, who delete it. One student monitor said, "Our job consists of guidance, not control." Critics argue that the practice amounts to nothing more than the censorship common to other areas of Chinese life. Chinese officials acknowledged that more than two million images and 600 online forums have been deleted for being "unhealthy." Some students dismissed the efforts, saying that with the Internet, you can always go elsewhere to share your opinions. "It's easy to bypass the firewalls," said one student, "and anybody who spends a little time researching it can figure it out."

Category 32.2 Censorship outside the USA

2006-05-12 EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/14563324.htm

CHINA REJECTS WIKIPEDIA, STARTS ITS OWN VERSION

Baidu, the leading search engine in China, has launched a site that approximates Wikipedia but with none of the content that prompted the Chinese government to block Wikipedia last year. Chinese authorities exert strong control over Internet content available in the country, and Wikipedia includes enough material deemed objectionable that the entire site is unavailable. Robin Li, chairman of Baidu, said his company's new site, Baike, was inspired by Wikipedia, though he said he has never actually seen Wikipedia. China is second only to the United States in Internet users, and Chinese users have reportedly written more than 25,000 Baike entries in the past week. Li said, "I certainly hope our encyclopedia will be the most authoritative one for any Chinese users."

Category 32.2 Censorship outside the USA

2006-06-07 EDUPAGE; BBC http://news.bbc.co.uk/2/hi/asia-pacific/5055170.stm

CHINA LIMITS USERS TO CENSORED GOOGLE

According to a report from Reporters Without Borders, Chinese authorities have blocked access to the Google.com Web page following the introduction in January of the Google.cn domain that meets the country's strict filtering requirements. Google was criticized by some for conceding to demands that it offer a version of its search service that excludes material the Chinese government finds offensive or inflammatory, including any reference to the Tiananmen Square massacre.

Microsoft, Yahoo, and Cisco Systems have also been faulted for similar actions. "It was only to be expected that Google.com would be gradually sidelined," according to Reporters Without Borders, "after the censored version was launched." Google News and Google Mail have also been blocked to Chinese users. Sergey Brin, cofounder of Google, said, "We felt that perhaps we could compromise our principles but provide ultimately more information for the Chinese and be a more effective service." He continued, "Perhaps now the principled approach makes more sense."

Category 32.2 Censorship outside the USA

2006-07-03 EDUPAGE; CNET http://news.com.com/2100-7348_3-6090437.html

ACADEMICS SNEAK PAST CHINESE FIREWALL

Researchers at the University of Cambridge have discovered a way to circumvent the firewall operated by the Chinese government and also to use it to launch denial-of-service attacks. Chinese authorities implemented the firewall to try to prevent computer users in the country from accessing any information deemed inflammatory by the government. According to Richard Clayton of the university's computer lab, the firewall allows packets in and out of the country, but, when a packet contains prohibited information, the firewall initiates a reset, which causes the connection between the sending and receiving computers to fail. "If you drop all the reset packets at both ends of the connection, which is relatively trivial to do," said Clayton, "the Web page is transferred just fine." At the same time, spoofed return addresses for Internet transmissions will cause the firewall to temporarily block traffic to and from those computers. Clayton noted that even with a single dial-up connection, a hacker could create a very disruptive attack. The researchers have reported their findings to the Chinese Computer Emergency Response Team.

Category 32.2 Censorship outside the USA

2006-07-13 EDUPAGE; CNET http://news.com.com/2100-1028_3-6094022.html

CHINA SENDS INTERNET REPORTER TO PRISON

Chinese courts have convicted another individual of using the Internet to distribute content deemed inappropriate and subversive. Li Yuanlong was accused of writing essays critical of unemployment and rural poverty and e-mailing them to Chinese-language news outlets based in the United States. Charges filed in February against Li said the essays "fabricated, distorted and exaggerated facts, incited subversion of the state, and [sought] to overthrow the socialist system." The court found Li guilty and sentenced him to two years in prison. Li's lawyer noted that although he believes the ruling was unjust, the sentence could have been much longer. Similar charges in other cases have resulted in prison terms of five and even ten years for those found guilty.

Category 32.2 Censorship outside the USA

2006-07-19 EDUPAGE; BBC http://news.bbc.co.uk/2/hi/south_asia/5194172.stm

INDIA CLAMPS DOWN ON BLOGS

The Indian government has ordered the country's 153 ISPs to block access to 17 Web sites, some of them blogs, causing an outcry among the country's bloggers. The government issued a directive in 2003 noting that it has the authority to restrict Web sites if they are deemed threatening to the state or its relationship with other countries or could potentially incite crime. The blogging community in India has reacted strongly, criticizing the government for censoring free speech. One blogger, Amit Agarwal, said his country has "joined the Internet Filtering Club of China, Saudi Arabia, Pakistan, and Ethiopia." Others expressed fears that the government is trying to restrict all blogs in the country, a charge the government denied.

Category 32.2 Censorship outside the USA

2006-08-02 EDUPAGE; CNET http://news.com.com/2100-1028_3-6101267.html

CHINA CLOSES LIBERAL WEB SITE

Government officials in China have taken another step in limiting what Internet users in the country can access, causing an uproar among intellectuals and others critical of the Communist Party. During the past week, access inside China to the Century China Web site has been cut off, prompting a petition that accuses the government of trying to control public opinion. More than 100 outspoken individuals--both inside the country and abroad--have signed the petition, which was sent by e-mail to the media. The petition states, in part, "The shutdown of Century China is just another instance of the Chinese government suppressing the freedom of its people." It also describes the Century China Web site as "the one spiritual home we had in the cyberworld."

Category 32.2 Censorship outside the USA

2006-10-16 EDUPAGE; New York Times (registration req'd)
http://www.nytimes.com/2006/10/16/technology/16wikipedia.html

CHINESE ALLOW ENGLISH WIKIPEDIA BUT NOT CHINESE

The Chinese government unexpectedly lifted its block of the English version of Wikipedia, though users inside China still cannot access the Chinese-language version of the site. China is widely known for censoring content it deems inflammatory, such as discussions of human rights in the country or events such as those in Tiananmen Square in 1989. A year ago, access to all of Wikipedia was blocked inside the country, though officials from Wikipedia said they were never told why the site was not allowed. Companies that want to operate in China frequently face the quandary of abiding by the government's strict restrictions on what is allowed or of not being allowed to operate in the country at all. After the ban was lifted, users in China were again able to access Wikipedia--or most of it, at least. One user said that although he could access material on controversial topics, he could not see content about Tiananmen Square.

CHINA UNBLOCKS WIKIPEDIA

Following the recent unblocking of the English-language version of Wikipedia in China, users in the country can now access the Chinese version of the Web site. Chinese officials made no comment about the change, but Andrew Lih, a Chinese-American academic who specializes in Wikipedia, said in his blog that he believes "consensus among the authorities determined the benefits of Wikipedia far outweigh the risks." China is notorious for blocking content it considers subversive, such as material on democracy or human rights. Paris-based Reporters Without Borders has routinely criticized Internet companies that make concessions to Chinese authorities' demands to censor online content. Those companies, including Yahoo, Google, and Microsoft, have argued that the benefits of having a presence in the country justify the concessions. Reporters Without Borders said that Wikipedia, which made no changes to its content to satisfy Chinese authorities, has shown that no such compromises are necessary. "The Chinese government is pragmatic," the group said, "and does not want to do without foreign businesses in the Internet sector."

[BBC, 16 November 2006 http://news.bbc.co.uk/2/hi/asia-pacific/6154444.stm]

Category 32.2 Censorship outside the USA

2006-11-08 EDUPAGE; Silicon Valley http://www.siliconvalley.com/mld/siliconvalley/15955567.htm

ORGANIZATION IDENTIFIES WORST INTERNET CENSORS

Paris-based Reporters Without Borders has issued a list of 13 countries it says are the most egregious censors of Internet speech. On the list are Belarus, China, Cuba, Egypt, Iran, Myanmar, North Korea, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan, and Vietnam. According to the organization, these countries stifle online speech they deem subversive or threatening to the government, including sentencing to prison individuals accused of posting such material. Reporters Without Borders also criticized Yahoo and other Internet companies for cooperating with the governments of these countries in identifying individuals targeted for prosecution. In the case of Jiang Lijun, a Chinese man sentenced to four years in prison for pro-democracy remarks, Reporters Without Borders said Yahoo's assistance was key to Chinese authorities' ability to identify him. "It's one thing to turn a blind eye to censorship," said Lucie Morillon, a spokesperson with the organization. "It's another thing to collaborate."

Category 32.2 Censorship outside the USA

2006-11-27 EDUPAGE; BBC http://news.bbc.co.uk/1/hi/technology/6187486.stm

DODGING THE CENSORS

Researchers at the Citizen Lab at the University of Toronto have developed software that they hope will allow Internet users in nations that practice censorship to have full access to the Web. Available as of December 1, the software, called psiphon, operates using social networking principles. Users in countries without censorship will download the application, which allows their computers to function as proxies. Users in countries with government censors can then access the Internet through the psiphon software, sidestepping Internet filters. The software merely indicates that a user is connected to another machine, without divulging details about that machine or what Web pages are visited. Ronald Deibert, director of the Citizen Lab, said psiphon is an effort to counterbalance what he called the militarization of Internet censorship, restoring free access to online resources. Officials from the Citizen Lab cautioned, however, that use of psiphon could constitute a criminal offense in some countries and advised potential users to understand the risks.

33.1 Acceptable-use policies

Category 33.1 Acceptable-use policies

2006-10-01 China Staff (Hong Kong) Oct 2006 12(9):36

EMPLOYEE BLOGS AFFECT CORPORATE IMAGE

Pattie Walsh, Head of Minier Ellison's Employment Practice in Greater China, wrote a succinct summary of how to handle employee blogging. The abstract of her paper reads in part, "Internet blogging -- posting comments and reflections on an online journal -- has become a growing phenomenon, and workplace-related blogging by employees has given rise to a host of new legal problems for employers to tackle. Blogs, which are widely accessible by those surfing the Internet, are a powerful new medium for sharing opinions and disseminating views -- and when they reference a writer's employer or a company's product they can potentially be great PR for companies, or a poisoned chalice. You have the option to allow the employee to continue her employment, and to discipline her for her blogging activities. Many companies have some degree of monitoring of employee's Internet use on work computers during work hours. To deter conduct of this behavior in the future and restrict the types of blogs being written by your employees, you may want to review your employment policies and contracts."

Category 33.1 Acceptable-use policies

2007-01-11 DHS Daily OSIR; New York Times
http://www.nytimes.com/2007/01/11/technology/11email.html

FIRMS FRET AS OFFICE E-MAIL JUMPS SECURITY WALLS.

Companies spend millions on systems to keep corporate e-mail safe. If only their employees were as paranoid. A growing number of Internet-literate workers are forwarding their office e-mail to free Web-accessible personal accounts offered by Google, Yahoo and other companies. Their employers, who envision corporate secrets leaking through the back door of otherwise well-protected computer networks, are not pleased. It is a battle of best intentions: productivity and convenience pitted against security and more than a little anxiety. Corporate techies want strict control over internal company communications and fear that forwarding e-mail might expose proprietary secrets to prying eyes. Employees just want to get to their mail quickly, wherever they are, without leaping through too many security hoops. So far, no major corporate disasters caused by this kind of e-mail forwarding have come to light. But security experts say the risks are real. Also, because messages sent from Web-based accounts do not pass through the corporate mail system, companies could run afoul of federal laws that require them to archive corporate mail and turn it over during litigation.

Category 33.1 Acceptable-use policies

2007-01-30 Effector Online http://www.eff.org/deeplinks/archives/005096.php

WORST PRACTICES FOR ONLINE SERVICE PROVIDERS.

In an instant, Seclists.org, including thousands of pages, vanished from the Internet this week. And if your online service providers have as weak a backbone as GoDaddy, the same thing could happen to your site. Here's the story (as recounted by News.com): A list of MySpace user names and passwords began floating around online weeks ago, including in a Seclists.org post. Rather than ask Seclists.org's owner, Fyodor Vaskovich, to remove a single offending page, MySpace wrote to his domain name registrar GoDaddy, which shut down all 250,000 Seclists.org pages. Did GoDaddy demand to receive a court order first? Was it at any legal risk? No. Apparently all it took was a single informal request from MySpace, and Seclists.org was gone, a mere 52 seconds after GoDaddy notified Vaskovich. "I think the fact that we gave him notice at all was pretty generous," said GoDaddy's general counsel Christine Jones, in what has to be in the running for most ironic comment of the week. All too often, that's what passes for customer service when your free speech is at stake. Internet intermediaries owe their customers more than that. GoDaddy should have given Vaskovich meaningful notice, time, and information to respond, and it should have been willing to stand up for his rights.
Read the News.com article for more: http://news.com.com/2100-1025_3-6153607.html
Check out EFF's Best Practices for Online Service Providers for more on how companies like GoDaddy ought to behave: http://www.eff.org/osp/
For this post and related links: http://www.eff.org/deeplinks/archives/005096.php

33.2 Spam, spim, spit, splogs, phish, vish & pharms

Category 33.2 Spam, spim, spit, splogs, phish, vish & pharms

2006-01-24 DHS Daily OSIR; http://www.techweb.com/wire/security/177103408

BILL GATES' SPAM PREDICTION MISSES TARGET.

On January 24, 2004, Bill Gates told a group at the World Economic Forum that "two years from now, spam will be solved." During the talk, Gates pinned his prediction on the creation of an authentication scheme to verify senders' identities, as well as the hope that some kind of micropayment structure could be created for levying fees on e-mail. "We have a long way to go before we solve the spam problem," said Scott Chasin, the chief technology officer for Denver, CO-based e-mail security firm MXlogic. Neither of the proposals Gates mentioned two years ago have made much headway. Although Microsoft uses its own Sender ID authentication protocol for the company's Web-based Hotmail service, neither Sender ID nor the competing DomainKeys from Yahoo have anything like broad acceptance by ISPs or enterprises. And the micropayment concept for e-mail is as dead now as it was two years ago. Microsoft may take the position that "solving" the spam problem means containing spam with filtering technology, Chasin said, but even using that definition, spam remains a huge problem.

Category 33.2 Spam, spim, spit, splogs, phish, vish & pharms

2006-01-31 DHS Daily OSIR; China Daily
http://english.peopledaily.com.cn/200701/31/print20070131_346292.html

FOR CHINESE HACKERS, IT'S A GAME.

Money is by far the primary motivation for most of today's virus writing and spamming in the world of computers except when it comes to China. For Chinese hackers, gaming prestige outweighs financial gain, according to a new report on Internet security. The target of Chinese Internet malicious software, or malware, is to steal better online weapons and the profiles of the most famous gamers. According to Sophos' Security Threat Report 2007, Chinese hackers accounted for 30 percent of the malware written last year, surpassed only by the U.S. The report also reveals some national characteristics of hackers. Brazilian hackers tend to produce simulations of banks' Websites, attempting to get your credit card information; while hackers from Russia and Sweden create backdoors to vulnerable computers. The motivation is financial gain. In contrast, the Chinese malware aims at "health", "power" and gaming profiles.

Category 33.2 Spam, spim, spit, splogs, phish, vish & pharms

2006-05-04 DHS Daily OSIR; http://www.smh.com.au/news/breaking/spammer-identifies-do-not-spam-addresses/2006/05/04/1146335837392.html

SPAMMER IDENTIFIES 'DO NOT SPAM' ADDRESSES.

One spammer has managed to identify e-mail addresses on Blue Security's Blue Frog "do-not-spam" list, taking advantage of an obvious flaw with such lists and prompting critics to wonder what took so long. The lists are generally encrypted so spammers can't mine them for new addresses. However, John Levine, co-author of Fighting Spam for Dummies, said spammers merely have to run their lists, see what's been removed and compare that with the original to find out the addresses on the "do-not-spam" lists.

Category 33.2 Spam, spim, spit, splogs, phish, vish & pharms

2006-06-12 DHS Daily OSIR; Register (UK)
http://www.theregister.co.uk/2006/06/12/spam_distribution_study_ciphertrust/

TAIWAN FINGERED AS THE HUB OF SPAM DISTRIBUTION.

Sixty-four percent of servers controlling spam traffic are located in Taiwan, according to a survey by e-mail security firm CipherTrust. The U.S. accounts for 23 percent of the machines identified on CipherTrust's spam server blacklist with China in a fairly distant third place (three percent). CipherTrust obtained its figures after deploying a network of zombie-like machines across the world to gather intelligence on spamming operations.

Category 33.2 Spam, spim, spit, splogs, phish, vish & pharms

2006-06-28 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/06/06/28/HNspammers_1.html

FOR SPAMMERS, A PICTURE IS BETTER THAN 1,000 WORDS.

Spam is again on the rise, led by a flood of junk images that spammers have crafted over the past few months to trick e-mail filters, according to security vendors. Called "image-based" spam, these junk images typically do not contain any text, making it harder for filters that look for known URLs or suspicious words to block them. Instead of a typed message, users will see only an embedded .gif or .jpeg image file urging them to buy pharmaceuticals or invest in penny stocks. Anti-spam vendor Cloudmark says that half of the incoming spam is now image-based on the "honeypot" systems it puts out on the Internet to lure spammers.

Category 33.2 Spam, spim, spit, splogs, phish, vish & pharms

2006-08-21 DHS Daily OSIR; Register (UK)
http://www.channelregister.co.uk/2006/08/21/sec_spam_scam_suit/

SEC SUES OVER STOCK MARKET SPAM SCAM.

A U.S. couple has been charged over an allegation they made $1 million via a stock market pump-and-dump scam, promoted using spam e-mails. Jeffrey Stone and Janette Diller Stone face a lawsuit from the Securities and Exchange Commission (SEC) over their alleged use of junk mail tactics to artificially increase the value of stock they held in start-up firm WebSky Inc. They allegedly bought 288 million WebSky shares through various front organizations they controlled before selling them weeks later for a profit of $1 million. The SEC alleges spam e-mails sent by stock promoters on behalf of the Stones falsely stated that WebSky's business in Argentina was bringing in revenues of $40 million. In reality, the start-up had little or no revenue from Argentinaat the time the spam e-mails began circulating. The junk e-mail campaign helped ramp up WebSky's share value by around 300 percent, according to the SEC. The dishonest promotion of WebSky shares is an example of so-called pump-and-dump stock campaigns which Sophos estimates currently account for approximately 15 percent of all junk mail.

Category 33.2 Spam, spim, spit, splogs, phish, vish & pharms

2006-09-29 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2165311/coming-inbox-soon-personalised

PERSONALIZED SPAM SET TO FLOOD INBOXES.

Spammers are less than a year away from mass-mailing messages with personalized subject lines, greatly increasing the chances of users opening the message, a security expert warned Friday, September 29. Technical staff, for example, are currently receiving messages with subject lines such as "DNS change request." Matt Sergeant, senior anti-spam technologist at MessageLabs, believes this is a trial run for more widespread spam using the same social engineering principles. "The end game is for spammers to pull together information from the site where they harvested your address and generate highly specific subject lines using text automatically extracted from the source," he said. Such an e-mail stands a greater chance of slipping through a single-technology filter.

Category 33.2 Spam, spim, spit, splogs, phish, vish & pharms

2006-11-27 DHS Daily OSIR; Associated Press
http://news.yahoo.com/s/ap/20061128/ap_on_hi_te/eu_spam

EU SAYS MORE THAN HALF E-MAILS ARE SPAM.

Unsolicited e-mails continue to plague Europeans and account for between 50 and 80 percent of all messages sent to mail inboxes, the European Commission said Monday, November 27. A European Union (EU) report found that only two EU nations -- the Netherlands and Finland -- were making inroads in enforcing the 2002 law to crack down on spam. Dutch authorities were able to reduce spam by 85 percent by using fines to get businesses to fall in line with the EU rule. EU officials have said they will put forward new legislation next year to make it easier to prosecute spammers.

Category 33.2 Spam, spim, spit, splogs, phish, vish & pharms

2007-01-24 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2173254/wikipedia-shuts-link-spammers

WIKIPEDIA SHUTS OUT LINK SPAMMERS.

Wikipedia has started to instruct search engines to ignore links on its pages which point to external Websites. The user-created encyclopedia has started to include "nofollow" tags in all external links. This prevents the links from being spidered by search engines, or used to determine a Website's popularity by mechanisms such as Google's PageRank. Wikipedia took the action in response to a search engine optimization contest in which Webmasters were challenged to gain the highest ranking with major search engines for the query "Global warming awareness 2007." One of the contestants created a spam entry on Wikipedia which included a link to his own Webpage. The "nofollow" tag was first introduced by companies providing blogging services in an effort to curb the flow of spam links in comments on blogs.

Category 33.2 Spam, spim, spit, splogs, phish, vish & pharms

2007-03-29 DHS Daily OSIR; Sophos http://www.sophos.com/pressoffice/news/articles/2007/03/php-spam.html

SPAMMERS HACK PHP WEBSITES TO MAKE MONEY FROM ONLINE PHARMACIES.

Sophos has warned Internet users of the importance of properly securing their Websites after it has uncovered evidence that spammers are hacking into sites in their attempt to sell goods. Spam campaigns advertising Internet pharmacies peddling drugs are directing users to Webpages hosted on hacked innocent Websites that then automatically redirect surfers to the online store. The hacked Websites are all using PHP, a scripting language used by many Internet sites, which has suffered from serious security vulnerabilities in the past. Because the spam messages point to an innocent Website rather than directly to the online pharmacy, there is a risk that sites unaware of the spam campaign may have their reputations tarnished. Anti-spam products often use information about the Webpage pointed to by an e-mail as an indicator of whether the message is spam or not.

Category 33.2 Spam, spim, spit, splogs, phish, vish & pharms

2007-03-30 DHS Daily OSIR; Computerworld http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9015195&intsrc=hm_list

PILL SPAMMERS TURN HACKERS TO 'JOE JOB' SITES.

Spammers are hacking into legitimate Websites through unpatched vulnerabilities in the PHP scripting language to sidestep blacklists that block spam or bar access to known spammer sales sites, a security company said Thursday, March 29. The tactic, said Sophos PLC, is a form of "joe job" -- a term usually given to spam attacks expressly designed to blacken the reputation of a legitimate user or company. Here, though, the intention is to slip by antispam defenses. The spammers first hack a genuine site by exploiting any of several unpatched PHP bugs. Once inside a legitimate site's server, the spammer can set up a redirect so that specific traffic heading its way will be shunted to the junk mailer's selling site. Most of the spam, Cluley said, touts cheap pharmaceuticals. Last week, Canadian coroners said that a 57-year-old British Columbian woman, Marcia Bergeron, died from taking pills tainted with strontium and uranium. Bergeron had purchased the medications from an online pharmacy pretending to be based in Canada.

33.4 Risk analysis & management

Category 33.4 Risk analysis & management

2006-03-21 DHS Daily OSIR; http://www.securitypipeline.com/news/183701727

MANY DATA CENTERS STILL HAVE NO RISK MANAGEMENT PLAN.

Business technology managers are facing tough challenges as data centers grow larger and more complex. More than 75 percent of all companies have experienced a business disruption in the past five years, including 20 percent who say the disruption had a serious impact on the business, according to a recent survey of data center managers. Despite the critical nature of data center operations to business, nearly 17 percent reported they have no risk management plan, and less than 5 percent have plans that address viruses and security breaches. The results, which were announced Tuesday, March 21, at the Data Center World conference in Atlanta, are part of survey of nearly 200 members of AFCOM, a leading association for data center managers. Some of the predictions: Within the next five years, one out of every four data centers will experience a serious disruption; by 2015, the talent pool of qualified senior-level technical and management data center professionals will shrink by 45 percent; and over the next five years, power failures and limits on power availability will halt data center operations at more than 90 percent of companies.

Category 33.4 Risk analysis & management

2006-07-11 DHS Daily OSIR; Government Executive
http://www.govexec.com/story_page.cfm?articleid=34527

REPORT: VETERANS AFFAIRS TREATED DATA BREACH WITH INDIFFERENCE.

Senior Veterans Affairs (VA) officials failed to understand the significance of the department's early May data breach and responded with "indifference and little sense of urgency," according to an inspector general (IG) report released Tuesday, July 11. The report from VA Inspector General George Opfer reviews the circumstances surrounding the May 3 theft of a laptop computer and external hard drive from the home of a data analyst. The equipment contained personal information on more than 26 million veterans. Department policies and procedures for protecting personal and proprietary data were not followed, though none of the policies prohibited the removal of protected information from the worksite, the report said. Information security weaknesses remain uncorrected, the IG added. The report recommended that VA Secretary James Nicholson establish a clear and concise policy on protecting sensitive information on and off agency systems and modify mandatory cybersecurity and privacy awareness training. In response to the report, Nicholson said he has initiated four administrative investigations of the offices involved in both the breach and the response. He also said the agency has "embarked on a course of action to wholly improve its cyber and information security programs." IG Report: http://www.va.gov/oig/51/FY2006rpts/VAOIG-06-02238-163.pdf

Category 33.4 Risk analysis & management

2006-07-21 DHS Daily OSIR; Information Week http://www.informationweek.com/showArticle.jhtml

UBS TRIAL AFTERMATH: EVEN GREAT SECURITY CAN'T PROTECT YOU FROM THE INSIDER.

The recent UBS PaineWebber computer sabotage trial is a perfect example of the damage that can be caused by a knowledgeable insider with high-level access and an axe to grind. A company employee is already inside the perimeter, where the vast majority of the protective technologies sit. That same employee also knows what information is most vital to the company's ability to make money and sustain itself. He has knowledge of passwords, and he also probably knows what kind of machines and operating systems the company is running. An IT professional has all this information, plus he has access to the inner workings of the infrastructure. He has high-level privileges that allow him access to key servers and databases, and possibly even root-level access, which would give him all-encompassing power over the system. UBS PaineWebber's network was hit by a logic bomb in March of 2004. A jury last week found Roger Duronio of Bogota, NJ, guilty of two crimes: computer sabotage for building, planting and distributing the malicious code that brought down nearly 2,000 servers on the company's nation-wide trading network; and securities fraud.

Category 33.4 Risk analysis & management

2006-07-31 DHS Daily OSIR; Security Focus http://www.securityfocus.com/brief/267

FIRM CLASSIFIES SOFTWARE FLAWS TO HELP DEVELOPERS.

Security firm Fortify announced on Monday, July 31, that the firm had created a hierarchy for labeling security issues in hopes that giving names to software flaws will enable programmers to avoid making the same mistakes. The hierarchy consists of 115 categories split among seven "kingdoms" or top-level classes and a catch-all external class. The top-level seven kingdoms are input validation and representation, API abuse, security features, time and state, errors, code quality, and encapsulation. Fortify also announced on Monday that the firm had donated the research project to the Open Web Application Security Project.

The taxonomy was created by Dr Gary McGraw and his colleagues and is available from < http://www.fortifysoftware.com/security-resources/taxonomy.jsp >. The description begins as follows:

* * *

This site presents a taxonomy of software security errors developed by the Fortify Software Security Research Group together with Dr. Gary McGraw. Each vulnerability category is accompanied by a detailed description of the issue with references to original sources, and code excerpts, where applicable, to better illustrate the problem.

The organization of the classification scheme is described with the help of terminology borrowed from Biology: vulnerability categories are referred to as phyla, while collections of vulnerability categories that share the same theme are referred to as kingdoms. Vulnerability phyla are classified into "seven plus one" pernicious kingdoms presented in the order of importance to software security:

1. API Abuse
2. Code Quality
3. Encapsulation
4. Errors
5. Input Validation and Representation
6. Security Features
7. Time and State

*. Environment

The first seven kingdoms are associated with security defects in source code, while the last one describes security issues outside the actual code. To browse the kingdom and phylum descriptions, simply navigate the taxonomy tree on the left. [There are links on the original Web page.]

The primary goal of defining this taxonomy is to organize sets of security rules that can be used to help software developers understand the kinds of errors that have an impact on security. By better understanding how systems fail, developers will better analyze the systems they create, more readily identify and address security problems when they see them, and generally avoid repeating the same mistakes in the future.

When put to work in an analysis tool, a set of security rules organized according to this taxonomy is a powerful teaching mechanism. Because developers today are by and large unaware of the myriad ways they can introduce security problems into their work, making a taxonomy like this available should provide tangible benefits to the software security community.

Defining a better classification scheme can also lead to better tools: a better understanding of the problems will help researchers and practitioners create better methods for ferreting them out.

* * *

Category 33.4 Risk analysis & management

2006-08-24 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/06/08/24/HNreportcybercrime_1.html

U.S. AIR FORCE SPECIAL AGENT SAYS 75 PERCENT OF DDOS VICTIMS DO NOT REPORT THE ATTACKS.

Companies that work with law enforcement agencies on cybercrime can get valuable information, including lists of hostile IP (Internet Protocol) addresses and information on new types of attacks, said U.S. Air Force cybercrime investigator Wendi Whitmore at the 2006 InfraGard National Conference. The shared information between law enforcement and private businesses can help both groups develop better defenses, she said. About three-quarters of the victims of DDOS (distributed denial-of-service) extortion scams don't report the crimes to law enforcement agencies. In extortion scams, criminals use networks of compromised computers called botnets to flood a company's network with traffic, then ask the company for money to make the DDOS attack stop. If the company refuses to pay, the attacker floods the company's network with more traffic, often from thousands of zombie computers, then demands more money, she said. Financial companies such as banks and gambling Websites are favorite targets for these botnet extortion scams. Botnets of compromised computers are responsible for sending many viruses and worms and phishing scam e-mails, Whitmore said. In addition to DDOS attacks, compromised computers can send out the owner's personal information.

Category 33.4 Risk analysis & management

2006-11-15 DHS Daily OSIR; IDG News Service
http://news.yahoo.com/s/pcworld/20061115/tc_pcworld/127889

HUMANS CALLED WEAK LINK IN TECH SECURITY.

The SANS Institute has some controversial advice for computer security professionals looking to lock down their networks: spear-phish your employees. That's what the U.S. Military Academy at West Point did in 2004 to a group of 512 cadets, selected for a test. The cadets were sent a bogus e-mail that looked like it came from a fictional colonel, who claimed to be with the academy's Office of the Commandant. More than 80 percent of the cadets clicked on the phishing link. Even after hours of computer security instruction, 90 percent of freshmen cadets still clicked on the link. Because these attacks rely on cooperation from their victims, it's hard to prevent them, said Alan Paller, director of research with SANS. "The only defense against spear phishing is to run experiments on your employees and embarrass them," he said. Paller's organization compiles an annual report on the top to Internet security targets. This year "human vulnerabilities" will make their first appearance on a list. That's because the human factor is being exploited in a growing number of targeted attacks as more and more online criminals come online in Eastern Europe and Asia, Paller said.

Category 33.4 Risk analysis & management

2007-03-30 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article98102-03-30-07-Web

SENATE BILL WOULD CREATE TELEWORK MANAGEMENT POSITION.

Senate proponents of federal teleworking have introduced a bill that would require agencies to establish a key management position for telework. Under the bipartisan Telework Enhancement Act of 2007, introduced March 28 by Senators Ted Stevens (R-AK) and Mary Landrieu (D-LA), agencies would have to designate a telework-managing officer, who would be responsible for implementing agency telework programs and serve as a liaison between employees and managers. The officer also would develop accountability and productivity criteria, and keep employees informed about their telework eligibility and other issues. Among other provisions, the bill also would reverse current telework eligibility law, which states that employees are ineligible to telework unless deemed otherwise by their agencies. If passed, the legislation would make all federal workers eligible unless shown otherwise by their employer. “By encouraging federal agencies to allow their employees to work from home, we will reduce their use of gasoline, save them thousands of dollars in fuel expenses each year and help protect the environment,” Stevens said.

Category 33.4 Risk analysis & management

2007-05-01 DHS Daily OSIR; San Francisco Chronicle http://sfgate.com/cgi-bin/article.cgi?file=/c/a/2007/05/01/M NGQUPIKHS1.DTL

MENTAL HEALTH TRAINING TO SPOT TROUBLED STUDENTS.

Two weeks after a disturbed student's killing spree at Virginia Tech in Blacksburg, VA, University of California- Berkeley is ramping up efforts to expand its training of faculty, staff and students in identifying and helping students in need of help. Nearly 600 people have already undergone the training and roughly 100 green stickers mark the campus doors and work spaces of some of those ready to help. Efforts are underway to increase the number of stickers and their visibility on the 34,000-student campus. "I think the Virginia Tech incident was a wake-up call to a lot of faculty and students that we're not really doing a very good job of looking out for the distressed student," said Mary Ann Mason, UC-Berkeley's graduate division dean and co-chair of the chancellor's advisory committee on student mental health. As part of its "Look for the Signs" training program, the campus is planning a training symposium later this month on how to identify the warning signs of depression and other mood trouble in students -- and what to do when a student needs help. One goal of the training is to create standards for all members of the campus community in identifying the warning signs of mood trouble and taking the first steps to aid a student.

Category 33.4 Risk analysis & management

2007-05-05 DHS Daily OSIR; Finance Tech http://www.financetech.com/showArticle.jhtml?articleID=199203702

FRAUD TECHNIQUES EVOLVE IN PARALLEL WITH BANK PRODUCTS AND DEFENSES.

While the crimes remain a constant for financial institutions, the methods for perpetrating them have become just as diverse as the products and services offered by banks. Today's financial institutions have to be on their toes more than ever to keep that one important step ahead of fraudsters. "The overall mix of fraud is changing it's becoming more diverse," observes Jerry Cranney of KeyBank. "[Scammers] are utilizing more tools and systems to commit fraud. We're in a world where fraud is perpetrated by check but the criminal uses ACH or wire transfer to actually move the funds more quickly. So it's more of a challenge for banks to recover the funds." Phillip Upton of PricewaterhouseCoopers says there are multiple layers to a fraud prevention strategy, including transaction monitoring, risk scoring and item investigation. Upton says that not many banks are at a point where they can obtain a single view of fraud activity across the enterprise because it requires the ability to draw data from different systems into one dashboard. The idea of pooling data throughout the bank to gain a single enterprisewide view of fraud is where many in the industry believe fraud prevention needs to go.

33.5 Data-encryption policies

Category 33.5 Data-encryption policies

2006-02-14 EDUPAGE; http://news.com.com/2100-1030_3-6039645.html

COURT SAYS UNENCRYPTED DATA OKAY

A federal judge in Minnesota has dismissed a case alleging that a student loan company was negligent in not encrypting customer data. The case was filed by Stacy Lawton Guin after a laptop containing unencrypted data on about 550,000 customers of Brazos Higher Education Service was stolen from an employee's home in 2004. Although he was not harmed by the loss of his personal information--indeed, there have been no reports of any fraud committed with the stolen information--Guin argued that the Gramm-Leach-Bliley (GLB) Act required Brazos to encrypt the data. Judge Richard Kyle rejected that claim, noting that the legislation does not specifically require encryption. The law states that financial services companies must "protect the security and confidentiality of customers' nonpublic personal information," but, according to Kyle's decision, "The GLB Act does not prohibit someone from working with sensitive data on a laptop computer in a home office."

Category 33.5 Data-encryption policies

2006-03-10 RISKS; CNET news.com http://tinyurl.com/ne3xx

USING SECURE WIPE UTILITY LEADS TO LAWSUIT FOR HACKING

Declan McCullagh summarized an interesting interpretation of law that occurred in the US Court of Appeals for the 7th Circuit in March 2006. It seems that Jacob Citrin used to work for International Airport Centers. He quit and returned his laptop computer to them. They prepared to sue him for allegedly violating his employment contract by going to business for himself in the same field. When they searched his hard drive looking for juicy files to undelete as part of their preparation for the civil case, they discovered that he had wiped files rather than deleted them: the old files were unrecoverable. So they accused him of violating 18 USC §1030, the Computer Fraud and Abuse Act of 1986.

McCullagh wrote:

>That law says whoever "knowingly causes damage without authorization" to a networked computer can be held civilly and criminally liable.

The 7th Circuit made two remarkable leaps. First, the judges said that deleting files from a laptop counts as "damage." Second, they ruled that Citrin's implicit "authorization" evaporated when he (again, allegedly) chose to go into business for himself and violate his employment contract.

The implications of this decision are broad. It effectively says that employees better not use OS X's Secure Empty Trash feature, or any similar utility, because they could face civil and criminal charges after they leave their job. (During oral argument last October, one judge wondered aloud: "Destroying a person's data--that's as bad as you can do to a computer.")

Citrin pointed out that his employment contract permitted him to "destroy" data in the laptop when he left the company. But the 7th Circuit didn't buy it, and reinstated the suit against him brought by IAC.<

Category 33.5 Data-encryption policies

2006-09-25 DHS Daily OSIR; Information Week
http://www.informationweek.com/news/showArticle.jhtml?articleID=193004775

ENCRYPTION WORKS WONDERS, BUT CAUSES ITS OWN IT HEADACHES.

The policy for some organizations that handle sensitive data has been to encrypt everything -- despite encryption's well-deserved reputation for adding cost, complexity, and latency to IT environments. More organizations need to encrypt more of their data, but blanket encryption policies still are a bad idea. The most aggressive users of encryption for PCs, databases, and networks can spend hundreds of thousands of dollars on product licenses, training, and support. The added software and hardware layers can slow systems performance, particularly when data packets must be decrypted to be examined by firewalls and intrusion-prevention systems. The alternative is to assume that all encrypted data is coming from a trusted source and let those packets through without inspection. Companies must view widespread encryption with their eyes wide open. Even by the vendors' own admissions, encryption technology presents many difficulties. It sucks up a lot of IT time and makes it harder to share information. Then there's the management of the keys used to decrypt messages. If they're stolen or otherwise fall into the wrong hands, encrypted data becomes vulnerable. If keys are lost, it can become impossible to retrieve data.

Category 33.5 Data-encryption policies

2007-03-06 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article97837-03-06-07-Web

VA TO CONTROL, RESTRICT USE OF MOBILE STORAGE DEVICES.

In the next month, the Department of Veterans Affairs (VA) will let employees plug into its network only those mobile storage devices issued by the chief information officer's office. Robert Howard, the department's CIO, said Tuesday, March 6, he will issue only 1G and 2G thumb drives and will not allow anything larger onto the network unless he approves it. The mobile storage devices also must be certified under the National Institute of Standards and Technology's Federal Information Processing Standard 140-2, he added. Besides controlling thumb drives, Howard aims to have a standard configuration for smart phones and personal digital assistants, eliminate unencrypted messages that travel on the VA's network and reduce the number of virtual private networks by the end of fiscal 2007. The department also is relying more on public-key infrastructure (PKI) and Microsoft's rights management system (RMS) in its Outlook e-mail system to do a better job of securing e-mail and documents.

Category 33.5 Data-encryption policies

2007-04-10 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/07/04/10/HNirslaptopsencrypted_1.html

IRS HEAD: ALL LAPTOPS TO BE ENCRYPTED WITHIN WEEKS.

After an auditor found serious security problems in the way it handled sensitive data on laptops, the Internal Revenue Service (IRS) said it will have all laptops encrypted within the next few weeks. IRS Commissioner Mark Everson said his organization was making the effort following a recently released audit that found unencrypted data on a large percentage of IRS laptop computers. Auditors tested 100 laptop computers used by IRS employees and found that 44 of them contained "unencrypted sensitive data, including taxpayer data and employee personnel data."

33.6 Outsourcing & offshoring

Category 33.6 Outsourcing & offshoring

2006-02-23 EDUPAGE; http://www.nytimes.com/2006/02/23/technology/23outsource.html

REPORT SAYS OUTSOURCING FEARS EXAGGERATED

A new report from the Association for Computing Machinery (ACM) argues that fears of a wholesale migration of high-tech jobs away from the United States are not supported by the data so far. Representing a year's work by a study group, the report predicts continued offshoring of 2 to 3 percent of IT jobs each year for the next decade, but it notes that the number of high-tech jobs continues to grow and already exceeds the number at the height of the dot-com boom. Although the report acknowledges losses to lower-wage markets and notes that the marketplace for technology is tightening, "the notion that information technology jobs are disappearing is just nonsense," according to Moshe Vardi, computer scientist at Rice University and cochair of the study group. David Patterson, president of the ACM and computer science professor at the University of California, Berkeley, said that exaggerated fears of outsourcing have hurt the U.S. market by discouraging college students from pursuing careers in IT, which, in turn, will lead to fewer qualified members of the U.S. IT workforce.

Category 33.6 Outsourcing & offshoring

2006-06-06 DHS Daily OSIR; Reuters http://news.com.com/IBM+to+pour+6+billion+into+India/2100-1014_3-6080346.html

IBM TO POUR $6 BILLION INTO INDIA.

IBM plans to invest nearly $6 billion in India over three years, underscoring the country's ever-increasing importance as a global hub for IT outsourcing and expertise. IBM, the world's largest computer services company, said Tuesday, June 6, that it plans to expand its services, software, hardware and research businesses in India, where it already is the largest multinational company with 43,000 employees in 14 cities, up from 4,900 in 2002. The deal, almost triple the $2 billion that IBM has already invested in India over the past three years, is the biggest investment by a multinational firm in India in recent years.

Category 33.6 Outsourcing & offshoring

2006-07-24 DHS Daily OSIR;
Government Executive http://www.govexec.com/dailyfed/0706/072406j1.htm

FEMA OUTSOURCES IDENTITY VERIFICATION FOR DISASTER ASSISTANCE.

The Federal Emergency Management Agency (FEMA) decided to outsource the process of verifying disaster assistance applicants' identities, after last year's debit card handout in the wake of Hurricane Katrina allowed fraudulent and wasteful purchases, officials said Monday, July 24. In connection with a Monday announcement that the agency will reduce each household's maximum share of government emergency funds, FEMA Director R. David Paulison, said the agency has opted to contract out identity verification. He acknowledged that the agency was not prepared to defend its fund against fraud last year. "FEMA did not have a system in place" to verify people's identities, Paulison said. David Garratt, deputy director of FEMA's recovery division, said hurricane relief registration continues to improve. The agency was only capable of handling about 100,000 evacuee claims after Hurricane Katrina, but it may be able to process twice that number this year, he said. FEMA also is doing away with the debit cards it distributed last year, which received a great deal of publicity after the funds were used for nonessential items -- including tabs at gentlemen's clubs, breast implants and pornography.

Category 33.6 Outsourcing & offshoring

2006-10-10 DHS Daily OSIR; Register (UK)
http://www.theregister.co.uk/2006/10/10/data_centre_probe_announced/

INFO GUARDIAN TO INVESTIGATE CALL CENTER DATA LEAKS.

The UK Information Commissioner is launching an investigation into outsourced data centers after a television program exposed security breaches at Indian call centers. Channel 4's Dispatches was offered individuals' banking details for a low cost by criminal networks in India. The Information Commissioner's Office (ICO) will investigate the practices of the mobile phone companies whose call centers were allegedly the source of the information. "It appears that some mobile phone companies' call centers in India are being targeted by criminals intent on unlawfully obtaining UK citizens' financial records and this will be the focus of our investigation," said David Smith, deputy information commissioner. "We are concerned by any breaches of security particularly if they involve confidential banking details." The ICO could prevent some companies sending their data outside the UK for processing, forcing them to carry out back office functions in the UK.

Category 33.6 Outsourcing & offshoring

2006-11-22 DHS Daily OSIR; Reuters http://www.eweek.com/article2/0,1895,2062804,00.asp

BANKS FACE GROWING THREAT OF INSIDE IDENTITY THEFT.

While banks are confident they can deal with phishing attacks by constantly warning customers of the dangers, they are now getting increasingly concerned about the physical theft of confidential client data by insiders or impostors. Widespread outsourcing of data management and other services has exposed some weaknesses and made it harder to prevent identity theft by insiders. In what many regard as the biggest wake-up call in recent memory for financial institutions, thieves disguised as cleaning staff last year narrowly failed to steal the equivalent of more than $400 million from the London branch of Sumitomo Mitsui. They installed programs to record keystrokes on computers that were used to handle international wire transfers of money. After analyzing user identifications and passwords recorded by the keylogging programs, they used the information to make a huge money transfer to an Israeli bank but were foiled at the last minute when police were tipped off. Banks are starting to respond to the threat by combining teams working on physical and information technology security, which have traditionally been separate functions, said Potter.

33.7 Facilities security

Category 33.7 Facilities security

2007-01-10 INNOVATION (Reuters/CNet 2 Jan 2007) <http://news.com.com/From+yap+to+growl%2C+Israeli+device+dogs+intruders/2100-7348_3-6146682.html>

WHEN A DOG'S BARK IS WORSE THAN ITS BITE

An Israeli security firm is using technology to harness the "early warning system" emitted by watchdogs who sense something out of the ordinary. Bio-Sense Technologies used computers to analyze 350 dog barks and found that canines of all breeds bark similarly when they sense a threat. The Dog Bio Security system, dubbed Doguard, uses sensors that pick up a dog's "alarm bark" and alerts human beings in the control room. The system is used at high-security Eshel Prison, as well as in Israeli military bases, water installations, farms, ranches, garages and Jewish settlements on the West Bank.

Category 33.7 Facilities security

2007-03-23 DHS Daily OSIR; CNET News http://news.com.com/A+new+day+for+business+security/2100-7355_3-6168256.html

A NEW DAY FOR BUSINESS SECURITY.

It might not seem as if a building security guard and a network administrator have much in common. But they do -- and the distinction between the two is blurring more every day. It's true that the people who control building access from security desks and those securing computer networks both watch traffic and walk perimeters to safeguard an organization's assets. But now, technology, tighter security controls, federal regulations and potential cost benefits are bringing the two traditionally separate worlds together. The next two years will prove important in bringing together the security disciplines, observers say. Challenges include creating interoperability and making sure the one system that controls all aspects of security is safe from breaches. Unifying technologies include network-connected surveillance cameras and mechanisms to control building access that tie into the same systems used to grant network access. Software can catch what the human eye might not, such as somebody sneaking into a building behind another person who just swiped a security badge. Also, a single system for credentials can replace multiple access systems and passwords. One badge, or smart card, could be used to enter buildings, log on to networks and buy lunch in the campus cafeteria.

Category 33.7 Facilities security

2007-04-21 DHS Daily OSIR; Los Angeles Times http://www.latimes.com/technology/la-fi-grid21apr21,1,5633750.story

ALLEGED SABOTEUR OF POWER GRID GAINED ACCESS DESPITE WARNING.

A contract technician accused of sabotaging computers at the California Independent System Operator (Cal-ISO) was able to enter the building and high-security inner rooms -- allowed in by electronic card readers and a handprint scanner -- even though his employer had warned days earlier that he should be denied access to the facility, authorities said. Lonnie Charles Denison, a 32-year-old computer specialist, has a "history of mental illness, drug abuse and alcohol issues," a prosecutor said Friday, April 20. Sunday's incident has raised alarms among state and federal energy regulators. Denison was arrested by the FBI on Wednesday and charged with attempted destruction of an electrical facility. Around midnight Sunday he broke a glass seal and pushed an emergency electricity shut-off button, plunging the Cal-ISO building in Folsom into darkness and crashing computers used to communicate with the power market. The act caused no blackouts but could have disrupted the western U.S. power grid had it happened during hours of peak demand for electricity, such as a summer afternoon. Denison early Sunday night tried and failed to log on to access the Cal-ISO computer network. However, a few hours later he succeeded in gaining physical entry to the building.

34.1 Net filter (site & content blocking)

Category 34.1 Net filter (site & content blocking)

2006-05-30 RISKS

COMPUTER C*CK-UP FINDS E-R-E-C-T-I-O-N HARD TO HANDLE

Yet another example of the perils of simple-minded content filtering:

>Two e-mail messages objecting to a home extension failed to reach a council planning department because their computer system blocked the word "e-r-e-c-t-i-o-n". Commercial lawyer Ray Kennedy, from Middleton, Greater Manchester, claims he sent three e-mails to Rochdale council complaining about his neighbour's plans. But the first two messages failed to reach the planning department because the software on the town hall's computer system deemed them offensive. When his third e-mail, containing the same word, somehow squeezed through, it was too late. A planning officer told Mr Kennedy that his next-door neighbour's proposals had already been given the go ahead.<

[Abstract by Nick Rothwill edited by Peter G. Neumann to reduce likelihood of blocking of the entire issue of RISKS]

[MK adds: another issue is that naïve users are increasingly unware that the technical specifications for e-mail do not include guaranteed delivery. If delivery matters to you, CHECK FOR IT. Why didn't Mr Kennedy write a letter if the issue was so important to him?]

Category 34.1 Net filter (site & content blocking)

2007-03-28 DHS Daily OSIR; CNET News
http://news.com.com/Web+filters+mistakenly+blocking+Yahoo/2100-1029_3-6171423.html

WEB FILTERS MISTAKENLY BLOCKING YAHOO.

Websense's products are meant to block malicious Websites, but on Tuesday and Wednesday, March 27-28, the Web filters also blocked Yahoo.com. The blockade is the result of an erroneous update sent out to Websense customers late Tuesday afternoon, a representative for the company said. "The details are still under investigation but some IP addresses associated with the Yahoo.com site were classified incorrectly," the representative said. As a result, Web surfers at organizations that use Websense filtering software are unable to access the popular Website.

Category 34.1 Net filter (site & content blocking)

2007-05-14 DHS Daily OSIR; Associated Press
http://news.yahoo.com/s/ap/20070514/ap_on_hi_te/military_sites_blocked;_ylt=AgUInoY8fReoSkZDdOPh5.sjtBAF

DOD BLOCKS SOME WEBSITES.

Soldiers serving overseas will lose some of their online links to friends and loved ones back home under a Department of Defense (DoD) policy that a high-ranking Army official said would take effect Monday, May 14. DoD will begin blocking access "worldwide" to YouTube, MySpace and 11 other popular Websites on its computers and networks, according to a memo sent Friday by General B.B. Bell, the U.S. Forces Korea commander. The policy is being implemented to protect information and reduce drag on the department's networks, according to Bell.

Category 34.1 Net filter (site & content blocking)

2007-05-21 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2134577,00.asp

IRONPORT REVAMPS SECURITY MONITORING SITE.

IronPort Systems has revised its Internet traffic monitoring Website, a resource for IT staffers searching for a real-time view into security threats. This Website provides e-mail administrators visibility into the e-mail and Web traffic coming into their networks and features a new graphical user interface company officials hope will make it easier than ever for every member of the Internet community to track spam trends, virus outbreaks, spyware and other Web-based threats. A free service, SenderBase.org can be used like a credit reporting service, providing comprehensive data that ISPs and companies can use to tell the difference between legitimate senders and attackers, IronPort officials said. Consumers, media and other parties can also use SenderBase to monitor threat activity and check their e-mail reputation scores, officials added.
SenderBase Website: http://www.senderbase.org/

34.2 Usage monitoring, audit trails (employees, children)

Category 34.2 Usage monitoring, audit trails (employees, children)

2006-09-22 DHS Daily OSIR; ZDNet News (UK) http://news.zdnet.com/2100-9588_22-6118547.html

ACTIVISTS UNVEIL STEALTH BROWSER.

Hacktivismo, a group of human-rights advocates and computer security experts, has released a Firefox-based browser designed to allow anonymous Web surfing. The Web browser, called "Torpark," is a modified version of Portable Firefox. It can be run directly from a USB drive, meaning it can be used on public terminals in cybercafes. It creates an encrypted connection to the Onion Router network, which supplies a succession of different IP addresses. "Torpark causes the IP address seen by the Website to change every few minutes, to frustrate eavesdropping and mask the requesting source," Hacktivismo said in a statement. Developers said the browser is different from other anonymous browsers, such as Anonymizer or SecretSurfer, in that it doesn't cost anything and is small and portable.

34.3 Web-site flagging

Category 34.3 Web-site flagging

2006-08-04 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/06/08/04/HNgoogleflags_1.html

NEW GOOGLE FEATURE FLAGS DANGEROUS SITES.

Google has begun alerting users whenever they click on a search result that may take them to a dangerous Website. The new feature, which had been spotted earlier last week, went live officially Friday, August 4, according to an announcement from The Stop Badware Coalition, which is collaborating with Google on this effort. When users attempt to click over to a Website considered to be potentially dangerous, Google shows users an alert page that informs them of the possible risk and gives them the option to click back to the results page or continue on to the questionable Website.

Category 34.3 Web-site flagging

2007-01-11 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/07/01/11/HNgooglemalwarealertsirk_1.html

GOOGLE IRKS WEBSITE OWNERS OVER MALWARE ALERTS.

Some Website operators are complaining that Google is flagging their sites as containing malicious software when they believe their sites are harmless. At issue is an "interstitial" page that appears after a user has clicked on a link within Google's search engine results. If Google believes a site contains malware, the page will appear, saying "Warning - visiting this Website may harm your computer!" Google does not block access to the site, but a user would have to manually type in the Website address to continue. Organizations are complaining their sites do not contain malicious software, and the warning is embarrassing. Google's warning page contains a link to Stopbadware.org, a project designed to study legal and technical issues concerning spyware, adware, and other malicious software. Organizations should work with their Web hosting provider to check for security problems, Stopbadware.org said.

35.1 Cybersquatting & DNS hijacking

Category 35.1 Cybersquatting & DNS hijacking

2006-02-08 DHS Daily OSIR; http://www.eweek.com/article2/0,1895,1923546,00.asp

EFFECTS OF DOMAIN HIJACKING CAN LINGER.

Malicious hackers who are able to hijack an organization's Web domain may be able to steal traffic from the legitimate Website long after the domain has been restored to its owner, according to a recent report. Design flaws in the way Web browsers and proxy servers store data about Websites allow malicious hackers to continue directing Web surfers to malicious Webpages for days or even months after the initial domain hijacking. The persistent attack could lead to information or identity theft, according to Amit Klein, a Web application security researcher with the Web Application Security Consortium. The problem, which Klein termed "domain contamination" exists because of features in Web proxy servers, which store versions of Webpages, and Web "clients," or browsers, including Microsoft's Internet Explorer, the Mozilla Foundation's Firefox and the Opera browser. Proxy servers and browsers both establish trust relationships with Web servers that are identified as the authoritative host for a Webpage in the DNS (domain name system), Klein said. "Once a client believes it is communicating with the legitimate server for some domain, there's an implicit trust that's placed in that server that is not revoked," said Klein. Report: Domain Contamination: http://www.webappsec.org/projects/articles/020606.shtml

---

Category 35.1 Cybersquatting & DNS hijacking

2007-01-23 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/07/01/23/HNgooglegermany_1.html

GOOGLE.DE DOMAIN GETS KIDNAPPED.

Visitors to the German Website of Google were met with a strange sight early Tuesday morning, January 23: Gone was the Google logo, replaced by the name of a local Internet service provider with the message that no content was available for the domain. The Internet address of google.de and the page name were transferred to the new ISP, Goneo Internet GmbH, in a domain name grab that has confused Google users and infuriated company officials. Not all of Google's German Websites were affected by the domain grab, and those that were got restored within approximately two hours. In Google's case, two key security measures to prevent domain hijacking failed, a situation that could lead to changes in German domain name regulations, according to German domain registry Denic eG.

Category 35.1 Cybersquatting & DNS hijacking

2007-02-06 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/07/02/06/HNrootserverattack_1.html

HACKERS SLOW INTERNET ROOT SERVERS WITH ATTACK.

Online attackers have briefly disrupted service on at least two of the 13 "root" servers that are used to direct traffic on the Internet. The attack, which began Tuesday, February 6, at about 5:30 a.m. EST, was the most significant attack against the root servers since an October 2002 DDoS attack, said Ben Petro, senior vice president of services with Internet service provider Neustar. Root servers manage the Internet's DNS, used to translate Web addresses such as Amazon.com into the numerical IP addresses used by machines. The attack appeared to have been launched by a botnet, Petro said. "Two of the root servers suffered badly, although they did not completely crash; some of the others also saw heavy traffic," said John Crain, chief technical officer with the Internet Corporation for Assigned Names and Numbers (ICANN). The two hardest-hit servers are maintained by the Department of Defense and ICANN. The botnet briefly overwhelmed these servers with useless requests, but did not disrupt Internet service, Petro said. By 10:30 a.m. EST, Internet service providers were able to filter enough of the traffic from the botnet machines that traffic to and from the root servers was essentially back to normal.

35.3 Politics & management of the DNS

Category 35.3 Politics & management of the DNS

2006-03-01 DHS Daily OSIR; http://news.zdnet.com/2100-9588_22-6044629.html

CHINA CREATES OWN INTERNET DOMAINS.

China has created three of its own top-level domains that will use the domain names .cn, .com and .net, in Chinese. The domain names were launched Wednesday, March 1, by the Chinese Ministry of Information Industry. The creation of Chinese character domain names has led to speculation that China could break away from the Internet Corporation for Assigned Names and Numbers completely, and undermine the global unity of the Domain Name System, the network of servers that resolves domain name requests. Internet experts are concerned that this move will see China administrating its top-level domains with its own separate root servers, which could cause a split in the Internet.

Category 35.3 Politics & management of the DNS

2006-03-28 DHS Daily OSIR; http://www.computerworld.com/developmenttopics/websitemgmt/story/0,10801,109972,00.html

TWO DNS SERVERS HIT BY DENIAL-OF-SERVICE ATTACKS.

In the second attack of its kind in the past few days, Domain Name System servers at Network Solutions Inc. were hit by a denial-of-service attack Tuesday afternoon, March 28, resulting in a brief performance degradation for customers, according to the company. The attacks, which started at around 2:20 p.m. EST, were targeted at the company's WorldNIC name servers and resulted in a service degradation for about 25 minutes before the server was restored to normal, a spokesperson for the company said. Over the weekend, Joker.com, a domain-name registrar in Germany, was hit with a similar distributed denial-of-service attack that disrupted service to customers.

Category 35.3 Politics & management of the DNS

2006-04-11 DHS Daily OSIR; http://www.infoworld.com/article/06/04/11/77325_HNregistryhijacked_1.html

EUROPE'S DOMAIN REGISTRY HIJACKED.

The registry for the new .eu domain has grown to 1.4 million Web addresses since Friday morning, April 7 -- but one registrar has accused the group that runs it of inept organization, allowing companies to cheat the system by setting up bogus registrars to work on their behalf. Eurid vzw, which runs the registry, required registrars to apply for accreditation before the "landrush" phase of registrations began. Bob Parsons, chief executive officer of domain name registrar GoDaddy.com Inc., claims that some companies spotted a loophole in the system: by creating additional registrars and applying for accreditation for them, they were able to multiply their chances of successfully making registrations.

Category 35.3 Politics & management of the DNS

2006-04-11 DHS Daily OSIR; http://www.lurhq.com/cachepoisoning.html

REPORT: DNS CACHE POISONING -- THE NEXT GENERATION.

The old problem of DNS cache poisoning has again reared its ugly head. While some would argue that the domain name system protocol is inherently vulnerable to this style of attack due to the weakness of 16-bit transaction IDs, the immediate threat cannot be ignored while waiting for something better to come along. There are new attacks, which make DNS cache poisoning trivial to execute against a large number of name servers running today. The LURHQ Threat Intelligence Group has released the report, "DNS Cache Poisoning -- The Next Generation," in order to shed light on these new attacks and recommend ways to defend against them. Refer to the source for the full report.

Category 35.3 Politics & management of the DNS

2006-05-22 EDUPAGE; BBC http://news.bbc.co.uk/2/hi/technology/5003852.stm

BACKER OF ADULT DOMAIN QUESTIONS U.S. ROLE

The Internet registrar that had pushed for a domain for adult content has asked the Internet Corporation for Assigned Names and Numbers (ICANN) to reconsider its decision to turn down the domain, saying that the group was misled by U.S. Officials. ICM Registry has filed Freedom of Information Act requests with the U.S. State Department and the U.S. Commerce Department, seeking documents that it believes will "shed light on what role the United States government played" in ICANN's decision. Specifically, ICM believes that U.S. Government officials were pressured by religious conservatives to lobby against the domain. Supporters of the .xxx domain said it would offer parents an easy way to prevent kids' accessing inappropriate content. Opponents of the domain pointed out that inclusion would have been voluntary and said it would offer another tool for those who want to censor the Internet.

Category 35.3 Politics & management of the DNS

2006-05-24 INNOVATION (Newsweek 15-22 May 2006) < http://www.msnbc.msn.com/id/12666393/site/newsweek/>

NATIONALISM AND ONLINE DATA INTEGRITY

Newsweek's international edition reports that much of the world, especially developing countries, is angry that the U.S. still holds so much sway over the Internet, the planet's most crucial technological resource. Fanning the rage, ICANN, which alone has the power to approve top-level domain names like .com and .net, has been slow to create local language domains. That makes it tougher for people who speak languages not based on the Roman alphabet to use the Net. This issue was front and center at last year's World Summit on the Information Society in Tunis, where some developing countries actively protested Western hegemony. Some countries, like Iran and the Arab nations, worry that Washington might someday simply turn off their national domain names for political reasons, cutting them off the Web entirely. Iran has even threatened to create its own alternative version of the Internet, similar to those run by anti-American tech activists in Europe. It's easy to do: you simply copy the information on the 13 key servers around the world that form the root of all Web traffic. One German group, the Open Root Server Network, has already done so. China, with the help of Google, censors the Web for its citizens. All these developments raise serious questions about the future integrity of information -- or misinformation -- found online.

Category 35.3 Politics & management of the DNS

2006-07-27 DHS Daily OSIR; Register (UK) http://www.theregister.co.uk/2006/07/27/ntia_icann_meeting/

UNITED STATES CEDES CONTROL OF THE INTERNET.

In a meeting that will go down in Internet history, the United States government Wednesday night, July 26, conceded that it can no longer expect to maintain its position as the ultimate authority over the Internet. Having been the Internet's instigator and, since 1998, its voluntary taskmaster, the U.S. government finally agreed to transition its control over not-for-profit Internet overseeing organization Internet Corporation for Assigned Names and Numbers, making the organization a more international body. However, assistant commerce secretary John Kneuer, the U.S. official in charge of such matters, also made clear that the U.S. was still determined to keep control of the net's root zone file -- at least in the medium-term.

Category 35.3 Politics & management of the DNS

2006-08-16 DHS Daily OSIR; BBC News (UK) http://news.bbc.co.uk/1/hi/technology/4799137.stm

INTERNET'S RULING BODY RENEWS U.S. LINKS.

The U.S. looks set to maintain its role as ultimate supervisor of the Internet's addressing systems until 2011. The U.S. Department of Commerce has signed a five-year deal with administrative body Internet Corporation for Assigned Names and Numbers that renews the body's role overseeing Internet domains.

Category 35.3 Politics & management of the DNS

2006-08-17 EDUPAGE; Internet News http://www.internetnews.com/infra/article.php/3627026

US DEPARTMENT OF COMMERCE RENEWS ICANN CONTRACT

The U.S. Department of Commerce renewed its contract with the Internet Corporation for Assigned Names and Numbers (ICANN), leaving the management of the technical details of the Internet with the nonprofit group. ICANN will continue its responsibility for Internet Assigned Numbers Authority (IANA), which includes allocating IP addresses, assigning protocol identifiers, and managing top-level domain names and root servers. The contract involves five one-year options.

U.S. RENEWS AGREEMENT WITH ICANN

The U.S. Department of Commerce said it would renew its Memorandum of Understanding (MOU) with the Internet Corporation for Assigned Names and Numbers (ICANN) for oversight of the naming system for the Internet. The current MOU will expire at the end of September, and international groups have called for responsibility of Internet names to be transferred to an organization such as the United Nations. Some within the U.S. government have criticized ICANN and pushed for changes. Rep. John Dingell (D- Mich.) said, "ICANN remains far from a model of effective and sustainable self-governance." Though details were not released, a new MOU is expected to be in force for between one and three years. Rep. Fred Upton (R-Mich.) was critical of the Commerce Department's vagueness about a renewed MOU. Nevertheless, Upton commented, "Allowing ICANN to continue to develop under the watchful eye of the Department of Commerce is not only the right thing to do, but the most prudent action, as well."

[Internet News, 22 September 2006 http://www.internetnews.com/bus-news/article.php/3633701]

Category 35.3 Politics & management of the DNS

2006-10-01 DHS Daily OSIR;
Reuters http://www.eweek.com/article2/0,1895,2022848,00.asp

GOVERNMENT KEEPS CONTROL OF WEB DOMAIN GROUP ICANN.

The U.S. Commerce Department said on Friday, September 29, it would retain oversight for three more years of the company that manages Internet domain names, renewing an agreement that was scheduled to expire last weekend. The government said it signed a new agreement with the Internet Corporation for Assigned Names and Numbers (ICANN), which controls addresses such as ".com" and country domain names such as ".cn" for China. The U.S. government has previously said it plans to eventually turn over complete control of ICANN, a nonprofit group, to the private sector. The new agreement calls for a review in 2008 of ICANN's progress toward becoming more accountable, the Commerce Department said. Joint agreement: http://www.ntia.doc.gov/ntiahome/domainname/agreements/jpa/s ignedmou290906.pdf

Category 35.3 Politics & management of the DNS

2006-11-01 DHS Daily OSIR; Associated Press
http://news.yahoo.com/s/ap/20061101/ap_on_hi_te/greece_un_internet_governance

ICANN: MULTI-LINGUAL SYSTEM COULD PERMANENTLY BREAK THE INTERNET.

The body that oversees global Internet functions warned Wednesday, November 1, that a mistake in a creating multi-lingual address system could "permanently break the Internet." The Internet Corporation for Assigned Names and Numbers (ICANN) made the warning at a United Nations-organized conference on the future of the Internet being held in Greece. More multi-lingual Internet is a key issue at the forum, with future Web growth predicted in developing countries where the Latin alphabet is often unfamiliar. "ICANN expects that these final tests and discussions will reach a resolution by the end of 2007," CEO Paul Towney said in a statement. "But this is no simple task. If we get this wrong we could very easily and permanently break the Internet." Experts at the forum have also warned that mixed use of alphabets in Internet addresses could allow cybercriminals a greater opportunity to post imitation Websites typically created for illegally collecting personal banking details. The four-day Internet Governance Forum ends Thursday, November 2.

Category 35.3 Politics & management of the DNS

2006-12-04 EDUPAGE; BBC http://news.bbc.co.uk/2/hi/technology/6199394.stm

VERISIGN KEEPS CONTROL OF .COM UNTIL 2012

The U.S. government has approved a deal under which VeriSign, which has operated the .com domain since 1999, will retain control of the domain until 2012. The proposal, drafted by VeriSign and the Internet Corporation for Assigned Names and Numbers (ICANN), was presented to the U.S. Department of Commerce in March of this year. Since that time, the National Telecommunications and Information Administration (NTIA), an agency of the Department of Commerce, has been reviewing the proposal and comments on it. Specifically, many international organizations complained that control of the world's most popular Internet domain should not lie with a U.S. company. Other criticisms included the length of the contract, which some said was too long. In the end, the agencies involved approved the contract, which includes limits on price increases.

Category 35.3 Politics & management of the DNS

2007-05-21 DHS Daily OSIR; Information Week
http://www.informationweek.com/news/showArticle.jhtml?ArticleID=199700668

THE IMPENDING INTERNET ADDRESS SHORTAGE.

The coming shortage of Internet Protocol addresses on Monday, May 21, prompted the American Registry for Internet Numbers to call for a faster migration to the new Internet Protocol, IPv6. The current version of the Internet Protocol, IPv4, allows for over 4 billion Internet addresses. Only 19 percent of the IPv4 address space remains. Somewhere around 2012-2013, the last Internet address bloc will be assigned and the Internet will be full, in a manner of speaking. IPv6 promises some 16 billion-billion possible addresses.

37.2 High school programs & courses

Category 37.2 High school programs & courses

2006-03-11 EDUPAGE; http://www.wired.com/news/wireservice/0,70396-0.html

PROGRAM TEACHES HIGH SCHOOLERS ABOUT COMPUTER SECURITY

High school students at a Catholic school in Rome, New York, are the first to participate in a computer-security course developed by the school, the U.S. Air Force's Research Lab in Rome, and Syracuse University. The 20-week course, which covers topics including data protection, network protocols and vulnerabilities, firewalls, data hiding, and wireless security, is based on a 10-week course developed at the Research Lab. Kamal Jabbour, principal computer engineer at the lab, said the new course was designed in part to encourage students to pursue college degrees and careers in computer security. Eric Spina, dean of Syracuse's engineering and computer science programs, said the program is considerably different from the kind of computer course available in many high schools today. This course, he said, exposes high school students to material not seen by many college students until their junior year. "A high school student with this kind of background," said Spina, "would be an asset anywhere they went." Starting next year, the course will be available statewide and could be offered nationally by 2008.

37.3 Undergraduate programs & courses

Category 37.3 Undergraduate programs & courses

2006-04-18 DHS Daily OSIR; http://www.news.navy.mil/search/display.asp?story_id=23208

NATIONAL SECURITY AGENCY SPONSORS CYBER DEFENSE EXERCISE

The U.S. Naval Academy joined forces with fellow service academies in the sixth annual Cyber Defense Exercise (CDX) held Monday-Friday, April 10-14, at the Academy in Annapolis, MD. Sponsored by the National Security Agency, CDX brings Midshipmen and their peers together to create a computer network they must then defend against attack from hackers. The service academy that best defends its portion of the network from attack wins the competition. Results will be announced between late April and early May. The hackers in the exercise tested the security of the network, observed how long it took the students to become aware of the attacks, and assessed how they responded.

Category 37.3 Undergraduate programs & courses

2006-06-05 DHS Daily OSIR; USA Today http://www.usatoday.com/tech/news/techinnovations/2006-06-05-digital-forensics_x.htm

CYBERCRIME SPURS COLLEGE COURSES IN DIGITAL FORENSICS.

One of the hottest new courses on U.S. college campuses is a direct result of cybercrime. Classes in digital forensics -- the collection, examination and presentation of digitally stored evidence in criminal and civil investigations -- are cropping up as fast as the hackers and viruses that spawn them. About 100 colleges and universities offer undergraduate and graduate courses in digital forensics, with a few offering majors. Students learn where to find digital evidence and handle it without contaminating it. Once preserved, students are shown how to examine evidence and present it clearly during court testimony.

Category 37.3 Undergraduate programs & courses

2006-06-19 EDUPAGE; The Register http://www.theregister.com/2006/06/19/hackers_background/

ETHICAL HACKING PROGRAM TO REQUIRE BACKGROUND CHECK

Students who want to take part in an ethical hacking program at the University of Abertay in Scotland will be required to pass a background check to weed out those who might apply the skills learned in the program to malicious ends. University officials will work with the Home Office and a Scottish disclosure service to screen applicants, looking for anyone with a criminal background. The program, called Ethical Hacking and Countermeasures, is a four-year degree intended to teach hacking skills to students who will then work with businesses to prevent hackers from doing damage to computer systems and data. It is the first program of its kind in the United Kingdom. Responding to concerns that the program will simply create more hackers, Lachlan McKinnon, a professor in the program, said the university will do all it can to ensure students use their skills in a positive manner. He added, however, that there are no guarantees. "Harold Shipman qualified as a doctor, after all," he said, "before deciding to become a murderer."

Category 37.3 Undergraduate programs & courses

2006-06-27 DHS Daily OSIR; Boston Globe http://www.boston.com/business/technology/articles/2006/06/27/colleges_craft_studies_to_fit_defense_firms/

COLLEGES CRAFT STUDIES TO FIT DEFENSE FIRMS.

Prodded by state government officials fearful of alienating a key Massachusetts industry, nine Bay State colleges and universities have agreed to adapt their engineering curriculums, and in some cases introduce new courses, to meet the needs of defense contractors. The new focus will be on skills that have become increasingly important to the state's makers of high-tech weapons systems but are in short supply in the job market: radio frequency engineering, systems engineering and integration, defense contract management, and specialized design for products used in combat. These were fields identified by military suppliers who have met in the past year with Ranch C. Kimball, the Massachusetts secretary of economic development, and with representatives of the Massachusetts Defense Technology Initiative, a group formed to capitalize on the momentum of the business and government coalition that successfully lobbied last year to save a pair of military research sites in the state. Under a program called Massachusetts Business Connect, launched last February, the state officials met with more than 50 defense contractors and conducted in-depth "needs assessments." The program will be extended to biotechnology and other business sectors.

37.4 Master's programs

Category 37.4 Master's programs

2006-04-17 DHS Daily OSIR; http://www.gcn.com/online/vol1_no1/40428-1.html

UNIVERSITY OF PENNSYLVANIA STUDENTS RESEARCH WIRETAP VULNERABILITIES.

A team of graduate students from the University of Pennsylvania working with a National Science Foundation grant set out to determine just how trustworthy the most common types of telephone wiretaps used by police and intelligence agencies are, said Professor Matt Blaze. The results of these taps are accepted uncritically by courts, Blaze said at the 2006 International Conference on Network Security being held in Reston, VA. “It turns out, it can fail in all sorts of unexpected ways,” he said. The techniques exploit vulnerabilities in the single signaling and audio channel used in analog telephone systems. Blaze said the project was an attempt to establish some baselines for network security by assessing how easy it is to conduct reliable eavesdropping on the century-old protocols used in analog voice phone systems.

37.8 Web sites, online courses

Category 37.8 Web sites, online courses

2006-01-25 DHS Daily OSIR; http://www.usatoday.com/tech/news/computersecurity/2006-01-2 5-spyware_x.htm

FREE WEBSITE TO LIST PROGRAMS WITH SPYWARE.

A free Website, StopBadware.org, launched Wednesday, January 25, plans to provide a list of programs that contain spyware and other malicious software. It will also identify companies that develop the programs and distribute them on the Internet. Consumers can then decide if a program is safe to download. "For too long, these companies have been able to hide in the shadows of the Internet," says John Palfrey, who heads the Berkman Center of Internet & Society at Harvard Law School and is spearheading the project. "What we're after is a more accountable Internet." The initiative is being run by Harvard and the Oxford Institute and is backed by high-tech heavyweights including Google and Sun Microsystems. Consumer Reports' WebWatch is serving as a special adviser. In addition to spyware, the hit list of the StopBadware coalition includes malicious "adware" programs that serve up onslaughts of pop-up ads or software that contains hidden viruses and worms. By checking StopBadware.org, its organizers say, consumers can choose, in the first place, not to download a program containing the malicious software. The coalition is encouraging consumers to visit the Website to log their experiences with harmful programs. StopBadwar.org Website: http://www.stopbadware.org/

Category 37.8 Web sites, online courses

2006-01-25 EDUPAGE; http://www.nytimes.com/2006/01/25/technology/25spy.html

NEW SITE AIMS TO IDENTIFY MAKERS OF MALICIOUS PROGRAMS

Researchers at Harvard Law School and Oxford University are launching a Web site that will identify organizations that distribute spyware, adware, and other unwanted computer programs, as well as the tactics they employ to intall their applications. StopBadware.org was financed initially by companies including Google, Lenovo, and Sun Microsystems. The site will also include an area where consumers can submit testimonials about their experiences with different software they have downloaded. John G. Palfrey Jr., executive director of the Berkman Center for Internet and Society at Harvard, said, "We want to turn the spotlight on the bad actors, but also give ordinary users a place to go and get an early warning before they download something that might harm their computer." According to the Pew Internet & American Life Project, 59 million U.S. adults said their computers were infected with spyware last year. Data from Consumer Reports indicate that despite consumer spending of $2.6 billion over the past two years on antivirus and antispyware tools, users still spent $3.5 billion in damages over the same period due to unwanted software.

Category 37.8 Web sites, online courses

2006-01-29 RISKS

SITE LISTS SPREADSHEET ERRORS

Gene Wirchenko reported on a site that lists signficant errors in spreadsheets:
< http://www.eusprig.org/stories.htm >. The site is managed by the European Spreadsheet Risks Interest Group (EuSpRIG); their description reads, "These stories illustrate common problems that occur with the uncontrolled use of spreadsheets. We say how we think the problem might have been avoided. An obvious form of risk avoidance is simply to check your work before sending it out. For important spreadsheets, a second pair of eyes ('peer review') is even better. Where stakes are high, a thorough test and audit is a further defence." The group runs an annual conference that concentrates on quality assurance for spreadsheets.

Category 37.8 Web sites, online courses

2006-02-28 DHS Daily OSIR; http://news.com.com/Symantec+keeps+weather+eye+out+for+Net+threats/2100-7349_3-6043873.html?tag=cd.top

SYMANTEC LAUNCHES FREE THREAT METER.

Symantec on Tuesday, February 28, launched the Symantec Internet Threat Meter, a free service meant to inform consumers about the state of Internet security. "There are other threat indicators on the Web," Dave Cole, a director at Symantec Security Response, said. "But what was missing was a place for consumers that breaks it down in plain English and gives actionable advice." Available on the Symantec Website, the new threat meter will provide information on the current risk level associated with specific online activities: e-mail, Web surfing, instant messaging and file-sharing. Symantec Internet Threat Meter: http://www.symantec.com/avcenter/home_homeoffice/index.html

Category 37.8 Web sites, online courses

2006-03-01 DHS Daily OSIR; http://www.f-secure.com/news/items/news_2006030101.shtml

NEW F-SECURE WORLD VIRUS MAP OFFERS CURRENT GLOBAL PERSPECTIVE AT A GLANCE.

F-Secure has launched a comprehensive online tool for those interested in understanding the world virus situation at a glance. The resource, which was developed for research purposes at F-Secure is now available to the general public in four languages, respectively English, French, German and Finnish. F-Secure World Map: http://worldmap.f-secure.com/vwweb_1_2/en/previous_day

Category 37.8 Web sites, online courses

2006-03-15 DHS Daily OSIR; http://www.techweb.com/wire/security/181504133

QUIZ REVEALS SPYWARE CHICANERY.

Security vendor SiteAdvisor unveiled an online quiz Wednesday, March 15, that tests consumers' ability to spot sites hosting spyware and adware. Dubbed "Spyware Quiz" by SiteAdvisor, the 12-URL test covers five categories of sites notorious for distributing adware and spyware, including those dedicated to screensavers, smileys (emoticons), games, musical lyrics, and file sharing. SiteAdvisor's spyware quiz: http://www.siteadvisor.com/quizzes/spyware_0306.html

Category 37.8 Web sites, online courses

2006-03-27 DHS Daily OSIR; http://news.zdnet.co.uk/software/applications/0,39020384,39259531,00.htm

MICROSOFT CREATES PUBLIC BUG DATABASE FOR INTERNET EXPLORER.

Microsoft is for the first time encouraging people to give public feedback on Internet Explorer (IE), with the creation of a bug database for the next version of its browser, IE 7 beta. The bug database is accessible from the Microsoft Connect site and can be accessed by anyone that has a Microsoft Passport account.

Category 37.8 Web sites, online courses

2006-07-17 DHS Daily OSIR; Department of Homeland Security
http://www.dhs.gov/dhspublic/display?content=5744

DEPARTMENT OF HOMELAND SECURITY LAUNCHES UPDATED EMERGENCY PREPAREDNESS WEBSITE.

The tornados, flooding and wildfires recently experienced in parts of the country are another reminder of how critical it is for Americans to prepare for emergencies. The Department of Homeland Security's Ready Campaign Monday, July 17, launched an updated version of its Website, www.ready.gov, to educate Americans about the simple steps they should take to be ready for a variety of emergencies. For more information: http://www.ready.gov/

Category 37.8 Web sites, online courses

2007-05-09 Effector Online http://www.eff.org/deeplinks/archives/005238.php

VIRTUAL CLASSES ON CYBERLAW

Learn cyberlaw without leaving cyberspace through the State of Play Academy. The Academy offers free classes through the virtual world There.com. The Spring Semester has already started and runs through June 8. The virtual classes will teach you the sort of fascinating stuff your real college never gets around to offering, like "Claims of Copyright Misuse based on First Amendment Interests," "The Viacom-Youtube Lawsuit," and "Election 2008 and the Remix Culture." EFF staff attorney Kevin Bankston is signed up to teach a class called "Every Move You Make: Location Tracking and the Law." More information, including how to log on and participate in SOPA classes, at: http://www.stateofplayacademy.com
For this post: http://www.eff.org/deeplinks/archives/005238.php

Category 37.8 Web sites, online courses

2007-05-10 DHS Daily OSIR; Government Technology
http://www.govtech.net/magazine/channel_story.php/105412

NEW WEBSITE FOR HAZARDOUS MATERIALS RESPONDERS.

Created by the National Oceanic and Atmospheric Administration (NOAA) Office of Response and Restoration, CAMEO Chemicals, is the latest component of NOAA's popular CAMEO (Computer-Aided Management of Emergency Operations) software suite, and the first to be available for use online. Over the past two decades, the CAMEO suite has brought first responders from an era in which they gleaned emergency response information from maps and reference books spread out on the hoods of their trucks to a time when up-to-date, comprehensive information on chemical plumes, toxicity risks and susceptibility of chemical mixtures to burn or explode can be displayed with a few strokes on a computer keyboard.

37.9 White papers & reports

Category 37.9 White papers & reports

2006-06-14 DHS Daily OSIR; The Infrastructure Security Partnership
http://www.tisp.org/news/newsdetails.cfm?&newsID=944

TISP RELEASES REGIONAL DISASTER RESILIENCE GUIDE.

The Infrastructure Security Partnership (TISP) has developed a much needed resource, Regional Disaster Resilience: A Guide for Developing an Action Plan. The Guide was developed by the TISP Regional Disaster Resilience Committee, comprised of more than 100 practitioners, policy makers, and technical and scientific experts from across the nation. The Guide provides a strategy to develop the necessary level of preparedness for communities to manage major disasters in today's complex and interdependent world.

The Guide is available at: http://www.tisp.org/rdr_guide

TISP Website: http://www.tisp.org/tisp.cfm

Category 37.9 White papers & reports

2006-06-16 DHS Daily OSIR; Department of Homeland Security
http://www.dhs.gov/dhspublic/display?content=5695

DHS RELEASES REVIEW OF NATIONWIDE CATASTROPHIC EVENT PREPAREDNESS.

The Department of Homeland Security (DHS) issued findings Friday, June 16, from a national assessment of the country's catastrophic planning capabilities. Responding to directives from President Bush and the Congress, following Hurricane Katrina, the Nationwide Plan Review looked at whether existing emergency operations plans for states and urban areas are sufficient for managing a catastrophic event. The Review also presents conclusions on actions needed by the federal government to improve and coordinate planning. Conducted in all 56 States and territories and 75 urban areas over six months, the Nationwide Plan Review was the most comprehensive assessment of emergency operations plans to date relative to planning for a catastrophic event. Reviewers examined nearly 2,800 emergency operations plans and related documents with participation from more than 1,000 emergency managers and homeland security officials. The National Plan Review findings demonstrate the need for all levels of government across the country to improve emergency operations plans for catastrophic events such as a major terrorist attack or category-five hurricane strike. After completing the assessments and findings, the reviewers also provided more detailed follow-up briefings to individual States and urban areas.

Fact Sheet - Nationwide Plan Review: http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0928.xml

Fact Sheet - Nationwide Plan Review Initial Conclusions:
http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0929.xml

Nationwide Plan Review (PDF): http://www.dhs.gov/interweb/assetlibrary/Prep_NationwidePlan Review.pdf

Category 37.9 White papers & reports

2006-08-15 DHS Daily OSIR; Federal Financial Institutions Examination Council
http://www.ffiec.gov/press/pr081506.htm

FFIEC RELEASES FREQUENTLY ASKED QUESTIONS ON GUIDANCE REGARDING INTERNET BANKING AUTHENTICATION.

The Federal Financial Institutions Examination Council (FFIEC) on Thursday, August 17, released a frequently asked questions document (FAQs) to aid in the implementation of the interagency guidance on Authentication in an Internet Banking Environment issued October 12, 2005. The authentication guidance, which applies to both retail and commercial customers, addresses the need for risk-based assessment, customer awareness, and security measures to reliably authenticate customers remotely accessing their financial institutions' Internet-based financial services. The FAQs are designed to assist financial institutions and their technology service providers in conforming to the guidance by providing information on the scope of the guidance, the timeframe for compliance, risk assessments, and other issues. FFIEC FAQs:
http://www.ffiec.gov/pdf/authentication_faq.pdf

Category 37.9 White papers & reports

2006-08-30 DHS Daily OSIR; North American Electric Reliability Council http://www.nerc.com/

NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL RELEASES DASHBOARD OF RELIABILITY INFORMATION.

The North American Electric Reliability Council's newly released Dashboard of Reliability Information includes several sections that cover standards and compliance; a disturbances map that provides users with basic information regarding all reported North American energy incidents and disturbances for the current year; performance and operations information; and an alert/watch list that displays significant and immediate concerns wihin the electric power industry.

Dashboard: http://www.nerc.net/dashboard/

Category 37.9 White papers & reports

2006-09-01 DHS Daily OSIR; Department of Homeland Security http://www.dhs.gov/interweb/assetlibrary/OIG_06-62_Sep06.pdf

DHS OIG RELEASES REPORT ON ITS INFORMATION SECURITY PROGRAM.

The Department of Homeland Security (DHS) Office of
Inspector General (OIG) has released a report entitled, "Evaluation of DHS' Information Security Program for Fiscal Year 2006." This report assesses the strengths and weaknesses with employees and officials of DHS, direct observations, and a review of applicable documents.

Category 37.9 White papers & reports

2007-02-16 DHS Daily OSIR; Government Computer News http://www.gcn.com/online/vol1no1/43141-1.html

NIST RELEASES INFO SECURITY DOCUMENTS.

The National Institute of Standards and Technology (NIST) has published two new interagency reports designed to help auditors, inspectors general and senior management understand and evaluate information security programs. NISTIR 7359, titled “Information Security Guide for Government Executives,” is an overview of IT security concepts that senior management should grasp. NISTIR 7358, titled “Program Review for Information Security Management Assistance (PRISMA),” lays out a standardized approach for measuring the maturity of an information security program. PRISMA is a methodology developed by NIST for reviewing complex requirements and posture of a federal information security program. It is intended for use by security personnel, as well as internal reviewers, auditors and IGs. Tools laid out in NISTIR 7358 should help identify program deficiencies, establish baselines, validate corrections and provide supporting information for Federal Information Security Management Act scorecards.
NISTIR 7359: http://csrc.nist.gov/publications/nistir/ir7359/NISTIR-7359.pdf
NISTIR 7358: http://csrc.nist.gov/publications/nistir/ir7358/NISTIR-7358.pdf

Category 37.9 White papers & reports

2007-04-06 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2112120,00.asp

NAC ATTACK: TODAY'S PRODUCTS WILL FAIL, REPORT SAYS.

Forrester Research analysts are urging corporations to prepare for a shift in the Network Access Control (NAC) market in the years to come, as NAC vendors move toward new software-based tools that leverage endpoint technology to proactively manage risk. In a report titled "Client Management 2.0," Forrester analysts Natalie Lambert and Robert Whiteley forecast the death of modern NAC products, which they say feature too much complexity and not enough interoperability. Operations management teams want a unified solution, Lambert said. The report also contends that many NAC products focus solely on compliance with security policies instead of the remediation problematic machines, and are not able to defend against newly emerging threats. In addition, the researchers stated that existing NAC systems often result in multiple policies being established to control the same processes.

Category 37.9 *White papers & reports*

2007-04-18 INNOVATION (Guardian 9 Apr 2007)
<http://www.guardian.co.uk/science/story/0,,2053020,00.html>

A GRIM VISION OF TOMORROW

The technology that has made our lives easier could make the future a grim, even terrifying, place. A UK Ministry of Defense team recently painted a picture of the "future strategic context" likely to face Britain's armed forces. The 90-page report includes an analysis of tomorrow's key risks and shocks, including an implantable "information chip" that could be wired directly to the brain. Instantaneous information communications technology like that could let states, terrorists or criminals mobilize instant "flashmobs" to challenge, even overpower, security forces in a small area. By 2035, the report predicts, an electromagnetic pulse will probably become operational, able to destroy all communications systems in a selected area, or to be used against a "world city" such as an international business service hub. By 2035 more than 60% of the world's population will be living in urban rather than rural environments, leading to social deprivation, the growth of shanty towns and new instability risks. "The middle classes could become a revolutionary class," warns the report, "taking the role envisaged for the proletariat by Karl Marx." This thesis is based on the growing gap between the middle classes and the super-rich on one hand and an urban under-class threatening social order. "The world's middle classes might unite, using access to knowledge, resources and skills to shape transnational processes in their own class interest." In other words, a revival of Marxism because of global inequality.

Category 37.9 *White papers & reports*

2007-05-30 DHS Daily OSIR; Government Computer News
http://www.gcn.com/online/vol1_no1/44383-1.html

NIST READIES GUIDANCE ON IT SECURITY ASSESSMENTS.

The National Institute of Standards and Technology (NIST) has finished the third and possibly final draft of its revised guidelines for assessing the adequacy of IT security. Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, will be released for comment June 4. Comments on the current version will be accepted by the Computer Security Division of NIST's IT Laboratory through July 31. Comments can be e-mailed to sec-cert@nist.gov. All of the FISMA-related security standards and guidelines can be found at http://csrc.nist.gov/sec-cert . Final publication of SP 800-53A is expected early next year. NIST will decide on whether additional public drafts are needed based on comments received on the present draft.

37.A Books

Category 37.A Books

2006-01-29 RISKS

GARY MCGRAW ON SOFTWARE SECURITY

Gary McGraw (2006). Software Security: Building Security In.
Addison-Wesley (ISBN 0-321-35670-5)

This book is a "hands-on, how-to guide for software security" for software security professionals. It completes a trilogy together with McGraw's Building Secure Software (Addison-Wesley, 2001) and Exploiting Software (Addison-Wesley, 2004), but it also stands alone as a useful book. It considers best practices for software security in detail, as a fundamental part of the development lifecycle. It is very much in the spirit of what RISKS has promulgated in the past 20.5 years.

[Review by Peter G. Neumann]

37.B Public education & awareness

Category 37.B Public education & awareness

2006-01-18 DHS Daily OSIR; http://www.gcn.com/vol1_no1/daily-updates/38026-1.html

DEPARTMENT OF HOMELAND SECURITY GRANT KIT OFFERS CYBERSECURITY GUIDANCE

The Department of Homeland Security's (DHS) new preparedness unit is urging state governors to prepare cybersecurity plans, adopt a new national XML-based model for information-sharing and implement newly developed common rules for geospatial content. The recommendations are some of the most detailed that the federal government has made to state and local governments on using IT in the fight against terrorism. The IT-related guidance is included in the fiscal 2006 grant application kit for the distribution of $3.9 billion in federal homeland security grants to states and localities this year, published by the preparedness directorate. Cybersecurity guidance was attached as an appendix for the first time. Guidelines for topics to be included in the cyberplans are somewhat open-ended. Recommendations cover about two-dozen questions related to policy, training, IT deployment and vulnerability. In addition, DHS is recommending that states, local and tribal government adopt geospatial data guidelines developed by the Information Content Subgroup of the Federal Geographic Data Committee Homeland Security Working Group in October 2005.

Category 37.B Public education & awareness

2006-05-23 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2156679/panda-launches-phishing

PANDA LAUNCHES PHISHING EDUCATION CAMPAIGN.

Security firm Panda Software launched a campaign this week designed to help surfers recognize and defend against phishing scams. Simple protection techniques listed in Panda's 10 Tips to Combat Phishing include typing URLs directly into the browser bar instead of accessing internet services through links. The April virus trends report from BlackSpider Technologies, another security vendor, found that the total number of virus-laden emails fell by 56 percent compared with March. Virus-infected emails now makes up just 0.79 percent of inbound emails. However, the Panda study found that the number of phishing emails in April rose by 35 percent compared with March, indicating that phishing attacks are becoming the more favored form of attack.

Category 37.B Public education & awareness

2006-05-31 DHS Daily OSIR; InfoWorld http://www.infoworld.com/article/06/05/31/78787HNeunetworksecurity_1.html

EUROPEAN UNION LAUNCHES NETWORK SECURITY CAMPAIGN.

Europe remains woefully unaware of the security risks to computer networks, the European Commission said Wednesday, May 31, as it unveiled a new awareness campaign called IT Security for Europe. The Commission wants to compare national policies on network and information security to improve the dialogue among public authorities across the European Union, to identify best practices and to raise the security awareness of end-users. ENISA, the European Network and Information Security Agency in Heraklion, Greece, will be entrusted to develop a data collection plan to handle security incidents and measure levels of consumer confidence from all over Europe.

Category 37.B Public education & awareness

2006-06-16 DHS Daily OSIR; Federal Emergency Management Agency http://www.fema.gov/news/newsrelease.fema?id=27079

IS YOUR BUSINESS READY FOR A DISASTER?

When disaster strikes, businesses can be affected too. According to disaster recovery officials, preparing for a disaster, and mitigating the damage a business most likely would suffer, is something every company should do. There are four critical parts to disaster preparation: making the company's physical location less vulnerable, ensuring that business data such as sales records, customer lists, tax information, etc. is backed up offsite, purchasing adequate insurance coverage, and formulating a contingency plan to continue operating even if the company's location is heavily damaged or destroyed.

FEMA Contingency Planning Materials: http://www.fema.gov/plan/index.shtm

Category 37.B Public education & awareness

2006-07-17 DHS Daily OSIR; National Journal's Technology Daily
http://www.govexec.com/story_page.cfm?articleid=34571

OMB PUBLISHES ONLINE CATALOG OF IT GUIDELINES.

Part of the challenge of implementing change is following the guidelines -- and knowing exactly what the changes are. To that end, the White House Office of Management and Budget (OMB) on Monday, July 17, announced the release of an online catalog to make guidelines on information technology practices easier to access. OMB is sending a memorandum to the chief information officers and chief architects of the different federal agencies to explain the launch of the federal transition framework, which consolidates guidance to agencies on policies and best practices on tech solutions. OMB's online catalog: http://www.whitehouse.gov/omb/egov/a-2-EAFTF.html

Category 37.B Public education & awareness

2006-07-18 Effector Online http://www.eff.org/IP/faq/

FREQUENTLY AWKWARD QUESTIONS FOR THE ENTERTAINMENT INDUSTRY.

The RIAA and MPAA trot out their spokespeople at conferences and public events all over the country, repeating their misleading talking points. Innovators are pirates, fair use is theft, the sky is falling, up is down, and so on. Their rhetoric shouldn't be given a free pass. To that end, EFF has prepared a sample list of tough questions for times when you hear entertainment industry representatives speaking and want to challenge their positions. Asking hard questions is a way of "keeping honest people honest" and revealing when they're actually being deceptive. Feel free to republish these and add your own questions, or send additions to us at editor@eff.org.
For the questions: http://www.eff.org/IP/faq/

Category 37.B Public education & awareness

2006-07-27 DHS Daily OSIR; Federal Financial Institutions Examination Council
http://www.ffiec.gov/press/pr072706.htm

FFIEC RELEASES UPDATED INFORMATION SECURITY BOOKLET.

The Federal Financial Institutions Examination Council (FFIEC) Thursday, July 27, issued revised guidance for examiners and financial institutions to use in identifying information security risks and evaluating the adequacy of controls and applicable risk management practices of financial institutions. The Information Security Booklet is one of twelve that, in total, comprise the FFIEC IT Examination Handbook. In addition to the revised Information Security Booklet, the agencies also released an Executive Summary that contains high level synopses of each of the twelve booklets and describes the handbook development and maintenance processes. The Information Security Booklet describes how an institution should protect and secure the systems and facilities that process and maintain information. The booklet calls for financial institutions and technology service providers (TSPs) to maintain effective security programs tailored to the complexity of their operations. Information Security Booklet and Executive Summary: http://www.ffiec.gov/guides.htm

Category 37.B Public education & awareness

2006-08-01 DHS Daily OSIR; Department of Homeland Security
http://www.dhs.gov/dhspublic/display?content=5773

DHS FACT SHEET: COMBATING FRAUDULENT DOCUMENTS.

The Department of Homeland Security (DHS) has been working closely with the Department of State to implement the Western Hemisphere Travel Initiative. This initiative will require travelers to present secure identity documentation when entering the United States. U.S. Customs and Border Protection (CBP) officers undergo security training to determine what genuine documents look like and how documents can be altered. CBP also trains officers to watch for imposters -- people who use genuine documents but are not the legitimate bearer of those documents. CBP Officers working primary inspection are taught to recognize possible fraudulent documents and to refer those questionable documents to secondary for further review and consultation. DHS is also harnessing 21st century technology and biometric information to increase the likelihood of apprehending criminal or terrorist elements attempting to enter the U.S. US-VISIT has processed more than 61 million people applying for admission at U.S. ports of entry. Nearly 1,200 criminals and immigration violators have been intercepted upon entry into the United States based on the biometric alone. US VISIT owes a great deal of its success to the power of biometrics. Biometrics identify the traveler, protect privacy, and make it virtually impossible to cross borders using fraudulent documents or to assume another's identity.

Category 37.B *Public education & awareness*

2006-08-11 DHS Daily OSIR; Department of Homeland Security
http://www.dhs.gov/dhspublic/display?content=5795

FACT SHEET: GUIDANCE FOR AIRLINE PASSENGERS. INCREASED AVIATION SCREENING PROCEDURES.

The Transportation Security Administration (TSA) is implementing a series of security measures, some visible and some not visible, to ensure the security of the traveling public and the nation's transportation system. Measures will be constantly evaluated and updated as circumstances warrant. Related Information Threat Level Change for the Aviation Sector: http://www.tsa.gov/press/happenings/threat-change.shtm
Frequently Asked Questions: New Security Measures: http://www.tsa.gov/press/where_we_stand/security_measures.shtm

Category 37.B *Public education & awareness*

2006-09-08 DHS Daily OSIR; Department of Homeland Security
http://www.dhs.gov/dhspublic/display?content=5821

FACT SHEET: PROTECTING THE HOMELAND POST SEPTEMBER 11.

The Department of Homeland Security (DHS) has taken significant action to improve the nation's security since the terrorist attacks of September 11, 2001. By improving security measures for the nation's aviation system, implementing measures designed to protect our critical infrastructure, using biometrics to establish and verify identity, strengthening border security, reflecting the lessons-learned from Hurricane Katrina, increasing the nation's preparedness for a disaster, and enhancing information sharing among federal, state, local, and international partners, DHS is leading the effort to protect the homeland. Information about this effort is available in the full text of this Fact Sheet.

Category 37.B *Public education & awareness*

2006-10-31 Effector Online http://www.eff.org/news/archives/2006_10.php#004970

EFF RELEASES BLOGGERS' GUIDE FOR INVESTIGATING GOVERNMENT AGENCIES FREEDOM OF INFORMATION. ACT CAN HELP RESEARCHERS UNCOVER IMPORTANT RECORDS.

Washington, D.C. - Bloggers across the Internet have shown that you don't have to be part of the mainstream media to uncover an important story and tell it to the world. But how do you start investigating a big story for your blog? The Electronic Frontier Foundation (EFF) has released tips for bloggers who want the inside story on government agencies. The Bloggers' FAQ on the Freedom of Information Act (FOIA) outlines how to use open government laws to get access to records kept by federal agencies like the Federal Bureau of Investigation (FBI), the Environmental Protection Agency (EPA), or the Food and Drug Administration (FDA). "Online journalism makes a unique contribution to America's vibrant culture of free speech," said EFF Staff Attorney Marcia Hofmann. "Using the Freedom of Information Act is a powerful way to shed light on government activities and foster critical public debate about the discoveries." The guide walks bloggers through making a FOIA request -- addressing what to ask for, which government offices must comply, and what you can and cannot obtain through FOIA. It also explains how to put requests on the fast track and get processing fees waived. The guide is the most recent product of EFF's FLAG Project, which uses FOIA requests and litigation to expose the government's expanding use of technologies that invade privacy. Earlier this month, the FLAG Project filed lawsuits demanding that the FBI release records concerning the development of two electronic surveillance tools as well as information about the FBI's "Investigative Data Warehouse" (IDW) -- a huge database that contains hundreds of millions of entries of personal information. "The FLAG Project investigates privacy-invasive tools and policies fostered by the government. There are many other important issues out there in which a blogger can make a difference," EFF Senior Counsel David Sobel said. "Everyone has the ability through FOIA to discover government corruption, fraud and waste, and to publicize those abuses of power."
For the Bloggers' FAQ on the Freedom of Information Act: http://www.eff.org/bloggers/lg/faq-FOIA.php
For the complete Legal Guide for Bloggers: http://www.eff.org/bloggers/lg/
For more on EFF's FLAG Project: http://www.eff.org/flag/
For this release: http://www.eff.org/news/archives/2006_10.php#004970

Category 37.B *Public education & awareness*

2006-11-13 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article96796-11-13-06-Web

NIST PROVIDES SECURITY GUIDE FOR MANAGERS.

The National Institute of Standards and Technology (NIST) has put together a guide to information security tailored specifically for top-level managers. The publication, "Information Security Handbook: A Guide for Managers," was written for chief information officers, chief information security officers and other officials who have a vested interest in the security of agency systems but who do not necessarily need to get into the nuts and bolts on a daily basis. The guide focuses on issues that typically arise when planning and implementing a security program. NIST handbook: http://csrc.nist.gov/publications/nistpubs/800-100/sp800-100.pdf

Category 37.B Public education & awareness

2007-02-08 DHS Daily OSIR; Federal Trade Commission http://www.ftc.gov/opa/2007/02/fyi0716.htm

FTC ISSUES ADVICE ON PREVENTING COUNTERFEIT CHECK SCAMS.

A new scam is swindling consumers: counterfeit checks that seem legitimate to both bank employees and consumers. The Federal Trade Commission (FTC) is issuing a new brochure, Giving the Bounce to Counterfeit Check Scams, which explains these scams and how to avoid them. The basics of counterfeit check schemes are the same. The consumer receives a generous check with an explanation that they've just won an award, a prize, a lottery or some other windfall. The consumer is instructed to deposit the check and wire a portion back to pay fees, taxes, or the like. The consumer deposits the check, the bank credits the funds to the consumer's account, and the consumer wires the money to the sender. Some time later, both the bank and the consumer learn the check was bogus. Unfortunately, the consumer is out of luck: the money that was wired can't be retrieved and, by law, the consumer is responsible for the deposited check. Among other guidelines, the FTC advises consumers not to rely on funds from checks unless they know and trust the person who gave them the check or, better yet, until the bank confirms that the check has cleared.
FTC Brochure: http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre40.htm

Category 37.B Public education & awareness

2007-02-22 DHS Daily OSIR; InformationWeek
http://www.informationweek.com/news/showArticle.jhtml

DESPITE GOVERNMENT DATA LOSSES, SECURITY EDUCATION SPENDING NOT GROWING.

While laptop and data loss continue to plague government agencies, a new report shows that federal spending on user education remains stagnant. Out of an annual IT security budget of $5.6 billion, the U.S. is spending $140 million to $150 million annually on security awareness and training, according to information security analyst Prabhat Agarwal. That user education number is expected to hold steady through 2012. Agarwal estimates that government employs between six million and 10 million people. In his report, Agarwal says users are the weakest link in the government's security -- much like they are in the corporate world.
Report: http://www.input.com/corp/press/detail.cfm?news=1311

38.1 Consumer/employee/individual profiling & surveillance (non-governmental)

Category 38.1 Consumer/employee/individual profiling & surveillance (non-governmental)

2006-01-04 INNOVATION <http://news.bbc.co.uk/2/hi/programmes/click_online/4534674.stm>

NEW CLOCK 'FACE' HAS EYES

As if the hands of time weren't enough, the new Whereabouts Clock has eyes. Instead of the time, it shows you whether your spouse or kids are at work, at the gym, or en route. Inventor Abigail Sellen says her studies of family life revealed that today's parents want to know things like, "Are my kids still at school, have they left yet, has my husband left work yet, shall I get the dinner on? This kind of thing. Knowing where your family is very important to family life." Sellen's Whereabouts Clock, which was among the futuristic goodies Microsoft demonstrated in Brussels earlier this month, operates by tracking the mobile phone signals of loved ones. It cross-references the cell they're currently in with pre-programmed locations like home, school or workplace. Sound a little Big Brother-ish?

Abusing it might tempt certain bosses, but Sellen insists her invention "is not very specific at all about where people are, and that's deliberate. We don't want to invade people's privacy too much." Sellen added, "If I'm at home I might want to know if my kids have left school, but I don't necessarily want to know exactly where they are." This new concept in clocks is still at least a year or two away. (BBC News 16 Dec 2005)

Category 38.1 Consumer/employee/individual profiling & surveillance (non-governmental)

2006-01-19 EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4627214.stm

APPLE CHANGES ITUNES IN RESPONSE TO COMPLAINTS

Responding to complaints that its iTunes software infringed on user privacy, Apple has made changes to the application. At issue is a feature called MiniStore, which recommends songs to users based on what they are listening to. When the new feature was released earlier this month, some users discovered that the feature transmitted information about iTunes users to Apple with unique identifiers. Those ID numbers exposed the users of the service to violations of their privacy because the iTunes software did not alert users to the feature and how it works. Critics also pointed out that Apple did not disclose what exactly it does with the data that is transmitted to the company. Apple has changed the software to include a pop-up that tells users about the feature and allows them to turn it off. Apple also said that it has not done anything with the data it has collected. Kirk McElhearn, one of the users who first reported the concerns about MiniStore, commended Apple for its response, saying it had "done the right thing."

Category 38.1 Consumer/employee/individual profiling & surveillance (non-governmental)

2006-01-24 DHS Daily OSIR; http://www.theregister.co.uk/2006/01/24/google_privacy_poll/

77% OF GOOGLE USERS DON'T KNOW IT RECORDS PERSONAL DATA.

More than three quarters of Web surfers don't realize Google records and stores information that may identify them results of a new opinion poll show. The phone poll which sampled over 1000 Internet users was conducted by the Ponemon Institute. Google maintains a lifetime cookie that expires in 2038 and records the user's IP address. But more recently it has begun to integrate services which record the user's personal search history e-mail shopping habits and social contacts. After first promising not to tie its e-mail service to its search service Google went ahead and opted its users in anyway. It's all part of CEO Eric Schmidt's promise to create a "Google that knows more about you."

Category 38.1 Consumer/employee/individual profiling & surveillance (non-governmental)

2006-06-15 EDUPAGE; Wall Street Journal (sub. req'd)
http://online.wsj.com/article/SB115030869031780267.html <
http://www.educause.edu/email/edupage/ep061406/track.asp?id=story_3>

NIELSEN TO TRACK ONLINE VIEWERSHIP

Responding to a changing landscape of media, Nielsen Media Research has said it will begin tracking viewership of television programs over the Internet. Media companies have criticized Nielsen for only tracking shows that people watch on televisions in their homes, even as growing numbers of consumers watch shows on computers, cell phones, or other devices, both at home and away from home. The new tracking tools will be introduced over several years and could have a considerable bearing on ratings of shows, particularly sporting events, which analysts believe are especially likely to be watched outside the home. Nielsen said it would provide its "Nielsen families"--those whose television viewing provides ratings data--with portable devices so they can keep tabs on any television they watch away from their homes.

Category 38.1 Consumer/employee/individual profiling & surveillance (non-governmental)

2006-11-21 DHS Daily OSIR; Associated Press
http://www.newsday.com/news/local/wire/newjersey/ny-bc-nj--carding-personald1121nov21,0,5564944.story?coll=ny-region-apnewjersey

ID SWIPE AT NEW JERSEY BARS STORES AGE, PERSONAL INFORMATION.

Bouncers at some New Jersey bars and nightclubs are using a high-tech identification device to obtain more information than just the ages of their patrons. A small, yellow electronic device scans a bar code on a driver's license that immediately reveals a customer's age. The box also reads personal information on the license -- name, address and license number -- and physical descriptions such as height, weight and eye color. At KatManDu, a popular Trenton nightclub, manager Joseph Surdo the club has created a database of more than 15,000 names in a year. Neither federal nor state law prohibit bars from collecting and storing data from driver's licenses, but they are not allowed to sell or share it.

Category 38.1 Consumer/employee/individual profiling & surveillance (non-governmental)

2007-01-03 INNOVATION (NewScientist 26 Dec 2006)
<http://www.newscientisttech.com/article/dn10862-cellphone-tells-the-world-what-mode-youre-in.html>

SWARM MOBILE PHONE SYSTEM SIGNALS WHAT YOU'RE UP TO

Researchers at the University of Melbourne in Australia are developing a mobile phone system that can communicate to your friends, family or co-workers where you are and what you're up to, based on a color-coded icon system. Each color corresponds to one of six activities: holiday, social, driving, leisure, sleep or work. Adding icons such as a cocktail glass to indicate a bar can provide additional options. The Swarm system allows users to categorize various potential callers into different groups, such as "work" or "friend," allowing different information to be transmitted to each, meaning that while your friends are seeing that cocktail glass, your boss is receiving your "hard at work" icon.

Category 38.1 Consumer/employee/individual profiling & surveillance (non-governmental)

2007-02-26 DHS Daily OSIR; Associated Press
http://www.boston.com/business/technology/articles/2007/02/26/surveillance_cameras_latest_job_interpret_the_threats_they_see/

SURVEILLANCE CAMERAS' LATEST JOB: INTERPRET THE THREATS THEY SEE.

Never-blinking surveillance cameras, rapidly becoming a part of daily life in public and even private places, may soon get a lot smarter. Researchers and security companies are developing cameras that not only watch, but also interpret what they see. Soon, some cameras may be able to find unattended bags at airports, guess your height, or analyze the way you walk to see if you are hiding something. Most of the cameras used today are used to identify crooks after-the-fact. But so-called intelligent video could transform cameras from passive observers to eyes with brains, able to detect suspicious behavior and potentially prevent crime. The innovations could mean fewer people would be needed to watch what cameras record, and make it easier to install more in public places and private homes. Companies that make the latest cameras say the systems, if used broadly, could make video surveillance much more powerful. Cameras could monitor airports and ports, help secure homes, and watch over vast borders. Intelligent surveillance uses computer algorithms to interpret what a camera records. The system can be programmed to look for particular things.

Category 38.1 Consumer/employee/individual profiling & surveillance (non-governmental)

2007-04-03 DHS Daily OSIR; Times West Virginian
http://www.timeswv.com/local/local_story_091005553.html

NEW TRACKING SYSTEM PROVEN.

Three months after they glued button-sized radio frequency identification, or RFID, tags to the hard hats of more than 2,000 of its underground coal miners, a top Alliance Coal official says the company -- and its miners -- are "very pleased" with their new tracking system. The new tracking system -- which improves on tracking systems used in Australia -- probably wouldn't survive a worst-case scenario, such the methane explosion January 2, 2006 at the Sago Mine, Mark Watson of Alliance Coal acknowledges. Neither would any other known system, however, which shows the dilemma the nation's underground coal producers face since the loss of 12 miners at Sago. The industry's rescue and safety practices have been in the national spotlight since. A key issue is whether Alliance and other producers should spend hundreds of thousands of dollars on communications and tracking systems available now or work on developing "next-generation" systems.

Category 38.1 Consumer/employee/individual profiling & surveillance (non-governmental)

2007-04-11 INNOVATION (The Engineer Online 26 Mar 2007)
<http://www.e4engineering.com/Articles/298743/Tune+in,+track+down.htm>

WIFI TRACKING UPS THE ANTE IN SURVEILLANCE

Researchers at University College London are working on a WiFi-based tracking system that could enable continuous, real-time monitoring of people or objects, both in- and out-of-doors. "The system could be deployed anywhere with a WiFi capability using the existing infrastructure," says UCL engineering professor Karl Woodbridge. "All you would have to do is to install a relatively simple receiver to build a detection system." The system works by analyzing how the WiFi signal changes when it hits a target and is refined by examining other factors, such as how a person is standing. Researchers believe it may be possible to use this motion detection for identification. The technology makes use of both WiFi and WiMax technologies, enabling ranges up to 25 miles, and in combination with video cameras, could be used for local surveillance to detect unusual behavior in public or military-controlled areas. Woodbridge hopes to have a working prototype by August 2009, capable of demonstrating detection, tracking, location and imaging performance.

Category 38.1 Consumer/employee/individual profiling & surveillance (non-governmental)

2007-05-30 INNOVATION (National Post 19 May 2007)
<http://www.canada.com/nationalpost/story.html?id=42620fdf-6339-40c6-9775-dcad5d623f51&k=8721>

PRIVACY THREATS OF PERVASIVE COMPUTING

What happens to your privacy when technology is literally everywhere, both on your person and part of your physical environment? It might sound cool to have a personal robotic butler or to locate misplaced car keys by tapping "keys" into your cell phone, but there are grave implications, says Adam Greenfield, author of "Everyware: The Dawning Age of Ubiquitous Computing." Police and government surveillance could go beyond wiretapping to body-tapping. Big business already tracks your spending and shopping habits. Now that our every location is broadcast to the world, criminals could use it for more efficient stalking, theft, even kidnapping. The only way to have privacy in the future is to have it legislated, insists Darren Leigh of Mitsubishi Electric Research Laboratories. "People are gathering data right now. It's shocking how people gather data on us: financial transactions, going to the grocery store....People want our data." Greenfield believes the only bastion for privacy in this technological future may be in the home: "I think in public space, the battle is already over, and the forces of privacy have lost." Remember HAL in "2001: A Space Odyssey"? A similar scenario -- users unable to control a technology run amok -- is "more than a possibility," says Mr. Greenfield. "I think it's already an issue."

38.2 Legal trade in personal information

Category 38.2 Legal trade in personal information

2006-01-12 RISKS

CELL PHONE CALL RECORDS FOR SALE TO ANYONE

Locatecell.com seems to have a good thing going. According to this Chicago Sun Times story:

To test the service, the FBI paid Locatecell.com $160 to buy the records for an agent's cell phone and received the list within three hours, the police bulletin said.

Representatives of Data Find Solutions Inc., the Tennessee-based operator of Locatecell.com, could not be reached for comment.

Frank Bochte, a spokesman for the FBI in Chicago, said he was aware of the Web site.

"Not only in Chicago, but nationwide, the FBI notified its field offices of this potential threat to the security of our agents, and especially our undercover agents," Bochte said.

Funny how the FBI's first reaction is to go on the defensive. Funny how this is a big surprise to the FBI.

The Chicago Sun-Times paid $110 to Locatecell.com to purchase a one-month record of calls for this reporter's company cell phone. It was as simple as e-mailing the telephone number to the service along with a credit card number.

Locatecell.com e-mailed a list of 78 telephone numbers this reporter called on his cell phone between Nov. 19 and Dec. 17. The list included calls to law enforcement sources, story subjects and other Sun-Times reporters and editors.

Cheating spouse? Disloyal employees? Need to find out what your competition is doing? Hey, no problem. Telecom services are just information services these days.

[Contributed by Lauren Weinstein]

Category 38.2 Legal trade in personal information

2006-01-27 EDUPAGE; http://www.nytimes.com/2006/01/27/business/27choice.html

CHOICEPOINT SETTLES WITH FTC

Data broker ChoicePoint has reached a $15 million settlement with the Federal Trade Commission (FTC) following the company's disclosure a year ago that it had turned over sensitive personal data for about 150,000 people to bogus customers. The FTC alleged that ChoicePoint did not have adequate procedures in place to prevent such fraud and that the company ignored what should have been red flags about the identity of the customers requesting data, including credit reports. ChoicePoint, which has over the past year taken steps to address the problems that led to the incident, said it disagrees with some of the FTC's findings but supports the settlement. The settlement covers a $10 million fine, the largest ever meted out by the FTC, and $5 million that will be held in an account and used to reimburse consumers who can demonstrate losses due to the ChoicePoint incident. Sen. Charles Schumer (D-N.Y.), who introduced tough legislation to regulate the data-brokerage industry after the ChoicePoint scandal, said he thinks the fine was too low and will encourage others to see such penalties as "just the cost of doing business."

Category 38.2 Legal trade in personal information

2006-02-08 DHS Daily OSIR; http://www.nytimes.com/aponline/technology/AP-Phone-Records.html?_r=1&oref=slogin

WEBSITES HAWKING PHONE RECORDS SHUT DOWN.

Following a wave of negative publicity and pressure from the government, several Websites that peddled people's private phone records are calling it quits. "We are no longer accepting new orders" was the announcement posted Wednesday, February 8, on two such sites, locatecell.com and celltolls.com. The Federal Trade Commission (FTC) this week conducted a sweep of 40 sites known to have been selling private phone records. According to the FTC's Lydia Parnes, more than 20 sites have recently shut down or stopped advertising for new business. The agency has sent letters to about 20 other sites, warning them that they may be violating the law and should review their business practices, said Parnes, director of the FTC's Bureau of Consumer Protection. While some sites appear to be closing up shop, others have seen a boom in business with the recent media attention, said Marc Rotenberg, executive director of the Electronic Privacy Information Center. Rotenberg urged lawmakers to ban a practice known as "pretexting," in which data brokers or others call a phone company, impersonate a customer and then persuade the company to release the calling records.

Category 38.2 Legal trade in personal information

2006-03-21 RISKS; Philadelphia Inquirer http://tinyurl.com/puqul ; MediaMatters http://tinyurl.com/k2t29

IRS PLANS TO ALLOW TAX-PREPARERS TO SELL CLIENT DATA

Chris Hoofnagle reported in RISKS on news that the IRS was pushing for new rules allowing commercial tax preparers to sell information from tax returns. "If consent is given, the FULL RETURN can be given to other entities for marketing purposes, and the tax preparer does not have to even ensure that these other entities are legit or following the preparer's privacy policy."

Jeff Gelles of the Philadelphia Inquirer wrote, "The change is raising alarm among consumer and privacy-rights advocates. It was included in a set of proposed rules that the Treasury Department and the IRS published in the Dec. 8 Federal Register, where the official notice labeled them 'not a significant regulatory action.' IRS officials portray the changes as housecleaning to update outmoded regulations adopted before it began accepting returns electronically. The proposed rules, which would become effective 30 days after a final version is published, would require a tax preparer to obtain written consent before selling tax information. Critics call the changes a dangerous breach in personal and financial privacy. They say the requirement for signed consent would prove meaningless for many taxpayers, especially those hurriedly reviewing stacks of documents before a filing deadline."

Media watchdog MediMatters For America reported that "On the CBS Evening News, Washington correspondent Bob Orr characterized a recent Internal Revenue Service (IRS) regulations proposal allowing tax return preparers to sell information from returns to third parties as spelling out a 'loophole of sorts' that has 'been around for more than 30 years.' In fact, in permitting sales to third parties, the new proposal would allow tax preparers to do something they are not currently permitted to do; under current law, they can pass on such information only to affiliates."

The US Public Interest Research Group (U.S. PIRG) established a Web site to cover this developing issue. < http://www.uspirg.org/uspirg.asp?id2=24620 >

Category 38.2 Legal trade in personal information

2006-08-29 DHS Daily OSIR; Tech Web http://www.techweb.com/wire/security/192500110

BANK TO PAY $50 MILLION FINE FOR BUYING PERSONAL DATA.

A bank has been ordered to pay a $50 million settlement for buying more than 650,000 names and addresses from the Florida Department of Highway Safety and Motor Vehicles. The Electronic Privacy Information Center (EPIC) announced the decision this week. EPIC said Fidelity Federal Bank & Trust bought 656,600 names and addresses for use in direct marketing and the purchase violated the Drivers Privacy Protection Act.

38.3 Industry efforts for protection of personal information

Category 38.3 Industry efforts for protection of personal information

2006-01-30 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2088739,00.asp

DATA SECURITY FIRMS ALLY TO PROMOTE STANDARDS.

Eight leading data security companies have joined forces to create an organization to educate the business community on the value of global security standards that protect credit and debit card numbers. The newly formed Payment Card Industry Security Vendor Alliance will assist the PCI Security Standards Council—an organization composed of merchants, banks and point-of-sale vendors—in educating the business community on the requirements and business value of the Payment Card Industry Data Security Standard. The data security standard—a series of rules commonly called the "digital dozen"—sets requirements for security management, network architecture, software design and other critical protective measures. Each of the founding members of PCI SVA—ConfigureSoft, Cyber-Ark, Modulo Security, Proginet, Protegrity USA, Reflex Security, SafeNet and Verisign—will provide flexible PCI Data Security Standard solutions to address the needs of system integrators and business users.

Category 38.3 Industry efforts for protection of personal information

2006-02-10 DHS Daily OSIR; http://security.ithub.com/article/EFF+Dont+Use+Google+Desktop/171267_1.aspx

EFF: DON'T USE GOOGLE DESKTOP.

A high-profile privacy watchdog group has a terse warning for business and consumer users: Do not use the new version of Google Desktop. The nonprofit Electronic Frontier Foundation (EFF) said a new feature added to Google Desktop on Thursday, February 9, is a serious privacy and security risk because of the way a user's data is stored on Google's servers. The new "Share Across Computers" feature stores Web browsing history, Microsoft Office documents, PDF and text files on Google's servers to allow a user to run remote searches from multiple computers, but, according to the EFF, this presents a lucrative target to malicious hackers. Google said users can use a "Clear my Files" button to manually remove all files from its servers or a "Don't Search These Items" preference to remove specific files and folders from the software's index.

Category 38.3 Industry efforts for protection of personal information

2006-09-07 DHS Daily OSIR; ZDNet News http://news.zdnet.com/2100-1009_22-6113512.html

CREDIT CARD COMPANIES FORM SECURITY COUNCIL.

The five major credit card companies have teamed up in the interest of better security. American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International announced Thursday, September 7, the creation of an organization to develop and maintain security standards for credit and debit card payments. The newly formed Payment Card International (PCI) Security Standards Council will manage the PCI Data Security Standard, established in January 2005 to make its implementation more efficient for all parties involved in a payment card transaction. These include merchants, payment processors, point-of-sale vendors, financial institutions, and more than a billion card holders worldwide. Standards include instructions on proper data encryption, common technical standards, and security audit procedures. The council's first action was to update the PCI security standard. The revision gives instructions for how to implement the new standards and clarifies language that was previously considered vague.

38.4 International agreements on data security, individual privacy, Net law

Category 38.4 International agreements on data security, individual privacy, Net law

2007-01-10 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/07/01/10/HNusslapschinafor3 G_1.html

U.S. COMMERCE SECRETARY SAYS CHINA IS THWARTING GLOBAL TECHNOLOGY INNOVATION BY NOT EMBRACING 3G STANDARDS.

Secretary of the U.S. Department of Commerce Carlos M. Gutierrez Tuesday, January 9, criticized China for delaying the creation of a 3G (third generation) wireless network in that country, saying it is thwarting global technology innovation by not embracing standards. Speaking in a session at the International Consumer Electronics Show (CES) in Las Vegas, NV, Gutierrez said companies around the world must support common standards to promote a worldwide environment for technology innovation, not have their own "pockets of standards." He used China, where the government continues to hold out on granting licenses to build 3G networks, as an example of that misstep. China has delayed plans to build a 3G network for several years, he said. Many believe it is because the government wants to promote its own homegrown 3G standard, called TD-SCDMA (Time Division Synchronous Code Division Multiple Access), instead of embracing a version of CDMA (Code Division Multiple Access), on which other countries have built or are building 3G networks. To do its part to encourage competition in the technology industry, the U.S. has to revise current legislation that governs the technology industry and remain as hands-off as possible, he said.

38.5 EU case law, legislation & regulation concerning data security, individual privacy

Category 38.5 *EU case law, legislation & regulation concerning data security, individual priv*

2006-02-09 DHS Daily OSIR; http://news.yahoo.com/s/ap/20060209/ap_on_hi_te/eu_internet_security;_ylt=AqJsTFxWQORMKXpiJ5yFMsAjtBAF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA--

EUROPE URGED TO IMPROVE WEB SECURITY.

Europe must work harder to make the Internet more secure as the nature of online threats becomes increasingly criminal across the 25-nation bloc, a senior EU official warned Thursday, February 9. "We are still far from achieving the goal of secure and reliable networks that protect confidential and reliable information," said Viviane Reding, the EU's media commissioner, at a conference on trust in the Internet. Almost 80 percent of EU citizens are concerned about Internet security and half do not engage in electronic commerce because they worry about having their personal financial data stolen on the Web, she said. Speaking via video link from Brussels, Reding stressed the importance of international cooperation in promoting user trust in the Web and said she would soon announce a "strategy for enhanced security."

38.6 US case law, legislation & regulation concerning data security, individual privacy

Category 38.6 US case law, legislation & regulation concerning data security, individual priv

2006-01-26 DHS Daily OSIR; http://news.com.com/Politicians+call+for+better+phone+record+privacy/2100-1036_3-6031916.html?tag=cd.top

POLITICIANS CALL FOR BETTER PHONE RECORD PRIVACY.

In response to disclosures about phone records being sold on the Internet, politicians want federal regulators to verify that the biggest service providers are adequately protecting their customers' information. According to a letter sent by the chairmen of the U.S. House of Representatives Energy and Commerce Committee, all telecommunications providers must "certify annually" with the Federal Communications Commission (FCC) that they are in compliance with the federal rules. The politicians asked the FCC to turn over the latest certifications from the five largest wireless and wireline providers, along with statements from the companies describing "how their internal procedures protect the confidentiality of consumer information." Citing their ongoing investigation about the matter, the legislators imposed a Monday, January 30, deadline. The House returns from its winter recess Tuesday, January 31. The issue of the illicit brokering of phone records has drawn attention recently, with carriers such as T-Mobile, Verizon Wireless and Cingular Wireless and also the state of Illinois filing suits against third-party brokers accused of the practice. On Monday, January 23, T-Mobile landed a temporary restraining order, which prohibits at least two companies from directly or indirectly obtaining its customers' information. Letter sent by the chairman of the U.S. House of Representatives Energy and Commerce Committee: http://markey.house.gov/docs/privacy/iss_privacy_ltr060123.pdf

Category 38.6 US case law, legislation & regulation concerning data security, individual priv

2006-02-01 EDUPAGE; http://news.zdnet.com/2100-1035_22-6033688.html

CONGRESS HOLDS HEARINGS ON CELL-PHONE CUSTOMER PRIVACY

A Congressional hearing this week will address cell phone companies' efforts to protect the privacy of their customers. The hearing comes after recent revelations that a number of data brokers have been able to con cell phone companies into disclosing data about customers and their calling habits, which was then sold to third parties. The premise is that certain individuals, such as attorneys, might want details of cell phone calls, and data brokers supply that data. Cell phone companies and some members of Congress, however, object to the methods that data brokers use to obtain that information, including posing as people they are not and using information such as Social Security numbers without authorization. Some critics have pointed to weak policies and practices among cell phone companies for protecting such data as the root of the problem. Rep. Joe L. Barton (R-Tex.), chairman of the House Energy and Commerce Committee, said in a statement that he intends to make the practice of fraudulently obtaining such data "very illegal."

Category 38.6 US case law, legislation & regulation concerning data security, individual priv

2006-05-11 EDUPAGE; http://news.com.com/2100-7348_3-6071441.html

CONGRESS DEBATES SSN RESTRICTIONS

Members of Congress have vowed to enact legislation by the end of the year that will restrict use of Social Security numbers (SSNs), which have become a prime target of identity thieves. Several bills are before Congress now, including one introduced by Edward Markey (D-Mass.) and another by Clay Shaw (R-Fla.). Joe Barton (R-Tex.) said the current practice of allowing data brokers to sell SSNs to anyone able to pay for them should be banned outright. Federal Trade Commissioner Jon Leibowitz said SSNs are "overused" and "underprotected." Officials from financial services institutions cautioned, however, that appropriate use of SSNs is invaluable for sectors such as theirs. Oliver Ireland, representing the Financial Services Coordinating Council, said SSNs "are critical for fraud detection."

Category 38.6 US case law, legislation & regulation concerning data security, individual priv

2006-05-12 EDUPAGE; http://www.internetnews.com/bus-news/article.php/3605666

DATA-BREACH LEGISLATION ON THE AGENDA

Rep. James Sensenbrenner (R-Wis.), chairman of the House Judiciary Committee, has introduced the Cybersecurity Enhancement and Consumer Data Protection Act of 2006, which would require notification of government officials--but not of those affected--any time a computer breach exposes data for 10,000 or more individuals. Data-breach bills have previously been introduced by the House Financial Services Committee and the House Commerce Committee, with varying requirements for notification. In the Senate, two bills have been introduced in the Judiciary Committee and a third in the Commerce Committee. Some observers are concerned that the competing federal legislation, which would likely supersede any state laws concerning data-breach disclosure, risks being reconciled into a law that would be worse than if no law were passed. Susanna Montezemolo of the Consumers Union expressed support for one of the Senate bills, the Personal Data Privacy and Security Act, which has been approved by committee and is waiting for a vote in the full Senate.

Category 38.6 US case law, legislation & regulation concerning data security, individual priv

2006-05-16 RISKS

SSNs AS BOTH IDENTIFICATION AND AUTHENTICATION

Jeremy Epstein noted in RISKS that politicians do not necessarily understand security fundamentals. In congressional testimony from the American Financial Services Association, the spokesperson said, ""The Social Security number is the only unique identifier in our country that enables a credit grantor, or a credit bureau, or a bank, or an insurance company, or an investment firm to be sure that the consumer they are doing business with [is legitimate]." Epstein explained, "In other words, they're using it as both an identifier and an authenticator." He also wrote, "Switching to a different number … that is used for both purposes will have the same problem."

His final words were important: "Until Congress understands the problem, there's not much hope of solving it through legislation."

Category 38.6 US case law, legislation & regulation concerning data security, individual priv

2006-05-30 Effector Online http://www.eff.org/news/archives/2006_05. php#004698

HUGE WIN FOR ONLINE JOURNALISTS' SOURCE PROTECTION. EFF ARGUMENTS SECURE REPORTERS' PRIVILEGE FOR INTERNET NEWS GATHERERS.

San Jose - A California state appeals court ruled in favor of the Electronic Frontier Foundation's (EFF's) petition on behalf of three online journalists Friday, holding that the online journalists have the same right to protect the confidentiality of their sources as offline reporters do. "Today's decision is a victory for the rights of journalists, whether online or offline, and for the public at large," said EFF Staff Attorney Kurt Opsahl, who argued the case before the appeals court last month. "The court has upheld the strong protections for the free flow of information to the press, and from the press to the public." In their decision, the judges wrote: "We can think of no workable test or principle that would distinguish 'legitimate' from 'illegitimate' news. Any attempt by courts to draw such a distinction would imperil a fundamental purpose of the First Amendment, which is to identify the best, most important, and most valuable ideas not by any sociological or economic formula, rule of law, or process of government, but through the rough and tumble competition of the memetic marketplace." The case began when Apple Computer sued several unnamed individuals, called "Does," who allegedly leaked information about an upcoming product to online news sites PowerPage and AppleInsider. As part of its investigation, Apple subpoenaed Nfox -- PowerPage's email service provider -- for communications and unpublished materials obtained by PowerPage publisher Jason O'Grady. A trial court upheld the subpoena. But Friday, the court said that O'Grady is protected by California's reporter's shield law, as well as the constitutional privilege against disclosure of confidential sources. The court also agreed with EFF that Apple's subpoena to email service provider Nfox was unenforceable because it violated the federal Stored Communications Act, which requires direct subpoenas of account holders. "In addition to being a free speech victory for every citizen reporter who uses the Internet to distribute news, today's decision is a profound electronic privacy victory for everyone who uses email," said EFF Staff Attorney Kevin Bankston. "The court correctly found that under federal law, civil litigants can't subpoena your stored email from your service provider." EFF worked with co-counsel Thomas Moore III and Richard Wiebe in this case.
For the full decision in the case: http://www.eff.org/Censorship/Apple_v_Does/H028579.pdf
For more on Apple v. Does: http://www.eff.org/Censorship/Apple_v_Does/
For this release: http://www.eff.org/news/archives/2006_05. php#004698

Category 38.6 US case law, legislation & regulation concerning data security, individual priv

2006-06-05 Effector Online http://www.eff.org/news/archives/2006_06. php#004720

APPEALS COURT CORRECTS DANGEROUS WEB PRIVACY RULING. JUDGES AGREE WITH EFF BRIEF IN DIRECTV CASE.

San Francisco - The 11th Circuit Court of Appeals has corrected a dangerous lower court ruling that threatened Internet privacy. In doing so, it preserved the privacy of password-protected websites as well as the right to read public sites. The decision followed the arguments made in an amicus brief filed by the Electronic Frontier Foundation (EFF). "A real privacy disaster was averted today," said EFF Staff Attorney Kevin Bankston, who authored the brief. "The court affirmed important legal protections for truly private websites, and also protected your right to read public content on the Internet without getting sued." The case began when Michael Snow, the publisher of an anti- DirecTV website, sued the company for unauthorized access under the Stored Communications Act (SCA). Snow's site had a banner and purported Terms of Service forbidding DirecTV representatives from entering the site or using its message board, but it was configured such that anyone in the public could do so. A lower court had rightly dismissed the case, but for the wrong reasons -- holding that the SCA did not protect websites at all, even if they were configured to be private. However, the 11th Circuit clarified that websites are protected by the SCA, except when they are designed to be readily accessible to the general public. "Through the World Wide Web, individuals can easily and readily access websites hosted throughout the world. Given the Web's ubiquitous and public nature, it becomes increasingly important in cases concerning electronic communications available through the Web for a plaintiff to demonstrate that those communications are not readily accessible," the opinion reads. "If by simply clicking a hypertext link, after ignoring an express warning, on an otherwise publicly accessible webpage, one is liable under the SCA, then the floodgates of litigation would open and the merely curious would be prosecuted. We find no intent by Congress to so permit."
For the full opinion: http://www.eff.org/legal/cases/Snow_v_DirecTV/200513687.pdf
For EFF's brief: http://www.eff.org/legal/cases/Snow_v_DirecTV/EFF_amicus.pdf
For this release: http://www.eff.org/news/archives/2006_06. php#004720

Category 38.6 US case law, legislation & regulation concerning data security, individual priv

2006-09-01 DHS Daily OSIR; Government Computer News
http://www.gcn.com/online/vol1_no1/41854-1.html

NIST RELEASES RECOMMENDATIONS FOR SECURING WEB SERVICES.

The National Institute of Standards and Technology (NIST) has released for comment a draft of Guide to Secure Web Services. Special Publication 800-95 addresses security needs for networks in which automated Web services are being deployed in service-oriented architectures. Comments should be submitted by October 30. NIST draft publication: http://www.csrc.nist.gov/publications/drafts/Draft-SP800-95. pdf

Category 38.6 US case law, legislation & regulation concerning data security, individual priv

2006-10-10 Effector Online http://www.eff.org/news/archives/2006_10.php#004935

EFF SUES FOR INFORMATION ON ELECTRONIC SURVEILLANCE SYSTEMS. FBI WITHHOLDS RECORDS ON TOOLS TO INTERCEPT PERSONAL COMMUNICATIONS.

Washington, D.C. - The FLAG Project of the Electronic Frontier Foundation (EFF) filed its first lawsuit against the Department of Justice last week after the FBI failed to respond to a Freedom of Information Act (FOIA) request for records concerning DCS-3000 and Red Hook -- tools the FBI has spent millions of dollars developing for electronic surveillance. DCS-3000 is an interception system that apparently evolved out of "Carnivore," a controversial surveillance system the FBI used several years ago to monitor online traffic through Internet service providers. One Department of Justice report said DCS-3000 was developed to "intercept personal communication services delivered via emerging digital technologies" and that it was used "as carriers continue to introduce new features and services." According to the same report, Red Hook is a system to "collect voice and data calls and then process and display the intercepted information." The FLAG Project first filed its FOIA request for information about the surveillance systems on August 11, 2006. The FBI acknowledged receipt of the request, but the agency has not responded within the time limit required by law. "Recent allegations of domestic spying by the U.S. government already have both lawmakers and the general public up in arms. Americans have a right to know whether the FBI is using new technology to further violate their privacy," said EFF Staff Attorney Marcia Hofmann. "The Department of Justice needs to abide by the law and publicly release information about these surveillance tools." EFF's FLAG Project, launched last month, uses FOIA requests and litigation to expose the government's expanding use of technologies that invade privacy. "Transparency is critical to the functioning of our democracy, especially when the government seeks to hide activities that affect the rights of citizens," explained EFF Senior Counsel David Sobel, who directs the FLAG Project. "We have recently seen numerous instances where federal agencies have sought to conceal surveillance activities that raise serious legal issues."
For the full FOIA suit filed against the Department of Justice: http://www.eff.org/flag/dcs/dcs_complaint.pdf
For more on the FLAG Project: http://www.eff.org/flag/
For this release: http://www.eff.org/news/archives/2006_10.php#004935

Category 38.6 *US case law, legislation & regulation concerning data security, individual priv*

2006-10-24 DHS Daily OSIR;
New York Times http://www.nytimes.com/2006/10/24/business/24road.html

AT U.S. BORDERS, LAPTOPS HAVE NO RIGHT TO PRIVACY.

Many business travelers are walking around with laptops that contain private corporate information that their employers really do not want outsiders to see. Until recently, their biggest concern was that someone might steal the laptop. But now there's a new worry -- that the laptop will be seized or its contents scrutinized at United States customs and immigration checkpoints upon entering the United States from abroad. Although much of the evidence for the confiscations remains anecdotal, it's a hot topic this week among more than 1,000 corporate travel managers and travel industry officials meeting in Barcelona at a conference of the Association of Corporate Travel Executives. Last week, an informal survey by the association, which has about 2,500 members worldwide, indicated that almost 90 percent of its members were not aware that customs officials have the authority to scrutinize the contents of travelers' laptops and even confiscate laptops for a period of time, without giving a reason. Laptops may be scrutinized and subject to a "forensic analysis" under the so-called border search exemption, which allows searches of people entering the United States and their possessions "without probable cause, reasonable suspicion or a warrant," a federal court ruled in July.

Category 38.6 *US case law, legislation & regulation concerning data security, individual priv*

2006-11-29 Effector Online http://www.eff.org/news/archives/2006_11.php#005022

BRIEF ARGUES EMAIL DESERVES SAME CONSTITUTIONAL PROTECTIONS AS PHONE CALLS, POSTAL MAIL. EFF FIGHTS TO SHIELD EMAIL FROM SECRET GOVERNMENT SEARCHES.

San Francisco - The government must have a search warrant before it can search and seize emails stored by email service providers, according to a friend-of-the-court brief filed last week by the Electronic Frontier Foundation (EFF) and a coalition of civil liberty groups. EFF filed the brief in support of a landmark district court decision finding that the federal Stored Communications Act (SCA) violates the Fourth Amendment by allowing secret, warrantless searches and seizures of email stored with a third party. EFF's amicus brief was filed in Warshak vs. United States, a case brought in the Southern District of Ohio federal court by Steven Warshak to stop the government's repeated secret searches and seizures of his stored email using the SCA. The district court ruled that the government cannot use the SCA to obtain stored email without a warrant or prior notice to the email account holder. The government, which has routinely used the SCA over the past 20 years to secretly obtain stored email without a warrant, appealed the decision to the 6th U.S. Circuit Court of Appeals. That court is now primed to be the first circuit court ever to decide whether email users have a "reasonable expectation of privacy" in their stored email. "Email users clearly expect that their inboxes are private, but the government argues the Fourth Amendment doesn't protect emails at all when they are stored with an ISP or a webmail provider like Hotmail or Gmail," said EFF Staff Attorney Kevin Bankston. "EFF disagrees. We think that the Fourth Amendment applies online just as strongly as it does offline, and that your email should be as safe against government intrusion as your phone calls, postal mail, or the private papers you keep in your home." The EFF brief was also signed by the American Civil Liberties Union, the ACLU of Ohio, and the Center for Democracy and Technology.
For the full amicus brief: http://eff.org/legal/cases/warshack_v_usa/warshack_amicus.pdf
For this release: http://www.eff.org/news/archives/2006_11.php#005022

Category 38.6 US case law, legislation & regulation concerning data security, individual priv

2007-05-24 SC Magazine http://www.scmagazine.com/us/news/article/659814/after-myriad-data-breaches-feds-cut-use-social-security-numbers/

AFTER MYRIAD DATA BREACHES, FEDS TO CUT USE OF SSNs

Dan Kaplan, writing in SC Magazine, summarized the situation as follows:

"http://www.scmagazine.com/us/news/article/659814/after-myriad-data-breaches-feds-cut-use-social-security-numbers/

After myriad data breaches, feds to cut use of Social Security numbers

Dan Kaplan May 24 2007 17:19
Amid an avalanche of federal data breaches, agencies have been ordered to eliminate the unnecessary collection of personal information, including Social Security numbers.

Clay Johnson, deputy director of the Office of Management and Budget, issued the new mandates on Wednesday in a memo that also required agencies to develop training programs and breach notification policies.

"Safeguarding personally identifiable information in the possession of government and preventing its breach are essential to ensure that government retains the trust of the American public," Johnson wrote in the memo.

Asking agencies to be proactive, the memo ordered them to store the minimum number of personal records and to devise a plan to end the unnecessary use of Social Security numbers. That plan must be developed within four months and acted on within 18 months thereafter.

The memo comes almost a year to the day after thieves stole the laptop of a Department of Veterans Affairs employee, which contained the personal information of roughly 26.5 million veterans and current military personnel.

Since then, data exposures have affected a number of federal agencies. Most recently, the Transportation Security Administration announced an external hard drive containing the sensitive data of about 100,000 employees was either lost or stolen.

In April, federal agencies scored an average information security grade of C-minus under the Federal Information Security Management Act, a slight improvement from the prior year.

Allan Paller, director of research for the SANS Institute, told SCMagazine.com that he applauds the initiative but eliminating the use of personal information is only one piece of the information security puzzle.

He said the federal government should employ the Payment Card Industry
(PCI) audit guide when examining the security posture of an agency. Paller said PCI metrics contain more validity and reliability than the FISMA audit guide when trying to determine how well an agency can defend itself against an attack.

The 22-page memo from OMB also required agencies to institute a data breach-notification policy within four months, using existing FISMA guidelines and other privacy legislation built on National Institute of Standards and Technology (NIST) standards.

The memo also outlined training requirements for federal employees, including remote workers…."

38.7 Other case law, legislation & regulation concerning data security, individual privacy

Category 38.7 Other case law, legislation & regulation concerning data security, individual pr

2007-03-26 DHS Daily OSIR; Computerworld
http://www.infoworld.com/article/07/03/23/HNwindowssecuredeadline_1.html

WHITE HOUSE ISSUES DEADLINES TO SECURE WINDOWS.

Federal agencies have until February 1, 2008 to implement a common secure configuration setting for all Windows XP and Vista systems based on standards from the National Institute of Standards and Technology (NIST) and other organizations. But they only have until May 1, to provide details to the White House Office of Management and Budget on how they plan to do so. The deadlines were set by de facto federal CIO Karen Evans in a memorandum to agency CIOs Tuesday, March 20. The memo directs agency CIOs to provide details on a variety of issues, including plans to test the security configurations in nonproduction environments to identify potential problems, implementing and automating enforcement of these settings, and restricting administration of these configurations to authorized personnel only. Agencies must also be able to install Microsoft patches from DHS when new vulnerabilities are disclosed, the memo said. Evans also wants all agency IT acquisitions after June 30 to use a common secure configuration that application software vendors have certified their products will work with.

38.9 Medical information & HIPAA

Category 38.9 Medical information & HIPAA

2006-06-27 DHS Daily OSIR; Department of Health and Human Services
http://www.hhs.gov/ocr/hipaa/decisiontool/

HHS RELEASES DECISION TOOL FOR EMERGENCY PREPAREDNESS DISCLOSURES.

Emergency preparedness and recovery planners are interested in the availability of information they need to serve people in the event of an emergency. For example, planners seek to meet the special needs of the elderly or persons with disabilities in the event of an evacuation. The federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule protects individually identifiable health information held by "covered entities." The information protected is referred to as protected health information (PHI). The HIPAA Privacy Rule permits covered entities to disclose PHI for a variety of purposes. The Department of Health and Human Services' (HHS) Office of Civil Rights has released a decision tool which presents avenues of information flow that could apply to emergency preparedness activities. The rules regarding the use and disclosure of PHI apply to all individuals; no special rules apply to particular populations, such as persons with disabilities. Decision Tool: http://www.hhs.gov/ocr/hipaa/decisiontool/tool/

38.A Data mining & search engines

Category 38.A Data mining & search engines

2006-01-20 Effector Online; New York Times http://www.nytimes.com/2005/12/24/politics/24spy.html

ACTION ALERT: ILLEGAL NSA WIRETAPPING PROGRAM INVOLVED DATA-MINING.

News reports over the holidays revealed that the US National Security Agency (NSA)'s presidentially-approved domestic spying program is even broader than the White House acknowledged. First it was revealed that the Administration has been wiretapping the international phone and email communications of people inside the US without getting search warrants. Now we learn that, according to the New York Times and the Los Angeles Times, the NSA has gained access to major telecommunications switches inside the US, giving it essentially unchecked access not only to international communications but to purely domestic emails and phone calls as well. Those newspapers, and a new book by New York Times reporter James Risen, have further revealed that the NSA has been using that access--as well as access to telecommunications companies' databases--to data-mine Internet logs and phone logs for suspicious patterns, presumably to find new targets for the wiretapping program. The continuing revelations about the NSA's illegal surveillance activities make a mockery of the current debate over U.S.A.P.A.T.R.I.O.T. reform. The Administration has been vigorously arguing against adding any new checks and balances to its foreign intelligence capabilities in the new U.S.A.P.A.T.R.I.O.T. renewal bill, yet the White House has now admitted that it authorized the NSA to bypass the few checks and balances remaining after U.S.A.P.A.T.R.I.O.T.. What good is legislative reform if the Administration considers itself above the law? . . . .

New York Times, "Spy Agency Mined Vast Data Trove, Officials Report," 12/24/05:
http://www.nytimes.com/2005/12/24/politics/24spy.html
Los Angeles Times, "U.S. Spying Is Much Wider, Some Suspect," 12/25/05: http://www.eff.org/cgi/tiny?urlID=548
Excerpt from James Risen's "State of War," discussing "the Program": http://cryptome.org/nsa-program.htm

Category 38.A Data mining & search engines

2006-02-10 EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4700002.stm

EFF RAISES CONCERNS OVER GOOGLE DESKTOP

The Electronic Frontier Foundation (EFF) is warning users about what it says are privacy concerns with Google's new Desktop Search application. The tool indexes files from a computer, allowing users to search that content from other machines. According to the EFF, this process poses significant risks to personal privacy, particularly in light of recent government demands for access to usage logs from Google and other companies. EFF staff attorney Kevin Bankston said, "Unless you configure Google Desktop very carefully, and few people will, Google will have copies of...whatever...text-based documents the desktop software can index." If federal authorities obtain Google's records, he said, they would have access to all of those files. Officials from Google conceded that the new tool does represent a trade-off of some measure of privacy, but said such a compromise is one that many users will be willing to make. The company also said it would encrypt those files, would place strong limits on who can access the information, and would not store it for more than 30 days.

Category 38.A Data mining & search engines

2006-02-10 Effector Online http://www.eff.org/news/archives/2006_02. php#004400

GOOGLE COPIES YOUR HARD DRIVE - GOVERNMENT SMILES IN ANTICIPATION. CONSUMERS SHOULD NOT USE NEW GOOGLE DESKTOP.

San Francisco - Google announced a new "feature" of its Google Desktop software that greatly increases the risk to consumer privacy. If a consumer chooses to use it, the new "Search Across Computers" feature will store copies of the user's Word documents, PDFs, spreadsheets and other text- based documents on Google's own servers, to enable searching from any one of the user's computers. EFF urges consumers not to use this feature, because it will make their personal data more vulnerable to subpoenas from the government and possibly private litigants, while providing a convenient one-stop-shop for hackers who've obtained a user's Google password. "Coming on the heels of serious consumer concern about government snooping into Google's search logs, it's shocking that Google expects its users to now trust it with the contents of their personal computers," said EFF Staff Attorney Kevin Bankston. "Unless you configure Google Desktop very carefully, and few people will, Google will have copies of your tax returns, love letters, business records, financial and medical files, and whatever other text-based documents the Desktop software can index. The government could then demand these personal files with only a subpoena rather than the search warrant it would need to seize the same things from your home or business, and in many cases you wouldn't even be notified in time to challenge it. Other litigants--your spouse, your business partners or rivals, whomever--could also try to cut out the middleman (you) and subpoena Google for your files." The privacy problem arises because the Electronic Communication Privacy Act of 1986, or ECPA, gives only limited privacy protection to emails and other files that are stored with online service providers--much less privacy than the legal protections for the same information when it's on your computer at home. And even that lower level of legal protection could disappear if Google uses your data for marketing purposes. Google says it is not yet scanning the files it copies from your hard drive in order to serve targeted advertising, but it hasn't ruled out the possibility, and Google's current privacy policy appears to allow it. "This Google product highlights a key privacy problem in the digital age," said Cindy Cohn, EFF's Legal Director. "Many Internet innovations involve storing personal files on a service provider's computer, but under outdated laws, consumers who want to use these new technologies have to surrender their privacy rights. If Google wants consumers to trust it to store copies of personal computer files, emails, search histories and chat logs, and still 'not be evil,' it should stand with EFF and demand that Congress update the privacy laws to better reflect life in the wired world." Google can and should design its technologies to avoid these problems in the first place. For example, searching across computers can be accomplished without Google having to keep copies of those computers' contents. Alternatively, Google could encrypt the stored data such that only the user has access. "Google constantly touts its creative brainpower. More privacy-protective technologies are surely not beyond its reach, so long as its engineers make that a design priority," added Bankston.
For more on the new version of Google Desktop:
http://today.reuters.com/business/newsArticle.aspx?type=technology&storyID=nN08360109
For more on Google's data collection: http://news.com.com/FAQ+When+Google+is+not+your+friend/2100-1025_3-6034666.html?tag=nl
http://www.boston.com/news/nation/articles/2006/01/21/google_subpoena_roils_the_web/
http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2006/01/20/EDGEPGPHA61.DTL
http://news.com.com/%20Bill+would+force+Web+sites+to+delete+personal+info/2100-1028_3-6036951.html
For this release: http://www.eff.org/news/archives/2006_02. php#004400

Category 38.A Data mining & search engines

2006-02-15 DHS Daily OSIR; http://www.vnunet.com/articles/print/2150292

GOOGLE 'HACKING' OCCURS WITH THE OBJECTIVE TO FIND SENSITIVE INFORMATION ON THE INTERNET.

Malware authors are increasingly creating digital pests that use Google to find their next victim. Using the search tool for automated vulnerability detection is the latest trend in a technique known as 'Google hacking.' George Kurtz, senior vice president for risk management at security firm McAfee, told VNUNet about the phenomenon after a presentation at the RSA Conference in San José. The Santy.a worm, for instance, targeted a known vulnerability in some versions of the phpBB open source bulletin board application to deface Websites. It found its victims through an automated Google search query. Google eventually stopped the worm from spreading by blocking all searches that would turn up servers running the application. But the search engine is able to detect the abuse only if the queries stand out from other searches. Google 'hacking' does not mean breaking into the company's servers but involves online criminals using Google and other search engines to find sensitive information on the Internet. Pictures and screenshots of 'Google hacks':
http://www.siliconvalleysleuth.com/2006/02/things_you_dont.html

Category 38.A Data mining & search engines

2006-07-10 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,1986770,00.asp

WEBSENSE MINES FOR MALICIOUS CODE WITH GOOGLE.

Security researchers have a brand-new tool to use to go digging for malicious executables on the Web: The Google SOAP Search API. Malware hunters at Websense's Security Labs have figured out a way to use the freely available Google API to find dangerous .exe files sitting on thousands of Web servers around the world. The Google API uses the Simple Object Access Protocol (SOAP) and Web Services Description Language (WSDL) standards to offer developers an easy way to run search queries outside of the browser and, because of the way the search engine indexes executables, Websense was able to create code to look for strings associated with malware packers. Dan Hubbard, senior director of security and technology research at the San Diego-based Web filtering software firm, said the use of the Google API started as an experiment after bloggers noticed that some Google search queries were returning .exe files.

Category 38.A Data mining & search engines

2006-07-25 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,1994003,00.asp

BUGLE GOES GOOGLING FOR SOURCE CODE FLAWS.

The world's most popular search engine can be used to pinpoint software security bugs in source code available on the Internet, according to a new research project launched by a UK-based researcher. The project, called Bugle, is a collection of Google search queries that can be used to identify some of the most common vulnerabilities in open-source code indexed by the search giant. Emmanouel Kellinis, a security penetration tester and source code reviewer for KPMG in London, started working on Bugle privately to find pinpoints to some of the most common coding mistakes and decided to go public with the project to expand the list of search queries. Kellinis believes security researchers can combine Bugle queries with Google's "highly intelligent indexing algorithms" to identify vulnerable code indexed by the search engine. "Bugle will give you hints for a potential vulnerability, but you still require skill to identify an actual issue," he explained.

Category 38.A Data mining & search engines

2006-08-08 EDUPAGE; ZDNet http://news.zdnet.co.uk/communications/0,39020336,39280573,00.htm

AOL REGRETS DISCLOSING SEARCH RESULTS

Officials at AOL have apologized for making search records public, calling it a "screw-up" that would not have happened had it been properly reviewed. Researchers in a number of fields use, or would like to use, search records to understand Web surfing habits and how to make searches more efficient. AOL put randomly selected search histories for 658,000 subscribers online, where researchers and the public could access them. Although the records did not contain names, many said the posting puts those users at risk of being identified through inductive reasoning based on their searches. Ari Schwartz, deputy director of the Center for Democracy and Technology, said, "We think it's a major privacy concern, and we're glad to see AOL is taking it seriously." AOL said that despite their intention of assisting the research and academic communities, putting the search records online was wrong and they have since taken them down. Internet researcher Steve Beitzel noted that AltaVista and Excite have previously disclosed similar information and that no harm came from those disclosures.

ZDNet http://news.zdnet.co.uk/communications/0,39020336,39280573,00.htm

Category 38.A Data mining & search engines

2006-08-14 DHS Daily OSIR; Government Computer News
http://www.gcn.com/online/vol1_no1/41625-1.html

POSTAL BRANCH SEEKS RESEARCH ON ADVANCED SEARCH TOOLS.

The U.S. Postal Service is conducting market research for a commercially available advanced search and analysis tool for data and text material. In a recent notice, the U.S. Postal Inspection Service (USPIS) said the search tool must be able to parse and analyzecriminal information that will direct investigative resources in an efficient manner. Responses are due August 25. The USPIS is the Postal Service's law enforcement branch responsible for enforcing nearly 200 federal laws.

Category 38.A Data mining & search engines

2006-09-06 INNOVATION (AP 30 Aug 2006)
<http://apnews.excite.com/article/20060830/D8JR04TO2.html>

HIDE YOUR SEARCH HISTORY IN PLAIN SIGHT

In the wake of AOL's unauthorized divulgence of the search histories of more than 650,000 subscribers, two researchers at New York University have engineered a tool called TrackMeNot that fools the major search engines by sending fake, innocuous queries to make it more difficult to discern your actual search sequences. TrackMeNot sends random searchers, such as "boston clock" and "croissant" to the four largest search engines -- Google, Yahoo, Microsoft and AOL -- about every 12 seconds. It can generate millions of unique queries or users can add their own to the list. One drawback -- TrackMeNot currently works only with the Firefox browser, which has less than 10% market share.

Category 38.A Data mining & search engines

2006-10-04 EDUPAGE; New York Times (registration req'd)
http://www.nytimes.com/2006/10/04/us/04monitor.html

SOFTWARE TO MONITOR FOREIGN OPINIONS OF UNITED STATES

Funded by a $2.4 million grant over three years from the Department of Homeland Security, a group of major universities including Cornell, the University of Pittsburgh, and the University of Utah is developing software to monitor negative opinions of the United States or its leaders in foreign news media. Researchers plan to test the system on a database of articles from 2001 and 2002. The new software will automate existing services for monitoring global news.

Category 38.A Data mining & search engines

2006-10-06 DHS Daily OSIR; Security Focus http://www.securityfocus.com/news/11417

SECURITY PROFESSIONALS WARN OF NEW GOOGLE CODE SEARCH.

Security professionals warned developers on Thursday, October 5, that they need to be aware that their open-source repositories can now be easily mined, allowing attackers to target programs that are likely to be flawed. While Google could previously be used to look for specific strings, now the search engine riffles through code that much better. "It is going deeper into places where code is publicly available, and it's clearly picking up stuff really well," said Chris Wysopal, chief technology officer of security startup Veracode. "This makes it easier and faster for attackers to find vulnerabilities -- not for people that want to attack a (specific) Website, but for people that want to attack any Website." Google announced on Thursday that the tool is now available for public use. Google Code Search digs through open-source code repositories on the Internet, compiling the large amount of source code available on the Web into an easily searchable database. Google reiterated on Thursday that the tool is intended to help programmers to find coding examples and obscure function definitions, not parse for flaws. Google Code Search Engine: http://www.google.com/codesearch

Category 38.A Data mining & search engines

2006-10-13 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2166385/web-caches-harboring-exploit

WEB CACHES HARBORING EXPLOIT CODE.

Web caches used by search engines and ISPs are harboring malicious code thought to have been long-removed, according to a recent report. Security company Finjan said that the caching servers used by sites such as Google and Yahoo are holding exploit code that could be used by third parties to carry out an attack. "It is possible that storage and caching servers could unintentionally become the largest legitimate storage venue for malicious code," said Yuval Ben-Itzhak, chief technology officer at Finjan.
Finjan Trend Report October 2006: http://www.finjan.com/content.aspx?id=827

Category 38.A Data mining & search engines

2006-11-14 DHS Daily OSIR; Washington Technology
http://www.washingtontechnology.com/news/1_1/daily_news/29715-1.html?topic=homeland

DHS IG TO PUT KEY PROGRAMS UNDER MICROSCOPE.

A controversial data mining prototype developed by the Department of Homeland Security's (DHS) Science & Technology Directorate is getting close scrutiny from the department's inspector general (IG). The DHS IG plans to review the Analysis, Dissemination, Visualization, Insight and Semantic Enhancement, or Advise, program, over the next several months to determine how well it is meeting its goals in identifying potential threats, according to the IG's just-released fiscal 2007 Annual Performance Plan. The $40 million program is designed to extract terrorist threat information from large amounts of data. The upcoming evaluation is one of dozens of oversight investigations -- many of them for IT programs at DHS -- that the IG will conduct during the current fiscal year under the 94-page annual plan. Program areas to be reviewed include information security, information sharing, acquisition programs, disaster management, logistics programs, threat assessments, and data mining. 2007 Annual Performance Plan: http://www.dhs.gov/xoig/assets/OIG_APP_FY07.pdf

Category 38.A Data mining & search engines

2006-11-15 Effector Online: http://www.eff.org/deeplinks/archives/004980.php

HOMELAND SECURITY TO "TARGET" MILLIONS IN DATA-MINING SYSTEM.

The Department of Homeland Security (DHS) recently published a notice in the Federal Register disclosing the existence of a "new system of records" -- the Automated Targeting System (ATS) -- that assigns "risk assessments" to millions of U.S. citizens who seek "to enter or exit the United States" or whose work involves international trade. The system appears to involve the data-mining of massive amounts of information derived from a wide variety of sources, including Passenger Name Record (PNR) data obtained from commercial air carriers. The "risk assessments" generated by the system will be retained for "up to forty years," according to DHS, in order to "cover the potential lifespan of individuals associated with terrorism or other criminal activity." But wait -- just because you're currently innocent, that doesn't mean you get a free pass. As the notice goes on to explain: "All risk assessments need to be maintained because the risk assessment for individuals who are deemed low risk will be relevant if their risk profile changes in the future, for example, if terrorist associations are identified." DHS has exempted all of the data contained in the ATS from the "access" and "correction" requirements of the Privacy Act of 1974, which means that citizens have no right to learn about their own "risk assessments" or to challenge them. Franz Kafka, call your office.
For this post and related links: http://www.eff.org/deeplinks/archives/004980.php

Category 38.A Data mining & search engines

2006-11-15 DHS Daily OSIR; CNET News
http://news.com.com/Google,+Yahoo,+Microsoft+adopt+same+Web+index+tool/2100-1025_3-6136041.html

GOOGLE, YAHOO, MICROSOFT ADOPT SAME WEB INDEX TOOL.

Search engine rivals Google, Yahoo and Microsoft are teaming up to make it easier for Website owners to make sure their sites get included in the Web indexes. The companies are adopting Google's Sitemaps protocol, available since June 2005, which enables Website owners to manually feed their pages to Google and to check whether their sites have been crawled. Website owners have had to follow similar processes at each of the other major search engines separately. Now Website owners will be able to go to one place for alerting all three major search engines to their Webpages, something they have been requesting for some time, said Tim Mayer, director of product management at Yahoo Search.

Category 38.A Data mining & search engines

2007-04-15 DHS Daily OSIR; Washington Post http://www.washingtonpost.com/wp-dyn/content/article/2007/04

LENDERS MISUSING STUDENT DATABASE.

Some lending companies with access to a national database that contains confidential information on tens of millions of student borrowers have repeatedly searched it in ways that violate federal rules, raising alarms about data mining and abuse of privacy, government and university officials said. The improper searching has grown so pervasive that officials said the Department of Education is considering a temporary shutdown of the government-run database to review access policies and tighten security. Some worry that businesses are trolling for marketing data they can use to bombard students with mass mailings or other solicitations. Students' Social Security numbers, e-mail addresses, phone numbers, birth dates and sensitive financial information such as loan balances are in the database, which contains 60 million student records. In general, the department allows lenders to search records in the database only if they have a student's permission or a financial relationship with the student. The database, known as the National Student Loan Data System, was created in 1993 to help determine whether students are eligible for student aid and to assist in collecting loan payments. About 29,000 university financial aid administrators and 7,500 loan company employees have access to it.

Category 38.A Data mining & search engines

2007-05-19 DHS Daily OSIR; Stony Brook Independent (NY) http://www.sbindependent.org/node/1850

PERSONAL INFORMATION OF UP TO 90,000 COMPROMISED AT STONY BROOK UNIVERSITY.

The personal information of 90,000 people in a Stony Brook University database was accidentally posted to Google and left there until it was discovered almost two weeks later. According to a Website set up by the university, Social Security numbers and university ID numbers of faculty, staff, students, alumni, and other members of the community were visible on Google after they were posted to a Health Sciences Library Web server on April 11. The files were not easily accessible through Google and the "information could only be retrieved through the use of multiple criteria." The New York State Cyber Security Office contacted Google to have the information removed after it was discovered on April 24.

Category 38.A Data mining & search engines

2007-11-27 DHS Daily OSIR; SecurityFocus http://www.securityfocus.com/brief/367

REPORT: MINING OF BANK DATA BROKE EUROPEAN LAW.

The United States' access to data on international bank transfers, granted by the Society for Worldwide Interbank Financial Telecommunications (SWIFT), violated the privacy laws of the European Union (EU), stated the initial opinion of theArticle 29 Working Party, a government advisory group created to study privacy issues. In a five-page statement released on Thursday, November 23, the Working Party stated that Belgium-based SWIFT mirrored the transaction data in the United States without taking proper precautions that the information would be handled in accordance with EU law. Moreover, SWIFT violated EU privacy law when it gave the U.S. Treasury Department repeated access to the data, which includes the names of the sender and recipient in each fund transfer, to hunt for financial links to terrorist organizations. The Working Group has called for SWIFT to stop sharing data with the U.S. government and bring its data storage into compliance with European law. The group also criticized the European Central Banks for the lack of effective oversight in the matter and advised all other financial institutions that they must notify their clients of the privacy breach. Report: http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_Swift_Affair_23_11_06_en.pdf

41.1 New crypto algorithms

Category 41.1 New crypto algorithms

2007-01-24 DHS Daily OSIR; CNET News
http://news.com.com/Competition+planned+for+new+crypto+standards/2100-1029_3-6152936.html

COMPETITION PLANNED FOR NEW CRYPTO STANDARDS.

The National Institute of Standards and Technology (NIST) is planning a public competition to develop one or more cryptographic "hash" algorithms, it said Tuesday, January 23. Such algorithms are widely used by the federal government and others in applications such as digital signatures and message authentication. However, the current cryptographic standards are under continued attack, weakening their security. "Because serious attacks have been reported in recent years against cryptographic hash algorithms, including SHA-1, NIST is preparing the groundwork for a more secure hash standard," the organization, a federal agency within the U.S. Commerce Department's Technology Administration, said on its Website. Any newly approved algorithm is meant for federal use or to revise the current Secure Hash Standard, NIST said on its site. For more information: http://www.csrc.nist.gov/pki/HashWorkshop/index.html

41.2 Crypto algorithm weaknesses

Category 41.2 Crypto algorithm weaknesses

2006-07-13 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2160250/phishers-crack-two-factor

PHISHERS CRACK TWO-FACTOR AUTHENTICATION.

Security experts have detected a new type of phishing attack that could render two-factor authentication useless. A dual-factor security system typically uses a password and some kind of hardware security device such as a smartcard or token that issues temporary passwords. The Security Fix blog reported that researchers at Secure Science Corporation spotted a phishing Website targeting Citibank's Citibusiness service that attempted to steal both the user name and password as well as the temporary password issued by the security token. The site furthermore acted as a middleman that relayed the information to the Citibank server for authentication. It prompted users if the information they entered was incorrect.

Category 41.2 Crypto algorithm weaknesses

2007-04-27 DHS Daily OSIR; Nature http://www.nature.com/news/2007/070423/full/070423-10.html

QUANTUM CRYPTOGRAPHY IS HACKED.

A team of researchers has, for the first time, hacked into a network protected by quantum encryption. Quantum cryptography uses the laws of quantum mechanics to encode data securely. Most researchers consider such quantum networks to be nearly 100% uncrackable. But a group from the Massachusetts Institute of Technology (MIT) in Cambridge, MA, was able to 'listen in' using a sort of quantum-mechanical wiretap. The trick allowed them to tease out about half of the data, in a way that couldn't be detected by those transmitting or receiving the message. The group admits that their hack isn't yet capable of eavesdropping on a real network. "It is not something that currently could attack a commercial system," says Jeffrey Shapiro, a physicist at MIT and one of the authors on the study. But they expect that one day it will be able to do so, if quantum encryption isn't adequately adapted to stop such hackers from succeeding. The idea for this cunning trick has been around since 1998, but nobody had put it into practice until now. The team's experimental proof-of-concept is published in the 25 April issue of the journal Physical Review A. Abstract: http://scitation.aip.org/getabs/servlet/GetabsServlet?prog=normal&id=PLRAAN000075000004042327000001&idtype=cvips&gifs=Yes

41.3 Brute-force attacks & methods (e.g., rainbow tables, supercomputers)

Category 41.3 *Brute-force attacks & methods (e.g., rainbow tables, supercomputers)*

2006-06-20 EDUPAGE; New York Times (registration req'd)
http://www.nytimes.com/2006/06/20/technology/20chip.html

RESEARCHERS CLAIM FASTEST SILICON CHIP

A team of academic and industry researchers has demonstrated a speed of 500 gigahertz for a silicon-based computer chip they developed. The team included individuals from the Georgia Institute of Technology, Korea University in South Korea, and IBM. To reach 500 gigahertz, which is about 250 times faster than many chips used today, the researchers conducted the test in an environment 451 degrees below zero (Fahrenheit); at room temperature, the chip reportedly still reaches speeds of around 350 gigahertz. Technology consultant Dan Olds said the announcement indicates that "we're not coming anywhere near the end in what processors are capable of." IBM's Bernard Meyerson said the chips, which might be available in consumer devices within two years, could lead to significant leaps in the capabilities of computing devices.

[MK adds: security specialists should monitor such developments because of implications for brute-force cracking times of strong encryption keys.]

Category 41.3 *Brute-force attacks & methods (e.g., rainbow tables, supercomputers)*

2006-06-26 EDUPAGE; Federal Computer Week http://www.fcw.com/article95010-06-26-06-Web

DOE CONTRACTS FOR PETAFLOP SUPERCOMPUTER

The U.S. Department of Energy (DOE) has ordered the first petaflop supercomputing system and an upgrade of its Blue Gene system from Cray. DOE's Oak Ridge National Laboratory announced the $200 million arrangement last week, with plans for completion of the new supercomputer in 2008. The new system reportedly will attain 1,000 trillion floating-point operations per second (teraflops), or one petaflop. Oak Ridge scientists plan to use the system to tackle problems in energy, biology, and nanotechnology. The lab also expects to offer computing time to other researchers through a program that grants supercomputer access to academic and corporate institutions.

Category 41.3 *Brute-force attacks & methods (e.g., rainbow tables, supercomputers)*

2006-08-30 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2163177/boffins-plug-first-truly

SCIENTISTS CLAIM FIRST QUANTUM CRYPTOGRAPHIC NETWORK.

U.S. scientists on Wednesday, August 30, claimed to have developed the world's first truly quantum cryptographic data network. By integrating quantum noise-protected data encryption (QDE) with quantum key distribution (QKD), researchers from the Northwestern University and BBN Technologies of Cambridge, MA, have developed a complete data communication system which boasts "extraordinary resilience to eavesdropping." The QDE method, called AlphaEta, makes use of the inherent and irreducible quantum noise in laser light to enhance the security of the system and make eavesdropping much more difficult. QKD exploits the unique properties of quantum mechanics to securely distribute electronic keys between two parties.

Category 41.3 Brute-force attacks & methods (e.g., rainbow tables, supercomputers)

2006-09-07 EDUPAGE; BBC http://news.bbc.co.uk/2/hi/technology/5322704.stm

LOS ALAMOS LAB COMMISSIONS FASTEST SUPERCOMPUTER

The U.S. Department of Energy has commissioned IBM to build a supercomputer at the Los Alamos National Laboratory in New Mexico that will be as much as four times faster than the Blue Gene/L at the Lawrence Livermore National Laboratory, currently the world's fastest supercomputer. The new computer, dubbed Roadrunner, will use 16,000 standard processors and 16,000 so-called cell processors, which were designed for Sony's PlayStation 3 game console. Because each cell consists of eight individual processors, Roadrunner will be able to achieve its speed using far fewer processors than comparable systems. Other efforts have focused on using the power of cell processors to solve large computing problems. Researchers at Stanford University in August said they were working on a system that would allow PS3 game consoles to function as a large, distributed-computing system. According to the researchers, 10,000 game consoles would provide roughly 1 petaflop of processing--the amount expected from Roadrunner. The Stanford researchers said they hope eventually to recruit 100,000 game consoles to their project.

Category 41.3 Brute-force attacks & methods (e.g., rainbow tables, supercomputers)

2006-11-08 EDUPAGE; Wall Street Journal (sub. req'd)
http://online.wsj.com/article/SB116294179539416180.html

NEW SUPERCOMPUTER USES DIFFERENT APPROACH

A company called SiCortex Inc. has introduced a line of supercomputers that take a fundamentally different approach to the question of high-capacity processing than do so-called cluster systems, which have become the mainstay of the industry in recent years. The SiCortex computers take advantage of technology that allows placing the equivalent of six separate processors on a single chip, resulting in a system that uses considerably less power and takes up much less space. The company's top-of-the-line computer has 972 chips--equal to 5,832 processors--and fits in a single six-foot-tall cabinet. John Mucci, CEO of SiCortex, said a comparable cluster system would take as many as 10 cabinets and would use 10 times as much electricity. The company also markets a less-powerful system with 108 chips, or 648 processors. Horst Simon, director of the National Energy Research Scientific Computing Center, which manages supercomputers for the U.S. Department of Energy, said, "I'm surprised it took so long for someone to come up with this idea."

Category 41.3 Brute-force attacks & methods (e.g., rainbow tables, supercomputers)

2007-01-15 DHS Daily OSIR; SecurityFocus http://www.securityfocus.com/brief/407

RAINBOW TABLE TARGETS WORD, EXCEL CRYPTO.

Office workers looking to protect their documents may want to select a higher grade of encryption. Swiss information-technology firm Objectif Sécurité announced last week that its latest pre-generated list of passwords and their hashes, known as a rainbow table, can now crack the standard encryption on Word and Excel documents in about five minutes on average. Using about four gigabytes of data, the program -- named Ophcrack_office -- can quickly defeat almost 99.6 percent of all passwords, according to the company. "What happens is that we actually crack the 40-bit key that is used to encrypt Word and Excel documents," Philippe Oechslin, CEO of Objectif Sécurité and the inventor of rainbow tables. "We found a way to use the same tables for both Word and Excel, although they have different file formats." Rainbow tables sidestep the difficulty in cracking a single password by instead creating a large data set of hashes from nearly every possible password.

41.4 New crypto products

Category 41.4 New crypto products

2006-02-22 DHS Daily OSIR; http://www.networkworld.com/news/2006/022206-quantum-cryptography.html

STUDY SHOWS HOW PHOTONIC DECOYS CAN FOIL HACKERS.

A University of Toronto professor and researcher has demonstrated for the first time a new technique for safeguarding data transmitted over fiber-optic networks using quantum cryptography. Professor Hoi-Kwong Lo, a member of the school's Center for Quantum Information and Quantum Control, is the senior author of a study that sheds light on using what's called a photonic decoy technique for encrypting data. Quantum cryptography is starting to be used by the military, banks and other organizations that seek to better protect the data on their networks. This sort of cryptography uses photons to carry encryption keys, which is considered safer than protecting data via traditional methods that powerful computers can crack. Quantum cryptography is based on fundamental laws of physics, such that merely observing a quantum object alters it. Lo's study is slated to appear in the Friday, February 24, issue of Physical Review Letters.

Category 41.4 New crypto products

2006-03-13 DHS Daily OSIR; http://www.fcw.com/article92554-03-13-06-Print

MOBILE COMPUTING AND LARGER DATABASES POSE NEW RISKS FOR UNPROTECTED DATA.

As more companies disclose information losses and data theft, information technology companies have entered the market to sell products that encrypt entire hard drives. Those companies argue that encrypting all data on a disk is the best way to protect it from internal and external threats, including user carelessness. "It means the user can never make a mistake" that jeopardizes data security, such as putting classified material in an unclassified folder or onto a portable storage device, said Matt Pauker, co-founder of Voltage Security.

Category 41.4 New crypto products

2006-04-09 EDUPAGE; http://news.zdnet.com/2100-1009_22-6059276.html

IBM ADDS SECURITY TO HARDWARE

IBM has developed technology that adds hardware-level encryption to data on a range of electronic devices. Researchers at the company said that the technology, called Secure Blue, encrypts and decrypts data as it passes through a processor. Data are encrypted in RAM, as well, resulting in a high level of security for devices such as personal computers, cell phones, digital media players, and electronic organizers. The flip side to the protection that Secure Blue provides to users is a new level of control offered to other owners of content, such as media companies. Digital rights management (DRM), which dictates how content may be used, could be bolstered by IBM's new technology, allowing music producers, for example, another tool to restrict unauthorized usage of their intellectual property. Secure Blue has been demonstrated with IBM's PowerPC processor and is said to be compatible with processors from Intel and Advanced Micro Devices, though IBM said it is not currently in talks with those companies to add the technology to their chips.

Category 41.4 New crypto products

2006-08-16 EDUPAGE; The Register http://www.theregister.co.uk/2006/08/16/mobile_encryption/

ENCRYPTION FOR MOBILE PHONES

A British company said it has developed technology that encrypts transmissions on cell phones, allowing users to make calls with confidence that their conversations cannot be intercepted. One Day Mobile reportedly developed the technology with German company Safe.com and with the military. With the software, which must be installed on cell phones, users can decide which of their calls will be encrypted. Encrypted calls are sent over the data network, however, rather than the voice network, which can result in decreased performance. Voice networks are built to ensure smooth and fast transmission, but using the data network to transfer voice traffic can be slower and bumpier and can impose delays.

Category 41.4 New crypto products

2006-08-17 DHS Daily OSIR; BBC http://news.bbc.co.uk/1/hi/technology/5259594.stm

SPEEDY SILICON SETS WORLD RECORD.

A simple tweak to the way common silicon transistors are made could allow faster, cheaper mobile phones and digital cameras, say UK researchers. To achieve the speed gain, researchers at the University of Southampton added fluorine to the silicon devices. "It just takes a standard technology and adds one extra step," said Professor Peter Ashburn at the University of Southampton, who carried out the work. When the researchers tested the new device it clocked a speed of 110 GHz. Complete circuits usually operate at about a tenth of the speed of the component transistors. Although a product has not been built using the devices, Ashburn says they could be used to amplify the signal in mobile phones or to improve the way that handsets convert speech into digital signals. Complete circuits could also be used in digital cameras or scanners to improve the way they convert information from the real world into pixels.

Category 41.4 New crypto products

2006-09-12 DHS Daily OSIR; InformationWeek http://www.informationweek.com/showArticle.jhtml

NEW IBM TECHNOLOGY DESIGNED TO COMBAT CONSUMER DATA THEFT.

IBM on Tuesday, September 12, unveiled new technology it says will help curb the growing problem of businesses exposing sensitive consumer data, either through theft or carelessness, that's routinely stored on their computer networks. The technology, newly embedded in the company's TS1120 storage system, works to encrypt social security numbers, credit card information, and other customer data archived on magnetic tapes—the most common type of storage media in use by businesses today. The goal is to make the data inaccessible to thieves and others who wrongfully come into possession of such tapes. In the past 18 months alone, 90 million U.S. consumers have had their personal data unintentionally exposed, IBM says. Much of that information was held on storage tapes. IBM isn't the only major computer vendor that's adding encryption to its tape drive offerings. Sun Microsystems has developed encryption for its StorageTek T10000 systems. Thirty states now require customer notification if their personal data is lost or stolen.

Category 41.4 New crypto products

2007-01-08 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article97296-01-08-07-Web

DOD SEEKS COMMERCIAL ENCRYPTION SOFTWARE.

The Department of Defense (DoD) is looking to protect all data at rest (DAR) on mobile computers and storage devices using commercial encryption software. DoD will soon award one or more enterprisewide software agreements under the DoD Enterprise Software Initiative and the General Services Administration's Federal SmartBUY program. The department is calling on industry to submit software solutions to encrypt all DAR storage devices, including hard drives of laptop and desktop computers, tablet PCs, smart phones, personal digital assistants, and removable storage devices, according to a pre-solicitation notice. DoD estimates the agreements will cover more than one million laptops and one million other mobile devices.

41.5 Crypto product implementation flaws

Category 41.5 Crypto product implementation flaws

2006-04-13 RISKS; Redspin http://tinyurl.com/er74m

TRIPLE DES UPGRADES EXPOSE BANK ATM NETWORKS TO COMPROMISE

Redspin, Inc., an audit firm, published a white paper analyzing the unexpected effects of a combination of security upgrades to bank automated teller machine (ATM) networks. In brief, although the original intention of the industry plan was to upgrade DES encryption to Triple DES, additional changes included switching to TCP/IP networks instead of dedicated communications lines. The auditors discovered that the data being sent through the wider bank internal networks includes unencrypted data (except for the PIN): "The card number, the expiration date, the account balances and withdrawal amounts, they all go across the networks in cleartext…." The company's press release stated, "Our biggest concern is that not many bank managers know this," says John Abraham, the company's president. "They assume that everything is encrypted. It's not a terrible assumption, so it's no wonder that most bank managers we've talked to are unhappy to discover this after spending $60,000 to upgrade an ATM."

"Fortunately," continues Abraham, "prevention isn't that complicated, as long as bankers are aware that there is a potential problem. ATM machines need to be kept separate from the rest of the bank's computer network, to try to recreate that direct line to the processor. Also, Redspin is developing a tool to help bankers determine their level of vulnerability. This white paper is all about raising awareness."

Category 41.5 Crypto product implementation flaws

2006-05-11 DHS Daily OSIR; http://www.securiteam.com/unixfocus/5RP0E0AIKK.html

HOLES IN THE LINUX RANDOM NUMBER GENERATOR

A new paper was recently released which describes holes in Linux's random number generator, as well as a clear description of the Linux /dev/random. The Linux random number generator is part of the kernel of all Linux distributions and is based on generating randomness from entropy of operating system events. The output of this generator is used for almost every security protocol, including TLS/SSL key generation, choosing TCP sequence numbers, and file system and e-mail encryption. Although the generator is part of an open source project, its source code is poorly documented, and patched with hundreds of code patches. This paper presents a description of the underlying algorithms and exposes several security vulnerabilities. Analysis of the Linux Random Number Generator paper: http://www.gutterman.net/publications/GuttermanPinkasReinman 2006.pdf

Category 41.5 Crypto product implementation flaws

2006-07-17 DHS Daily OSIR; Government Computer News
http://www.gcn.com/online/vol1_no1/41371-1.html

OPEN SOURCE ENCRYPTION MODULE LOSES FIPS CERTIFICATION.

The National Institute of Standards and Technology (NIST) has revoked certification of the open-source encryption tool OpenSSL under the Federal Information Processing Standard (FIPS). OpenSSL in January became one of the first open-source software products to be validated under NIST's Computer Module Validation Program for FIPS-140-2. The certificate apparently was suspended in June when questions were raised about the validated module's interaction with outside software elements.

Category 41.5 Crypto product implementation flaws

2006-11-21 DHS Daily OSIR; Finextra (UK) http://finextra.com/fullstory.asp?id=16183

RESEARCHERS UNCOVER PIN SECURITY FLAW.

Security experts are warning that flaws in the way PINs are encrypted and transmitted across international financial networks could allow corrupt bank workers to access the four-digit codes. A research paper by two researchers at Tel Aviv University describes how the financial transaction processing system used by banks is open to abuse and could enable corrupt bank workers to discover PIN codes. One possible attack targets the translate function in switches which another abuses functions that are used to allow customers to select PINs online. In both cases flaws in the system could enable an attacker to discover PIN codes, for example, when entered by customers while withdrawing cash from an ATM. The numbers could then be used to make fraudulent transactions. "A bank insider could use an existing Hardware Security Module to reveal the encrypted PIN codes and exploit them to make fraudulent transactions, or to fabricate cards whose PIN codes are different than the PIN codes of the legitimate cards, and yet all of the cards will be valid at the same time," says a researcher at Tel Aviv University. An insider of a third-party Switching provider could also attack a bank in another continent.

Category 41.5 Crypto product implementation flaws

2007-01-26 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2173564/flaw-found-pgp-encryption

FLAW FOUND IN PGP DESKTOP ENCRYPTION TOOL.

Users of the popular PGP Desktop encryption tool are being urged to upgrade to the latest version of the software after the discovery of a flaw in the code. The flaw exists in the Windows Service which PGP Desktop installs, and could be used by any local or remote user to run code with escalated privileges. Vulnerability testers NGS Software rated the flaw as a "medium risk" and said that it affects versions of the software earlier than PGP Desktop 9.5.1. The company does not yet have a workaround and is urging all PGP Desktop users to upgrade as a matter of urgency.

43.1 Tokens

Category 43.1 Tokens

2006-05-02 RISKS

TWO-FACTOR "CHIP-AND-PIN" CREDIT CARDS MAY BE SUBJECT TO FRAUD

Nick Rothwell reported on a developing story from Britain, where SHELL UK withdrew the new "chip-and-PIN credit card payment facilities from 160 of their garages, following incidents of fraud." Rothwell wrote, "In this particular case, it appears that the card terminal devices designed by Trintech, although tamper-resistant (i.e. will fail to operate if tampered with), were tampered with to commit the fraud. Trintech are claiming that their equipment is not at fault, and the issue is one of the "environment" in which they were installed." He added, "According to [BBC Radio 4's news program] You and Yours, there have been previous incidents of chip-and-PIN fraud where unscrupulous retailers were able to add items to a customer's bill after the payment transaction."

Category 43.1 Tokens

2007-01-05 DHS Daily OSIR; Finextra (UK) http://finextra.com/fullstory.asp?id=16332

CHIP AND PIN HACKED; RESEARCHERS GET TERMINAL TO PLAY TETRIS.

Security researchers at the University of Cambridge in the UK have managed to hack a so-called tamper resistant Chip and PIN terminal and get it to play Tetris. Steven Murdoch and Saar Drimer got Tetris working by replacing most of the terminal's internal electronics. The hacking illustrates how scanners may be able to physically modify terminals. The researchers posted a video of the hack attack on YouTube. In a Web blog, the researchers say even a perfect tamper resistant terminal will only ensure that the device cannot communicate with a bank once opened. It does not prevent anyone from replacing a terminal's hardware and presenting it to customers as legitimate in order to collect card numbers and PINs.

43.2 Biometrics

Category 43.2 Biometrics

2006-01-05 EDUPAGE; http://www.fcw.com/article91877-01-05-06-Web

US-VISIT WANTS ALL 10 FINGERS PRINTED

Officials at the Department of Homeland Security (DHS) have announced a plan to begin requiring visitors to the United States to have all 10 of their fingers to be printed to be admitted to the country. Currently, the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program requires prints of two fingers; the change to 10 will reportedly increase both security and privacy and will decrease the number of visitors who must undergo a second inspection to enter or leave the country. DHS said biometric technology such as fingerprinting is already reliable, but the agency is working with technology vendors to develop products that are more accurate, faster, and more mobile.

Category 43.2 Biometrics

2006-01-18 INNOVATION (Popular Science Dec 2005) <http://www.popsci.com>

SMART GUN

Researchers at the New Jersey Institute of Technology are close to completion of the first commercially viable "smart gun," designed to recognize authorized users' grips. When seized by an unauthorized person -- like a child or a criminal -- the shooting mechanism automatically locks up. The secret is Dynamic Grip Recognition biometric technology embedded in the gun's handle. Sensors and microprocessors analyze the user's complex interplay of muscular tension and bone movement involved in pulling the trigger. "The way you hold a gun, curl your fingers, contract your hand muscles as you pull the trigger -- all of those measurements are unique,"
says NJIT VP Donald Sebastian, who says he expects commercial rollout in 2008. Buyers of the weapon would program it at a local police station's firing range by shooting 10 times, allowing microprocessors to analyze the data and create a permanent profile of the authorized user's grip.

Category 43.2 Biometrics

2006-02-23 DHS Daily OSIR; http://www.networkworld.com/news/2006/022706-fingerprint-security.html

RESEARCHERS CLAIM ADVANCES IN USING FINGERPRINTS TO SECURE NETWORKS.

University of Buffalo, NY, researchers say they have found a way to improve security of wireless handheld devices and Websites. The research specifies how big a keypad sensor needs to be and how big a fingerprint image should be, as a key shortcoming of biometric systems now is that sensors often only can take partial fingerprints, says Venu Govindaraju, a University of Buffalo professor of computer science and engineering, and director of the school's Center for Unified Biometrics and Sensors (CUBS). The researchers' work has been published in the journal Pattern Recognition.

Category 43.2 Biometrics

2006-03-06 DHS Daily OSIR; http://www.computerworld.com/securitytopics/security/holes/story/0,10801,109276,00.html

RESEARCHER HACKS MICROSOFT FINGERPRINT READER.

A security researcher with the Finnish military has shown how they could steal your fingerprint, by taking advantage of an omission in Microsoft Corp.'s Fingerprint Reader, a PC authentication device that Microsoft has been shipping since September 2004. Although the Fingerprint Reader can prevent unauthorized people from logging on to your PC, Microsoft has not promoted it as a security device. Hoping to understand why Microsoft had included the caveat about sensitive data, a researcher with the Finnish military, Mikko Kiviharju, took a close look at the product. In a paper presented at the Black Hat Europe conference last week, he reported that because the fingerprint image taken by the scanner is not encrypted, it could be stolen by hackers and used to inappropriately log in to a computer. Because the fingerprint image is transferred unencrypted from the Fingerprint Reader to the PC, it could be stolen using a variety of hardware and software technologies, called "sniffers," that monitor such traffic, said Kiviharju. Kiviharju's report: http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Kiviharju/bh-eu-06-kiviarju.pdf.

Category 43.2 Biometrics

2006-03-29 INNOVATION (Sci-Tech Today 14 March 2006) <http://www.sci-tech-today.com/news/Talking-Computers-Around-the-Corner/story.xhtml?story_id=033003ON4PO9>

HAL, IS THAT YOU? SPEECH RECOGNITION USE SPREADS

If you've ever been struck in "voice mail hell," it may seem hard to imagine, but voice recognition software has made tremendous strides in the past five years. Interactive voice response (IVR) technology is getting closer to interpreting speech the way humans do. So it probably shouldn't come as a surprise that IVR systems are spreading beyond the call center into fields like entertainment, health, business and security. In the court system and health care, for example, improved technology has led to more-accurate transcriptions. IVR is also getting so good at recognizing emotion and articulation, it's being used to interview prospective employees, and even screen potential dates. A UK-based dating Web site now offers a "Love Detector" voice analysis system developed by the Israeli Security Service. It can supposedly detect 129 distinct emotional layers in a person's voice, including excitement, confusion, stress, concentration and anticipation. That's supposed to help you gauge the "passion level" of a romantic prospect. Do you get frustrated talking to disembodied voices?
Soon they'll able to change scripts when they detect frustration in a caller's voice. "I can imagine a time when you call somewhere for support or you do an interview, and you're not sure if you're talking to a real person or not," said Ron Selewach, founder of the Human Resource Management Center.

Category 43.2 Biometrics

2006-05-22 DHS Daily OSIR; Finextra http://finextra.com/fullstory.asp?id=15341

EUROPEANS WILLING TO SWITCH BANKS FOR BIOMETRIC AUTHENTICATION

Over half of banking customers across Europe would be willing to switch their accounts to financial institutions that offer biometric authentication services, according to a study conducted by Vanson Bourne and commissioned by LogicaCMG. The study, which spans seven European countries, shows that 57 percent of people would be more likely to change their current account provider if all it took was an identity card and fingerprint to establish and prove identity. In Germany this average increases to 64 percent, says LogicaCMG. LogicaCMG says the research reveals that the introduction of biometrics could lead to much greater consumer confidence in switching between different bank accounts and other financial products. Commenting on the research, Paul Gribbon, of LogicaCMG says as banks have to proliferate across channels such as digital television, the Internet, telephone banking systems, and physical branches, biometrics will be a key method in establishing and verifying the identity of customers.

Category 43.2 Biometrics

2006-06-02 EDUPAGE; Inside Higher Ed http://www.insidehighered.com/news/2006/06/02/proctor

SOLVING THE PROBLEM OF DISTANCE EXAMS

Troy University is looking to technology to solve a problem created by technology. Working with a company called Software Secure Inc., officials at Troy are directing the development of an electronic proctor to oversee distance students when they take exams. The device, called Securexam Remote Proctor, sits next to a student's computer and connects through the Internet to the host campus. Students verify themselves by using a fingerprint reader in the device, which also includes a camera and a microphone that let instructors watch and hear students remotely as they take tests. Sallie Johnson, director of instructional design and education technologies, said the Remote Proctor "allows faculty members to have total control over their exams." The device is expected to cost about $200, and multiple students would be able to use the same device for different exams. Some said the device is unnecessary. Brian Douglas, chief technology officer for Umass Online, called it "an intrusion into a student's life." He said the incidence of cheating among distance students is often overstated, noting that his institution relies on the honor code and tests that make cheating difficult.

Category 43.2 Biometrics

2006-09-07 DHS Daily OSIR; Finextra (UK) http://finextra.com/fullstory.asp?id=15820

DIEBOLD RELEASES BRANCH-BASED FINGERPRINT SCANNING SYSTEM.

Diebold is releasing a biometric fingerprint scanning system designed to enable banks to authenticate the identity of customers at the branch counter. The IdentiCenter system links a customer's identity and account information to their unique fingerprint profile. Upon initiating a transaction at the branch counter, customers place their finger on an optical-scan fingerprint reader to verify their identity. The technology is designed to provide added protection for financial institutions and consumers against identity theft during branch-based financial transactions.

Category 43.2 Biometrics

2006-10-11 INNOVATION (The Guardian 28 Sep 2006) <http://technology.guardian.co.uk/weekly/story/0,,1882014,00.html>

ARE CLICKPRINTS THE KEY TO PREVENTING ONLINE ID THEFT?

Now there's a new way to track your online activities -- through your "clickprint," defined in a recently published paper as "a unique pattern of Web surfing behavior based on actions such as the number of pages viewed per session, the number of minutes spent on each page, the time or day of the week the page is visited, and so on." The authors, Wharton School professor Balaji Padmanabhan and University of California, Davis professor Catherine Yang, suggest that the manner in which a user roams an e-commerce site over several sessions, could enable that company to distinguish him or her from another anonymous surfer. "The paper is really a proof of concept that behavior and minimal information can be used to identify users," says Yang. And that might be handy in preventing fraud: if someone signed onto a site using another person's logon, but the clickprint differed, it could raise a red flag signaling possible ID theft. Whether or not that will engender an uproar over privacy issues is yet to be determined, says Padmanabhan.

Category 43.2 Biometrics

2006-10-24 DHS Daily OSIR; CNET News http://news.zdnet.com/2100-1009_22-6129174.html

TELEPHONE BANKING SYSTEM RECOGNIZES YOUR VOICE.

A system by RSA Security designed to help fight telephone banking fraud adds voice as a way for automated telephone banking services to identify users. "As we are strengthening security for the Web channel, phone banking is effectively becoming the next big target," said Christopher Young of RSA. The system generates a risk score by looking at the voiceprint as well as other parameters, such as the phone number and user behavior profiles, RSA said. Low-risk transactions proceed uninterrupted, while transactions with a high-risk score are verified with an additional layer of security, such as secret questions, it said. Current phone authentication techniques lack security, as they are typically conducted semi-manually, and are susceptible to social engineering attacks, RSA said. Crooks are learning to take advantage of that, it added.

Category 43.2 Biometrics

2006-11-21 DHS Daily OSIR; IDG News Service http://www.infoworld.com/article/06/11/21/HNcitibankbiometrics_1.html

CITIBANK DEBUTS BIOMETRIC PAY SYSTEM.

Citibank this month began rolling out biometric payment systems in Singapore that allow Citibank Clear Platinum credit card holders to pay using their fingerprints. "It's an investment for our future," said Anand Cavale of Citibank Singapore, noting this is the first time the bank has used a biometric payment system anywhere in the world. Before putting the biometric system into operation, Citibank officials took a long hard look at whether the system was secure -- and came away satisfied that it was, Cavale said. "We see this as the next step, which will enhance our already good fraud prevention systems," he said. But don't expect to see biometrics replace Citibank cards any time soon. "The technology will be used in conjunction with a credit card," Cavale said. So far, Citibank's biometric payment systems are only in place at a handful of outlets in Singapore, including local coffee shops. But the bank has plans to quickly expand the number of such systems and the number of Citibank card holders able to use them. "Our intention is to roll it out very quickly to other cards," Cavale said.

Category 43.2 Biometrics

2007-01-24 INNOVATION (Wired 19 Jan 2007) <http://www.wired.com/news/technology/0,72284-0.html?tw=wn_index_22>

BIOMETRIC ATMs

A pilot program in Chennai, India, is bringing 15 biometric ATMs to village kiosks in five districts across southern India. About 100,000 workers will have access to the machines, using fingerprint scanners, rather than ATM cards and PINs, to access their funds. Biometric ATMs are already deployed in Colombia and Japan, but have not caught on in the rest of the world. Officials hope that by giving rural poor access to e-banking, it will increase the number of rupees in national circulation while decreasing the opportunity for corruption by eliminating middlemen who often siphon off government-allocated funds earmarked for low-income workers. "The whole structure is designed so that only the people at the end get the money. No one in between can steal it along the way," says Nagaraj Mylandla, managing director of Financial Software and Systems, which helped design the machines' security protocol.

43.3 Passwords

Category 43.3 Passwords

2006-03-08 RISKS

AUSTRALIAN NATIONAL CREDIT UNION LIMITS INTERNET PASSWORD KEYSPACE

A RISKS correspondent noted, "A step backwards for customers of Australian National Credit Union (www.friendlybanking.com.au) where from 21 Mar 2006 all users of the credit union's Internet banking will be limited to choosing passwords of six characters, consisting only of the numbers 0-9. They have previously had the ability to choose alpha-numeric passwords of varying length.

The credit union's website claims that the changes are for enhanced security. . . ." The correspondent added, "After I enquired about this apparent backward step, the credit union's response claimed this was required for the implementation of two-factor authentication, amongst other security enhancements. Two-factor authentication might be great for those who use it, but those that don't will be left with the limited password options."

Category 43.3 Passwords

2006-03-08 RISKS http://catless.ncl.ac.uk/Risks/24.19.html#subj12

INSECURE APC BIOPOD ILLUSTRATES PROBLEMS WITH UNTRAINED STAFF

Gabe Goldberg provided a depressingly believable tale of wooden-headed stupidity in the face of his analysis of a design flaw in the APC "BioPod" password vault. The device provides biometric access control with or without a password. The password is derived automatically from the Windows password -- and Mr Goldberg correctly pointed out to the company that it accepts a null Windows password without warning the user that there is therefore no master password loaded on the device. Nothing he could say to the technical support person he spoke to could overcome the stock repetition of the very flaw he was trying to report. In the infuriating display of stubborn denial that characterizes very stupid people, the agent simply kept repeating the presumably written description of exactly what was wrong as if it were an explanation. Perhaps the best line in the entire dialog was "Officially the BioPod is not advertised as a security device, but a password manager, so it is not designed to increase the security of your computer, but provide a safe way to manage and store your passwords."

[MK adds: this design flaw also raises questions about the security experience of the people who designed the software.]

Category 43.3 Passwords

2006-05-08 DHS Daily OSIR; http://www.securityfocus.com/bid/16743/discuss

CISCO SECURE ACS INSECURE PASSWORD STORAGE VULNERABILITY.

Cisco Secure ACS is susceptible to an insecure password storage vulnerability. Analysis: With the master key, the user can decrypt and obtain the clear text passwords for all ACS administrators. With administrative credentials to Cisco Secure ACS, it is possible to change the password for any locally defined users. This may be used to gain access to network devices configured to use Cisco Secure ACS for authentication. If remote registry access is enabled on a system running Cisco Secure ACS, it is possible for a user with administrative privileges typically domain administrators to exploit this vulnerability. For a complete list of vulnerable products: http://www.securityfocus.com/bid/16743/info ACS 3.x for UNIX, and ACS 4.0.1 for Windows are not affected this issue. For more information: http://www.securityfocus.com/bid/16743/references

43.4 Kerberos

Category 43.4 Kerberos

2007-01-09 DHS Daily OSIR; US-CERT http://www.uscert.gov/cas/techalerts/TA07-009B.html

TECHNICAL CYBER SECURITY ALERT TA07-009B: MIT KERBEROS VULNERABILITIES.

The MIT Kerberos administration daemon contains two vulnerabilities that may allow a remote, unauthenticated attacker to execute arbitrary code. US-CERT is are aware of two vulnerabilities that affect the Kerberos administration daemon: Kerberos administration daemon fails to properly initialize function pointers and Kerberos administration daemon may free uninitialized pointers. These vulnerabilities are addressed in MIT krb5 Security Advisory 2006-002 and MIT krb5 Security Advisory 2006-003. Patches for these issues are also included in those advisories.

Category 43.4 Kerberos

2007-04-03 DHS Daily OSIR; US-CERT http://www.us-cert.gov/cas/techalerts/TA07-093B.html

TECHNICAL CYBER SECURITY ALERT TA07-093B: MIT KERBEROS VULNERABILITIES.

The MIT Kerberos 5 implementation contains several vulnerabilities. One of these vulnerabilities (VU#220816) could allow a remote, unauthenticated attacker to log in via telnet (23/tcp) with elevated privileges. The other vulnerabilities (VU#704024, VU#419344) could allow a remote, authenticated attacker to execute arbitrary code on a Key Distribution Center (KDC). Users should check with vendors for patches or updates. Alternatively, apply the appropriate source code patches referenced in MITKRB5-SA-2007-001, MITKRB5-SA-2007-002, and MITKRB5-SA-2007-003 and recompile. These vulnerabilities will also be addressed in krb5-1.6.1.
US-CERT Vulnerability Note VU#220816: http://www.kb.cert.org/vuls/id/220816
US-CERT Vulnerability Note VU#704024: http://www.kb.cert.org/vuls/id/704024
US-CERT Vulnerability Note VU#419344: http://www.kb.cert.org/vuls/id/419344
MIT krb5 Security Advisory 2007-001:
http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2007-0 01-telnetd.txt
MIT krb5 Security Advisory 2007-002:
http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2007-0 02-syslog.txt
MIT krb5 Security Advisory 2007-003:
http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2007-0 03.txt

43.6 E-mail authentication (e.g., SPF & SenderID)

Category 43.6 E-mail authentication (e.g., SPF & SenderID)

2006-04-19 DHS Daily OSIR; http://news.com.com/Danger+Authenticating+e-mail+can+break+it/2100-7349_3-6062953.html?tag=nefd.lede

DANGER: AUTHENTICATING E-MAIL CAN BREAK IT.

The promise of e-mail authentication is too good to ignore, but if it is implemented incorrectly it will break a company's mail system instead of fixing it, experts have cautioned. "Deploy smart. Don't just do it," Erik Johnson, a secure messaging executive at Bank of America, said in a presentation at the Authentication Summit Wednesday, April 19. "If you just do it, you may just break it." For the past two years, the technology industry has been advocating the use of systems to guarantee the identity of e-mail senders. It sees such authentication as key to the fight against spam and phishing, as it should help improve mail filters and make it harder for senders to forge their addresses. The industry also likes to advertise that these systems have practically no cost. The key problem for large companies is figuring out all the systems that send e-mail on their behalf, said Paul Judge, chief technology officer at e-mail security company CipherTrust. "If you are a large multinational organization, you may have e-mail gateways in 10 countries, you may have marketing companies that send e-mail on your behalf," he said.

Category 43.6 E-mail authentication (e.g., SPF & SenderID)

2007-05-17 DHS Daily OSIR; Finextra (UK) http://finextra.com/fullstory.asp?id=16929

SWIFT LAUNCHES SECURE E-MAIL SERVICE.

Financial messaging network Swift has launched SwiftNet Mail, a secure e-mail product that operates on the IP-based SwiftNet network rather than the Internet. The interbank co-operative said last October that it was moving into the person-to-person messaging market and was piloting its SwiftNet Mail service with a number of banks. The service allows users to securely transmit messages containing sensitive data over SwiftNet using the e-mail package of their choice. Messages are despatched between member banks via SwiftNet using a software program that sits on the SwiftAlliance interface device. Swift says the service eliminates the need for complex push-server and desktop client software and claims the network is free from spam and phishing threats.

43.7 IPv6 & Internet2

Category 43.7 IPv6 & Internet2

2006-01-09 DHS Daily OSIR; http://www.compliancepipeline.com/news/175803121

IPV6: WORLD'S LARGEST TECHNOLOGY UPGRADE ON DECK

Bugs, spam, viruses, software security issues, quality of service and more have spurred experts to push for commercial deployment and government reform on Internet Protocol version 6 (IPv6). A panel battled the topic of when companies should deploy IPv6 and where the technology will make the greatest impact. The discussion took place at the 2006 International Consumer Electronics show in Las Vegas, NV, last week. In the end, the four panelists agreed to disagree. IPv6, the latest version of Internet Protocol, provides more IP addresses than today's version 4. It supports auto-configuration to help correct most shortcomings in the current version, and has security, quality of service, digital rights management and mobile communications features. The debate has heated up in the U.S. now that Asian countries are mandating adoption where IP addresses are in short supply. The U.S. government and the Department of Defense, two of IPv6's strongest proponents, are estimated to spend billions to make the transition happen. The White House Office of Management and Budget has directed U.S. federal agencies to develop IPv6 transition plans by February and requires that agencies comply with the mandate by June 2008.

Category 43.7 IPv6 & Internet2

2006-06-15 EDUPAGE; Chronicle of Higher Education (sub. req'd)
http://chronicle.com/daily/2006/06/2006061501t.htm
<http://www.educause.edu/email/edupage/ep061606/track.asp?id=story_1>

INTERNET2 PROVIDES DETAILS OF ABILENE REPLACEMENT

Following a decision to let its current contract with Qwest expire in 2007, Internet2 has announced that the network that will replace Abilene will be built by Level 3 Communications and Internet2. Douglas Van Houweling, president of Internet2, said that in addition to common Internet transmissions, the new network will allow researchers to establish high-speed circuits for special demands on an as-needed basis. Harvey Newman, physics professor at the California Institute of Technology, said that offering researchers a somewhat dynamic network, one that can be modified and adjusted to meet varying demands, will "spark creativity in the way we exploit networks." Van Houweling said that the costs to Internet2 member institutions will not change considerably when the new network debuts. Internet2's new network is expected to be running in about a year.

Category 43.7 IPv6 & Internet2

2006-08-11 DHS Daily OSIR; Security Focus http://www.securityfocus.com/news/11406?ref=rss

COVERT CHANNEL TOOL HIDES DATA IN IPV6.

An independent security researcher showed off an early version of a tool for creating covert channels that, he claims, can pass undetected through most firewalls and intrusion detection systems. The tool, dubbed VoodooNet or v00d00n3t, uses the ability of most computers to encapsulate next-generation network traffic, known as Internet Protocol version 6 (IPv6), inside of today's network communications standard, or IPv4. Because most security hardware appliances and host-based intrusion detection programs have not been programmed to inspect IPv6 packets in depth, data can bypass most network security, said independent security researcher Robert Murphy, who presented the tool at the DEFCON hacking conference last weekend. The tool uses Internet Control Message Protocol version 6, or ICMPv6, to send ping packets from one computer to another, hiding information in certain fields of the packets without violating any existing Internet Request for Comment, said Joe Klein, a network expert with the North American IPv6 Task Force and a senior security consultant with Honeywell. Klein believes that the communications would not be detected by existing IPv4 devices, and that bot nets, among other threats, could use the technology for stealthier command and control channels.

Category 43.7 IPv6 & Internet2

2006-10-05 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article96365-10-05-06-Web

ADVISORY BOARD FOR NEXT-GENERATION INTERNET FORMED.

The Computing Research Association (CRA), at the request of the federal government, has formed an advisory board to help guide the design of a next-generation Internet. The nonprofit group's involvement is part of a new National Science Foundation initiative, called the Global Environment for Networking Innovations (GENI). GENI will be an experimental facility that tests possible architectures for a new and improved World Wide Web.

Category 43.7 IPv6 & Internet2

2007-02-20 DHS Daily OSIR; Government Computer News
http://www.gcn.com/online/vol1_no1/43184-1.html

MANY UNKNOWNS REMAIN IN MOVE TO IPV6.

On Tuesday, February 20, a panel of government and industry experts met during the IPv6 Tech Forum in Virginia to discuss uses for the new IPv6-enabled networks and the challenges users will face. The Department of Defense, along with civilian agencies, has set a goal of transitioning its networks to the next generation of Internet Protocols by July 2008. But a successful transition to IPv6 will merely establish parity with existing networks. The return on the investment will depend on how applications take advantage of the new functionality. Unfortunately, there still are many unanswered questions about what will happen when networks begin using IPv6. The federal government is a major driver in the industry's move to IPv6, because it has been requiring functionality for the new protocols in its networking equipment. The business rationale for moving to IPv6 will be improved productivity or functionality. The opportunity to strip proprietary protocols out of legacy systems and build everything on IPv6 should save money on licensing and simplified application development. But the steep learning curve in managing networks with the new protocols could delay these benefits. IPv6 Tech Forum: http://www.afcea.org/committees/technology/techforum/

Category 43.7 IPv6 & Internet2

2007-02-22 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article97731-02-22-07-Web

GSA CONSIDERS ESTABLISHING IPV6 PROGRAM OFFICE.

With the deadline for agencies to be IP Version 6-ready set for mid-2008, General Services Administration (GSA) officials are considering establishing a program office to guide GSA's compliance, and according to John Johnson, GSA's assistant commissioner for Integrated Technology Service, something could develop in the next several months. The Office of Management and Budget mandated in 2005 that agencies have an IPv6-ready network backbone by June 2008. Continuing on an evolution to IPv6-capable IT systems makes the deadline only a starting point, administration officials working closely with IPv6 transitions have said. Officials are mulling over what the office would do, specifically what its goals and objectives would be. They are analyzing the migration's size and complexity regarding GSA's Networx contract, governmentwide acquisition contract programs and Schedules.

Category 43.7 IPv6 & Internet2

2007-03-14 DHS Daily OSIR; CNET News.com
http://news.com.com/OpenBSD+hit+by+critical+IPv6+flaw/2100-1002_3-6167193.html

OPENBSD HIT BY IPV6 FLAW.

A vulnerability in the way OpenBSD handles IPv6 data packets opens systems running the traditionally secure open-source operating system to serious attack. A memory corruption vulnerability error exists in the OpenBSD code that handles IPv6 packets, Core Security Technologies said in an alert published Tuesday. Exploiting the flaw could let an attacker commandeer a vulnerable system, according to Core, which said it discovered the issue and crafted sample exploit code. Security update: http://www.openbsd.org/errata40.html

Category 43.7 IPv6 & Internet2

2007-05-09 DHS Daily OSIR; Security Focus http://www.securityfocus.com/news/11463

EXPERTS SCRAMBLE TO QUASH IPV6 FLAW.

A flawed feature that could amplify denial-of-service attacks on next-generation networks has vendors and engineers rushing to eliminate the potential security issue. This week, experts sent two drafts to the Internet Engineering Task Force (IETF)--the technical standards-setting body for the Internet--proposing different ways of fixing a problem in the way that Internet Protocol version 6 (IPv6) allows the source of network data to determine its path through the network. The drafts recommend that the IPv6 feature should either be eliminated or, at the very least, disabled by default. The specification, known as the Type 0 Routing Header (RH0), allows computers to tell IPv6 routers to send data by a specific route. Originally envisioned as a way to let mobile users to retain a single IP for their devices, the feature has significant security implications. During a presentation at the CanSecWest conference on April 18, researchers Philippe Biondi and Arnaud Ebalard pointed out that RH0 support allows attackers to amplify denial-of-service attacks on IPv6 infrastructure by a factor of at least 80. IETF: http://www.ietf.org/

45.1 PKI (Digital signatures / certificates)

Category 45.1 PKI (Digital signatures / certificates)

2006-03-23 DHS Daily OSIR; http://securitytracker.com/alerts/2006/Mar/1015813.html

VERISIGN MANAGED PKI INPUT VALIDATION FLAW IN 'HAYDN.EXE' PERMITS CROSS-SITE SCRIPTING ATTACKS.

A vulnerability was reported in VeriSign's Managed PKI. A remote user can conduct cross-site scripting attacks. Analysis: The 'haydn.exe' script does not properly filter HTML code from user-supplied input before displaying the input. A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The code will originate from the site running the Managed PKI software and will run in the security context of that site. As a result, the code will be able to access the target user's cookies (including authentication cookies), if any, associated with the site, access data recently submitted by the target user via Web form to the site, or take actions on the site acting as the target user. Affected version: 6.0. Solution: The vendor indicates that, as a solution, a default HTML file must be constructed by creating a blank html file in the '/htmldocs/' directory labeled 'fdf_noHTMLFile.html'.

Category 45.1 PKI (Digital signatures / certificates)

2007-03-07 DHS Daily OSIR; CNET News http://news.com.com/Bug+may+expose+encrypted+e-mail/2100-1002_3-6165277.html

BUG MAY EXPOSE ENCRYPTED E-MAIL.

A problem related to a widely used open-source cryptography technology could let miscreants tamper with digitally signed and encrypted e-mails. The problem lies in how certain e-mail applications display messages signed using the GNU Privacy Guard, also known as GnuPG and GPG, the GnuPG group said in a security alert Tuesday, March 6. It may not be possible to identify which part of a message is actually signed if GPG is not used correctly, it said. This poses a risk to those who use the cryptographic technology to authenticate or encrypt e-mail messages. According to security company Core Security Technologies, the affected applications include KDE's KMail, Novell's Evolution, Sylpheed, Mutt and GnuMail.org, and Enigmail. The GnuPG group has issued updates to prevent tampering with signed or encrypted messages, but it notes that individual e-mail applications might need updating as well, to correctly display signed messages after applying the GPG update. Enigmail software has already been updated.

45.2 Digital cash, cash cards

Category 45.2 Digital cash, cash cards

2006-05-16 DHS Daily OSIR; Finextra http://finextra.com/fullstory.asp?id=15319

PRE-PAID INTERNET PAYMENT CARD LAUNCHED IN THE UK

A plastic payment card that can be loaded with funds at e-pay mobile top-up terminals and used to pay for purchases made via the Internet has been launched in the UK. TeleGlobal says its new Snap card will enable customers who do not have a credit or debit card, or do not want to use their credit card on the Internet, to make online purchases. Erik Holst-Roness, chief executive of TeleGlobal, says: "The kind of people who will benefit range from kids who want to download music and games, to the thousands of families without credit cards, to people who don't want to put their credit details on the Internet or those who just want to make their online purchases private." He says online merchants can now connect with an entirely new group of consumers without the fear of fraud.

Category 45.2 Digital cash, cash cards

2007-01-15 DHS Daily OSIR; BusinessWeek
http://www.businessweek.com/magazine/content/07_03/b4017054.htm

PITFALLS OF GIFT CARDS.

In the biggest year for gift cards ever, with annual sales rising seven percent, to $53 billion, according to researchers Mercator Advisory Group, buyers and receivers are learning the pitfalls of the prepaid cards issued by retailers. Fraud schemes generally fall into three basic types: stealing data such as bar codes and magnetic strip information, planting data, and indulging in checkout scams. Thieves may copy data off unsold cards, then use the store's Website or 800 number to check their status. Once the cards are bought and loaded with dollars, crooks use the data to buy goods online or to create bogus cards. Other scammers clone cards they own and plant the copies in stores to be sold. When the cards are activated, the money goes onto the thieves' cards. Employees may also pretend a card is empty or deactivated and persuade the customer to hand over the "worthless" card, hoping to use it later. They may just swap them, pocketing activated cards at the register while slipping customers look-alikes. Or they may clone cards using information off discarded receipts.

45.4 E-payments; e.g., credit-cards, e-brokers

Category 45.4 E-payments; e.g., credit-cards, e-brokers

2006-06-21 DHS Daily OSIR; Computing (UK) http://www.computing.co.uk/computing/news/2158771/rbs-trials-rfid-payment-cards

BANK OF SCOTLAND TO CUT WAITING LINES WITH RFID CARDS.

The Royal Bank of Scotland (RBS) has this week started testing RFID-equipped payment cards to reduce waiting lines in shops. The bank is working with MasterCard to test the contactless card payment system at its Edinburgh headquarters. A third of RBS's 3,000 staff have been issued with the cards, which allow them to pay for goods costing less than approximately US$10. Microscopic antennas fitted into the cards will allow employees to pay for goods by pressing the Maestro card onto a reader. Eight retail outlets, including Starbucks, Tesco, and a hairdresser's are participating in the pilot and have had their systems fitted with RFID reader pads. While payments using the contactless wipe method do not require pilot participants to enter a PIN security number, the bank will carry out random checks during the trial. MasterCard is carrying out a number of other tests with other banks across the world.

Category 45.4 E-payments; e.g., credit-cards, e-brokers

2006-07-04 DHS Daily OSIR; Finextra http://finextra.com/fullstory.asp?id=15532

PAYPAL TO ROLL OUT VIRTUAL DEBIT CARD.

PayPal is set to roll out a new virtual debit card system to millions of account holders. The virtual card will function like a regular debit card and enable customers to shop online with the funds in their PayPal accounts at any e-merchant that accepts MasterCard cards. The system generates single use account numbers and one-time card verification codes that are linked to customers' PayPal accounts. To use the system, a customer downloads an application that is added to the toolbar in a Web browser. When they want to use the virtual card, the application generates a pre-populated form for payment which includes the single-use MasterCard number and card verification code which is connected to their PayPal account. A PayPal spokesperson said that the virtual card will enable customers to use their person-to-person payment accounts with merchants that don't currently accept its payment system. The functionality is likely to be rolled out to the firm's 105 million accountholders by the end of the year.

Category 45.4 E-payments; e.g., credit-cards, e-brokers

2006-07-22 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,1993067,00.asp

VISA CHANGES RETAIL SECURITY RULES.

Visa on Friday, July 21, changed its retail security requirement structure, which will -- because of a change in definition of what a qualifying transaction is -- force more retailers to use its more stringent security procedures. The core change includes all transactions when determining what level a retailer should be; Visa uses four levels to group retailers based on their volume of transactions. The criteria was previously limited to online purchases. "The most significant modification involves the Level 2 merchant category, which previously only applied to merchants processing between 150,000 and six million Visa e-commerce transactions per year," a Visa statement said. "Level 2 has now been broadened to include all acceptance channels and applies to any merchant processing one million to six million Visa transactions per year." Visa statement: http://www.usa.visa.com/about_visa/newsroom/press_releases/n r325.html

Category 45.4 E-payments; e.g., credit-cards, e-brokers

2006-10-24 DHS Daily OSIR; Register (UK)
http://www.channelregister.co.uk/2006/10/24/rfid_credit_card_hack/

HACKING CONTACTLESS CREDIT CARDS MADE EASY.

U.S. security researchers have demonstrated how easy it might be for crooks to read sensitive personal information from RFID-based credit and debit cards. Researchers from the RFID Consortium for Security and Privacy have shown how crooks might be able to skim sensitive information from cards -- including card number, expiration, and issue dates, and a cardholder's name -- without actually physically stealing the latest generation of credit cards. The attack uses off-the-shelf radio and card reader equipment that could cost as little as $150. Although the attack fails to yield verification codes normally needed to make online purchases, it would still be possible for crooks to use the data to order goods and services from online stores that don't request this information. Despite assurances by the issuing companies that data contained on RFID-based credit cards would be encrypted, the researchers found that the majority of cards they tested did not use encryption or other data protection technology.

45.5 Digital-rights management (DRM); e.g., copy protection, digital watermarks

Category 45.5 Digital-rights management (DRM); e.g., copy protection, digital watermarks

2006-11-15 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/06/11/15/HNpiratedvistauseless_1.html

PIRATED VISTA MAY BE USELESS, MICROSOFT SAYS.

Microsoft said supposedly pirated copies of its new Vista computer operating system "will be of limited value" to those who use them. Microsoft responded Tuesday, November 14, to reports that some Websites have been circulating pirated copies of Vista and the Office 2007 applications suite. But Microsoft said in a prepared statement that those pirated copies of the OS won't work for long. "The copies available for download are not final code and users should avoid unauthorized copies which could be incomplete or tampered. This unauthorized download relies on the use of pre-RTM [release-to-manufacture] activation keys that will be blocked using Microsoft's Software Protection Platform. Consequently, these downloads will be of limited value," the statement said.

Category 45.5 Digital-rights management (DRM); e.g., copy protection, digital watermarks

2007-01-17 Effector Online http://www.freedom-to-tinker.com/?p=1104

FELTEN: NEXT GEN DVD DRM WILL BE BROKEN WIDE OPEN.

HD-DVD and Blu Ray discs haven't been on the market for long, but a tool called BackupHDDVD is already available to help users evade the discs' DRM. Is this tool the end of the AACS encryption scheme, or will the movie studios be able to repair the hole? Computer security experts Ed Felten and Alex Halderman have the answer in a series of posts that puts in layman's terms how AACS works and how it might be attacked. The bottom line: "[BackupHDDVD] isn't a big deal by itself, but it is the first step in the meltdown of AACS."
For the series on BackupHDDVD: http://www.freedom-to-tinker.com/?p=1104

45.6 Smart cards & other e-commerce security measures

Category 45.6 Smart cards & other e-commerce security measures

2006-07-24 DHS Daily OSIR; Register (UK)
http://www.theregister.co.uk/2006/07/24/unsolicited_credit_card_push/

UNSOLICITED CREDIT CARD PUSH IRKS SECURITY RESEARCHERS.

A top UK security expert has criticized the practice of issuing unsolicited credit cards. Professor Ross Anderson of Cambridge University reports how his wife recently received a pre-approved, unsolicited Gold Mastercard from UK store Debenhams. Cutting up the card and throwing it in the bin simply doesn't pass muster, he argues. For one thing, the UK's move to Chip and PIN on plastic cards as an alternative to signature-authorized transactions complicates the problem of disposing of unwanted plastic cards. "The average customer has no idea how to 'cut up' a card now that it's got a chip in it," he writes. According to Anderson, bisecting the plastic using scissors leaves the chip functional. Anderson's statement: http://www.lightbluetouchpaper.org/2006/07/20/new-card-security-problem/

Category 45.6 Smart cards & other e-commerce security measures

2006-10-23 EDUPAGE; New York Times (registration req'd)
http://www.nytimes.com/2006/10/23/business/23card.html

RESEARCHERS QUESTION SECURITY OF NO-SWIPE CARDS

Using a scanner built from commonly available components, researchers at the University of Massachusetts, Amherst, were able to retrieve sensitive data from credit cards that use RFID technology. Creditors have issued millions of such cards, saying that they can speed transactions, and many retailers now have technology that accepts the cards, which, instead of being swiped, transmit cardholder and account information through radio waves. Supporters of the technology, including major credit card companies, argue that scanners must be within a few inches of a card to read it and that data on the cards is typically encrypted. Other tests have shown that often the data on RFID chips can be read several feet away, and the researchers in this test pointed out that even if closer proximity is necessary, someone could walk among people in a crowd and easily get within a few inches of credit cards in wallets and purses. Although the test was of a relatively small sample, the researchers also found that many of the cards transmit name and card number without encryption or with encryption that was easily cracked. Tom Heydt-Benjamin, a graduate student and one of the researchers, compared the situation to walking down a street "wearing your name, your credit card number, and your card expiration date on your T-shirt."

Category 45.6 Smart cards & other e-commerce security measures

2007-02-06 DHS Daily OSIR; CNET News http://news.com.com/U.K.+researchers+devise+smart-card+hack/2100-7349_3-6156601.html

UK RESEARCHERS DEVISE SMART-CARD HACK.

Two Cambridge researchers have created a scenario in which hackers can bypass the latest bankcard security measures. Saar Drimer and Steven Murdoch, members of the Cambridge University Computer Laboratory, demonstrated last month how they could modify a supposedly tamper-proof chip-and-PIN payment terminal to play Tetris. They have now extended the hack to demonstrate how they can compromise the system by relaying card information between a genuine card and a fake one. Chip and PIN, a government-backed initiative introduced last year in England, is a security measure in which a customer must enter a four-digit code when they use a credit or debit card for face-to-face transactions. "Chip and PIN currently does not defend against this attack, despite assertions from the banking community that customers must be liable for frauds in which the PIN was used," the researchers said in an as-yet-unpublished paper. "When customers pay with a chip and PIN card, they have no choice but to trust the terminal when it displays the amount of the transaction. The terminal, however, could be replaced with a malicious one, without showing any outward traces," the researchers warned in their paper. Prototype attack details: http://www.cl.cam.ac.uk/research/security/projects/banking/r elay/

Category 45.6 Smart cards & other e-commerce security measures

2007-03-01 DHS Daily OSIR; Boston Globe
http://www.boston.com/business/globe/articles/2007/03/01/firms_prodded_to_try_smarter_credit_cards/

FIRMS PRODDED TO TRY SMARTER CREDIT CARDS.

Faced with increasing threats of theft of consumer data, credit-card companies are rolling out higher security plastic. European and Asian banks in recent years have spent billions of dollars to make the switch to credit and debit cards containing a tiny microprocessor chip that stores encrypted customer information and requires a personal identification number, or PIN. American financial institutions also are starting to offer similar so-called smart cards that promise to better protect consumer data following credit- and debit-card theft from retailers. Most American banks and card networks use cards with magnetic stripes which are coded with information, such as customer names and account numbers, and allow merchants to quickly authorize a transaction over phone lines with a single swipe of a card through a computer. But the data on the magnetic stripes is relatively easy for thieves to copy. The chips, like those on cards in Europe, store encrypted data to make it harder for thieves to use if the card is lost or stolen.

Category 45.6 Smart cards & other e-commerce security measures

2007-05-03 DHS Daily OSIR; Finextra http://finextra.com/fullstory.asp?id=16885

U.S. CONTACTLESS CARDS TO HIT $109 MILLION BY 2011.

The number of contactless credit and debit cards in circulation in the U.S. is set to increase from 27 million in 2006 to 109 million in 2011, according to research by market intelligence firm Packaged Facts. Total purchase volume in the U.S. with contactless payment cards neared an estimated $15 billion in 2006 -- registering a compound annual growth rate (CAGR) of some 700 percent from 2004 to 2006. Packaged Facts says the number of contactless transactions will rise from 777 million in 2006 to a massive 2.2 billion by 2011. Says Tatjana Meerman, managing editor of Packaged Facts: "Increasing consumer awareness of the technological, safety, and convenience factors inherent in smart cards will only serve to make penetrating the consumer market much easier in the coming years."

48.1 Computer-crime laws (US)

Category 48.1 Computer-crime laws (US)

2006-01-25 EDUPAGE; http://news.zdnet.com/2100-1009_22-6031108.html

LAWSUITS TARGET MAKER OF BOGUS SYPWARE TOOLS

The State of Washington and Microsoft have filed separate lawsuits against Secure Computer, a company they accuse of running a bogus antispyware racket. According to the complaints, Secure Computer used pop-up ads and other tools to tell computer users that their computers were infected with spyware and to offer a service, Spyware Cleaner, that would remove the unwanted software for $49.95. Microsoft and Washington Attorney General Rob McKenna said that the scan that supposedly revealed spyware was bogus and that the removal service in fact left computers more vulnerable to spyware. Moreover, the complaints contend that Secure Computer's messages implied that the service was in some way connected to or endorsed by Microsoft. The lawsuits allege that Secure Computer violated a recently enacted Washington Computer Spyware Act and three other laws. An attorney representing Secure Computer said the company was shocked at the legal action and would respond shortly.

Category 48.1 Computer-crime laws (US)

2006-01-27 DHS Daily OSIR; http://www.theregister.com/2006/01/27/schumer_phone_records/

NEW LEGISLATION WOULD CRIMINALIZE SOCIAL ENGINEERING.

New legislation proposed by Senator Chuck Schumer (D-NY) and backed by both major parties, seeks to criminalize both the practitioners and the dupes of "social engineering." Social engineering is a way of smooth-talking someone out of information they shouldn't normally impart, but it has been the most effective technique for scammers, hackers and private eyes over the years. Schumer's bill, the proposed Consumer Telephone Records Protection Act of 2006, makes disclosing a subscriber's phone records an offense. It specifically outlaws making false statements or providing phony documentation to a phone provider in order to obtain the records, and accessing an account over the Internet without the subscriber's authorization. According to the Electronic Privacy Information Center, over 40 Websites including celltolls.com and locatecell.com have been trading in a black market in call records.

Category 48.1 Computer-crime laws (US)

2006-03-31 DHS Daily OSIR; http://news.zdnet.co.uk/internet/security/0,39020375,3926060 1,00.htm

YAHOO CALLS FOR EFFECTIVE CYBERCRIME LAWS.

Yahoo on Thursday, March 30, called for "effective" legislation combined with industry self-regulation, to deal with online fraud, child abuse, and other cybercrime. The Internet services giant called on policy makers to concentrate on defining illegal use of technology, rather than how an action breaks the law. "The lack of global legislation adds to the complexity of the situation. It's not realistic 17 to have global legislation, but we do need international consistency," said Robin Pembrooke, director of product operations for Yahoo Europe. Pembrooke advocated a combination of legislation and self-regulation of Internet businesses in order to combat cybercrime.

Category 48.1 Computer-crime laws (US)

2007-05-15 DHS Daily OSIR; IDG News Service http://www.infoworld.com/article/07/05/15/new-cybersecurity- bill_1.html

TECH GROUPS SUPPORT NEW CYBERSECURITY BILL.

A tech trade group and a leading cybersecurity vendor applauded new legislation introduced in Congress that would broaden penalties for cybercrime, including first-time penalties for botnet attacks. The Cyber Security Enhancement Act, introduced Monday, May 14, would create for the first time criminal penalties for botnet attacks often used to aid identity theft, denial-of-service attacks, and the spread of spam and spyware. The bill would also allow prosecutors to pursue racketeering charges against cybercriminal groups, would expand sentencing guidelines for cybercrime by allowing the forfeiture of property used to commit the crime, and would add $30 million a year to the budgets of federal agencies fighting cybercrime. The Business Software Alliance, a trade group, and Symantec, a security vendor, both offered support for the legislation.

48.2 Computer-crime laws (non-US)

Category 48.2 Computer-crime laws (non-US)

2006-03-28 DHS Daily OSIR; http://www.electricnews.net/frontpage/news-9676885.html

AUSTRALIA TACKLES SPAM WITH NEW CODE.

Australia has cracked down on junk mail with what is believed to be the world's first industry code for tackling spam. Under the new code, Internet service providers (ISPs) will bear some of the responsibility for helping fight spam. Service providers must offer spam-filtering options to their subscribers and advise them on how to best deal with and report the nuisance mail. In addition to Australian ISPs, global e-mail operators like MSN Hotmail and Yahoo will be hit by the legislation.

Category 48.2 Computer-crime laws (non-US)

2006-09-28 DHS Daily OSIR; IDG News Service
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=government&articleId=9003712&taxonomyId=13&intsrc=kc_feat

COMPUTER CRIME LAWS WORRY SECURITY PROFESSIONALS.

Moves by several European countries to tighten laws against computer hacking worry security professionals, who often use the same tools as hackers but for legitimate purposes. The UK and Germany are among the countries that are considering revisions to their computer crime laws in line with the European 2001 Convention on Cybercrime and a similar European Union measure passed in early 2005. But security professionals are scrutinizing those revisions out of concern for how prosecutors and judges could apply the laws. Security professionals are especially concerned about cases where the revisions apply to programs that could be used for bad or good. Companies often use hacking programs to test the mettle of their own systems.

48.3 Cryptography laws & regulations (US)

Category 48.3 Cryptography laws & regulations (US)

2006-01-25 EDUPAGE; http://news.zdnet.com/2100-3513_22-6030879.html

MICROSOFT TO LICENSE SOURCE CODE

In an effort to avoid a stiff fine issued by the European Commission, Microsoft has agreed to license some of its source code. European antitrust regulators have found Microsoft guilty of abusing its monopoly power and have insisted on changes to the company's practices to address the violations, including offering a version of its operating system without the Microsoft Media Player and providing access to its source code to rivals so they can develop software that will properly interoperate with Windows computers. Microsoft met the first condition, but commissioners last month said that if the company continued to deny access to competitors, it would face a fine of nearly $2.5 million per day, retroactive to December 15 of last year. Microsoft is appealing the rulings against it but has said that while those appeals are pending, it will license the source code for its Windows Server System. The European Commission will review Microsoft's proposal before deciding whether to fine the company.

Category 48.3 Cryptography laws & regulations (US)

2006-01-27 EDUPAGE; http://news.bbc.co.uk/2/hi/entertainment/4653662.stm

BRITISH COURTS FIND IN FAVOR OF RECORDING INDUSTRY

In the first two cases of illegal file trading that went to trial in the United Kingdom, the High Court has ruled against two men, ordering them to pay damages to the British Phonographic Industry (BPI). The two defendants and three other individuals were accused of illegally sharing nearly 9,000 songs over the Internet. One defendant argued that there was no evidence against him. The court rejected that position and ordered him to make an initial payment of 5,000 pounds; his fine is expected to rise to at least 13,500 pounds. The other defendant said he did not know that what he was doing was illegal and pointed out that he sought no profit. A judge said that "Ignorance is not a defense" and ordered the man to make an initial payment of 1,500 pounds. The other three individuals have refused to settle and are awaiting trial. Officials from the BPI said the rulings were a "massive step forward" in their efforts to curb illegal file trading. Many of the other defendants in BPI lawsuits have settled out of court, but more than 50 cases remain outstanding. The BPI has given those individuals a deadline of January 31 to avoid court action.

Category 48.3 Cryptography laws & regulations (US)

2006-03-22 http://www.theregister.com/2006/03/22/creative_commons_dutch_court_ruling/;
EDUPAGE; http://news.com.com/2100-1030_3-6052292.html
http://www.theregister.com/2006/03/22/creative_commons_dutch_court_ruling/

DUTCH COURT UPHOLDS CREATIVE COMMONS LICENCE

In March 2006, a Dutch court upheld the validity of a Creative Commons license and ruled that a commercial gossip magazine should have obtained the permission of televesion personality Adam Curry before publishing pictures he had posted on a photo-sharing Web site. The magazine's attorneys argued that the limitations on use of the photos were not clearly stated; the Court rejected this defense, stating that the magazine should have investigated the terms of the license before using the material. The Creative Commons license < http://creativecommons.org/ > is similar to the GNU General Public License < http://www.gnu.org/copyleft/gpl.html > and allows authors to grant general permission to their materials for non-commercial use while restricting use for commercial applications.

Category 48.3 Cryptography laws & regulations (US)

2006-04-12 EDUPAGE; http://news.bbc.co.uk/1/hi/technology/4902976.stm

CHINA ADOPTS NEW RULE TO ADDRESS SOFTWARE PIRACY

Following trade talks with the United States, Chinese authorities have issued a new guideline requiring PC manufacturers to load a licensed operating system on all computers before they leave the factory. Although an official from the State Copyright Bureau in China denied that the new regulation is in response to foreign pressure -- insisting it was implemented for "the country's economic development" -- China has long been seen as a haven for software pirates, with piracy rates as high as 90 percent. Under the new rule, computer makers must install legally licensed operating systems on all systems, and retailers who sell imported computers must do the same. Furthermore, computer manufacturers and vendors of operating systems must report the numbers of computers made and operating systems installed each year to the country's Ministry of Information Industry (MII). The MII also stated that software makers should provide "favorable pricing and qualified service" to computer manufacturers.

Category 48.3 Cryptography laws & regulations (US)

2006-07-16 DHS Daily OSIR; Aviation Week
http://www.aviationnow.com/avnow/news/channel_awst_story.jsp?id=news/aw071706p1.xml

INDUSTRY, GOVERNMENT MAKE RENEWED PUSH TO CHANGE U.S. EXPORT CONTROL REGIME.

With industry concerns growing that the arms export control system is hurting business and hampering cooperation with foreign partners, advocates of reform are coalescing around plans for a renewed push to change. Under current law, export controls are delegated to the State Department, whose Office of Defense Trade Controls is responsible for processing export licenses. With the end of the Cold War, industry and government officials alike felt there was a need to reform a system that many felt took too long, tried to control too much and was aimed at a problem that no longer existed: trying to keep advanced technology out of the hands of the Soviet Union. Everyone involved in the export debate agrees -- to some degree -- that the licensing process could and should work better. One of the lessons, however, is that good intentions aren't enough -- reforms have to be workable, and perhaps even more important, they have to be agreeable to all sides. That understanding has led many to advocate a new approach: start with improving the current system, and then work for bigger changes.

Category 48.3 Cryptography laws & regulations (US)

2006-09-20 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/06/09/20/HNbannedexportstoiran_1.html

U.S. COMPUTER FIRM ADMITS SELLING BANNED EXPORTS TO IRAN.

Super Micro Computer, of San Jose, CA, pleaded guilty to one felony count of knowingly exporting items subject to export regulations without obtaining a license and has agreed to pay a $150,000 fine, according to a statement from the office of Kevin V. Ryan, the U.S. Attorney for the Northern District of California. Super Micro Computer, which sells high-end servers, computer cases, motherboards, and other components, reportedly sold the equipment when exporting to Iran "was banned at the time for reasons of national security," according to the U.S. Attorney. According to the plea agreement approved by federal District Judge Ronald M.Whyte, Super Micro sold 300 computer motherboards worth about $27,600 between December 28, 2001, and January 29, 2002, to a company named Super Net in Dubai, United Arab Emirates, "knowing that the items were to be transhipped to Iran," the U.S. Attorney's Office release stated. According to Commerce Department records, this is one of the first criminal convictions in the U.S. for exporting items controlled for national security reasons to Iran. U.S. Attorney's Office Press Release: http://www.usdoj.gov/usao/can/press/2006/2006_09_19_SuperMic ro.guiltyplea.press.html

Category 48.3 Cryptography laws & regulations (US)

2006-10-29 AP

CHINESE OFFICIALS STUDY U.S. INTELLECTUAL PROPERTY SYSTEM

Concerned about intellectual-property piracy in China, a 19-person Chinese delegation visited the United States in October for 20 days to study US intellectual-property laws and enforcement. According to Associated Press writer Juliana Barbassa, "A report issued by the European Commission earlier this month named China as the world's top producer of faked goods. Intellectual property attorneys say Chinese companies are increasingly being hauled into U.S. courts for patent infringement. Despite its bad reputation, China has ratcheted up efforts to reduce rampant intellectual property theft. Over the past two years, authorities have increased the number of intellectual property-related arrests, destroyed millions of counterfeit CDs and shuttered thousands of shops, publishing companies and Web sites involved in their distribution."

49.1 US-government surveillance

Category 49.1 *US-government surveillance*

2006-01-05 EDUPAGE; http://news.com.com/2100-1028_3-6018702.html
http://news.com.com/2100-1028_3-6018702.html
http://news.com.com/2100-1028_3-6018702.html

GOVERNMENT KEEPING TABS WHEN IT SHOULDN'T

Despite a federal directive forbidding the use of Web-tracking technologies for federal agencies, recent reports have shown that the majority of agencies do in fact employ permanent cookies or other tools that track users. The technologies can be used to identify repeat visitors to federal Web sites and sometimes to track users' surfing on nongovernmental sites. Last week, the Associated Press found that the National Security Agency was using permanent cookies (temporary cookies are allowed), a practice it has since discontinued. Separately, reporters at CNET News.com looked at the Web sites of all agencies listed in the U.S. Government Manual and evaluated what tracking tools they were using. Results showed dozens of agencies using tools that appear to contravene the directive, including sites for the military, cabinet departments, and election commissions. When contacted about the tracking tools, officials at many agencies reportedly said they were unaware that their sites used such technologies. Peter Swire, law professor at Ohio State University, who participated in the drafting of an earlier Web-tracking policy for the Clinton administration, said, "It's evidence that privacy is not being taken seriously."

Category 49.1 *US-government surveillance*

2006-01-31 EDUPAGE; http://news.yahoo.com/s/ap/20060201/ap_on_hi_te/domestic_spying_lawsuit

EFF SUES AT&T OVER COOPERATION WITH NSA

The Electronic Frontier Foundation (EFF) has filed suit against AT&T for allegedly cooperating with the National Security Agency (NSA) in eavesdropping on individuals without a warrant. President Bush ordered the wiretaps following the terrorist attacks of 2001 and has vigorously defended them, saying the Constitution and Congressional resolutions allow them. Civil liberties groups and others reject that, saying that the wiretaps violate existing laws on surveillance. The EFF said it identified AT&T as one company involved in the activities and has filed suit "to stop this invasion of privacy, prevent it from occurring again, and make sure AT&T and all the other carriers understand there are going to be legal and economic consequences when they fail to follow the law." The EFF alleges that AT&T provided the NSA with access to its network, which carries both voice and data, and to its vast databases that store information on phone calls and Internet activity. AT&T refused to comment on the litigation.

Category 49.1 US-government surveillance

2006-03-10 Effector Online

U.S.A.P.A.T.R.I.O.T. RENEWAL RUBBER STAMPED, NSA SPYING MAY BE NEXT.

Despite the best efforts of EFF, other civil liberties organizations, and their supporters, Americans' privacy rights took some serious body-blows from Congress this week. The U.S.A.P.A.T.R.I.O.T. Act was renewed without meaningful reform, and key Congressmen backed away from a full investigation of the NSA's domestic spying program, instead making a deal with the White House to legalize it. Whether because of election year fears or White House pressures, Republican Senators who had been holding out for significant new checks on the U.S.A.P.A.T.R.I.O.T. Act dropped the fight when offered a few sham reforms. The renewal bill was then quickly approved by the Senate and, this week, approved by the House and signed by the President. Why are the "compromise" bill's three reforms worthless? Let's take each in turn. The bill provides a procedure for recipients of super-secret National Security Letters (NSLs) to challenge the never- ending gag orders that accompany these FBI-issued subpoenas. But the ACLU (with help from EFF) already demonstrated that these gag orders could be successfully challenged in court without a change to the law. This new "reform" actually makes things worse: under the new law, these gag orders can't be challenged at all within a year of being issued, and if the government simply tells the court that lifting the gag order will hurt national security, the government wins. We think this procedure is just as unconstitutional as the original law.

The bill didn't include a requirement that NSL recipients seeking legal advice disclose their lawyer's name to the FBI. But this "reform" simply removed something bad from one of the renewal bill's earlier versions; it didn't change the original U.S.A.P.A.T.R.I.O.T. Act at all. Finally, the bill clarified that NSLs can't be served on libraries that don't provide electronic communication services. But NSLs already can't be served on libraries lacking those services. Unfortunately, it gets worse. Senate Republicans this week stated that they had reached a deal with the White House to legalize the NSA's domestic spying program. The agreement allows government investigators to conduct warrantless wiretaps for up to 45 days before having to go to a court, even in non-emergency situations. Currently, the law only allows such surveillance without a warrant for 72 hours in emergencies and for 15 days by the Executive when war is declared. Because of this deal, an in-depth Congressional investigation of the NSA program -- what it actually involves and whether it broke the law -- has been deflected for now. Nevertheless, this week's events shouldn't be taken as final defeats. Members of Congress who were dissatisfied with the U.S.A.P.A.T.R.I.O.T. bill -- Democrats and Republicans alike -- are already proposing new non-sham reforms, while the plan to legalize the NSA Program still has opponents on both sides of the aisle. EFF believes that the spying program did in fact break the law and violate the Constitution, as we have alleged in our lawsuit against AT&T for helping the NSA with this massive fishing expedition into Americans' private communications. As always, EFF will stay on the front lines and fight hard to ensure that your civil liberties are protected.
New York Times, "G.O.P. Plan Would Allow Spying Without Warrants":
http://www.nytimes.com/2006/03/09/politics/09nsa.html
AP, "Bush to Sign Patriot Act Renewal": http://www.abcnews.go.com/Politics/print?id=1700403
For more on the NSA domestic spying program: http://www.eff.org/Privacy/Surveillance/NSA/
For more on EFF's suit against AT&T: http://www.eff.org/legal/cases/att/
For more on the U.S.A.P.A.T.R.I.O.T. Act: http://www.eff.org/patriot/

[MK adds: I converted the propaganda spelling of the act's name into a punctuated acronym as a matter of the well-known principle, "Illegitimi non carborundum."]

Category 49.1 US-government surveillance

2006-03-30 EDUPAGE; http://news.yahoo.com/s/ap/20060331/ap_on_hi_te/internet_blocking

JUSTICE DEPARTMENT CASTS A WIDE NET FOR INFORMATION

Subpoenas obtained through the Freedom of Information Act indicate that the U.S. Justice Department is seeking Internet usage data from at least 35 companies in its efforts to defend the 1996 Child Online Protection Act (COPA) against court challenges. One of the subpoenas sparked a legal showdown between the government and Google, which challenged the request for millions of records of Internet searches. In that case, the government significantly scaled back its request, which the judge ruled was allowable. Other companies that received similar subpoenas are Comcast, EarthLink, AT&T, Cox Communications, Verizon Communications, Symantec, and other makers of computer security products. The Supreme Court has ruled twice that COPA is likely unconstitutional, and the government will go to trial in October to defend it. David McGuire, spokesman for the Center for Democracy and Technology, expressed concerns echoed by other critics that the government is seeking large amounts of information to defend a questionable law.

Category 49.1 US-government surveillance

2006-04-13 EDUPAGE; http://www.nytimes.com/2006/04/13/nyregion/13library.html

LIBRARY GROUP WINS DISPUTE WITH FBI

Following a recent change in terms of the U.S.A.P.A.T.R.I.O.T. Act, federal authorities said they will end their efforts to prevent a library organization from identifying itself as a part of an antiterrorism investigation. Last year, the FBI sent a so-called national security letter to the Library Connection, an organization of 26 libraries in Connecticut, seeking patron records and e-mail messages. As it was originally enacted, the U.S.A.P.A.T.R.I.O.T. Act authorized the letters and forbade recipients from disclosing that they had been sent the letter. The group protested, saying the gag order violated their First Amendment rights, and last September a federal judge agreed. Ironically, it was during those proceedings that the government inadvertently identified the group in question as the Library Connection when attorneys for the government filed court documents with the group's name not redacted. Congress has since revised the U.S.A.P.A.T.R.I.O.T. Act, which now grants the government discretion to allow some recipients of national security letters to identify themselves. Kevin O'Connor, the United States attorney in Connecticut, said that in light of the changed legislation, the government would end its appeal of the decision to allow the Library Connection to come forward.

Category 49.1 US-government surveillance

2006-04-14 EDUPAGE; http://news.zdnet.com/2100-9588_22-6061187.html

LEGISLATORS GET BEHIND ISP TRACKING

A number of government officials, including state and federal legislators, have endorsed the notion of requiring ISPs to keep detailed records of users' activities online. A data retention would force ISPs to collect and store some data that they currently do not capture and to keep other records far longer than they currently do. Officials including Rep. Ed Whitfield (R-Ky.), head of a Congressional subcommittee on oversight and investigations, have said that such a law would aid law enforcement. Michael Chertoff, secretary of homeland security, has also voiced support for such legislation. Critics of the idea have questioned whether storing such records would genuinely benefit law enforcement; raised concerns about who would have access to such records; and noted that it's not clear who would have to pay for such data warehouses.

Category 49.1 US-government surveillance

2006-04-29 RISKS; CNET news.com http://tinyurl.com/gb663

PROPOSAL TO FORCE DATA RETENTION BY ISPs

Rep. Diana DeGette (D-CO) has proposed legislation to force Internet Service Providers to store log files with complete records of all Internet activity by their customers until at least one year after closure of their accounts -- or indefinitely for people who continue their subscriptions. The proposed rationale for this extraordinary burden was that "America is the No. 1 global consumer of child pornography, the No. 2 producer. This is a plague we had nearly wiped out in the seventies, and sadly the Internet, an entity that we practically worship for all the great things it has brought to us, is being used to commit a crime against humanity." Declan McCullag, writing for CNET news.com, said, "For their part, Internet providers say they have a long history of helping law enforcement in child porn cases and point out that two federal laws already require them to cooperate. It's also unclear that investigations are really being hindered, according to Kate Dean, director of the U.S. Internet Service Provider Association."

Lauren Weinstein commented in RISKS,

>It was only a few months ago that people were screaming bloody murder about DoJ demanding Search Engine records -- a demand that apparently only Google had the backbone to appropriately resist, noting the sensitivity of the data involved. This controversy triggered calls (including in some legislative quarters) for a law mandating the destruction of much related data after some reasonable, relatively short interval, with appropriate designated exceptions for R&D, business development, and the like.

Now, by waving the red flag of fighting child pornography, seemingly intelligent and usually well-meaning legislators appear ready to create the mother of all big-brother database laws, a treasure trove of personal data that will ultimately be available for every fishing expedition under the sun.

For those persons who trust the government not to abuse such data, I hasten to note that these kinds of infrastructures, once in place, tend to be self-perpetuating, and will be available to *future* governments as well, including administrations who might not be as "benign" as the current one.<

In a later posting, Weinstein added,

>The irony of the situation relating to proposals for required data retention … is that many incredibly bad and dangerous concepts -- like government-mandated data retention of this sort -- will virtually always be linked to laudable ideas (like fighting child abuse) that we all agree are important goals. A cynical view would be to assume that this is done purposely to push "evil" laws using "noble" hooks. This clearly does happen sometimes.

But I believe that in the majority of these cases we're dealing with legislators and others who genuinely believe in their causes, and either don't have the will or background to recognize or understand the horrible collateral damage that their proposals would do.

Casting such persons as being purposefully evil is probably unproductive and unfair. Instead, we need to help them see the "big picture," rather than just the narrow focus of their good intentions.

For after all, the road to hell still does indeed remain paved with good intentions.<

And in RISKS 24.31, Weinstein wrote:

>If Internet users must live in fear that their actions on the Net are subject to retrospective analysis -- not only based on today's criteria but potentially on tomorrow's as well -- the effects on how we view and use the Net will be drastic, with vast unintended negative consequences that strike to the heart of our democracies.

This issue is ultimately more important than network neutrality, Internet governance, or most (if not all) of the other technically-related concerns that we bandy about here in IP or in most other forums, because it strikes to the very core of basic privacy concerns and personal freedoms.

Government-mandated Internet data retention could be the most potent single technological move in recent history toward enabling future tyranny against both individuals and groups.<

Category 49.1 US-government surveillance

2006-05-22 Wikipedia http://en.wikipedia.org/wiki/NSA_warrantless_surveillance_controversy

NSA WARRANTLESS SURVEILLANCE CONTROVERSY

The NSA warrantless surveillance controversy is a dispute about an eavesdropping and data mining program carried out by the National Security Agency (NSA) that the administration now refers to as the Terrorist Surveillance Program. Under the program, the NSA conducts surveillance on international and domestic phone calls, without Foreign Intelligence Surveillance Act (FISA) court authorization, which the text of FISA defines as a felony. [1] The Bush administration argues that the program is in fact legal on the grounds that FISA is an unconstitutional violation of the President's "inherent powers" and/or that FISA was implicitly overridden by other acts of Congress. Many legal scholars outside of the administration find these arguments unconvincing. In addition to the legality of the program, the controversy extends to questions of the duties of Congress, the press's role in exposing a classified program and the legality of telecommunications companies cooperating with the program.

The presidential authorization creating the Terrorist Surveillance Program is classified and only select members of the Congressional Intelligence committees and leadership were (partially) briefed. The existence of the program was not known to the American public until December 2005, when the New York Times, after learning about the program more than a year earlier, first reported on it.[2]

[Wikipedia]

References used in this introduction:
1. Article 50 United States Code, Section 1809 (In FISA, subchapter 1)
http://caselaw.lp.findlaw.com/casecode/uscodes/50/chapters/36/subchapters/i/sections/section_1809.html
2. NYT's Risen & Lichtblau's December 16, 2005 "Bush Lets U.S. Spy on Callers Without Courts". Retrieved on February 18, 2006.
http://www.commondreams.org/headlines05/1216-01.htm

Category 49.1 US-government surveillance

2006-06-02 EDUPAGE; San Jose Mercury News
http://www.mercurynews.com/mld/mercurynews/news/local/14720891.htm

GOVERNMENT WANTS ISPS TO KEEP DATA FOR TWO YEARS

The Department of Justice is working to require ISPs to keep records on customer activities for two years to help law enforcement officials fight crimes including terrorism and child pornography. Officials from the department met recently with leading Internet companies to discuss details about how such a plan could be put into place. Representatives of those companies said that while they want to aid efforts to stop or prevent crime, they have concerns about exactly what information the Justice Department wants them to keep and how it would be used. A spokesperson from the Justice Department said they want to see records of Web searches and e-mail exchanges but not the content of those actions. He also said access to those records would be restricted and subject to existing protocols covering who is allowed to see it and under what circumstances. Marc Rotenberg, executive director of the Electronic Privacy Information Center, said the proposal amounts to "a radical departure from current practices" and would pose "an unnecessary risk to privacy and security of Internet users."

Category 49.1 US-government surveillance

2006-10-10 Effector Online http://www.eff.org/deeplinks/archives/004938.php

ANOTHER COURT SAYS "NATIONAL SECURITY" ISN'T BLANK CHECK FOR ILLEGAL SPYING.

Last week, a federal court shot down yet another attempt by the government to use "national security" as a blank check for illegal surveillance. The government claimed that it could not even confirm or deny whether it had listened in on calls between attorneys at the Center for Constitutional Rights and their clients. In rejecting this argument, the court ordered the government to provide that information to the court in secret first, then set up a process to provide that information to the attorneys involved. The court confirmed: "It is a cardinal rule of litigation that one side may not eavesdrop on the other's privileged attorneyclient communications." That should have been obvious to the government from the beginning. But the fact that the government refused to confirm that it wasn't violating this "cardinal rule" protecting attorney-client communications should raise concerns for all of us. Kudos to yet another court for holding the government to the basic rule of law. The government's overreaching attempts to prevent courts from considering cases where it asserts "national security" are now starting to fail, including, of course, in EFF's case against AT&T for helping the government's massive and illegal NSA spying program.
For this post and related links: http://www.eff.org/deeplinks/archives/004938.php

49.2 Non-US-government surveillance

Category 49.2 Non-US-government surveillance

2006-02-02 RISKS; Wikipedia http://en.wikipedia.org/wiki/Greek_telephone_tapping_case_2004-2005

GREEK GOVERNMENT PHONES TAPPED ILLEGALLY

More than 100 mobile phone numbers belonging mostly to members of the Greek government and top-ranking civil servants were found to have been illegally tapped for a period of at least one year. The details of the case were presented at a press conference given by three government ministers on Thursday February 2, 2006. The phones tapped included those of the Prime Minister Costas Caramanlis and members of his family, the Mayor of Athens, Dora Bakoyannis, most phones of the top officers at the Ministry of Defense, the Ministry of Foreign Affairs, and the Ministry of Public Order, members of the ruling party, the Hellenic Navy General Staff, the previous Minister of Defense (at the time a member of the opposition party), one phone of the American Embassy. Moreover, the mobile phones of former National Defence Minister Giannos Papantoniou and businessmen of Arab descent were also at the foresight of the wiretapping ring, as well as of former governemnental officials from the Panhellenic Socialist Movement (PASOK).

Prime minister Costas Caramanlis has known of this surveillance since March 11, 2005, lifting concerns about his reasons of not previously revealing it. Greek medias suspected the United States of having organized the wiretaps, as an anonymous important official quoted by the AFP declared that "it is evident that the wiretaps were organized by foreign intelligence agencies, for security reasons related to the 2004 Olympic Games." Leader of the PASOK socialist opposition George Papandreou said that the Greek governement itself had pointed towards the US as responsible of the wiretaps by giving up the zone of listening range, in which the US embassy was included.

[From Wikipedia, the free encyclopedia]

Category 49.2 Non-US-government surveillance

2006-02-09 EDUPAGE; http://www.internetnews.com/xSP/article.php/3584191

GROUP SAYS YAHOO AIDED CHINESE AUTHORITIES

For the second time recently, Yahoo has been accused of helping the Chinese government identify and prosecute individuals accused of political crimes. In 2005, Yahoo was criticized for providing information that helped Chinese authorities prosecute journalist Shi Tao, who was convicted of revealing state secrets. Reporters Without Borders said that another case has surfaced in which the ISP provided information to the Chinese government that led to the conviction of Li Zhi. According to the group, Li was found guilty of "inciting subversion" after he posted comments online critical of local officials and was sentenced to eight years in prison. Mary Osaka, a spokesperson from Yahoo, said that at the time the company was unaware of the nature of the investigation. In addition, she reiterated the company's position that it is better for Yahoo to have a presence in the country, "providing services we know benefit China's citizens," even if that requires compliance with local laws that run counter to U.S. beliefs and values.

Category 49.2 Non-US-government surveillance

2006-02-17 Effector Online http://www.eff.org/news/archives/2006_02.php#004411

INTERNET COMPANIES NEED CODE OF CONDUCT IN AUTHORITARIAN REGIMES. EFF CALLS FOR LIMITS ON DATA COLLECTION AND RETENTION.

San Francisco - In the midst of Congressional hearings about how U.S. Internet companies do business in China, the Electronic Frontier Foundation (EFF) is calling for the industry and government to work together to develop simple guidelines to decrease the harm done by participating in authoritarian regimes. "Without careful thought, even wellmeaning Internet companies can become the handmaidens of state repression. Internet routers can be turned into powerful wiretapping tools," said EFF Activism Coordinator Danny O'Brien. "Web servers and search engines can become honeypots of personal data, plundered by state police to identify dissidents." In an open letter to the Subcommittee on Africa, Global Human Rights, and International Operations and the Subcommittee on Asia and the Pacific, EFF says the best course of action for companies concerned about human rights violations and censorship is to avoid repressive countries all together. However, EFF believes that companies deciding to go forward can mitigate some of the harm. "In considering how these companies might construct their services to best serve global human rights, we believe that simple guidelines, consciously followed, could significantly limit the damage caused by corporate engagement with these regimes," said EFF Legal Director Cindy Cohn. EFF's letter gives five courses of action for companies and the US government to consider, including restricting the collection and storage of personal data in oppressive regimes, "bearing witness" and documenting acts of state control, innovating around censorship, and offering encrypted connections to their web services by default. The joint Subcommittee hearing, "The Internet in China: A Tool for Suppression?" took place on Wednesday.
For EFF's open letter: http://www.eff.org/deeplinks/archives/004410.php
For this release: http://www.eff.org/news/archives/2006_02.php#004411

Category 49.2 Non-US-government surveillance

2006-08-25 DHS Daily OSIR; OUT-LAW News (United Kingdom) http://www.out-law.com/page-7229

AUSTRALIAN CITIZEN DATABASE SUBJECTED TO SNOOPING BY GOVERNMENT EMPLOYEES.

Australia's citizen database was routinely searched for personal reasons by government agency employees, some of whom have been fired. Police are now investigating allegations of identity fraud resulting from the security breaches. There were 790 security breaches at government agency Centrelink involving 600 staff. Staff were found to have inappropriately accessed databases containing citizens' information. The databases are used to administer social security, pension and unemployment benefits. Australian police have confirmed that investigations are ongoing after five referrals were made to it from Centrelink. At least one of the cases is believed to involve allegations of the establishment of fake identities to be used to receive payments.

Category 49.2 Non-US-government surveillance

2006-11-10 DHS Daily OSIR; CNET News http://news.com.com/U.K.+outlaws+denial-of-service+attacks/2100-7348_3-6134472.html

UK OUTLAWS DENIAL-OF-SERVICE ATTACKS.

A UK law has been passed that makes it an offense to launch denial-of-service attacks, which experts had previously called "a legal gray area." Among the provisions of the Police and Justice Bill 2006, which gained Royal Assent on Wednesday, November 8, is a clause that makes it an offense to impair the operation of any computer system. Other clauses prohibit preventing or hindering access to a program or data held on a computer, or impairing the operation of any program or data held on a computer. The maximum penalty for such cybercrimes has also been increased from five years to 10 years.

49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2006-04-13 DHS Daily OSIR; http://www.washingtonpost.com/wp-dyn/content/article/2006/04/12/AR2006041201968.html?nav=rss_technology/special/08

TERRORISTS' WEB CHATTER SHOWS CONCERN ABOUT INTERNET PRIVACY.

Terrorist groups, which for years have used the Internet and its various tools to organize and communicate, are paying more attention to addressing security and privacy concerns similar to those of other Web users, counterterrorism experts say. Recently, postings on jihadist Websites have expressed increasing concern about spyware, password protection, and surveillance on chat rooms and instant-messaging systems. One forum recently posted a guide for Internet safety and anonymity on the Internet, advising readers of ways to circumvent hackers or government officials. "The Shortened Way of How to be Cautious; To the User of the Jihadi Forums, In the Name of Allah, the most Gracious and Merciful" was posted last month by an al-Qaeda-affiliated group calling itself the Global Islamic Media Front. The posting advised Internet cafe users to set up a proxy -- a software program that erases digital footsteps such as Web addresses or other identifiable information -- before Web surfing. "There's a lot of things like that," said Evan Kohlmann, a consultant on international terrorism. Last month, Kohlmann said, he found a jihadist Website posting pirated McAfee anti-spyware software, which the site encouraged users to download to avoid monitoring.

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2006-05-23 DHS Daily OSIR; Associated Press
http://www.timesdispatch.com/servlet/Satellite?pagename=RTD%2FMGArticle%2FRTD_BasicArticle&c=MGArticle&cid=1137836259739&path=!news&s=1045855934842

NETWORK WOULD HELP DETECT BIOTERRORISM.

The Wildlife Center of Virginia is developing a national surveillance network that would help detect diseases in wildlife that may be linked to bioterrorism. While there are already systems designed to detect diseases in humans and domestic animals, Project Tripwire would be the first comprehensive effort to monitor wildlife for signs of bioterrorism, Wildlife Center President Ed Clark said Monday, May 22. The Wildlife Center entered into a $166,000, six-month contract with the Institute for Defense and Homeland Security last month to plan a database that would initially link 20 to 25 of North America's largest wildlife hospitals. The hospitals would enter information about animals they treat into the database, which would be programmed to pick up statistical anomalies, such as a higher-than-usual number of animals in one area suffering from an infection. Anything that could be the result of bioterrorism would be reported to the Department of Defense, the Centers for Disease Control and Prevention, and other federal and state agencies.

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2006-07-06 EDUPAGE; Chronicle of Higher Education (sub. Req'd)
http://chronicle.com/daily/2006/07/2006070601n.htm

PENTAGON ACKNOWLEDGES MONITORING STUDENT E-MAIL

Surveillance reports obtained through the Freedom of Information Act indicate that the Department of Defense monitored student e-mail as part of its efforts to identify and track potential terrorist suspects. The Servicemembers Legal Defense Network filed requests for the information, and the reports released so far cover e-mail surveillance at the State University of New York at Albany, Southern Connecticut State University, the University of California at Berkeley, and William Paterson University of New Jersey. Student e-mail was monitored when it dealt with protests against the war in Iraq or against the military's "don't ask, don't tell" program concerning gay and lesbian members of the armed forces. Instances of monitoring were evidently prompted by reports of suspicious behavior, but a Pentagon spokesperson would not say who submitted the reports that led to the monitoring described in the surveillance reports. Kermit Hall, president of SUNY-Albany, said his institution is investigating the nature of the monitoring and how it was conducted and would decide later how to proceed.

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2006-07-15 DHS Daily OSIR; Forum of Incident Response and Security Teams https://www.first.org/newsroom/globalsecurity/37271.html

REPORT: TREASURY'S TERRORIST FINANCE PROGRAM'S ACCESS TO INFORMATION HELD BY THE SOCIETY FOR WORLDWIDE INTERBANK FINANCIAL TELECOMMUNICATION (SWIFT).

Recent press reports have raised questions about the Department of the Treasury's Terrorist Finance Tracking Program's access to information on international financial transactions held by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), an organization owned by banks in many countries, which serves as a hub for international funds transfers. Its records contain names, addresses, and account numbers of senders and receivers of international wire transfers between banks and between securities firms, thus providing a useful source for federal officials responsible for following money trails across international borders. On June 29, 2006, the House of Representatives passed H.Res. 895 voicing support for the Treasury program as fully compliant with all applicable laws; condemning the unauthorized disclosure of classified information; and calling upon news media organizations not to disclose classified intelligence programs. H.Res. 904 was introduced to discourage government censorship of the press. This report addresses these issues and will be updated as legislative events merit. Report: http://www.fas.org/sgp/crs/natsec/RS22469.pdf

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2006-07-26 DHS Daily OSIR; SecurityFocus http://www.securityfocus.com/print/news/11402

SCADA SYSTEM MAKERS PUSHED TOWARD SECURITY.

Idaho National Laboratory and the New York State Office of Cyber Security and Critical Infrastructure have teamed up with utilities and makers of distributed control system software to offer advice on how to make system security a major part of the critical infrastructure. Later this week, the group will release the latest draft of a set of guidelines for utilities and manufacturers that offers specific requirements for suppliers of supervisory control and data acquisition (SCADA) systems. The guidelines aim to elevate system security to an explicit part of negotiations between customer and supplier with the goal of making the next generation of critical infrastructure systems more secure than today's software and hardware. "We think we can identify the common weaknesses in regards to security and also identify places were the technology's security can be tightened up," said Michael Assante of Idaho National Laboratory. The security issues of real-time control systems, of which the best known are SCADA systems, has become a focus of both private industry and the government as worries mount that such systems could be used as the vector for a criminal or terrorist attack.

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2006-08-10 DHS Daily OSIR; Associated Press http://www.usatoday.com/news/nation/2006-08-10-missing-egyptian-students_x.htm

SIX OF 11 MISSING EGYPTIAN STUDENTS NOW IN CUSTODY; MORE ARRESTS MADE.

Six of the 11 Egyptian exchange students who failed to show up for their college program are now in custody after three additional students were arrested Thursday, August 10, the FBI said. El Sayed Ahmed Elsayed Ibrahim, 20, and Alaa Abd El Fattah Ali El Bahnasawi, 20, were arrested at a residence in Dundalk, MD, by U.S. Immigration and Customs Enforcement agents. Chicago police detained Ahmed Mohamed Mohamed Abou El Ela, 22, at OHare International Airport as he was attempting to book a flight to Montana, the FBI said. All are being held on immigration violations because they did not report on time to their month-long program at Montana State University in Bozeman, MT. The other five Egyptians still are being sought.

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2006-08-16 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article95678-08-16-06-Web

NEW INFORMATION CULTURE NEEDED TO FIGHT THE WAR ON TERRORISM.

The military must jettison its longstanding concepts regarding information ownership and adapt information technology systems that meet the new threats, according to a speaker at the Air Force IT conference. "We have to build a culture that is gathering that kind of information and making it available to commanders in the field," said Gen. Lance Smith, commander of the U.S. Joint Forces Command. Military information management must become more decentralized and agile, Smith said. U.S. forces must get inside the enemy's decision cycle by pushing information and decision-making down to the squad or company level, he added. The structure of terrorist organizations requires a new approach, Smith said. Terrorist groups operate at the cellular level, with only broad guidance from their command structure. Terrorist cells have a short decision-making cycle, so they can act on intelligence quickly, he noted. "We cannot operate against [the terrorists] until we give our guys out there fighting in the field the same capability, as much information as we can and the authority to act on that information in real time," Smith said.

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2006-08-17 DHS Daily OSIR; Los Angeles Times http://www.latimes.com/news/nationworld/nation/la-na-terror17aug17,1,2257285.story?coll=la-headlines-nation&track=crosspromo

ATTORNEY GENERAL: EXTREMISTS ARE HOMING IN ON THE INTERNET.

Attorney Gen. Alberto R. Gonzales said Wednesday, August 16, that more than 5,000 Internet sites were being used by extremists to train and coordinate internationally, filling the gap caused by the crackdown on the Al Qaeda terrorist network. Gonzales' estimate suggests a significant expansion of the Internet infrastructure used by Islamic extremists in recent years to mobilize their efforts. Since late 2001, the United States and its allies have demolished Al Qaeda's home base in Afghanistan, killed or captured some of its leaders, cut off many outside funding channels and disrupted some means of communication. But those efforts have driven Al Qaeda members to the Internet, "where their ideology has inspired and radicalized others," Gonzales said in a speech to the World Affairs Council of Pittsburgh. "This radicalization is happening online and can therefore develop anywhere, in virtually any neighborhood, and in any country," said Gonzales.

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2006-09-05 DHS Daily OSIR; The White House http://www.whitehouse.gov/infocus/nationalsecurity/

NATIONAL STRATEGY FOR COMBATING TERRORISM RELEASED.

On Tuesday, September 5, President Bush released his updated National Strategy for Combating Terrorism (NSCT), which outlines the U.S. government strategy to protect and defend American interests at home and abroad from terrorism. This updated strategy builds directly from the National Security Strategy issued in March 2006 as well as the February 2003 National Strategy for Combating Terrorism, and incorporates our increased understanding of the enemy.

Fact Sheet: The President's National Strategy for Combating Terrorism:
http://www.whitehouse.gov/news/releases/2006/09/20060905.html
HTML version of the NSCT: http://www.whitehouse.gov/nsc/nsct/2006/index.html
PDF version of the NSCT: http://www.whitehouse.gov/nsc/nsct/2006/nsct2006.pdf March 2006
National Security Strategy: http://www.whitehouse.gov/nsc/nss/2006/February 2003 NSCT:
http://www.whitehouse.gov/news/releases/2003/02/20030214-7.html

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2006-09-13 DHS Daily OSIR; Gannett News Service http://www.usatoday.com/travel/news/2006-09-13-travel-security_x.htm

U.S. OFFICIALS WORK TO PLUG TRAVEL SECURITY HOLES.

Department of Homeland Security (DHS) officials are rushing under a rapidly approaching deadline to plug dangerous intelligence gaps that occur in the collection and use of basic travel data on U.S.-bound foreign passengers from Europe, which is gathered by the travel industry when tickets are purchased. That information, called the Passenger Name Record data, is available to DHS officials. But under a current U.S.-European Union agreement they are limited in how they can use it and how long they can hold it. It consists of up to 34 pieces of data on each passenger, including ticket purchase details, method of payment, e-mail addresses, destination addresses, phone numbers, and other information. The problem for DHS is that it can't freely share this information with U.S. intelligence and law enforcement agencies. Those agencies have extensive databases of terrorist cell phone numbers and other information which, when cross-matched against the travel data, could raise red flags that would otherwise go undetected. DHS officials are hoping to renegotiate their agreement with the EU, which expires at the end of the month under a legal snag, in talks that have been given a boost by the London plot.

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2006-09-18 DHS Daily OSIR; Boston Globe
http://www.boston.com/news/local/articles/2006/09/18/hundreds_play_the_part_for_antiterrorism_drill/

LARGEST ANTI-TERRORISM DRILL IN NEW ENGLAND CONDUCTED.

Federal, state, and local agencies Sunday, September 17, staged the largest anti-terrorism drill ever in New England, simulating the response to a mock explosion of a radioactive dirty bomb at the CambridgeSide Galleria in Cambridge, MA. The exercise, dubbed Operation Poseidon, was monitored by roving teams of federal, state, and local observers, who will use the exercise to better prepare for a real terrorist attack. Authorities said their critique of the drill is months away and declined to talk about mistakes made, though they said the lessons learned are often simple. "Certain equipment that was designed for certain operations may not lend itself to going up and down stairs," said Fire Chief Gerald Reardon. He added that such drills also help ferret out something as basic as an inactive pager or cell phone. The volunteers described passing rescue workers failing to ask them if they needed help, despite the index cards the volunteers wore indicating the seriousness of their condition: bleeding to death, radiation exposure, in shock. Other volunteers said officials were slow to bring buses to evacuate people fleeing the scene.

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2006-09-21 DHS Daily OSIR; Federal Energy Regulatory Commission http://www.ferc.gov/press-room/press-releases/2006/2006-3/09-21-06-E-13.asp

FERC ACTS TO IMPROVE SECURITY OF NATION'S POWER GRID.

The Federal Energy Regulatory Commission (FERC) Thursday, September 21, approved an innovative agreement among electric utilities on electric transformer sharing that will maintain the integrity of the nation's transmission system in the event of a future terrorist strike. In an initiative put forth by the Edison Electric Institute, a group of transmission owners has established the Spare Transformer Equipment Program, designed to increase the industry's inventory of spare electric transformers. According to the application, this will ensure that the industry has sufficient capability to restore service in the event of "coordinated, deliberate destruction of utility substations." Any investor-owned utility, government-owned utility or rural electric cooperative in the U.S. or Canada that owns transformers may participate in the program. At present, 43 entities have signed on to the Spare Transformer Sharing Agreement, representing more than 60 percent of the Commission-jurisdictional bulk-power transmission system. "[T]he industry's efforts to voluntarily coordinate the sharing of spare transformers will enhance the reliability of the transmission system and security of our energy supply infrastructure in the event of an act of deliberate destruction," the Commission said.

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2006-10-02 DHS Daily OSIR;
http://www.statesman.com/news/content/news/stories/nation/10/02/2scada.html

SECURITY LACKING IN NETWORKS CONTROLLING NUCLEAR POWER STATIONS, ELECTRICAL GRIDS, WATER LINES.

Supervisory Control and Data Acquisition (SCADA) networks control nuclear power stations, water and gas lines, chemical plants, and other critical infrastructure. Many of them could be just as vulnerable today to attacks from computer hackers —- or terrorists —- as the Soviet system was nearly 25 years ago. Or even more vulnerable. That's because today, machines and computers are increasingly connected in a haphazard way to the Web. Rapid growth in easy-to-access wireless networks and the use of off-the-shelf software from Microsoft Corp. and others have also contributed. Hence the fear that five years after September 11, SCADA networks could become "the new airplanes," said Alan Paller of the SANS Institute. SCADA computers monitor and control the flow of electricity across the nation's power grids. Despite its importance, SCADA security is often an afterthought for corporate cybersecurity departments. That's because, so far, the networks haven't attracted computer hackers like financially oriented e-mail and online billing systems and corporate Websites have. "It's kind of like out of sight, out of mind," said Brian Davison of Austin Energy. At many utilities, "management has been away from the table," Davison said. Austin American-Statesman (TX)

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2006-10-03 DHS Daily OSIR; VNUNet http://www.vnunet.com/articles/print/2165511

U.S. INTERNET 'HIGHLY RESILIENT' TO TERROR ATTACK.

The Internet infrastructure in the U.S. would still be able to function even if terrorists were able to knock out key physical network hubs, researchers have claimed. According to academics who have completed a simulation of a major attack on the U.S. Internet infrastructure, it would be "very difficult" to cause major disruptions across the country. However, the research reveals that the destruction of some key elements could "seriously degrade" Internet quality. Morton O'Kelly, co-author of the study, said "There are so many interconnections within the network that it would be difficult to find enough targets, and the right targets, to do serious damage to Internet reliability nationwide." The researchers developed computer simulations in which they studied a simplified nationwide Internet network. They then simulated disruption or failures of parts of the network to see what would happen to Internet connectivity between 946 pairs of cities. For some city pairs, disruptions in nearly a dozen specific nodes would not make much difference in Internet reliability, but a disruption in a single critical node would cause major problems.

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2006-10-14 DHS Daily OSIR; Associated Press http://www.cnn.com/2006/EDUCATION/10/13/defending.the.classr

TEACHING KIDS TO FIGHT BACK AGAINST CLASSROOM INVADERS.

Youngsters in Burleson, TX, school district, a suburb of Fort Worth, are being taught not to sit there like good boys and girls with their hands folded if a gunman invades the classroom, but to rush him and hit him with everything they've got -- books, pencils, legs and arms. "Getting under desks and praying for rescue from professionals is not a recipe for success," said Robin Browne, a major in the British Army reserve and an instructor for Response Options, the company providing the training to the Burleson schools. That kind of fight-back advice is all but unheard of among schools, and some fear it will get children killed. But school officials in Burleson said they are drawing on the lessons learned from a string of disasters such as Columbine in 1999 and the Amish schoolhouse attack in Pennsylvania last week. The school system in this working-class suburb of about 26,000 is believed to be the first in the nation to train all its teachers and students to fight back, Browne said. At Burleson -- which has 10 schools and about 8,500 students -- the training covers various emergencies, such as tornadoes, fires and situations where first aid is required.

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2006-10-17 DHS Daily OSIR; CNET News http://news.com.com/FBI+director+wants+ISPs+to+track+users/2100-7348_3-6126877.html

FBI DIRECTOR WANTS ISPS TO TRACK USERS.

FBI Director Robert Mueller on Tuesday, October 17, called on Internet service providers (ISPs) to record their customers' online activities, a move that anticipates a fierce debate over privacy and law enforcement in Washington next year. "Terrorists coordinate their plans cloaked in the anonymity of the Internet, as do violent sexual predators prowling chat rooms," Mueller said in a speech at the International Association of Chiefs of Police conference in Boston. Law enforcement groups claim that by the time they contact ISPs, customers' records may have been deleted in the routine course of business. Industry representatives, however, say that if police respond to tips promptly instead of dawdling, it would be difficult to imagine any investigation that would be imperiled. It's not clear exactly what a data retention law would require. One proposal would go beyond Internet providers and require registrars, the companies that sell domain names, to maintain records too.

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2007-01-25 DHS Daily OSIR; University of New Hampshire http://www.unh.edu/news/cj_nr/2007/jan/lw25cyber.cfm

UNH UNVEILS CYBER THREAT CALCULATOR.

Hackers, terrorists and nations all use computers, but who really is capable of damaging U.S. critical infrastructure? The University of New Hampshire (UNH) Thursday, January 26, unveiled the UNH Cyber Threat Calculator, which assesses the level of threat any attacker poses to specific sectors in the country that rely on information technology. The UNH Cyber Threat Calculator was developed by researchers at UNH Justiceworks and students, and offers a new method to identify and quantify the threats posed to the United States' cyber infrastructure. To determine the overall threat level, analysts enter data for a particular organization or country into the calculator, which assigns a value to variables that measure the actor's intent and technological capabilities. These variables assess the actor's intent to use cyber warfare means, as well as its technical capabilities to put such means into practice. The higher number assigned to a possible attacker by the calculator, the greater the threat.

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2007-03-27 DHS Daily OSIR; Washington Post http://www.washingtonpost.com/wp-dyn/content/article/2007/03/26/AR2007032602088.html

ORDINARY CUSTOMERS FLAGGED AS TERRORISTS.

Private businesses such as rental and mortgage companies and car dealers are checking the names of customers against a list of suspected terrorists and drug traffickers made publicly available by the Department of the Treasury, sometimes denying services to ordinary people whose names are similar to those on the list. The Office of Foreign Asset Control's (OFAC) list of "specially designated nationals" has long been used by banks and other financial institutions to block financial transactions of drug dealers and other criminals. But an executive order issued by President Bush after the September 11, 2001, attacks has expanded the list and its consequences in unforeseen ways. Molly Millerwise, a Department of the Treasury spokesperson, said that the department has extensive guidance on compliance, both on the OFAC Website and in workshops with industry representatives. OFAC Website: http://www.treas.gov/offices/enforcement/ofac/

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2007-03-28 DHS Daily OSIR; Los Angeles Times http://www.latimes.com/news/nationworld/nation/la-na-guard28mar28,1,7908287.story

NATIONAL GUARD ILL-EQUIPPED AT HOME, COMMANDER SAYS.

The head of the National Guard warned Tuesday, March 27, that units nationwide have less than half the equipment they need to deal with natural disasters, terrorist attacks and other threats at home. Lieutenant General H. Steven Blum told members of the House armed services subcommittee on readiness that guardsmen being deployed to Iraq and other foreign hot spots are adequately equipped but that Army National Guard units stateside have, on average, just 40 percent of their required equipment on hand. That deficit cuts into the Guard's ability to respond to national emergencies and keep its "citizen soldiers" adequately trained for rapid deployment, he said.

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2007-04-24 DHS Daily OSIR; KSL (UT) http://www.ksl.com/?nid=148&sid=1143878

SECURITY CAUSING MAJOR POSTAL DELAYS TO CONGRESS.

Special security measures are still causing major postal delays more than five years after a mysterious murderer sent anthrax germs to Congress. For example, if a letter is addressed to a lawmaker in Washington, it could take two or three weeks or even a couple of months to arrive. Some staff have suggested that constituents e-mail or fax or even call. Security workers open every letter and package, shaking out any powders and testing for germs. Mail officials claim it all takes less than two weeks. But congressional staffers say it’s lucky if it's less than three weeks. In spite of the hassles, there's no major move afoot to make changes. Each year House and Senate members receive something like 20 million pieces of mail in their Washington offices. It shows that many Americans consider the mail a vital link to their voice in Washington, but it also shows just how big the security problem is.

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2007-04-26 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article102563-04-26-07-Web 30

HARVARD TO STUDY GOVERNMENT RESPONSE TO CRISES.

Harvard University’s John F. Kennedy School of Government has launched a research initiative aimed at helping government leaders better respond to and manage crisis situations. Harvard officials say the program, called Acting in Time, will generate research, discussion, and ideas to overcome the incapacity of governments to react quickly to catastrophic events. The program will not focus on specific solutions to disasters, such as Hurricane Katrina or terrorist acts, but rather will explore why governments are unable or unwilling to act when such events occur, officials said. “It is important to look beyond the crisis of the moment to the fundamental ability of governments and leaders to take action when they need to do so,” said Christopher Stone, faculty chairman of Acting in Time and a professor of the practice of criminal justice at Harvard. Solutions are rarely missing when governments face critical challenges, he said. “What’s missing is the ability of governments to act on what we know and to act in time to make a difference,” he said. “That’s the leadership skill set we will be trying to define through this initiative.”

Category 49.3 Anti-terrorist measures (e.g., public-area or school surveillance)

2007-04-30 DHS Daily OSIR; Associated Press http://www.foxnews.com/story/0,2933,269305,00.html

DEBATE REVIVED OVER PRIVATE USE OF TERROR WATCH LISTS.

The Lawyers Committee for Civil Rights of the San Francisco Bay Area alleges that more Americans than ever are being mistakenly connected to the Treasury Department's Office of Foreign Assets Control (OFAC) list of persons and companies engaging in or affiliated with terrorism. The report, titled "How a Treasury Department Terrorist Watchlist Ensnares Everyday Customers," concludes that "a growing number of Americans have endured stigma and lost opportunities in ordinary consumer settings" like buying a car or home. OFAC spokesperson Molly Millerwise said: "We have seen success, being able to choke off terror financing and proliferation financing...It's hard to set markers. Your success is the attack that didn't happen. But it's making it harder for terrorists to make, move and store money." The Terrorist Assets Report reports that as of 2005, the government has blocked $13.7 million in terror funds specifically through persons and entities listed on the Specially Designated Nationals and Blocked Persons list. In 2005, the U.S was blocking $479 million in funds connected to six countries listed as state sponsors of terrorism. Report: How a Treasury Department Terrorist Watchlist Ensnares Everyday Customers: http://www.lccr.com/03%202007%20OFAC%20Report.pdf

49.4 Airport &Air Transport security

Category 49.4 Airport &Air Transport security

2006-04-26 RISKS

PERSONAL ELECTRONIC DEVICES ON COMMERCIAL AIRCRAFT

Prof Peter Ladkin summarized the current state of knowledge about personal electronic devices (PEDs) on aircraft in a report for RISKS. He began with a summary of the problem:

"There has been plenty of discussion of the risks of operating personal electronic devices (PEDs) such as mobile telephones, gameboys and computers on board commercial transport aircraft. In the U.S., the use of mobile telephones on board flying aircraft is forbidden by the Federal Communications Commission, inter alia because such a phone would be within receiving range of many cells simultaneously and the technology is neither designed nor implemented to accommodate such cases. However, there is also the possibility of interference with the aircraft avionics."

His review of the literature strongly supports the aviation industry's concerns about electromagnetic interference (EMI) with avionics and points to widespread ignorance on the part of passengers about why PEDs are to be turned off during flight.

Category 49.4 Airport &Air Transport security

2006-05-18 DHS Daily OSIR; Reuters http://abcnews.go.com/US/wireStory?id=1977556 May 18, 2006

U.S. TO MONITOR BEHAVIOR AT MORE AIRPORTS

The U.S. Transportation Security Administration (TSA) will soon use more behavioral profiling at American airports to detect suspicious activity, a top official said on Thursday, May 18. TSA Director Kip Hawley said the agency would expand a pilot program that has trained officers to observe passengers' behavior currently at about a dozen airports. He said it will be expanded after the summer travel rush. The program began at Boston's Logan International Airport. It is also being implemented in Miami among other airports. George Naccara, the federal security director at Logan, said the TSA program is modeled on behavior detection systems used in Israel and some other countries. "It's been very effective overseas," Naccara said, where the effort "is much more confrontational and much more aggressive." Officers are taught to look for abnormal behavior in passengers, such as people wearing coats when it's warm in order to disguise bombs, or people acting fidgety or nervous. Naccara said they look for signs of "stress, fear and deception."

Category 49.4 Airport &Air Transport security

2006-07-24 DHS Daily OSIR; San Francisco Chronicle http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/07/24/BUGEHK1UA21.DTL

SURVEILLANCE VIA SOFTWARE HELPS AIRPORT.

In the Security Operations Center at San Francisco International Airport, a technician watches a dozen monitors fed by the 1,500 surveillance cameras scattered through the sensitive facility. At the far right sits the newest tool in the airport's security toolkit -- a computer monitor that displays images, selected by a new type of software, that sifts through that stream of surveillance video, sending out alerts when it detects certain actions or situations. The software being evaluated represents an emerging technology called video analytics. The idea is to use software algorithms to scan surveillance video gathered by closed circuit television cameras and to search for specific visual patterns -- such as two airport workers scooting through a security door at the same time, when they should enter one at a time, or a vehicle parked too long at a place where it shouldn't be. Jason Halverson, a security industry analyst with Frost & Sullivan in San Antonio, said these programs try to make better use of all the surveillance video that is currently captured giving security officials a better chance to thwart danger. Security experts say video analytics has been spurred by advances in computer technologies, and by reaction to terrorist attacks.

Category 49.4 Airport &Air Transport security

2006-08-08 DHS Daily OSIR; Associated Press http://www.usatoday.com/travel/news/2006-08-08-LAX-problems_x.htm

LAX MALFUNCTIONS RAISE SAFETY QUESTIONS.

A computerized system that guides arriving planes onto a runway at Los Angeles International Airport (LAX) failed, marking the second serious problem to disable the world's fifth-busiest airport in the past three weeks, officials said. The latest malfunction on Monday, August 7, caused flight delays across the nation. Aviation experts said the equipment failures raise questions about the nation's aviation system, which is straining under passenger loads that have rebounded to their highest levels since September 11, 2001. LAX, for example, averages 1,800 daily flights and will serve an estimated 18.7 million passengers this summer, 200,000 more than last year. "The FAA's complete instrument system, as we know, is somewhat accident prone," said Jack Keady, an aviation consultant who has followed the problems at LAX. Monday's malfunctioning equipment, called a localizer, acts as a beacon to guide arriving planes onto runways. It is most crucial when it is foggy or hazy. It was foggy at the airport on Monday. The problem was compounded because one of the airport's four runways was closed for a major construction project. To compensate, one of the departure runways was handling both departures and arrivals and it was that shared runway that had the problem.

Category 49.4 Airport &Air Transport security

2006-08-16 DHS Daily OSIR; Associated Press http://seattlepi.nwsource.com/national/1103AP_Britain_Airport_Security.html

MAN, BOY BYPASS LONDON'S GATWICK AIRPORT SECURITY.

Police briefly detained a man after he attempted to board an aircraft at Gatwick Airport to retrieve a lost wallet, authorities said Wednesday, August 16, one day after a 12-year-old boy got on a plane without a ticket or a passport. The incidents raised new concerns over airport security because the man had managed to bypass heightened security measures at London's second-largest airport. The boy was detected by the cabin crew before the flight took off.

Category 49.4 Airport &Air Transport security

2006-08-30 DHS Daily OSIR; United Press International http://www.upi.com/NewsTrack/view.php?StoryID=20060830-102959-6583r

IRAQI BARRED FROM NYC FLIGHT OVER ARABIC LETTERS ON T-SHIRT.

Security officials at New York's John F. Kennedy International Airport refused to allow a man to board his flight because of an Arabic inscription on his t-shirt. Iraqi-born architect Raed Jarrar said security staff told him his t-shirt, which said, "We will not be silent" in Arabic and English was upsetting other passengers, New York Public Radio, reported on Wednesday, August 30. Jarrar ended up putting on another t-shirt provided by Jet Blue airline staff over the original one.

Category 49.4 Airport &Air Transport security

2006-09-05 DHS Daily OSIR; CBC News (Canada) http://www.cbc.ca/canada/montreal/story/2006/09/05/qc-hasidicprayeronplane.html

JEWISH MAN REMOVED FROM AIRPLANE FOR PRAYING.

Some fellow passengers are questioning why an Orthodox Jewish man was removed from an Air Canada Jazz flight in Montreal last week for praying. The man was a passenger on a September 1 flight from Montreal, Quebec, Canada to New York City when the incident happened. The crew had to act in the interest of the majority of passengers, said Air Canada Jazz spokeswoman Manon Stewart. Jewish leaders in Montreal criticized the move as insensitive, saying the flight attendants should have explained to the other passengers that the man was simply praying and doing no harm.

Category 49.4 Airport &Air Transport security

2006-09-12 DHS Daily OSIR; Aero-News (FL) http://www.aero-news.net/index.cfm?ContentBlockID=d2fb9dcd-eee7-42d4-8815-2b88c80a1e88&

NEW YORK REQUIRES BACKGROUND CHECK ON STUDENT PILOTS.

New York Governor George Pataki signed a law that will require student pilots to undergo criminal background security checks. On Saturday, September 9, the governor finally put his signature on the bill that had been originally drafted in 2002. In a statement released by his office, Pataki wrote, "We'll now have the vital information that can help prevent people harboring bad intentions from gaining access to this critical knowledge, an important part of our firm commitment of doing everything we can to help keep New Yorkers as safe as possible." In addition to undergoing the background checks, the prospective flight student must wait for specific written approval from the Division of Criminal Justice Services before sitting in the airplane with an instructor.

Category 49.4 Airport &Air Transport security

2006-09-12 DHS Daily OSIR; CanWest News Service (Canada) http://www.canada.com/topics/news/national/story.html?id=b6eb4101-ee1f-4bae-9439-2157789eee2f

CANADA NEEDS TO RETHINK AIRPORT SECURITY, WARNS ISRAELI EXPERT.

Canada's intense focus on trying to search every traveler for weapons has created too much reliance on airport screeners while creating potential security hazards in long lineups, says Rafi Sela, a former member of the Israel Defense Forces and a security consultant who works with Tel Aviv's Ben-Gurion International Airport. Israeli airports would never allow large numbers of passengers to queue up for security checks because the lines themselves would be attractive targets to terrorists. The Israeli approach, Sela says, is to make the security check point just one stop in a broader security net that begins when passengers enter the airport terminal. Passengers checking in at Ben Gurion are greeted by an Israeli Airports Authority agent who looks directly into their eyes and asks seemingly benign questions intended to reveal signs of nervousness or stress. "They know what to look for. They know how suicide bombers act, how they look, how they walk," Sela said. Even staff at duty-free shops are trained to detect suspicious behavior. The Israelis are confident enough in their approach that, while other countries raced to ban liquids after the terrorism scare at London's Heathrow Airport last month, no such changes were made at Ben-Gurion.

Category 49.4 Airport &Air Transport security

2006-09-18 DHS Daily OSIR; Associated Press http://www.telegram.com/apps/pbcs.dll/article?AID=/20060914/APN/609141929

NEW SCREENING MEASURES FOR AIR CARGO.

Packages taken to airline ticket counters for shipment on passenger planes will have to go through the same security screening as checked baggage, Department of Homeland Security Secretary Michael Chertoff announced Thursday, September 14. Such packages -- brought to an airline's counter by individuals looking to get a package to another destination or by courier services -- already were being screened for the past several months at most airports around the country. But the screening now will be mandatory for 100 percent of those packages, Chertoff said at a news conference at Boston's Logan International Airport. "We closed that gap earlier this year, but we're now making this a legal requirement," Chertoff said, announcing that a formal directive was signed Thursday. Chertoff cited Logan as being the first airport in the country to begin screening 100 percent of its passengers' checked baggage for explosives. Logan had begun the package screening four months ago, using X-ray and explosive sensors that are used to screen passenger baggage on a system of conveyor belts. Most of the cargo on passenger planes, which comes from larger freight shippers, is subjected only to random checks.

Category 49.4 Airport &Air Transport security

2006-09-19 DHS Daily OSIR; Agence France-Presse http://www.usatoday.com/travel/flights/2006-09-19-passport-mistake_x.htm

BRITISH MAN FLIES TO HOLLAND ON HIS TWO-YEAR-OLD DAUGHTER'S PASSPORT.

At a time of heightened security at British airports, a businessman was allowed to fly from London to Amsterdam using his two-year-old daughter's passport. Car rental firm boss Mark Coshever picked up the wrong passport but was twice waved through passport checks at London Luton Airport and onto his EasyJet flight to Holland. The 29-year-old told the Daily Mirror he only realized his mistake when he touched down at Amsterdam and pointed out the fact to the immigration desk there. Dutch officials then checked his identity and gave him a letter allowing him to stay in the country for 48 hours. EasyJet admitted that staff misread Coshever's passport and had been disciplined.

Category 49.4 Airport &Air Transport security

2006-09-25 DHS Daily OSIR; Associated Press
http://news.kypost.com/apps/pbcs.dll/article?AID=/20060925/NEWS01/609250365/1014/NEWS02

EXPERT: AIRPORT ERRORS NOT SYSTEMIC.

Experts who study airplane accidents say the errors that lead to crashes are similar to the common mistakes people make in their everyday lives, akin to locking keys in the car or forgetting an item on a grocery list. "In an airplane, it gets you in trouble," said Scott Shappell, a professor at Clemson University who studies aviation accidents and the human errors that cause them. Shappell believes investigators will ultimately conclude that the errors that contributed to the crash of Comair Flight 5191 in Lexington are not systemic, but rather local, particular to that flight and that morning, he said. The jetliner crashed after trying to take off from the wrong runway at Blue Grass Airport. Scholars said as many as 80 percent of airplane accidents are caused by human error. An entire field of study is devoted to human factors in aviation. The discipline embraces not only how a cockpit is run but also how mechanical repairs are made. Its practitioners want to prevent mistakes, knowing, however, that mistakes are inevitable.

Category 49.4 Airport &Air Transport security

2006-09-28 DHS Daily OSIR; Associated Press http://www.washingtonpost.com/wp-dyn/content/article/2006/09/28/AR2006092801213.html

BEARDED MAN BRIEFLY FORCED OFF PLANE BY FELLOW PASSENGERS.

A Spanish university professor with a long beard and dark complexion said Thursday, September 28, he was briefly forced off an airliner during a layover on the Spanish island of Mallorca by passengers who feared he was an Islamic terrorist. Pablo Gutierrez Vega told The Associated Press that three German passengers on an Air Berlin flight approached him during a layover in Palma de Mallorca on August 30 en route from Seville, Spain, to Dortmund, Germany, and asked to search his carry-on luggage. The men told him that other passengers were frightened by his appearance, said Gutierrez Vega, a 35-year-old law professor at the University of Seville. The airline confirmed the incident. After realizing the men were not undercover police officers, Gutierrez Vega refused to hand over his luggage. The pilot then approached the group and led the professor to the runway so they could speak in private. On the runway, the pilot said he was willing to expel the passengers who confronted Vega. The pilot also said he could take Gutierrez Vega's luggage into the cockpit to pacify the other passengers.

Category 49.4 Airport &Air Transport security

2006-09-28 DHS Daily OSIR; Associated Press
http://www.iht.com/articles/ap/2006/09/28/america/NA_GEN_US_Air_Security.php

OFFICIALS DETAIN PASSENGER WHOSE BAG HAD MESSAGE DERIDING AIRPORT SECURITY CHIEF.

A businessman was detained when he tried to go through airport security with a message scrawled on his plastic bag of toiletries. "Kip Hawley is an Idiot" said the Baggie carried by Ryan Bird. His ire was aimed at the director of the Transportation Security Administration (TSA), the agency in charge of security at the nation's airports. Bird was detained by sheriff's deputies at the airport in Milwaukee, WI, for 25 minutes on Tuesday, September 26. Bird, a senior executive for a manufacturing company who travels weekly, said he is frustrated by the TSA's rules and by overbearing security personnel. Byrd first described the incident on an Internet forum called Flyertalk.com, saying that a TSA supervisor told him he had no free speech rights inside the airport's security checkpoint. TSA spokesperson Yolanda Clark said Bird was free to express his opinion, and there is no prohibition on writing on bags. "The passenger was never detained by TSA. Local law enforcement briefly interviewed him and determined he had not broken any laws, and he was allowed to fly," Clark said.

Category 49.4 Airport &Air Transport security

2006-10-02 DHS Daily OSIR; Voice of America http://www.voanews.com/english/AmericanLife/2006-10-02-voa40.cfm

U.S. AIRPORT SCREENERS LOOK FOR BEHAVIORS.

Five years after the attacks of September 11, U.S. transportation officials are rolling out a new type of screening program at airports across the country. It doesn't require computers or high-tech X-ray machines. Instead, it simply calls for screeners to watch. Officials won't say exactly what they're looking for, but Sergeant Peter Didomenica, who pioneered the Behavior Assessment Screening System (BASS) program at Boston's Logan Airport, says someone en route to a suicide mission can't help but display fear. "Adrenaline causes specific reactions to the body," he points out, "like increased heart rate, like perspiration, like sweaty palms, like increased breathing." So while terrorists may be getting better at outsmarting technology, there's almost no way to outsmart the primitive emotion of fear, according to George Naccarra, with the government's Transportation Security Administration in Boston. Boston's Logan Airport was the first in the country to use this type of behavioral screening. The state troopers' BASS program started shortly after September 11th, 2001. The federal program debuted about two years later and was tested at a handful of airports around the country. The TSA's Naccarra says the federal program, known as Screening of Passengers by Observation Techniques, or SPOT, is now making a nationwide debut.

Category 49.4 Airport &Air Transport security

2006-10-12 DHS Daily OSIR; Register (UK) http://www.theregister.co.uk/2006/10/12/airport_rfid/

AIRPORT TO TAG PASSENGERS.

Airport security chiefs and efficiency geeks will be able to keep close tabs on airport passengers by tagging them with a high-powered radio chip developed at the University of Central London. The technology is to be trialed in Debrecen Airport in Hungary after being in development for two-and-a-half years by University College London as part of an European Union-funded consortium called Optag. People will be told to wear radio tags round their necks when they get to the airport. The tag would notify a computer system of their identity and whereabouts. The system would then track their activities in the airport using a network of high definition cameras.

Category 49.4 Airport &Air Transport security

2006-10-18 DHS Daily OSIR; 24dash.com (United Kingdom) http://www.24dash.com/communities/11750.htm

'MAJOR SECURITY FLAWS' IN THE AIR CARGO INDUSTRY REVEALED.

Cargo on passenger flights is being sent without checks or X-rays in oversights that could potentially threaten the lives of passengers, BBC Radio 4's The World Tonight said on Tuesday, October 17. The security gaps emerged following a drug smuggling case at Kingston Crown Court in southwest London. The BBC said it began an investigation when the hearing revealed that the "known shipper" system used by air courier and cargo companies had been broken by drug smugglers and used to import large amounts of cocaine into the UK from America. During the case, a former employee of Federal Express (FedEx) admitted selling the confidential account numbers of reputable firms at FedEx's depot in Vauxhall, south London, the BBC said. This reportedly allowed a student and his accomplices abroad to smuggle in drugs using the security clearance and accounts of innocent companies. The BBC also reported that Brian Fenn, head of UK security for FedEx, admitted in evidence during the case that the known shipper system could also potentially be used to smuggle a bomb on to a plane undetected. The BBC said its investigation revealed that the Web-based system for tracking parcels could be used by terrorists to target particular flights.

Category 49.4 Airport &Air Transport security

2006-11-13 DHS Daily OSIR; Washington Technology http://www.washingtontechnology.com/news/1_1/daily_news/29709-1.html

BIOMETRIC AIRPORT ID CARDS COMING TO CANADA.

Canadian officials said they intend to deploy a new biometric identification card for 120,000 aviation workers at 29 major airports by year's end. Minister of Transport Lawrence Cannon proposed to implement the new Restricted Area Identity Card for airport personnel including flight crews, refuelers, and caterers. Authorized by Transport Canada and the Canadian Air Transport Security Authority, the card will incorporate fingerprints and iris scans, according to a November 10 government news statement. The card is touted as "the world's first-ever dual-biometric airport identification system," because it will use both fingerprint and iris biometrics, the announcement said.

Category 49.4 Airport &Air Transport security

2006-11-15 Effector Online http://www.eff.org/news/archives/2006_11.php#005000

BRIEF URGES SUPREME COURT TO TACKLE SECRET LAW. AMERICANS HAVE THE RIGHT TO SEE LAWS THEY MUST FOLLOW.

San Francisco - EFF and a coalition of nonprofit organizations asked the U.S. Supreme Court Monday to hear a case challenging a secret law governing travelers in American airports. The case centers on the Transportation Security Agency (TSA) requirement that travelers show identification before boarding commercial aircraft. So far, the TSA has refused to disclose the terms of the identification requirement to the public, claiming that they are "sensitive security information." In the amicus brief urging the Supreme Court to hear Gilmore v. Gonzales, EFF demonstrates that Congress never intended agencies to have unfettered discretion to impose requirements upon the public without allowing the public to review them. "The TSA is allowed to withhold some information from the public, but only in cases where transportation security is at risk," said EFF Staff Attorney Marcia Hofmann. "Simply showing Americans the rules they must follow can't possibly compromise security. The real danger here is meaningless secrecy, which can hide security flaws, frustrate the justice system, create confusion, and undermine government accountability." The Constitution and laws like the Freedom of Information Act (FOIA) prohibit the government from imposing secret laws on the public. But if the lower court decision permitting the secrecy is allowed to stand, it opens the door to other government agencies creating undisclosed rules and regulations without oversight. "'Security' shouldn't be a magic password allowing the government to escape accountability," said Hofmann. "The Supreme Court should hear this case and review why the TSA insists on keeping this basic information secret." The amicus brief was also signed by the American Association of Law Libraries, American Library Association, Association of Research Libraries, Center for Democracy and Technology, National Security Archive, Project on Government Secrecy of the Federation of American Scientists, and Special Libraries Association.
For the full amicus brief: http://www.eff.org/legal/cases/gilmore_v_gonzales/gilmore_amicus.pdf
For this release: http://www.eff.org/news/archives/2006_11.php#005000

Category 49.4 Airport &Air Transport security

2006-11-20 DHS Daily OSIR; United Press International
http://www.upi.com/NewsTrack/view.php?StoryID=20061120-120207-6418r

US AIRWAYS DENIES BOARDING TO AIR MARSHALS.

The government and Republic Airlines are reviewing a recent incident where federal air marshals were prohibited from boarding a plane in Washington, DC. The Federal Air Marshal Service confirms that its agents were removed from US Airways Express Flight 3464 flight leaving Ronald Reagan Washington National Airport on November 8 for Connecticut. After being seated on the plane, the marshals were reportedly called to the jet bridge where a gate agent demanded paperwork intended for off-duty law enforcement agents carrying weapons. The marshals returned to their seats after telling the gate agent they were on mission status and the paperwork was not applicable. Minutes later officers from the Metropolitan Washington Airport Authority ordered the marshals to exit the plane and even officials at the Department of Homeland Security could not persuade the airline to let them reboard. Federal Air Marshal spokesperson Conan Bruce said the agency was reviewing boarding rules that marshals say vary from airline to airline.

Category 49.4 Airport &Air Transport security

2006-11-21 DHS Daily OSIR; Associated Press
http://www.cnn.com/2006/US/11/21/passengers.removed.ap/index.html

SIX MUSLIM IMAMS TAKEN OFF PLANE.

Six Muslim imams were removed from a US Airways flight at Minneapolis-St. Paul International Airport on Monday, November 20, and questioned by police for several hours before being released, a leader of the group said. The six were among passengers who boarded Flight 300, bound for Phoenix, around 6:30 p.m. CST, airport spokesperson Pat Hogan said. A passenger initially raised concerns about the group through a note passed to a flight attendant, according to Andrea Rader, a spokesperson for US Airways. She said police were called after the captain and airport security workers asked the men to leave the plane and the men refused. The six Muslim scholars were returning from a conference in Minneapolis of the North American Imams Federation, said Omar Shahin, president of the group. Three of them stood and said their evening prayers together on the plane, Shahin said. The other passengers on the flight, which was carrying 141 passengers and five crewmembers, were re-screened for boarding, Rader said. The plane took off about three hours after the men were removed from the flight.

Category 49.4 Airport &Air Transport security

2007-03-23 DHS Daily OSIR; Information Week
http://www.informationweek.com/news/showArticle.jhtml

FCC SAYS 'NO' TO CELL PHONES ON AIRPLANES, BUT EUROPE SAYS 'YES'.

While the Federal Communications Commission (FCC) is moving to kill the idea of cell phone service on commercial aircraft in the United States, European regulatory agencies remain positive on in-flight mobile phone calling. FCC Chairman Kevin Martin on Thursday, March 22, told reporters that his agency would give up looking into whether to approve the use of cell phones on airplanes. An opposite situation is under way in Europe, however, where regulatory agencies are working to pave the way for cell phone use on commercial aircraft. It's going through the approval process right now," said Charlie Pryor, a London-based spokesperson for OnAir, a planned mobile phone service sponsored by European aircraft manufacturer Airbus. According to Pryor, the Europeans have been testing their system for months and certification is being reviewed by the European Aviation Regulatory Authority. Another process involves the use of radio spectrum, being studied by the European Conference of Postal and Telecommunications Administrations (CEPT). CEPT has been working to coordinate some 44 European nations so they can allocate spectrum for mobile phone service providers. One of the FCC's concerns is the potential for cell phones on airplanes to disrupt other radio communications, according to the New York Times.

Category 49.4 Airport &Air Transport security

2007-04-13 DHS Daily OSIR; Maui News (HI) http://www.mauinews.com/story.aspx?id=29469

SUSPECT FOUND WITH FORGED IDS BY TSA SCREENER IN HAWAII.

The name on the duffel bag read Robert Folsom. But when a federal Transportation Security Administration (TSA) screener looked through the bag March 29 at Lanai Airport, she found a Hawaii driver's license with a different name. As she continued to examine the traveler's belongings, she turned up 43 Hawaii driver's licenses, each with photos of the same man but with 35 different names, addresses and Social Security numbers, said Deputy Prosecutor John Tam. The suspect's is Shane James Deighan, a 33-year-old Honolulu resident with a prior forgery conviction. Also found in his baggage were 19 credit cards, 11 of them matching one of the Hawaii driver's licenses, with four of the credit cards signed on the back; three other apparently stolen Hawaii driver's licenses with other people's names and photos; two apparently stolen Texas driver's licenses with other people's names and photos; three Social Security cards, two blank checks, one military identification and a Canadian birth certificate. Deighan also had the personal information of a Maui police lieutenant whose name, address, Social Security number, and birth date were written in a notebook, possibly stolen last year from missing U.S. Department of Veterans Affairs records.

Category 49.4 Airport &Air Transport security

2007-05-08 DHS Daily OSIR; Associated Press http://www.sanluisobispo.com/349/story/36206.html

ISRAELI AIRPORT SECURITY METHODS STUDIED.

Airport directors from a half dozen U.S. cities are meeting with top Israeli security officials this week to learn about one of the world's most rigorous and effective, airline screening processes. The visitors noted the main difference between the two countries: Israeli security openly employs profiling, singling out passengers for stricter screening based on their appearance or ethnic group, a practice that is banned in the U.S. The directors, representing airports from California to Florida, inspected at the security arrangements at Ben Gurion International Airport near Tel Aviv, where safety concerns affect the design of everything from windows to trash bins. No successful hijacking has occurred on a plane leaving the airport, and no attack has taken place inside the terminal since the 1970s, although Israel and planes entering and leaving the country are prime targets for Islamic extremists. Israeli experts say bolstering security efforts requires an extensive, and at times intrusive, interrogation process. Upon reaching the departure terminal, all passengers undergo individual questioning by security officers, who probe everything from their religious beliefs to travel companions inside the country. Foreigners almost automatically receive closer scrutiny, and racial or other types of profiling can trigger extensive questioning and searching.

Category 49.4 Airport &Air Transport security

2007-05-11 DHS Daily OSIR; Reuters http://uk.reuters.com/article/technologyNews/idUKL2016544320070511

SMART CAMERAS TO TACKLE ABANDONED LUGGAGE ALARMS.

A suitcase lies abandoned in a busy airport terminal. Was it planted by a bomber, or carelessly left for a couple of minutes while the owner went to buy coffee? One of the commonest headaches facing security staff may soon be remedied with the help of "intelligent security cameras" developed by European scientists. A newly concluded research project relies on formulae known as algorithms to enable computers to analyze video images and spot potential threats, from abandoned baggage to people loitering suspiciously. For security staff at airports or railway stations, often monitoring images from dozens of surveillance cameras at once, the new technology offers the promise of picking out dangers that might otherwise be missed. "The idea is to automatically analyze and intelligently filter all of that video, but also to add a next level of intelligence," said James Ferryman, a specialist in 'computational vision' at the University of Reading in England.

Category 49.4 Airport &Air Transport security

2007-05-15 DHS Daily OSIR; Reuters http://www.eweek.com/article2/0,1895,2130462,00.asp

AMSTERDAM AIRPORT DEPLOYS BODY-SCANNING MACHINES.

Amsterdam's Schiphol airport began using new body-scanning machines at security checkpoints on Tuesday, May 15, the first major airport to use the technology to find metals and explosives hidden under clothing. The "security scan" system, which uses harmless radio waves to display head-to-toe images of people, is also being used by other airports on a trial basis, but Schiphol is the only one to deploy the technology for regular use at its checkpoints. Going through the scanner takes about three seconds, allowing users to avoid metal detectors or body searches. For privacy, the digital images are viewed by security personnel in another room and deleted after they are viewed. Schiphol handles about 160,000 passengers per day at peak times and is Europe's fourth-busiest hub. So far the security scan is voluntary but officials are hoping to expand it to include all passengers, crew and personnel. Schiphol is one of the world's most modern airports, with flat-panel screens, airport-wide Web access, and iris-scanners already on offer to those who want to bypass passport lines.

49.5 Rail, Port & Trucking security

Category 49.5 Rail, Port & Trucking security

2006-07-07 DHS Daily OSIR; Department of Homeland Security
http://www.dhs.gov/dhspublic/display?content=5727

SECURING THE NATION'S RAIL SYSTEMS.

Since the terrorist attacks of September 11, 2001, the 7/7 London subway bombings, and the Madrid rail bombings, the Department of Homeland Security (DHS) has taken several steps to manage risk and strengthen our nation's rail and transit systems by: (1) Providing funding to state and local partners; (2) Training and deploying manpower and assets for high risk areas; (3) Developing and testing new technologies, and; (4) Performing security assessments of systems across the country. While the majority of mass transit systems in this country are owned and operated by state and local government and private industry, securing these systems is a shared responsibility between federal, state, and local partners. Since 9/11 the Administration has provided significant resources to bolster these security efforts. Funds from DHS grants programs may be used for planning, training, equipment, and other security enhancements. DHS has provided roughly $18 billion in awards to state and local governments for programs and equipment that help to manage risk.

Category 49.5 Rail, Port & Trucking security

2007-01-03 Transportation Security Administration
http://www.tsa.gov/press/releases/2007/press_release_01032007.shtm

DHS ISSUES CREDENTIALING RULE TO SECURE ACCESS TO U.S. PORTS.

The Department of Homeland Security (DHS) on Wednesday, January 3, announced the issuance of the final rule for the Transportation Worker Identification Credential (TWIC) program, which enhances port security by checking the backgrounds of workers before they are granted unescorted access to secure areas of vessels and maritime facilities. The rule was posted publicly on Transportation Security Administration's (TSA) Website January 1, 2007, and has been delivered to the Federal Register for posting in the coming days. The rule lays out the enrollment process, disqualifying crimes, usage procedures, fees, and other requirements for workers, port owners, and operators. These guidelines allow the industry, government and public to prepare for the implementation of this important security program. The TSA and the U.S. Coast Guard held four public meetings around the nation and received more than 1,900 comments regarding the initial draft of this federal rule. Comments were filed by workers, port facility owners and operators, small businesses and others who would be affected by the new program. The rule is expected to impact more than 750,000 port employees, longshoreman, mariners, truckers and others who require unescorted access to secure areas of ports and vessels.
TWIC Implementation in the Maritime Sector final rule http://www.tsa.gov/assets/pdf/1652-AA41_twic_fr.pdf
U.S. Coast Guard's Homeport information: http://homeport.uscg.mil/mycg/portal/ep/home.do
TWIC program: http://www.tsa.gov/what_we_do/layers/twic/index.shtm

Category 49.5 Rail, Port & Trucking security

2007-04-12 DHS Daily OSIR; Reuters http://news.zdnet.com/2100-1009_22-6175410.html

NUCLEAR SCANNERS SAID READY FOR USE AT U.S. PORTS.

Tests underway at the New York Container Terminal have gone well enough that the director of the Department of Homeland Security's (DHS) Domestic Nuclear Detection Office said he was inclined to recommend deployment at 400 sites nationwide. "We're very optimistic that when we go to the secretary this summer he will give us permission to go to production," Vayl Oxford told reporters. Oxford is due to report to DHS Secretary Michael Chertoff in mid-July on the performance of three competing portals being tested alongside current technology at the terminal. The current technology can be set off by the radiation coming from a load of bananas or granite, slowing commerce when such cargo is flagged for further inspection. The ports of Los Angeles and Long Beach experience 400 to 500 such alerts a day, officials said. The advanced portals are meant to reduce false alarms by distinguishing natural radiation from enriched uranium or weapons-grade plutonium.

Category 49.5 Rail, Port & Trucking security

2007-05-16 DHS Daily OSIR; Department of Transportation http://www.dot.gov/affairs/fra1607.htm

FRA LAUNCHES AUTOMATED INSPECTION VEHICLES TO DETECT TRACK FLAWS.

Two new custom-built inspection vehicles equipped with state of the art technology to help identify track flaws that could lead to train derailments are now in service and will allow the Federal Railroad Administration (FRA) to triple the amount of track it inspects each year by automated means to nearly 100,000 miles, announced FRA Administrator Joseph H. Boardman. Boardman explained that the new automated track inspection vehicles increase the FRA's fleet to five and are primarily used on high-volume rail lines that carry hazardous materials and passenger trains. The new vehicles, known as the T-19 and the T-20, use a variety of technology to measure track geometry flaws such as whether two rails are level, if the width between the rails is acceptable, and if the shape of each rail meets federal standards to avoid derailments. Boardman said that acquiring and deploying the T-19 and T-20 is a major component of the FRA National Rail Safety Action Plan, which focuses on the most frequent, highest-risk causes of train accidents; optimizes the use of data to target federal inspection and enforcement resources; and accelerates research initiatives that hold promise to mitigate the greatest potential safety risks.

49.6 International border security, passports

Category 49.6 International border security, passports

2006-05-18 DHS Daily OSIR; Agence France-Presse http://www.usatoday.com/travel/news/2006-05-17-japan-fingerp rint_x.htm

JAPAN TO FINGERPRINT AND PHOTOGRAPH FOREIGN VISITORS

Japan's parliament narrowly approved on Wednesday, May 17, 2006
a bill to follow the United States in fingerprinting and photographing foreign visitors. Under the bill, which will go into effect by November 2007, all foreigners aged 16 or older will be photographed and electronically fingerprinted when they enter Japan. Permanent residents, including ethnic Koreans born in Japan, will be exempt from the law, along with state guests and diplomats. The information will be stored in a database for potential criminal investigations. Prime Minister Junichiro Koizumi's government says the law will help prevent terrorism and other crime in Japan, one of the United States' closest allies.

Category 49.6 International border security, passports

2006-07-25 DHS Daily OSIR; Seattle Times http://seattletimes.nwsource.com/html/localnews/2003149964_portsecurity25.html

PIERCING PORT SECURITY AS EASY AS HITCHING A RIDE.

Ever since 9/11, U.S. seaports have been preparing for an attack. Fences are up, cameras and lights are on, and anational computer system is crunching data on all cargo coming into the U.S. on ships. But many ports appear to have left at least one gaping hole in their security: simply by riding along with truck drivers to drop off and pick up cargo, an investigative reporter for the Seattle Times easily penetrated the security of ports in Los Angeles-Long Beach and Seattle, two of the nation's largest port complexes. In the only instance where identification was sought, flashing an expired driver's license was all it took before a uniformed guard waved the truck and reporter through the gate. Port officials nationwide know about this lapse in security and say they are doing what they can. A new federal driver-identification system is planned over the next two years as one effort to secure "the land side." Most ports lease their docks to private companies. Those tenants -- the terminal operators -- develop their own security plans, which are approved by the Coast Guard, the agency with overall security responsibility for port facilities.

Category 49.6 International border security, passports

2006-08-07 DHS Daily OSIR; VNUNet http://www.vnunet.com/computing/news/2161836/kacers-crack-biometric

US, UK RFID BIOMETRIC PASSPORTS CRACKED.

Biometric passports used by the UK, U.S. and other countries have been cloned by a German security consultant, raising furtherdoubts over the technology. Lukas Grunwald, a consultant with DN-Systems, told a Defcon security conference in Las Vegas that the data, stored on RFID chips, could be copied on to blank chips which could then be used in fake passports. Grunwald says it took just two weeks to figure out how to clone the passport chip, and cost him $200. He tested the attack on a new European Union German passport, but the method would work on any country's e-passport, since all of them will be adhering to the same standard. Although he can clone the tag, Grunwald says it's not possible, as far as he can tell, to change data on the chip, such as the name or birth date, without being detected. Although countries have talked about encrypting data that's stored on passport chips, this would require that a complicated infrastructure be built first, so currently the data is not encrypted.

Category 49.6 International border security, passports

2006-08-11 EDUPAGE; San Jose Mercury News
http://www.siliconvalley.com/mld/siliconvalley/15254772.htm

US PRESSES AHEAD WITH ELECTRONIC PASSPORTS

The U.S. State Department is expected to begin issuing passports that include electronic chips containing all of the holder's information, including a photo, in electronic format. Government officials say the new passports will increase border security while speeding up the process of entering or leaving the country at airports and seaports. Privacy and security experts disagree, however. A German security expert recently demonstrated how the information on an electronic passport could be copied. Others expressed concern that the electronic signals between the passports and the readers could be intercepted, giving hackers access to personal information. Randy Vanderhoof, executive director of the Smart Card Alliance, said that copying an electronic passport represents no more risk than copying a conventional one. Because the information is encrypted, he said, changes to the information--which would compromise security--are not possible. Sherwin Siy, staff counsel at the Electronic Privacy Information Center, said that the shortcomings of the new passports outweigh any benefits from them.

U.S. ROLLS OUT E-PASSPORTS

After lengthy delays resulting from security concerns, the United States has begun issuing passports equipped with RFID tags. The tags, which transmit data including the passport holder's photo and signature, are susceptible to illicit scanners that "skim" the information from unsuspecting individuals, according to those opposed to e-passports. The U.S. State Department said it has implemented measures to address security concerns, including a metallic mesh woven into the cover of the passport that "makes it nearly impossible to access the chip when the book is closed." Additionally, starting this week, all U.S. points of entry will have equipment to read and process information in e-passports issued by the more than two dozen countries in the Visa Waiver Program. All of those countries issue e-passports, and visitors from those nations are not required to obtain a visa to enter the United States. Critics said U.S. authorities have not addressed the problems associated with e-passports. Kevin Mahaffey of security firm Flexilis wrote a report indicating that despite the mesh in the cover, the passports can still be read if they are open "even a fraction of an inch."

[Internet News, 23 October 2006 http://www.internetnews.com/wireless/article.php/3639411]

Category 49.6 International border security, passports

2006-09-04 DHS Daily OSIR; Washington Times (DC) http://washingtontimes.com/national/20060903-112722-4471r.htm

NATIONAL GUARD PRESENCE A 'VITAL ASSET,' SAYS BORDER CHIEF.

The head of the U.S. Border Patrol says the deployment of National Guard troops along the U.S.-Mexico border by President Bush has given his agency personnel, equipment and engineering capabilities at unprecedented levels. "Operation Jump Start continues to be beneficial for the Border Patrol and the National Guard," said Chief David V. Aguilar. "The National Guard continues to serve as a vital asset in the effort to protect America from future terrorist attacks and mitigate illegal border incursions." Nearly 6,200 Guard troops have been deployed along the border from California to Texas as part of Mr. Bush's $760 million plan to upgrade border security and give the Border Patrol time to recruit, hire and train 6,000 additional agents for assignment along the U.S.-Mexico border. The Guard troops are building roads and fences, adding cameras and sensors, conducting aerial reconnaissance, providing medical aid and communications support, and assisting at highway checkpoints.

Category 49.6 International border security, passports

2006-11-15 DHS Daily OSIR; National Journal's Technology Daily
http://www.govexec.com/dailyfed/1106/111506tdpm1.htm

INSPECTOR GENERAL OUTLINES FLAWS IN BORDER SECURITY PLAN.

An estimated $2 billion program for border security faces numerous financial and management risks similar to those that doomed past border security efforts, Department of Homeland Security (DHS) Inspector General (IG) Richard Skinner said Wednesday, November 15, in prepared testimony. The department has not adequately defined the operational requirements and acquisition baseline for the initial phases of the Secure Border Initiative (SBInet). SBInet is intended to gain control of the nation's borders by integrating technology, personnel, infrastructure, and processes. DHS Secretary Michael Chertoff has said he believes the department can achieve operational control of the borders by 2008. Skinner, however, said SBInet is vulnerable to changing schedule and cost estimates. "Until the department fully defines, validates and stabilizes the operational requirements underlying the SBInet program, the program's objectives are at risk, and effective cost and schedule control are precluded," Skinner wrote. He added, "The absence of an acquisition program baseline is a significant risk to the success of the SBInet program." Skinner noted that previous programs to achieve border security, such as the Integrated Surveillance Intelligence System and America's Shield Initiative, failed due to improper management. IG congressional testimonies: http://www.dhs.gov/xoig/rpts/gc_1163620428568.shtm Risk Management Advisory for the SBInet Program Initiation, OIG-07-07: http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_07-07_Nov06.pdf

Category 49.6 International border security, passports

2007-05-23 DHS Daily OSIR; Canadian Press
http://www.canada.com/topics/news/world/story.html?id=07fe2b24-66f3-4cc6-9edf-f9fff4b966f4&k=89370

SENATORS INTRODUCE BILL TO USE DRIVER'S LICENSES INSTEAD OF PASSPORTS.

Canada's push for an alternative to passports at the border has a major endorsement: Two U.S. senators have introduced legislation to create a secure driver's license for Americans to use instead. Minnesota's Norm Coleman and Susan Collins of Maine say it would be foolish not to allow the voluntary program since there have been a lot of improvements in the security of licenses. The bill would require U.S. officials to wait on the passport plan at land crossings until a pilot project using enhanced licenses in Washington state and British Columbia is finished.

49.7 National ID cards/documents; REAL ID

Category 49.7 National ID cards/documents; REAL ID

2007-01-30 Effector Online

MAINE REJECTS REAL ID.

The Real ID Act took a blow last week, when Maine became the first state to formally declare its opposition. The Maine legislature voted overwhelmingly to refuse to comply with the act's mandates, and requested that Congress repeal the law. The Real ID Act essentially forces states to create a national ID. Under the law, state drivers licenses will only be accepted for "federal purposes" -- like accessing planes, trains, national parks, and court houses -- if they conform to certain uniform standards. The law also requires a vast national database linking all of the ID records together. Estimated costs of $12 billion or more will be passed on to the states and, ultimately, average citizens in the form of increased DMV fees or taxes. "It's not only a huge federal mandate, but it's a huge mandate from the federal government asking us to do something we don't have any interest in doing," said Maine's House Majority Leader Hanna Pingree. Meanwhile, opposition in other states is growing. Similar measures rejecting the Real ID Act are under consideration in 11 states, including Montana, Georgia, Massachusetts and Washington state. For information about the dangers of Real ID: http://www.eff.org/Privacy/ID/RealID/
For this post and related links: http://www.eff.org/deeplinks/archives/005098.php

Category 49.7 National ID cards/documents; REAL ID

2007-03-06 Effector Online http://www.eff.org/Privacy/ID/RealID/

CONGRESS CONSIDERS REPEALING THE REAL ID ACT

The federal government took another step last week towards forcing you to carry a national ID in order to get on airplanes, open a bank account, enter federal buildings, and much more. . . . On Thursday, the Department of Homeland Security (DHS) released draft regulations for implementing REAL ID, which makes states standardize drivers' licenses and create a vast national database linking all of the ID records together. Once in place, uses of the IDs and database will inevitably expand to facilitate a wide range of tracking and surveillance activities. Remember, the Social Security number started innocuously enough, but it has become a prerequisite for a host of government services and has been co-opted by private companies to create massive databases of personal information. REAL ID won't just cost you your privacy. The states and individual taxpayers bear the estimated 23 billion dollar burden of implementing the law, and that figure is probably low given that the necessary verification systems don't exist yet. And what will you get in return? Not improved national security, because IDs do little to stop those who haven't already been identified as threats, and wrongdoers will still be able to create fake documents. REAL ID is fundamentally flawed, and DHS' proposed regulations do nothing to change that. Thankfully, the tide is turning against REAL ID in a big way -- state legislatures around the country are passing or considering legislation rejecting its implementation, and Congress is considering repealing it. The DHS regulations mean that states must have an implementation plan ready by October 2007. . . .
Read the San Jose Mercury News' editorial, "Time to drop expensive, unrealistic ID plan":
http://www.mercurynews.com/mld/mercurynews/news/opinion/16843010.htm
For more information about the REAL ID Act: http://www.eff.org/Privacy/ID/RealID/

[MK notes: title altered, some text elided and outdated links to political-action pages removed.]

Category 49.7 National ID cards/documents; REAL ID

2007-03-21 DHS Daily OSIR; Charlotte Observer (NC) http://www.charlotte.com/112/story/58095.html

AUDIT REVEALS LICENSE FLAWS.

North Carolina has issued nearly 27,000 driver's licenses based on invalid Social Security numbers, presenting possible security threats and potentially worsening the problem of identify theft, the state auditor's office reported Tuesday, March 20. In August, however, the state Division of Motor Vehicles instituted a tougher law that, along with an existing online verification program, can ensure that the state issues only valid licenses, according to the auditor's office. Commissioner George Tatum said the DMV will notify state and federal authorities in cases involving licenses with invalid numbers that were obtained fraudulently. State officials said it's difficult at this point to estimate how many might be cases of fraud. North Carolina State Auditor Les Merritt's office discovered the problem when it compared the 8.1 million N.C. driver's licenses currently in use with the Social Security Administration's database of valid numbers, as well as the federal agency's list of numbers issued to people who are now deceased.

Category 49.7 National ID cards/documents; REAL ID

2007-05-09 DHS Daily OSIR; Government Technology
http://www.govtech.net/magazine/channel_story.php/105401

BARCODE IN PROPOSED REAL ID DRIVER'S LICENSE WOULD BE INADEQUATE FOR SECURITY, PRIVACY.

According to the Smart Card Alliance, the Department of Homeland Security (DHS) should not rely on static 2-D barcode technology to store citizens' personal information on Real ID driver's licenses or identification cards due to its inherent security drawbacks. These comments were made in response to the DHS Notice of Proposed Rulemaking on minimum standards for Real ID cards. Instead, the Alliance strongly recommends that DHS raise the security level for state-issued driving credentials to equal that which has been mandated in other federal programs, namely by using smart card technology. The Alliance suggests that smart cards represent a much more secure platform for preventing forgery, cloning, counterfeiting and theft or alteration of personal data stored on Real ID cards, tactics which are far easier to employ against barcode-based systems. The Alliance also notes that Real ID credentials will become high-profile targets for identity thieves and fraudsters, since they will be used to establish identity, the right to drive and the right to travel. These factors make it all the more crucial that DHS get the choice of protective technology for Real ID documents right.

49.8 Background checks & security clearances

Category 49.8 Background checks & security clearances

2006-05-01 EDUPAGE;

PENTAGON HALTS CONTRACTOR CLEARANCES

The Pentagon stopped processing security clearances for government contractors this week, potentially exacerbating a shortage of employees authorized to work on the government's most secret programs. The Defense Security Service (DSS) blamed overwhelming demand and a budget shortfall for the halt, which caught the government contracting community by surprise. Already, 3,000 applications have been put on hold, said Cindy McGovern, a DSS spokesperson. "We're holding them [the applications] now to see if we can resolve the issue. The more drastic step would be not accepting them" at all, McGovern said, a step the agency considered but dropped for now. The demand for security clearances among private companies has grown dramatically since the September 11, 2001, terrorist attacks as the government increasingly relies on contractors to do intelligence gathering and work on classified programs. There has been growing frustration with the wait time, which some companies have described as up to a year, to obtain clearances for new employees. The move affects not only defense contractors, but also those who work on projects for more than 20 other agencies, including NASA and the Department of Homeland Security. DSS blames, in part, the sheer volume of requests. Between October and March, more than 100,000 security-clearance applications were submitted.
http://www.washingtonpost.com/wp-dyn/content/article/2006/04/28/AR2006042801878.html

Category 49.8 Background checks & security clearances

2006-08-08 DHS Daily OSIR; Washington Technology
http://www.washingtontechnology.com/news/1_1/daily_news/2909 9-1.html

DOD REVISES SECURITY CLEARANCE GUIDANCE.

The Pentagon has cleared the way for defense industrial workers who are facing delays in renewing their security clearances to remain on the job, Rep. Rob Simmons (R-CT), said in a news release. Budget constraints prompted the Department of Defense (DoD) in April to halt processing of industry clearances for several weeks. As a result, many re-investigations are overdue.

News release: http://simmons.house.gov/UploadedFiles/DoDClearances%20--%20 Aug2.pdf

Category 49.8 Background checks & security clearances

2007-01-08 DHS Daily OSIR; Federal Computer Week http://www.fcw.com/article97293-01-08-07-Web

REPORT: BOOM EXPECTED IN HIRING SECURITY-CLEARED WORKERS.

The hiring of workers with security clearances is expected to surge the first quarter of 2007 as a result of the many multimillion-dollar Department of Defense contracts that were awarded in December, according to the first edition of the ClearanceJobs Report for 2007. According to ClearanceJobs.com, an online recruiting service, those estimates could change because although some employers post jobs online that are contingent upon a contract award, many job seekers don't like applying for positions that don't yet exist. ClearanceJobs said the job postings in December showed a strong increase in the number of positions requiring higher-level clearances. When compared to the preceding month, there were 10 percent more jobs posted requiring a Top Secret or higher clearance the final month of 2006.

Category 49.8 Background checks & security clearances

2007-02-14 DHS Daily OSIR; USA TODAY http://www.usatoday.com/news/washington/2007-02-14-top-secret-clearances_x.htm

WHITE HOUSE LOOKS FOR FASTER TOP-SECRET CLEARANCES.

The White House is considering making it easier for people to obtain top-secret security clearances by eliminating some time-consuming background checks, says the Bush administration's point man on clearances. The goal, says Clay Johnson III, deputy director of the Office of Management and Budget, is to speed up a process that, according to a series of government reports, wastes millions of dollars and endangers public safety by leaving thousands of defense, homeland security, and intelligence jobs unfilled for more than a year. Johnson reported to Congress on Wednesday, February 14, that the executive branch is making "significant progress" toward clearing a backlog of uncompleted clearance applications that government contractors and others say exceeds 350,000. Johnson's report is required by a December 2004 intelligence-reform law that said 80 percent of clearance applications should be investigated, granted or rejected within 120 days. Clearances are "long overdue" for an overhaul, says Rep. Tom Davis, of Virginia, the top Republican on the House Oversight and Government Reform Committee. Davis' district in the Washington suburbs includes thousands of government workers and contractors.

Category 49.8 Background checks & security clearances

2007-05-20 DHS Daily OSIR; Associated Press http://www.journalnow.com/servlet/Satellite?pagename=WSJ%2FMGArticle%2FWSJ_BasicArticle&c=MGArticle&cid=1173351272752&path=!localnews&s=1037645509099

COMPANY HIRED TO CHECK LOTTERY SECURITY NOT CHECKED.

A company hired to audit the security systems of the North Carolina Lottery wasn’t checked by state officials, who would have found that the company isn’t registered to do business in the state, The Charlotte Observer reported Saturday, May 19. Tidwell Dewitt LLC of Alabama was picked to check computer systems that allow printing of lottery tickets at stores and other locations. The company has also been named in a $4 million negligence lawsuit in Atlanta, claiming that it failed to find an embezzlement at a company whose books it audited for years. Tidwell official Drew Sipos said that Tidwell didn’t have to register because a computer-services company is handling the audit for it, not an accounting company. Sipos also said that the lawsuit filed in Atlanta was meritless. But Robert Brooks, the executive director of the state Board of CPA Examiners, said that any company hired to work in North Carolina has to register.

Category 49.8 Background checks & security clearances

2007-05-22 DHS Daily OSIR; SC Magazine http://scmagazine.com/us/news/article/659068/los-alamos-beefs-security-wake-data-breach/

LOS ALAMOS INCREASES SECURITY IN WAKE OF DATA BREACH.

The theft of classified information by a contractor's former employee has forced the Los Alamos National Laboratory to implement a variety of tactical and strategic security policies commonly found in a private enterprise. The lab has disabled all ports, including USB ports, on classified computers -- some via physically gluing the port shut, others with locking devices or software -- and has begun encrypting personal information on laptop hard drives.

Category 49.8 Background checks & security clearances

2007-05-29 DHS Daily OSIR; Associated Press http://us.rd.yahoo.com/dailynews/ap/brand/SIG=br2v03;_ylt=AmgAQi9nF7cKLuH6HOFnWsKWwvIE/*http://www.ap.org

PRIVATE GUARDS A WEAK LINK IN SECURITY.

Legions of ill-trained, low-paid private security guards are protecting tempting terrorist targets across the U.S. The security guard industry found itself involuntarily transformed after September 2001 from an army of "rent-a-cops" to protectors of the homeland. Yet many security officers are paid little more than restaurant cooks or janitors. The industry is governed by a maze of conflicting state rules, according to a nationwide survey by The Associated Press. Wide chasms exist among states in requirements for training and background checks. Tens of thousands of guard applicants were found to have criminal backgrounds. Paul Maniscalco, a senior research scientist at George Washington University, is helping to change the security guard culture. He recently developed an anti-terrorism computer course for shopping mall guards, who are being taught that they now have more concerns than rowdy teenagers and shoplifters. Congressional investigators reported last year that 89 private guards working at two military bases had histories that included assault, larceny, possession and use of controlled substances and forgery. The security businesses' own trade group, representing the largest firms, acknowledges the industry as a whole isn't ready to recognize signs of terrorism and respond to an attack.

49.9 Search & seizure or wiretap laws, warrants, court orders

Category 49.9 Search & seizure or wiretap laws, warrants, court orders

2006-05-27 EDUPAGE; New York Times
http://www.nytimes.com/2006/05/27/technology/27apple.html

COURT PROTECTS ONLINE JOURNALISTS

A California appeals court has overturned a lower-court ruling, saying that online journalists have as much protection under the First Amendment as traditional journalists. The case involved an action by Apple Computer to discover the identity of individuals responsible for revealing company secrets online. Apple had argued that the information was shared not by legitimate reporters but by people who were violating the company's trade secrets. The appeals court said that online journalists are covered by a state law that guarantees the confidentiality of journalists' sources. The three judges on the panel said there is no reasonable method to distinguish legitimate from illegitimate news and that First Amendment rights trump Apple's demand to know who leaked the information. Observers said the case could have far-reaching implications for bloggers and others who post information and opinions online outside the context of traditional journalism.

Category 49.9 Search & seizure or wiretap laws, warrants, court orders

2006-06-09 EDUPAGE; San Jose Mercury News
http://www.mercurynews.com/mld/mercurynews/14781403.htm
<http://www.educause.edu/email/edupage/ep061206/track.asp?id=story_2>

COURT REJECTS CHALLENGE TO CALEA EXPANSION

A federal appeals court has ruled against a challenge to an expansion of the Communications Assistance for Law Enforcement Act (CALEA) to cover network traffic. CALEA requires providers of telecommunications services to make their systems available to law enforcement for authorized wiretapping. The FCC has sought to expand CALEA to cover Internet networks also. The appeals court ruled 2-1 that the FCC is permitted to apply CALEA to networks. A coalition representing higher education had challenged the expansion of CALEA, saying that the law was not written with data networks in mind and that such an expansion would impose considerable costs on higher education for compliance.

Speaking for the majority, Judge David Sentelle said the FCC's interpretation of CALEA to cover data networks was reasonable. Judge Harry Edwards, who dissented in the opinion, said the FCC discounted an exemption in the law for information services.

Category 49.9 Search & seizure or wiretap laws, warrants, court orders

2006-08-07 EDUPAGE; Inside Higher Ed http://www.insidehighered.com/news/2006/08/07/wireless

BOWDOIN BACKS AWAY FROM CITY WI-FI, CITES CALEA

A planned rollout of wireless Internet service by Bowdoin College to the residents of in Brunswick, Maine, has been halted, at least temporarily, due to concerns over the Communications Assistance for Law Enforcement Act (CALEA). The FCC has said that the law, which mandates law enforcement access to communications systems, should apply to network operators, including colleges and universities. Higher education has opposed that decision, saying it would be extremely costly for them to comply and that there are other ways for institutions to cooperate with law enforcement. Following legal action and lobbying, a court allowed an exception for "private" networks. Bowdoin, which is in Brunswick, had been working to implement a wireless network in the city for students and town residents. Saying that it isn't clear whether allowing town residents to access the network would compromise its being a "private" network, officials from the college have decided that the network will only be available to students. Mitch Davis, CIO at Bowdoin, noted that the plan to open the network to everyone in town is currently suspended, not dead.

Category 49.9 Search & seizure or wiretap laws, warrants, court orders

2007-03-13 Effector Online http://www.eff.org/patriot/sunset/505.php

ABUSE OF SURVEILLANCE POWERS

The FBI has blatantly abused a key U.S.A.P.A.T.R.I.O.T. Act provision and knowingly violated the law to spy on Americans' telephone, Internet, and other personal records, as documented in a report released by the Justice Department last week. . . . Before U.S.A.P.A.T.R.I.O.T., the FBI could use so-called National Security Letters [NSLs] only for securing the records of suspected terrorists or spies. But under U.S.A.P.A.T.R.I.O.T., the FBI can use them to get private records about anybody without any court approval as long as it believes the information could be relevant to an authorized terrorism or espionage investigation. According to the Justice Department's Inspector General, the FBI's misuse of its authority included issuing NSLs to spy on people who weren't the subject of any existing investigation whatsoever. The FBI also lied to Congress and underreported its use of NSLs by many thousands. Worse still, the FBI has ignored its own lawyers' advice and intentionally evaded U.S.A.P.A.T.R.I.O.T.'s thin bounds, improperly requesting and obtaining personal records through so-called "exigent letters" that Congress never authorized. That's only a sampling of the horror story painted by the report, and, had Congress not ordered the Inspector General to review the FBI's activities last year, these abuses might have never been revealed. From the moment U.S.A.P.A.T.R.I.O.T. was passed, we said the NSL power was ripe for abuse and unconstitutional, and it's clearer than ever that Congress should repeal U.S.A.P.A.T.R.I.O.T.'s expansion of NSL powers and reform the U.S.A.P.A.T.R.I.O.T. Act as a whole. Moreover, Congress must broadly investigate the Administration's use of surveillance powers, including the NSA's massive and illegal domestic spying program. Congress and the American public have been kept in the dark about such clear violations of the law and Americans' privacy for far too long. Immediate and thorough oversight hearings are necessary to uncover the truth and hold the Administration accountable. . . .

EFF press release about the report: http://www.eff.org/news/archives/2007_03.php#005152
For a brief summary of U.S.A.P.A.T.R.I.O.T.'s expansion of the NSL power: http://www.eff.org/patriot/sunset/505.php
For the Inspector General's report: http://www.usdoj.gov/oig/special/s0703b/final.pdf

[MK notes: acronym converted to fully-punctuated version for political principle: fighting propaganda value of usual acronym.]

Category 49.9 Search & seizure or wiretap laws, warrants, court orders

2007-05-16 Effector Online http://www.eff.org/legal/cases/att

HOUSE AFFIRMS LIMITS ON WARRANTLESS SPYING

Last week, the House passed legislation aimed at preventing illegal government spying. Attached as an amendment to the intelligence budget authorization bill, the legislation reaffirms that the NSA's domestic surveillance program must comply with Congress' laws. Meanwhile, the House did not pass a Bush Administration proposal that would radically expand the government's ability to spy without warrants while also threatening to let telecom providers off the hook for assisting in the illegal NSA program. Aggressive Congressional action to stop the illegal spying is long overdue, and this is an important first step in the right direction.
To learn about EFF's case against AT&T for illegally assisting the NSA: http://www.eff.org/legal/cases/att

Category 49.9 Search & seizure or wiretap laws, warrants, court orders

2007-05-16 Effector Online http://www.eff.org/effector/20/19.php

AP: ACTING AG REFUSED TO REAUTHORIZE SPYING PROGRAM IN 2004

The AP reports: "President Bush's warrantless wiretapping program was so questionable that a top Justice Department official refused for a time to reauthorize it, sparking a battle with top White House officials at the bedside of an ailing attorney general, a Senate panel was told Tuesday. "Former Deputy Attorney General James Comey told the Senate Judiciary Committee on Tuesday that he refused to recertify the program because Attorney General John Ashcroft had reservations about its legality just before falling ill with pancreatitis in March 2004."
For the whole article: http://www.abcnews.go.com/Politics/wireStory?id=3175945
On January 1, 2006, the NY Times recounted a similar set of events, though Mr. Comey declined to comment on the story: http://www.nytimes.com/2006/01/01/politics/01spy.html?ex=1179374400&en=cb8221ee6567f18f&ei=5070
During his testimony Tuesday, Comey stated "The program was reauthorized without us and without a signature from the Department of Justice attesting as to its legality."
You can read the full transcript of Comey's testimony here:
http://gulcfac.typepad.com/georgetown_university_law/files/comey.transcript.pdf

4A1 Framing, mashups

Category 4A1 Framing, mashups

2007-01-18 DHS Daily OSIR; CNET News
http://news.com.com/At+Mashup+Camp%2C+geeks+plot+future+of+Web/2100-1012_3-6151162.html

MASHUPS: THE FUTURE OF THE WEB?

Alan Taylor is living in the Wild West of Web development, and he has the scars to prove it. In his spare time, Taylor builds mashups -- Web applications that combine content from more than one source and have caught on as Web providers from Amazon.com to Microsoft make their data programmatically available to outsiders. But while he is breaking new ground on the Internet, he is also pushing legal and business boundaries. His Amazon Light application -- a stripped-down site for buying and renting goods through Amazon -- attracted two cease-and-desist orders a couple of years back, one from Amazon and another from Google. Taylor, who holds a day job as a senior Web developer at Boston.com, survived the legal threats without much trouble, but his experience points to the relative immaturity of mashups, which advocates believe represent the Web's cutting edge. Large software vendors catering to corporate software developers or independent software vendors have spent years establishing a suite of Web services standards and infrastructure software while advocating a modular design, called a service-oriented architecture. Mashups, by contrast, tend to focus on speed and simplicity, wiring together different Websites using quick and lightweight methods.

4A2 Pointing, linking, deep linking, metatext

Category 4A2 Pointing, linking, deep linking, metatext

2006-09-18 EDUPAGE; CNET http://news.com.com/2100-1030_3-6116591.html

COURT IN BELGIUM ORDERS GOOGLE TO STOP REPOSTING NEWS

A Belgian court has ordered Google to stop using news stories from a number of French-language newspapers on its Web site. An organization called Copiepresse, which manages copyright for French and German newspapers in Belgium, had complained that Google does not ask permission to use the papers' content, nor does it reimburse the papers, even though Google sells advertising and makes money from the content it posts on its site. The court agreed and ordered Google to stop using the disputed news articles. If Google does not comply, it will be subject to a fine of US$1.3 million per day. Margaret Boribon, general secretary for Copiepresse, said she would inform other news organizations in Europe of the decision, which might allow them to pursue similar injunctions in other markets.

PUBLISHERS TAKE HEART FROM BELGIAN COURT RULING

Buoyed by a recent ruling from a court in Belgium, the World Association of Newspapers (WAN) is leading the development of an automated system for coordinating content permissions with search engines. The Belgian court found that Google violates the rights of content producers when it indexes news stories and reposts parts of those stories on its own site. News organizations have long complained that search engines profit from the efforts of news outlets, and the court ruling, which Google is appealing, strengthens their position in trying to restrict how search engines are allowed to use online content. Search engines typically rely on applications that scour the Web for content and incorporate it into search results without human intervention. The Automated Content Access Protocol being developed by the WAN will reportedly give news organizations the ability to include parameters about how their content may be used inside online content. The applications that search engines use to index content will be able to interpret those parameters and treat the content accordingly. Gavin O'Reilly, chairman of the WAN, said, "This system is intended to remove completely any rights conflicts between publishers and search engines."

[CNET, 22 September 2006 http://news.com.com/2100-1030_3-6118523.html]

Category 4A2 Pointing, linking, deep linking, metatext

2007-01-09 Effector Online http://www.eff.org/news/archives/200701.php#005058

EFF DEFENDS RIGHT TO LINK FROM WIKI. LEGAL BATTLE OVER CONTROVERSIAL PRESCRIPTION DRUG ZYPREXA.

San Francisco - Last week, the Electronic Frontier Foundation defended the First Amendment rights of a citizen-journalist to link from a public "wiki" to electronic copies of damaging internal Eli Lilly documents relating to the controversial prescription drug Zyprexa. At the hearing, federal district Judge Jack B. Weinstein refused to change his order blocking publication of material that would "facilitate dissemination" of the Lilly documents. A further hearing on the issue is set for Tuesday, January 16. EFF's client, an anonymous citizen-journalist, posted the links on the wiki located at http://zyprexa.pbwiki.com . Eli Lilly complained, and Judge Weinstein issued his order on January 4. EFF went to court to challenge this order as an unconstitutional prior restraint on free speech in violation of the First Amendment and to ensure that the right of nonparties in the litigation to link to publicly important information remains protected. "Preventing a citizen-journalist from posting links to important health information on a public wiki violates the First Amendment," said EFF Senior Staff Attorney Fred von Lohmann. "Eli Lilly's efforts to censor these documents off the Internet are particularly outrageous in light of the information reported by The New York Times, which suggests that doctors and patients who use Zyprexa need to know the information contained in those documents." According to The New York Times reports, the Eli Lilly documents show that the company intentionally downplayed the drug's side effects, including weight gain, high blood sugar, and diabetes, and marketed the drug for "off-label" uses not approved by the Food and Drug Administration (FDA). The documents were leaked from the ongoing Zyprexa products liability lawsuit, where Weinstein is the presiding judge. Copies of the leaked Eli Lilly documents have appeared on a variety of websites and other Internet sources. The links to the documents that were posted on the wiki at http://zyprexa.pbwiki.com/ were part of extensive, indepth analysis from a number of citizen journalists. A wiki is a website that allows many users to collaborate on its content, creating a kind of simple database for collecting information -- in this case, about the controversy surrounding Zyprexa. Zyprexa is Eli Lilly's best selling drug, used to treat schizophrenia and bipolar disorder. Last week, Eli Lilly agreed to pay up to $500 million to settle claims relating to Zyprexa. This latest settlement brings the total paid by Eli Lilly to resolve lawsuits involving Zyprexa to more than $1.2 billion.
For the full motion filed in the Zyprexa products liability litigation:
http://www.eff.org/legal/cases/zyprexa/zyprexa_motion.pdf
For the court's order of January 4: http://eff.org/legal/cases/zyprexa/jan4_order.pdf
For this release: http://www.eff.org/news/archives/200701.php#005058

4A6 Defamation (libel, slander, misrepresentation)

Category 4A6 *Defamation (libel, slander, misrepresentation)*

2006-11-21 DHS Daily OSIR; VNUNet http://www.vnunet.com/vnunet/news/2169219/california-court-rules-web

CALIFORNIA COURT RULES ON WEB DEFAMATION.

The California Supreme Court has ruled that Internet service providers and bloggers cannot be sued for third-party comments posted on their sites. In the case of Barrett versus Rosenthal the court found that only the originator of the content could be sued, but that third parties who repost the material should be immune from prosecution. The ruling has profound implications for the future of Internet content. "We acknowledge that recognizing broad immunity for defamatory republications on the Internet has some troubling consequences," said the court. "Until Congress chooses to revise the settled law in this area, however, plaintiffs who contend they were defamed in an Internet posting may only seek recovery from the original source of the statement."

Category 4A6 *Defamation (libel, slander, misrepresentation)*

2006-11-27 EDUPAGE; New York Times (registration req'd) http://www.nytimes.com/2006/11/27/technology/27youtube.html

YOUTUBE STUNT BACKFIRES ON STUDENTS

Two teenage students in Gatineau, Quebec, found themselves in hot water after a classroom stunt involving YouTube. The two students, and a third who has not been identified, intentionally aggravated a teacher to the point that he lost his temper. Meanwhile, the students videotaped the incident and then posted the footage on YouTube. According to the school district, the teacher involved is highly respected, both by his peers and his students, and has been teaching for more than 30 years. He has taken voluntary sick leave, and the district said he may choose not to return to the classroom. Jocelyn Blondin, president of the school board, noted that it was other students at the school who notified school officials about the video's being on YouTube, saying, "Other students in the school know he's a good teacher." Similar instances have occurred at other schools, and officials in Gatineau are deciding what punishment they will administer and what steps they might take to prevent such actions in the future, including a temporary ban on all electronic devices in the school.

Category 4A6 *Defamation (libel, slander, misrepresentation)*

2007-01-01 Effector Online http://www.eff.org/news/archives/2006_12.php#005052

EFF BACKS DONTDATEHIMGIRL.COM IN DEFAMATION CASE. CONTROVERSIAL WEBSITE SHIELDED BY FEDERAL LAW PROTECTING INTERNET FREE SPEECH.

Pittsburgh - The Electronic Frontier Foundation (EFF) urged a Pennsylvania court to dismiss defamation claims against the controversial website DontDateHimGirl.com, arguing that federal law shields the website from liability to protect the free flow of information online. DontDateHimGirl.com was created by Tasha Joseph as a forum for women to share information about men. One of the men discussed on the site, Todd J. Hollis, claims that some participants posted defamatory statements about him on the website. In its amicus brief, EFF argues that DontDateHimGirl.com's owner cannot be held liable for comments written by others under Section 230 of the Communications Decency Act. Section 230 specifically protects hosts of interactive computer services from liability to encourage free discourse and robust debate. "The Internet allows people all over the world to share information and diverse opinions. Without Section 230, no one would risk creating a website where others express ideas," said EFF Staff Attorney Marcia Hofmann. "This doesn't mean that people like Hollis can't pursue defamation cases. They can. But they should sue the person who made the statement in the first place, not the person who created the forum where it was made." Nearly every court that has considered Section 230 has recognized the intent of the law and shielded website operators from liability. EFF has provided amicus support in a number of lawsuits, including one that recently held that Craigslist was not responsible for the content of posts made by the public. "Section 230 is key to fostering vital debate and discussion across the Internet. Craigslist and other online communities are thriving because of its protection," said EFF Staff Attorney Kurt Opsahl. The amicus brief was also signed by the Center for Democracy and Technology (CDT) and the American Civil Liberties Union (ACLU) of Pennsylvania.
For the full amicus brief: http://www.eff.org/legal/cases/ddhg/joseph_amicus_final.pdf
For this release: http://www.eff.org/news/archives/2006_12.php#005052

Category 4A6 Defamation (libel, slander, misrepresentation)

2007-04-16 Effector Online

DONTDATEHIMGIRL SUIT DISMISSED

A Pennsylvania judge has dismissed a lawsuit against the controversial website DontDateHimGirl.com, ruling that he did not have jurisdiction over the Florida-based site. But the jurisdiction question was not the only problem with this suit. Dontdatehimgirl is a forum created for women to share information about men, and the plaintiff in this case claims that participants posted defamatory statements about him. EFF filed an amicus brief in support of Dontdatehimgirl in December, arguing that the site cannot be held liable for comments written by others under Section 230 of the Communications Decency Act. Section 230 specifically protects hosts of interactive computer services from liability and is key to fostering free discourse online. Without Section 230, no one would risk creating a website where others could post opinions. It's important to note that the claims against the people who posted the messages in the first place still stand. If any defamation occurred, it's the speakers who should bear the responsibility, not the soapbox. The plaintiff in this case has not decided if he will refile the Dontdatehim girl suit in Florida. However, if he does, he will have to take on Section 230 and the strong protections it provides to Internet hosts of vigorous online debate.
For this post and related links: http://www.eff.org/deeplinks/archives/005194.php

Category 4A6 Defamation (libel, slander, misrepresentation)

2007-05-16 Effector Online http://www.eff.org/news/archives/2007_05.php#005246

WATCHDOG ORGANIZATION BATTLES BOGUS ONLINE DEFAMATION CASE. INTERNET FORUM SHIELDED BY FEDERAL LAW PROTECTING FREE SPEECH.

Washington, D.C. - The Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU) of the National Capital Area has asked a Washington, D.C., court to dismiss claims against a nonprofit watchdog organization and its operators, arguing that federal law and the First Amendment protect them from liability in a defamation lawsuit. DCWatch is a government watchdog organization run by Dorothy Brizill and Gary Imhoff to monitor Washington, D.C., city politics and public affairs. DCWatch's website, www.dcwatch.com, publishes articles and columns on local politics. Themail@dcwatch.com is an online newsletter and discussion forum devoted to reporting, analysis and commentary on local issues, past editions of which are archived on the DCWatch site. In articles printed in themail@dcwatch.com, Washington journalist Jonetta Rose Barras reported that Roslyn Johnson, then Deputy Director of Programs for the D.C. Department of Parks and Recreation, had inflated her employment and salary history to secure her position. A subsequent formal investigation by the D.C. Inspector General concluded that Johnson did in fact submit an inflated resume and was improperly hired for her position. But in a lawsuit filed earlier this year, Johnson claims that these articles were defamatory, placed her in a false light, and resulted in the termination of her employment with the city. In addition to suing reporter Barras, she also sued DCWatch and its operators, claiming that their Internet publication of these articles made them responsible for their content. EFF and the ACLU of the National Capital Area filed a motion to dismiss the lawsuit, pointing out that DCWatch and its operators are shielded by Section 230 of the Communications Decency Act, which expressly protects providers or users of interactive computer services from liability in order to encourage robust debate in online discussions. The motion also urged the court to dismiss Johnson's claims, because the First Amendment protects statements about public officials that are substantially true. "The Internet has played host to a renaissance of political speech, facilitating discussion on issues of local, national, and international importance," said EFF Staff Attorney Marcia Hofmann. "It's important that judges resist attempts by public officials to shut down online debate just because they don't like the speech." Courts throughout the country have recognized the critical role Section 230 plays in enabling open discourse on the Internet and have shielded website operators from liability for comments made by others. "The case against DCWatch must be dismissed. Congress has given online publications absolute immunity for claims based on third-party articles," said EFF Senior Staff Attorney Kurt Opsahl. "An Internet intermediary should not be liable for what the speaker has said." "This is a concept that should be expanded into all media: books, newspapers, radio and television," said Arthur Spitzer, Legal Director of the ACLU of the National Capital Area. "A speaker or writer should be responsible for his or her words. A bookstore or newsstand should not be responsible for the content of what it distributes."
For the full motion to dismiss and other legal documents: http://www.eff.org/legal/cases/johnson_v_barras
For more on DCWatch: http://www.dcwatch.com
For more on the ACLU of the National Capital Area: http://www.aclu-nca.org
For this release: http://www.eff.org/news/archives/2007_05.php#005246

4A7 Spam

Category 4A7 Spam

2006-01-05 EDUPAGE; http://www.wired.com/news/politics/0,69966-0.html

SPAMMER HIT WITH $11.2 BILLION FINE

A court has slapped a Florida spammer with an $11.2 billion fine, setting a new precedent for fines against spammers, though the ruling is unlikely to have much effect on the volume of spam. Internet service provider CIS Internet Services, which provides Internet service to parts of Iowa and Illinois, had sued James McCalla for sending more than 28 million e-mail solicitations that fraudulently used the CIS domain as the return address. In addition to the fine, McCalla is forbidden from accessing the Internet for three years. Robert Kramer III, owner of CIS, welcomed the ruling, calling it the "economic death penalty," though he acknowledged that he does not expect to receive any of the money awarded. John Mozena, co-founder and vice president of the Coalition Against Unsolicited Commercial E-mail, said this and other rulings against spammers have not had a significant effect on the total volume of spam, which he estimated continues to be about two-thirds of all e-mail traffic. What is needed, he argued, rather than current laws, which only forbid deceptive or fraudulent spam, is a prohibition against all spam.

Category 4A7 Spam

2006-01-05 DHS Daily OSIR; http://www.suntimes.com/output/news/cst-nws-privacy05.html

PHONE RECORDS ARE FOR SALE VIA ONLINE DATA BROKERS

The Chicago Police Department is warning officers their cell phone records are available to anyone -- for a price. Dozens of online services are selling lists of cell phone calls, raising security concerns among law enforcement and privacy experts. Criminals can use such records to expose a government informant who regularly calls a law enforcement official. Some online services might be skirting the law to obtain these phone lists, according to Sen. Charles Schumer (D-NY), who has called for legislation to criminalize phone record theft and use. In some cases, telephone company insiders secretly sell customers' phone-call lists to online brokers, despite strict telephone company rules against such deals, according to Schumer. And some online brokers have used deception to get the lists from the phone companies, he said. According to Schumer, a common method for obtaining cell phone records is "pretexting," involving a data broker pretending to be a phone's owner and duping the phone company into providing the information. "Pretexting for financial data is illegal, but it does not include phone records," Schumer said.

Category 4A7 Spam

2006-01-27 DHS Daily OSIR; http://www.siliconvalley.com/mld/siliconvalley/news/editoria l/13728469.htm

MARYLAND SPAM LAW CAN BE ENFORCED, JUDGE RULES.

Spam e-mails offering home financing deals or other offers can violate Maryland law, even if they're sent from another state, a state appeals court has ruled. Court of Special Appeals Judge Sally D. Adkins sided with a law student who argued that he could sue a New York e-mail marketer who had sent him advertising messages. The decision, issued Thursday, January 26, overturns a lower court ruling that Maryland's 2002 Commercial Electronic Mail Act was unconstitutional because it sought to regulate commerce outside state borders. Adkins, in a 60-page decision, blasted the marketer's claims that he should not be punished for violating Maryland law because he had no way of knowing whether his e-mails would be opened in Maryland. "This allegation has little more validity than one who contends he is not guilty of homicide when he shoots a rifle into a crowd of people without picking a specific target, and someone dies," the judge wrote. Maryland was one of the first states to try to control junk e-mail through legislation, and its 2002 law predates the 2004 federal CAN-SPAM Act. The federal law superseded most state laws unless they specifically addressed deceptive or fraudulent e-mail, which Maryland's does.

Category 4A7 Spam

2006-09-06 DHS Daily OSIR; CNET News
http://news.com.com/Virginia+court+upholds+antispam+law/2100 -7350_3-6112967.html

VIRGINIA COURT UPHOLDS ANTI-SPAM LAW.

The Virginia Court of Appeals upheld a state anti-spam law on Tuesday, September 5, by affirming the conviction of the first person in the United States to face prison time for spamming. Jeremy Jaynes was convicted in November 2004 of sending out bulk e-mails with disguised origins and being in possession of a stolen database of more than 84 million AOL subscribers' addresses. He was sentenced to nine years in prison.

Category 4A7 Spam

2006-09-14 EDUPAGE; CNET http://news.com.com/2100-7350_3-6116009.html

SPAMHAUS UNMOVED BY FINE

A federal court in Illinois has issued a default ruling against British antispam organization Spamhaus and ordered it to pay $11.7 million to e360insight, the plaintiff in the matter. Officials from e360insight complained that Spamhaus included the company on its blacklist, alerting users of the list that e-mail from e360insight is spam and should be filtered. Default judgments are issued when a defendant offers no defense; in this case, Spamhaus did not offer a defense. The court also ordered Spamhaus to remove e360insight from its blacklist and publish an apology. Officials from Spamhaus said e360insight in indeed a spammer and would publish no such apology. Further, they said that because Spamhaus is based in the United Kingdom, a ruling from a U.S. court is meaningless. If David Linhardt, chief of e360insight, wants a court ruling that will have an effect, he must file his case in the United Kingdom, according to Spamhaus officials. Dean Drako, CEO of Barracuda Networks, which makes antispam appliances and uses Spamhaus's blacklists, supported Spamhaus and accused e360insight of taking advantage of the U.S. courts to gain what he sees as a meaningless judgment.

JUDGE REFUSES TO DISABLE SPAMHAUS

A judge in Illinois has rejected a petition by e360 Insight to force the closure of the Internet domain of antispam company Spamhaus. Last month, the U.S. District Court for the Northern District of Illinois ordered Spamhaus to pay e360 Insight $11.7 million in damages for blacklisting the company, which keeps users of Spamhaus's antispam list from accepting messages from the e360 Insight domain. Following that ruling, e360 Insight asked the court to suspend the spamhaus.org domain, but Judge Charles Kocoras rejected that request. Blocking the Spamhaus domain, he said, would prevent the company from engaging in activities that the court considers legitimate and would be unduly severe. For its part, Spamhaus insists that e360 Insight is in fact a spammer. Spamhaus, which is based in the United Kingdom, has also said it is under no obligation to pay the fine imposed by the Illinois court because that court has no jurisdiction over Spamhaus's actions.

[Silicon.com, 23 October 2006 http://management.silicon.com/government/0,39024677,39163463,00.htm]

Category 4A7 Spam

2006-09-14 DHS Daily OSIR; Federal Trade Commission
http://www.ftc.gov/opa/2006/09/spammers.htm

FTC PUTS A PERMANENT HALT TO ILLEGAL SPAMMING OPERATIONS.

The Federal Trade Commission (FTC) has brought a permanent halt to four illegal spamming operations -- including one that offered the opportunity to "date lonely wives" and two that hijacked the computers of unwitting third parties and used them to pelt consumers with graphic sexually explicit e-mail. The FTC charged the operators with sending spam that violated provisions of the CAN-SPAM Act, and has halted the illegal spamming. Cleverlink Trading Limited and its partners will give up $400,000 in ill-gotten gains to settle FTC charges that their spam, or that of their affiliates, violated federal law. The FTC charged that Zachary Kinion sent spam hawking adult sites, mortgage rates, and privacy software and paid other spammers commissions to send spam messages for him. One spam operation used "spam zombies" to conceal the source of the sexually explicit spam. Another operator was a professional "button pusher," who used spam to drive traffic to Websites run by third parties.

Category 4A7 Spam

2006-09-14 DHS Daily OSIR; CNET News
http://news.com.com/Spam+fighter+hit+with+11+million+judgment/2100-7350_3-6116009.html?tag=cd.top

SPAM FIGHTER HIT WITH $11 MILLION JUDGMENT.

The manager of a popular blacklist used to block spam was hit with a multimillion-dollar judgment on Wednesday, September 13, but the order may not be enforceable. The U.S. District Court for the Northern District of Illinois has ordered Spamhaus to pay $11,715,000 in damages to e360insight and its chief, David Linhardt, who had sued the UK-based organization earlier this year over illegal blacklisting. The court also barred Spamhaus from causing any e-mail sent by e360insight or Linhardt to be "blocked, delayed, altered, or interrupted in anyway" and ordered Spamhaus to publish an apology for that states that Linhardt and his company are not spammers, according to a copy of the order.

Category 4A7 Spam

2006-10-12 DHS Daily OSIR; IDG News Service http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9004111

SPAMHAUS CASE COULD CAUSE ICANN CRISIS.

Last month, the District Court for the Northern District of Illinois ruled against anti-spam black-lister The Spamhaus Project Ltd. in a lawsuit brought by e-mail marketer e360Insight LLC. The court ordered Spamhaus to remove the company from its database of spammers and to pay $11.7 million in damages, but Spamhaus initially ignored the ruling, saying that the U.S. court had no jurisdiction over the UK-based project. On Friday, October 6, the judge issued a proposed order that told both the Spamhaus.org domain name registrar, Tucows Inc., and the Internet Corporation for Assigned Names and Numbers (ICANN) to pull the project's domain name. Though the order is only proposed and does not have the force of law, observers said they worry that any attempt by U.S. courts to exert control over ICANN could be bad for the Internet. The Marina Del Rey, California-based ICANN has come under fire in the past for lacking transparency and being U.S.-centric. "Suppose a U.S. court ordered ICANN to yank a prominent .com name belonging to a non-U.S. company," said Princeton University's Edward Felten. "Such a decision, if seen as unfair outside the U.S., could trigger a sort of constitutional crisis for the Net," he said.

Category 4A7 Spam

2006-11-28 EDUPAGE; CNET http://news.com.com/2100-1030_3-6138874.html

COURT SAYS CAN-SPAM TRUMPS STATE LAWS: REALLY DOES MEAN "YOU CAN SPAM"

The 4th Circuit Court of Appeals concluded in mid-November that unsolicited e-mails advertising cruise vacations were permitted under the federal antispam law called the CAN-SPAM Act, even though they included a false Internet address and a nonworking "From" address. In the case involving antispam activist Mark Mumma of Oklahoma, the three-judge panel ruled that the federal law preempts state statutes. Declan McCullagh wrote,

>When antispam activist Mark Mumma received unsolicited e-mails advertising cruise vacations two years ago, he posted a report on his Web site and threatened to sue Omega World Travel.

But Mumma met with an unpleasant surprise: He was the one sued in federal court by Omega World Travel and its subsidiary Cruise.com, which demanded $3.8 million in damages for defamation. Mumma, who owns Oklahoma-based MummaGraphics and runs a one-man Web design and hosting shop at Webguy.com, filed counterclaims against the companies and CEO Gloria Bohan.

The 4th Circuit Court of Appeals sided with the alleged spammers. In a little-noticed opinion issued in mid-November, a three-judge panel acknowledged the e-mail messages in question may have included a false Internet address and a nonworking "From:" address, but concluded that they nevertheless were permitted under the federal antispam law known as the Can-Spam Act. <

[MK comments: Antispam activists, including myself, have long criticized the CAN-SPAM act as a deeply flawed law that interferes with attempt to shut down spammers. It did, however, provide the opportunity for my all-time favorite column title in Network World Security Strategies: "Can CAN-SPAM Can Spam?" Apparently not.]

4A8 Liability

Category 4A8 Liability

2006-06-27 EDUPAGE; Houston Chronicle
http://www.chron.com/disp/story.mpl/ap/nation/4005150.html

OHIO UNIVERSITY FACES LAWSUIT OVER DATA BREACH

Two graduates of Ohio University have filed a lawsuit following the institution's disclosure of a series of computer breaches that may have compromised personal information on about 175,000 people. After announcing a breach at one of its units in April, the university later said similar break-ins had taken place at the alumni office, the health center, and an office that handles contracts. In the wake of the problems, the university has suspended two IT staff and pledged to spend $4 million to improve computer security. An independent consultant* investigating the incidents said the university had for a decade not paid enough attention to its computer security. In the suit, Donald Jay Kulpa and Kenneth Neben seek class-action status for those affected and ask the court to require the university to pay for credit-monitoring service and for any losses suffered as a result of the compromised data.

[*MK Note: Dr Peter Stephenson, CISO of Norwich University and Associate Program Director of the MSIA in the School of Graduate Studies at Norwich.]

Category 4A8 Liability

2006-11-16 DHS Daily OSIR; Federal Trade Commission
http://www.ftc.gov/opa/2006/11/guidance.htm

GUIDANCE SOFTWARE INC. SETTLES FTC CHARGES.

Guidance Software Inc. has agreed to settle Federal Trade Commission (FTC) charges that its failure to take reasonable security measures to protect sensitive customer data contradicted security promises made on its Website and violated federal law. According to the FTC, Guidance's data-security failure allowed hackers to access sensitive credit card information for thousands of consumers. The settlement will require the company to implement a comprehensive information-security program and obtain audits by an independent third-party security professional every other year for 10 years. According to the FTC complaint, Guidance failed to implement simple, inexpensive and readily available security measures to protect consumers' data. In contrast to claims about data security made on Guidance's Website, the company created unnecessary risks to credit card information by permanently storing it in clear readable text.

4A9 Net neutrality

Category 4A9 *Net neutrality*

2006-03-15 DHS Daily OSIR; http://news.com.com/Debate+heats+up+over+Net+neutrality/2100 - 1037_3-6049863.html?tag=nl

DEBATE HEATS UP OVER NET NEUTRALITY.

Speculation that the two biggest phone companies in the country, AT&T and Verizon Communications, are planning to create a tiered Internet system that would require big bandwidth users like Google or Yahoo to pay more for their access has become a hot-button issue in the tech industry. Increasingly, it's also an issue on Capitol Hill, where some lawmakers are developing rules to maintain so-called Net neutrality and prevent the emergence of a tiered system. At the Voice over the Net conference at the San Jose Convention Center on Tuesday, March 14, companies on both sides of the bandwidth aisle debated how much Internet regulation is needed. CEOs from network owners AT&T and Verizon Communications have made comments suggesting they plan to create a system where some companies would have to pay more for their data-intensive use of the Net, which, they argue, slows access for regular customers. On the other side of the debate are companies such as Google, eBay and Yahoo, which are against any companies taking on the role of "IP traffic gatekeeper." They support the idea of federal rules that would further restrict network owners from blocking or restricting traffic.

Category 4A9 *Net neutrality*

2006-04-26 EDUPAGE; http://news.zdnet.com/2100-9595_22-6065465.html

COMMITTEE KILLS NET NEUTRALITY BILL

The House Energy and Commerce Committee has killed an amendment designed to guarantee net neutrality. The amendment would have prevented Internet service providers from delivering different content at different speeds based on content providers' having paid extra fees. Supporters of the amendment, including Microsoft, Amazon, and Google, argued that the Internet was built on ideas antithetical to the notion of paying fees to have content available to consumers. They called on Congress not to drop the issue but to "enact legislation preventing discrimination" against certain content providers. Opponents of the amendment, including cable and phone companies, suggested that the landscape of online content, including such material as movie-quality video, could be available to consumers if content providers paid a surcharge for it. Joe Barton (R-Tex.), chairman of the committee, commented that net neutrality is "still not clearly defined" and that he doubts the dire predictions of the amendment's supporters.

Category 4A9 *Net neutrality*

2006-05-20 RISKS; NYT http://www.freepress.net/news/15726

NET NEUTRALITY DEBATE HEATS UP

Sir Tim Berner-Lee, inventor of the World Wide Web, publicly critized proposals to move to a multi-tiered Internet in which high-paying corporate clients could receive preferential allocations of bandwidth while non-profits and individuals might stagnate in a mire of slow -- or no -- access. Writer Adam Cohen presented a summary of the issues in a New York Times article on May 29, 2006. Key points:

* ISPs and large corporations are pushing for permission to discriminate among content providers by charging for bandwidth. More fees, more speed.

* A growing movement is organizing to push the US Congress to block such attacks on "net neutrality."

* Breaking down net neutrality could permit open censorship of content providers -- for example, blocking or interfering with access based on political preferences.

* Fees for higher bandwidth could curtail new developments such as shared images from cellphones that could generate three-dimensional images of news events.

* Tiered pricing may harm even the ISPs because users may reject paying for services that they expect to be free (once their ISP subscriptions are paid).

Category 4A9 Net neutrality

2006-05-23 DHS Daily OSIR; BBC (United Kingdom)
http://news.bbc.co.uk/1/hi/technology/5009250.stm

WEB INVENTOR WARNS AGAINST TWO-TIER INTERNET.

The Web should remain neutral and resist attempts to fragment it into different services, Web inventor Tim Berners-Lee has said. Recent attempts in the U.S. to try to charge for different levels of online access Web were not "part of the Internet model," he said. The open Internet model, backed by Berners-Lee and the World Wide Web Consortium, is based on the concept of network neutrality, where everyone has the same level of access to the Web and that all data moving around the Web is treated equally. But some telecom companies in the U.S. do not agree. They would like to implement a two-tier system, where data from companies or institutions that can pay are given priority over those that cannot. The Internet community believes this threatens the open model of the Internet as broadband providers will become gatekeepers to the Web's content.

Category 4A9 Net neutrality

2006-06-09 DHS Daily OSIR; IDG News
http://www.infoworld.com/article/06/06/09/79138_HNnetneutral itydefeat_1.html

U.S. HOUSE DEFEATS NET NEUTRALITY PROVISION.

The U.S. House of Representatives has defeated a provision to require U.S. broadband providers to offer the same speed of service to competitors that's available to partners, a major defeat to a coalition of online companies and consumer groups. The vote against the net neutrality amendment late Thursday, June 8 came after a last-minute push for the measure from many technology companies. After the House defeated the net neutrality amendment, it passed the underlying bill, a wide-ranging broadband bill focused partly on speeding the roll-out of television over Internet Protocol (IPTV). The underlying broadband bill, the Communications Opportunity, Promotion, and Enhancement Act, passed by a vote of 321-101 and will allow the U.S. Federal Communications Commission to investigate complaints about broadband providers blocking or impairing Internet content only after the fact. The bill also streamlines local franchising requirements for telecom carriers that want to offer IPTV services in competition with cable television. The bill in essence creates a national franchise, allowing AT&T and Verizon to roll out their IPTV services without going through lengthy franchising negotiations with each local government where they want to provide service.

4AA Disintermediation

Category 4AA Disintermediation

2006-06-17 EDUPAGE; New York Times (registration req'd) http://www.nytimes.com/2006/06/17/technology/17wiki.html

WIKIPEDIA ADJUSTS EDITING POLICY

Wikipedia, the online encyclopedia based on the model that anyone can contribute to or edit any entry, has placed new restrictions on editing. Certain entries in any reference work are bound to be contentious, and with Wikipedia, disagreements can escalate to a "revert war," in which competing factions simply change an entry back and forth to reflect their opinions. Such disputes have resulted in a status of "protected" for 82 entries, meaning they cannot be changed at all, and a status of "semi-protected" for another 179 entries.

Semi-protected entries can only be changed by someone who has been a registered user for more than four days, the idea being that such a "cooling off" period will avoid most of the problems resulting from disagreements. Despite the steps Wikipedia has taken away from the ideal of "anyone can edit," founder Jimmy Wales says the resource works and is valuable. Most entries are only protected for a short period of time, he said, and they represent a fraction of the 1.2 million entries in the English-language version.

Category 4AA Disintermediation

2006-10-16 EDUPAGE; ZDNet http://news.zdnet.com/2100-9588_22-6126469.html

CITIZENDIUM FORKS FROM WIKIPEDIA USING NEW RULES FOR AUTHENTICITY & ACCURACY

One of the founders of Wikipedia has announced a new online encyclopedia that he hopes will embody the foundation of Wikipedia while overcoming some of its shortcomings. Larry Sanger's new project, called Citizendium, will use a number of tactics to elicit credible, useful content from a community of volunteers while avoiding the kinds of intentional distortions that have been a problem for Wikipedia. On Citizendium, contributors must register with their real names, and a team of editors will enforce a set of community rules. Sanger said that Wikipedia is an "amazing" resource but believes that "an even better massive encyclopedia" can be produced by overlaying a system of "gentle controls" on how content is developed and edited. The creation of Citizendium will involve a "fork" of the existing Wikipedia content. All current content from Wikipedia will serve as the basis for Citizendium. From there, the two collections will evolve and diverge based on their different approaches.

4B Intellectual property law

Category 4B Intellectual property law

2006-06-22 Commweb

AG GONZALEZ: INTELLECTUAL PROPERTY THEFT IS A SCOURGE ON THE U.S. ECONOMY

Category 4B Intellectual property law

2006-09-13 PR Newswire

FINDLAW.COM LAUNCHES INTELLECTUAL PROPERTY CENTER;

Category 4B Intellectual property law

2006-09-28 Federal Information and News Dispatch

NIPLECC REPORT ON INTELLECTUAL PROPERTY ENFORCEMENT AND PROTECTION

4B1 Copyrights

Category 4B1 Copyrights

2006-01-27 Effector Online

NEVADA COURT RULES GOOGLE CACHE IS FAIR USE. IMPORTANT MILESTONE FOR DIGITAL COPYRIGHT LAW.

San Francisco - A federal district court in Nevada has ruled that Google does not violate copyright law when it copies websites, stores the copies, and transmits them to Internet users as part of its Google Cache feature. The ruling clarifies the legal status of several common search engine practices and could influence future court cases, including the lawsuits brought by book publishers against the Google Library Project. The Electronic Frontier Foundation (EFF) was not involved in the case but applauds last week's ruling for clarifying that fair use covers new digital uses of copyrighted materials. Blake Field, an author and attorney, brought the copyright infringement lawsuit against Google after the search engine automatically copied and cached a story he posted on his website. Google responded that its Google Cache feature, which allows Google users to link to an archival copy of websites indexed by Google, does not violate copyright law. The court agreed, holding that the Cache qualifies as a fair use of copyrighted material. "This ruling makes it clear that the Google Cache is legal and clears away copyright questions that have troubled the entire search engine industry," said Fred von Lohmann, EFF senior staff attorney. "The ruling should also help Google in defending against the lawsuit brought by book publishers over its Google Library Project, as well as assisting organizations like the Internet Archive that rely on caching."
Field v. Google ruling: http://www.eff.org/IP/blake_v_google/google_nevada_order.pdf
For this release: http://www.eff.org/news/archives/2006_01. php#004345

Category 4B1 Copyrights

2006-03-03 EDUPAGE; http://www.theregister.com/2006/03/03/european_digital_library_goes_live/

EC PUSHES FOR DIGITAL LIBRARY

The European Commission (EC) is supporting a plan to create a European Digital Library that may one day include as many as six million volumes from libraries around Europe. The commission acknowledged that opinions differ about intellectual property concerns for digitized works, noting that a study it conducted showed wide disagreement between rights holders and institutions such as libraries. Still, the EC said it will work to settle those differences and begin working on the project, which would involve collaboration among all of the national libraries in the European Union and potentially other organizations such as museums. The EC said that by 2008, two million books, photographs, and other materials will be available through the European Digital Library and that this total could rise to six million by 2010.

Category 4B1 Copyrights

2006-03-13 EDUPAGE; http://news.com.com/2100-1025_3-6048801.html

ONLINE LIBRARY TRIES TO AVOID PROBLEMS OF E-PUBLISHING

Houston-based Questia Media is a digital-library company whose executives believe they have seen past the errors of e-publishing. CEO Troy Williams and Chairman Rod Canion, who founded Compaq, survived the fallout from failed electronic publishing efforts and now count about 150,000 subscribers to their company's academic offerings, which target high schools and their students. Questia continues, in part, because although users did not warm to the idea of reading a novel on a screen, they are much more willing to conduct academic research online, said Williams. Much of Questia's current library of 65,000 books consists of hard-to-find materials. Much of the library content is copyrighted, so Questia has worked out agreements with publishers and other copyright holders, most of whom are happy to have high school students exposed to their materials.

Category 4B1 Copyrights

2006-04-23 EDUPAGE; http://news.com.com/2100-1028_3-6064016.html

COPYRIGHT LAW UPDATE FAVORS COPYRIGHT HOLDERS

Despite pressure from a number of quarters to introduce restrictions on the Digital Millennium Copyright Act, Congress appears to be headed the other direction. Drafts of the Intellectual Property Protection Act of 2006 are circulating among lawmakers, and a spokesperson for the House Judiciary Committee said the bill will likely be introduced soon. The bill adds a number of new layers to copyright law, including increasing fines for certain copyright crimes; criminalizing attempted copyright violations, even if they fail; and allowing copyright owners to impound "records documenting the manufacture, sale, or receipt of items involved in" violations. Jason Schultz, staff attorney at the Electronic Frontier Foundation, said of this last provision that the recording industry has long wanted the ability to obtain server logs that would indicate "every single person who's ever downloaded" certain files. Keith Kupferschmid, vice president for intellectual property and enforcement at the Software and Information Industry Association, welcomed the bill, saying that it gives government officials needed authority to prosecute intellectual property criminals.

Category 4B1 Copyrights

2006-06-07 EDUPAGE; Chronicle of Higher Education (sub. req'd)
http://chronicle.com/daily/2006/06/2006060701t.htm

FREE BOOKS, ELECTRONICALLY

Project Gutenberg is organizing a book fair featuring online texts from its own digital library as well as that of the World eBook Library Consortia. During the World eBook Fair, which will take place from July 4 to August 4, users can download free copies of books from Project Gutenberg's collection of 18,000 texts, which are always free, or from the World eBook Library Consortia, which otherwise cost $8.95 each.

Organizers hope the event will encourage more people to start reading books electronically, not only on desktop or laptop computers but also on portable devices. Michael S. Hart, founder of Project Gutenberg, said, "We get a lot of people reading Project Gutenberg e-books on PDAs, iPods, pocket PCs, cell phones, etc." Hart said electronic books benefit those who cannot get physical books from traditional libraries, noting that the goal of Project Gutenberg is to "break down the bars of ignorance and illiteracy." Daniel Greenstein, executive director of the California Digital Library, said that e-books are typically being used to find facts, not to facilitate "the reading experience that we all know and love."

Category 4B1 Copyrights

2006-07-01 http://www.copyright.gov/fls/fl102.html

COPYRIGHT OFFICE REAFFIRMS FAIR-USE DOCTRINE

In July 2006, the US Copyright Office revised its guidelines on Fair Use Doctrine. The document confirms that there is no bright line divising fair use from copyright infringement and reaffirms that four factors are paramount in helping to determine whether a particular unauthorized use of copyrighted material:

"1. the purpose and character of the use, including whether such use is of commercial nature or is for nonprofit educational purposes;
2. the nature of the copyrighted work;
3. amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
4. the effect of the use upon the potential market for or value of the copyrighted work."

Category 4B1 Copyrights

2006-07-31 EDUPAGE; The Register http://www.theregister.com/2006/07/31/itunes_law_rejected/

FRENCH COURT THROWS OUT ITUNES LAW

The French Constitutional Council has rejected parts of a law recently passed that would have required Apple Computer to open access to its iTunes music and to its iPod portable music players. Under the legislation, companies would be forced to allow their music formats to be played on other companies' devices, as well as to allow other music formats to be played on all devices. Apple Computer, with its extremely popular iPods and iTunes, stood to lose the most under the law. But the Constitutional Council, which reviews all laws passed in the country, ruled that the law violated Apple's right to be compensated for technology it developed. The council did not reject the notion of forced interoperability, however, saying only that Apple should be paid by competitors for the technology. The law may now need to be completely rewritten and resubmitted to parliament for a new vote.

Category 4B1 Copyrights

2006-09-25 EDUPAGE; CNET http://news.com.com/2100-1025_3-6119043.html

BRITISH LIBRARY SAYS COPYRIGHT LAW NEEDS UPDATING

The British Library has called for a wide-scale revision of existing copyright law, which, it said, inadequately addresses digital content, putting too much control into the hands of content producers and owners. Lynne Brindley, chief executive of the British Library, took aim at digital rights management (DRM) technology in particular, saying that it allows content producers to prevent legitimate uses of content, such as for academic purposes, for archival efforts, or for making content available to people with disabilities. Calling the problem a global issue, Brindley said that without "a serious updating of copyright law to recognize the changing technological environment, the law becomes an ass." The Open Rights Group supported the library's call for revising copyright law, saying that the current situation "allows publishers to write whatever license they like, which is what is happening now." The British Library also said the question of orphaned works should be addressed--works whose proper copyright owners cannot be located easily or at all.

Category 4B1 Copyrights

2006-11-08 Effector Online http://www.eff.org/news/archives/2006_11.php#004976

CRAIGSLIST SEX AD SCAMMER SEEKS TO SILENCE CRITICS. BASELESS COPYRIGHT CLAIMS USED TO SHUT DOWN DEBATE OVER PRIVACY CONTROVERSY.

San Francisco - The Electronic Frontier Foundation (EFF) filed suit last Wednesday against the man behind "craigslist-perverts.org" -- a website that publicized responses to fake personal advertisements posted on craigslist.org -- on behalf of an online journalist who criticized the controversial outing campaign and received legal threats in return. Michael Crook posted the fake ads earlier this year, claiming to be a young woman seeking a casual sexual encounter. Crook then displayed many of the replies on his craigslist-perverts.org website, including information such as the responders' names, photographs, phone numbers, and where they worked. Jeff Diehl, the editor of Internet magazine 10 Zen Monkeys, published an article in September critical of Crook's behavior and used an image of Crook being interviewed by Fox News to highlight how controversial a figure he was. Instead of responding to the criticism with words, Crook sent a legal notice to the magazine's online service provider, claiming to be the copyright holder of the image and demanding that it be removed under the Digital Millennium Copyright Act (DMCA). Such actions violate the DMCA's requirements that only the copyright holder or someone authorized by her can send such notices. "This is yet another case of someone intentionally misusing copyright law to try to shut down legitimate debate on an issue of public interest," said EFF Staff Attorney Jason Schultz. "Crook certainly doesn't own the copyright to the news footage -- Fox News does. Furthermore, a still shot of that footage, used as part of a commentary on the controversy surrounding him, is clearly a fair use. It's hypocritical for such an outspoken figure like Crook to attack other speakers just because they disagree with him." Because of Crook's misuse of the DMCA, Diehl was forced to switch web-hosting companies in order to continue to publish the photo. But even then, Crook sent another bogus DMCA notice to the new hosting company, and Diehl had to remove the photo for a second time. In the lawsuit filed last week, EFF asks that Diehl be compensated for the financial and personal expenses associated with responding to the meritless claims and switching web hosts -- as well as for the infringement to his free speech rights protected by the First Amendment. This lawsuit is part of EFF's ongoing work to protect online free speech in the face of bogus copyright claims. EFF recently filed an objection to a subpoena from Landmark Education, a group that claimed copyright infringement in a video uploaded to the Internet Archive. "The Internet is home to passionate debate on countless important issues. It is too bad that some people find the robust exercise of free speech so frightening that they use intimidation to try to silence it," said EFF Staff Attorney Corynne McSherry. "EFF is grateful that people like Jeffrey Diehl and the Internet Archive are fighting back."
For more on the lawsuit against Michael Crook: http://eff.org/legal/cases/diehl_v_crook
For more on the Internet Magazine 10 Zen Monkeys: http://10zenmonkeys.com/2006/11/01/eff-crook-dmca-lawsuit/
For this release: http://www.eff.org/news/archives/2006_11.php#004976

Category 4B1 Copyrights

2006-11-20 EDUPAGE; Seattle Post-Intelligencer
http://seattlepi.nwsource.com/business/292898_copyright20.html

PUBLISHERS CRITICIZE PROFESSORS FOR COPYRIGHT VIOLATIONS

The Association of American Publishers (AAP) is calling on colleges and universities to take steps to address what they see as rampant copyright abuse by faculty. According to the AAP, faculty who post protected content online for use in their courses cost the publishing industry at least $20 million each year in lost revenues. Before the advent of online reserves, faculty would often place hard-copy materials in the library for students to view. That practice has been largely replaced by making digital copies of course materials available online. The publishing industry objects, saying faculty who do this go beyond the scope of fair use. Allan Adler, vice president for legal and governmental affairs with AAP, said, "We can't compete with free." The organization pointed to a recent agreement with Cornell University in which the institution works to educate faculty on appropriate uses of copyrighted material and on best practices to avoid infringing uses. The AAP hopes that other institutions will implement programs similar to the one Cornell has adopted.

Category 4B1 Copyrights

2006-11-29 Effector Online http://www.eff.org/news/archives/2006_11.php#005024

BARNEY SURRENDERS IN COPYRIGHT CASE. PURPLE DINOSAUR BACKS OFF AND PAYS UP; FREE SPEECH RIGHTS PRESERVED.

San Francisco - The corporate owners of the popular children's television character Barney the Purple Dinosaur have agreed to withdraw their baseless legal threats against a website publisher who parodied the character and to compensate him for fees expended in defending himself. The agreement settles a suit filed by the Electronic Frontier Foundation (EFF) in August on behalf of Dr. Stuart Frankel against Lyons Partnership, owners of the Barney character. Frankel received repeated, meritless cease-and- desist letters from Lyons, claiming his online parody violated copyright and trademark law. EFF's suit asked the court to declare that Frankel's parody was a noninfringing fair use protected by the First Amendment. "We wish we hadn't had to file a lawsuit to finally get Barney's lawyers to stop harassing a man who was just expressing his opinion about a cultural phenomenon," said EFF Staff Attorney Corynne McSherry. "Hopefully Lyons Partnership has learned its lesson and will have more respect for fair use in the future." This settlement is the latest development in EFF's ongoing campaign to protect online free speech from the chilling effects of bogus copyright claims. . . .

For the original complaint: http://www.eff.org/legal/cases/barney/frankel_v_lyons_complaint.pdf
For more on Barney's copyright abuses: http://www.eff.org/legal/cases/barney/
For this release: http://www.eff.org/news/archives/2006_11.php#005024

Category 4B1 Copyrights

2006-12-15 EDUPAGE; CNET http://news.com.com/2100-1014_3-6144063.html

CHINA ENTERS COPYRIGHT AGREEMENT

Chinese authorities this week announced an agreement with four trade associations about the ongoing problem of copyright infringement, which is reportedly rampant in China. The Business Software Alliance and the Publishers Association (both in the United Kingdom), the Association of American Publishers, and the Motion Picture Association of America (in the United States) signed the memorandum of understanding, under which the organizations will provide the Chinese government with lists of products that should be protected by copyright law. The four groups will also keep Chinese authorities informed about legal actions against suspected copyright infringers. The National Copyright Association of China will oversee the information from the four groups and will work to improve the country's efforts at enforcing copyrights.

Category 4B1 Copyrights

2007-01-30 Effector Online http://www.eff.org/deeplinks/archives/005085.php

THE RIGHT WAY TO RESPOND TO PARODY.

Recently, Darren Barefoot posted Get a First Life, a hysterical parody of virtual world Second Life's website. Linden Labs, the creators of Second Life, responded with a letter that is so right-thinking and clever that it would horrify the over-reaching copyright and trademark holders whose missives litter the archives of ChillingEffects.org Instead of a cease-and-desist letter, Linden Labs sent a proceed-and-permit letter: http://www.darrenbarefoot.com/archives/2007/01/my-project-du-jour-getafirstlifecom.html#comment-75509 This letter is exactly what we would hope companies might do when faced with a parody. Not only does it acknowledge that the site is a fair use, it also provides an explicit license for trademark use. Kudos to Linden Labs, and shame on the rights holders who claim that they have to go after anyone who makes any use of their copyrights or trademarks.
For this post and related links: http://www.eff.org/deeplinks/archives/005085.php

Category 4B1 Copyrights

2007-02-01 DHS Daily OSIR; Reuters http://www.informationweek.com/showArticle.jhtml

PIRACY WORKED FOR US, ROMANIA PRESIDENT TELLS GATES.

Pirated Microsoft Corp. software helped Romania to build a vibrant technology industry, Romanian President Traian Basescu told the company's co-founder Bill Gates on Thursday, February 1. Basescu was meeting the software giant's chairman in Bucharest to celebrate the opening of a Microsoft global technical center in the Romanian capital. "Piracy helped the young generation discover computers. It set off the development of the IT industry in Romania," Basescu said during a joint news conference with Gates. Former communist Romania, which has just joined the European Union, introduced anti-piracy legislation 10 years ago but copyright infringements are still rampant. Experts say some 70 percent of software used in Romania is pirated.

Category 4B1 Copyrights

2007-02-12 DHS Daily OSIR; IDG News Service
http://www.infoworld.com/article/07/02/12/HNworstcopyrightviolators_1.html

CHINA AND RUSSIA TOP LIST OF WORST COPYRIGHT VIOLATORS.

China and Russia are the two worst foreign infringers of U.S. software and music copyrights and they should remain on the U.S. government's priority watch list, a group representing the software, music, books, and movie industries said Monday, February 12. The International Intellectual Property Alliance (IIPA) put out the figures as part of its recommendations to the U.S. Trade Representative. China topped all rivals on the IIPA most-wanted list by pumpingout $2.21 billion worth of pirated goods last year, mainly business software, according to IIPA figures. Russia ran a close second at $2.18 billion, it said.

Category 4B1 Copyrights

2007-02-13 Effector Online http://www.eff.org/deeplinks/archives/005114.php

BIG WIN FOR INNOCENT RIAA DEFENDANT

Debbie Foster, a single mom who was improperly sued by the RIAA back in 2004 for file sharing, has won back her attorneys' fees. The decision last week is one of the first in the country to award attorneys fees to a defendant in an RIAA case over music sharing on the Internet. Last year, Judge Lee R. West dismissed the case against her with prejudice after it became clear that Ms. Foster was simply the Internet access account holder in her home and had no knowledge or experience with file sharing software. EFF, Public Citizen, the ACLU, and the American Association of Law Libraries filed an amicus brief in the case, supporting Ms. Foster's motion for fees. In his ruling, Judge West found that the RIAA had asserted an untested and marginal theory that veered toward "frivolous and unreasonable" by suing Foster for contributory and vicarious copyright infringement when the only evidence against her was her name on the household Internet account. Much like the judge in Elektra v. Santangelo, West expressed skepticism that "an Internetilliterate parent, who does not know Kazaa from a kazoo" could be held liable for children in her home downloading music illegally unless the parent had knowledge of the conduct or had given her permission to do so. West also hinted that the RIAA might have pursued the secondary liability claims "to press Ms. Foster into settlement after they ceased to believe she was a direct or 'primary' infringer." Finding that in the face of these claims, "her only alternative to litigating ... was to capitulate to a settlement for a violation she insists she did not commit" and that "[s]uch capitulation would not advance the aims of the Copyright Act," the Court awarded Ms. Foster her attorneys fees and costs. We applaud Judge West for standing up to the RIAA and recognizing the importance of helping people like Debbie Foster push back against their overzealous litigation campaign.
For this post and related links: http://www.eff.org/deeplinks/archives/005114.php

Category 4B1 Copyrights

2007-03-21 Effector Online http://www.eff.org/news/archives/2007_03.php#005161

DMCA ABUSER APOLOGIZES FOR TAKEDOWN CAMPAIGN. MICHAEL CROOK AGREES TO STOP ATTACKS ON FREE SPEECH.

San Francisco - Michael Crook, the man behind a string of meritless online copyright complaints, has agreed to withdraw those complaints, take a copyright law course, and apologize for interfering with the free speech rights of his targets. The agreement settles a lawsuit against Crook filed by the Electronic Frontier Foundation (EFF) on behalf of Jeff Diehl, the editor of the Internet magazine 10 Zen Monkeys. Diehl was forced to modify an article posted about Crook's behavior in a fake sex-ad scheme after Crook sent baseless Digital Millennium Copyright Act (DMCA) takedown notices, claiming to be the copyright holder of an image used in the story. In fact, the image was from a Fox News program and legally used as part of commentary on Crook. But Crook repeated his claims and then attempted to use the same process to get the image removed from other websites reporting on his takedown campaign. "Crook's legal threats interfered with legitimate debate about his controversial online behavior," said EFF Staff Attorney Jason Schultz. "Public figures must not be allowed to use bogus copyright claims to squelch speech." In addition to withdrawing current complaints against Diehl and every other target of his takedown campaign and taking a copyright law course, Crook has also agreed to limit any future DMCA notices to works authored or photographed by himself or his wife, or where the copyright was specifically assigned to him. All future notices must also include a link to EFF information on his case, as well as the settlement agreement. Crook has also recorded a video statement to apologize and publicize the dangers of abusing copyright law. "We're pleased that Crook has taken responsibility for his egregious behavior," said EFF Staff Attorney Corynne McSherry. "Hopefully, this will set a precedent to prevent future abuse of the law by those who dislike online newsreporting and criticism." The settlement with Michael Crook is part of EFF's ongoing campaign to protect online free speech from the chilling effects of bogus intellectual property claims. EFF recently filed suit against the man who claims to have created the popular line dance "The Electric Slide" for misusing copyright law to remove an online documentary video that included footage of people trying to do the dance.
For the video statement from Michael Crook: http://blip.tv/file/169553
For more on Diehl v. Crook: http://www.eff.org/legal/cases/diehl_v_crook
For this press release: http://www.eff.org/news/archives/2007_03.php#005161

Category 4B1 *Copyrights*

2007-04-06 DHS Daily OSIR; Associated Press http://www.signonsandiego.com/news/tech/20070406-0438-china-productpiracy.html

CHINA TIGHTENS ANTI-PIRACY ENFORCEMENT AFTER FOREIGN COMPLAINTS.

China has extended criminal penalties for music and movie piracy to people caught with smaller amounts of DVDs or CDs, a state news agency said Friday, April 6, after foreign complaints that enforcement was too lenient. The decision by the Supreme People's Court comes amid pressure by foreign governments and the film and music industries to stamp out China's rampant product piracy industry. The court, in an order Thursday, cut in half the number of counterfeit DVDs, CDs or other audiovisual products that trigger criminal penalties of up to three years in prison, the Xinhua News Agency said. It said the court also raised fines for smaller offenders. Anyone caught with 500 pirated discs will face criminal prosecution instead of fines, down from the previous 1,000 discs, Xinhua said. It said the number of discs that triggers more severe penalties of up to seven years in prison was cut in half to 2,500. China is regarded as one of the world's leading sources of illegally copied movies, music, designer clothing and other products.

4B2 Patents

Category 4B2 Patents

2006-01-30 DHS Daily OSIR; http://news.zdnet.com/2100-3513_22-6032870.html

MICROSOFT PATENT SPAT FORCES BUSINESSES TO UPGRADE OFFICE.

Microsoft has begun e-mailing its corporate customers worldwide, letting them know that they may need to start using a different version of Office as a result of a recent legal setback. The software maker said Monday, January 30, that it has been forced to issue new versions of Office 2003 and Office XP, which change the way Microsoft's Access database interacts with its Excel spreadsheet. The move follows a verdict last year by a jury in Orange County, CA, which found in favor of a patent claim by Guatemalan inventor Carlos Armando Amado. Microsoft was ordered to pay $8.9 million in damages for infringing Amado's 1994 patent. That award covered sales of Office between March 1997 and July 2003. Although existing customers can keep using older versions on current machines, any new installations of Office 2003 will require Service Pack 2, released by Microsoft in September. Office XP will need to be put into use with a special patch applied. The software maker started notifying customers this month, in an e-mail sent via its sales channel. All those affected will have been informed by next month, Microsoft said. The company said the necessary downloads are available from its Website.

Category 4B2 Patents

2006-03-28 EDUPAGE; http://chronicle.com/daily/2006/03/2006032802n.htm

ANOTHER PATENT THREATENS CAMPUS TECHNOLOGY

Another company has contacted a number of colleges and universities about a technology patent they might be infringing, this time for systems that transfer money across the Internet to campus cards. in 1998, JSA Technologies applied for a patent, which was granted in 2005, that covers such transfers. Many institutions use campus cards for student expenses such as books, food in snack bars, or campus fees. Jon Gear, vice president of JSA, said the company has no intention of forcing institutions to discontinue their funds-transfer systems. The company, he said, is simply enforcing a patent that protects its intellectual property. Gear said JSA contacted a number of schools, though he declined to say how many or to name them, and will negotiate licensing fees, which he said would be "negligible." Lowell Adkins, executive director of the National Association of Campus Card Users, said his organization is working to clarify the issue. "It's still really unclear what the scope of the patent is," he said. "We need to understand how they're going to exercise their rights."

Category 4B2 Patents

2006-04-06 EDUPAGE; http://www.eff.org/news/archives/2006_04.php#004530

EFF CALLS FOR ONLINE-TESTING PATENT TO BE INVALIDATED

The Electronic Frontier Foundation (EFF) has called on the U.S. Patent and Trademark Office (USPTO) to invalidate a patent that broadly covers technologies that allow tests to be posted and taken online. In 2003, the USPTO granted the patent to Test.com, which has since contacted a number of colleges and universities, as well as businesses, that conduct online testing, saying those services violate the patent. Many of those approached by Test.com believe that the idea of putting tests on the Web is too obvious to warrant a patent. Now, the EFF says it has evidence that, even if the idea justifies a patent, Test.com was not the first to develop the technology to make it happen. According to the EFF, the IntraLearn Software Corporation began selling products with online testing capabilities in 1997, two years before Test.com applied for its patent. Jason Schultz, staff lawyer for the EFF, said that the USPTO would address the validity of the patent, which could take as long as a year or more. If the office determines that a patent is appropriate, said Schultz, it will "a tiny insignificant patent" rather than the very broad patent granted to Test.com.

Category *4B2* *Patents*

2006-05-22 Effector Online http://www.eff.org/news/archives/2006_05.php#004682

INTERNET TEST-TAKING PATENT DRAWS OFFICIAL SUSPICION. EFF WINS SECOND REEXAMINATION FROM PATENT OFFICE.

San Francisco - At the request of the Electronic Frontier Foundation (EFF), the U.S. Patent and Trademark Office (PTO) will reexamine a controversial patent for online test- taking from Test.com. The reexamination order is the second granted in just two months after petitions from EFF's Patent Busting Project. EFF filed the reexamination request because the extremely broad patent claims to cover almost all methods of online testing. Test.com has used this patent to demand payments from universities with distance education programs that give tests online. But EFF, in conjunction with Theodore C. McCullough of the Lemaire Patent Law Firm, showed that Test.com was not the first to come up with this testing method -- IntraLearn Software Corporation had been marketing an online test-taking system long before Test.com filed its patent request. "Bogus patents like these are hurting innovation and education in America," said EFF Staff Attorney Jason Schultz, who heads up the project. "This is a perfect example of how the patent system is broken and what needs to be fixed." Test.com now has the opportunity to file comments defending the patent, and then the PTO will determine whether to invalidate the patent. The PTO has narrowed or revoked roughly 70% of patents it has decided to reexamine. The successful reexamination request for the Test.com patent is the latest big victory for EFF's Patent Busting Project, which combats the chilling effects bad patents have on the public interest and innovation. . . .
For the full reexamination order: http://www.eff.org/patent/wanted/test/test_com_reexam_order.pdf
For more information about the Test.com patent reexamination: http://www.eff.org/patent/wanted/patent. php?p=test
For more on the Patent Busting Project: http://www.eff.org/patent/
For this release: http://www.eff.org/news/archives/2006_05.php#004682

Category 4B2 *Patents*

2006-08-02 EDUPAGE; Chronicle of Higher Education (sub. req'd) http://chronicle.com/daily/2006/08/2006080201t.htm

BLACKBOARD SUES TO PROTECT PATENT

Blackboard has filed a lawsuit against Desire2Learn for allegedly violating a patent that was granted in January. The patent covers 44 e-learning functions, such as providing users with predefined roles in multiple online courses. Matthew Small, senior vice president and general counsel for Blackboard, said that such features, which are common today, were novel ideas in the 90s when Blackboard applied for the patent. Blackboard officials also noted that the company has no intention of litigating against colleges or universities that might be infringing on the patent or against open source providers such as Moodle and Sakai. Officials from Desire2Learn said they could not comment on the suit because they had not had a chance to review it. Several observers believe the suit is overly broad, saying that the patent office does not have the staff to thoroughly investigate applications. Peter Schilling, director of information technology at Amherst College, said he thinks the patent will be invalidated if challenged.

DESIRE2LEARN RESPONDS TO BLACKBOARD PATENT CLAIM

In a legal filing responding to Blackboard's patent infringement lawsuit, Desire2Learn alleges not only that Blackboard's patent is invalid but also that senior Blackboard executives were aware of this when they filed the patent application in 1999. According to Desire2Learn, technology developed and marketed by the Instructional Management Systems (IMS) project in April 1998 represents so-called prior art, which would preclude granting a patent for such technology. Current Blackboard officials were paid consultants on that project and so were aware of those technologies, according to Desire2Learn. Matthew Small, senior vice president and general counsel for Blackboard, rejected Desire2Learn's contention and sought to reassure the broader community that its patent does not cover all learning systems. "We don't claim to have invented the course management system," he said. The IMS technology does not invalidate the Blackboard patent, Small suggested, though he declined to offer specifics about how the tools are different.

[Chronicle of Higher Education, 18 September 2006 (sub. Req'd) http://chronicle.com/daily/2006/09/2006091801t.htm]

LEGAL CENTER FILES CHALLENGE TO BLACKBOARD PATENT

A legal center has filed the first formal action against a Blackboard patent that has caused considerable anxiety in the higher education community. The patent covers certain aspects of learning management systems, and Blackboard has filed an infringement lawsuit against rival Desire2Learn. Many in higher education believe that the patent is too broad, that it does not account for prior art, and that Blackboard will use its patent power to stifle innovation. The new complaint, filed by the Software Freedom Law Center, an open source advocacy group, seeks a reexamination by the U.S. Patent and Trademark Office. The center said it has provided sufficient prior art to invalidate the patent. Officials from Blackboard have repeatedly denied any intention of pursuing patent litigation against the open source community, but they have also refused to put such claims into writing. According to Blackboard, the company welcomes the reexamination, saying its patent will be shown to be valid and will be stronger after the review.

[Chronicle of Higher Education, 1 December 2006 (sub. Req'd) http://chronicle.com/daily/2006/12/2006120101t.htm]

Category 4B2 *Patents*

2006-11-10 http://www.networkworld.com/news/2006/11106-software-patent-ignites-firestorm-in-higher-education.html

SOFTWARE PATENT IGNITES FIRESTORM IN HIGHER EDUCATION

Blackboard, the owners of WebCT and other online-learning software platforms, registered a patent on fundamental aspects of online learning and immediately sued Desire2Learn for patent infringement. Academics rose up in rage and protested that many of the patented ideas came from open-source, collaborative contributions that were part of prior art and should therefore never have been accepted by the US Patent and Trademark Office (USPTO) in the first place. Desire2Learn counterattacked with a lawsuit claiming intentional misconduct by Blackboard in failing to notify the USPTO of this prior art. The Board of Directors of EDUCAUSE weighed in with a public condemnation of Blackboard.

4B3 Reverse engineering

Category 4B3 Reverse engineering

2006-01-05 EDUPAGE; http://www.internetnews.com/security/article.php/3575441

EFF SEEKS PROTECTION FOR COMPUTER RESEARCHERS

The Electronic Frontier Foundation (EFF) has called on Sony EMI to pledge not to pursue prosecution of computer researchers who investigate the security of the company's products. Last fall, the company was caught in a public outcry over technology included in music CDs. The technology installed itself on users' computers and scanned them for potentially illegal activities. The company has removed those tools from CDs, but security researchers believe they have reason to reverse engineer copy protections on EMI CDs, a practice which would violate not only the Digital Millennium Copyright Act but also EMI's end user license agreement. Fred von Lohmann, senior staff attorney with EFF, said, "When it comes to computer security, it pays to have as many independent experts kick the tires as possible, and that can only happen if EMI assures those experts that they won't be sued for their trouble."

Category 4B3 Reverse engineering

2006-04-24 RISKS; CNET news.com http://tinyurl.com/k5ebw

CONGRESS PROPOSING TO STRENGTHEN DMCA

For the last few years, a coalition of technology companies, academics and computer programmers has been trying to persuade Congress to scale back the Digital Millennium Copyright Act.

Now Congress is preparing to do precisely the opposite. A proposed copyright law seen by CNET News.com would expand the DMCA's restrictions on software that can bypass copy protections and grant federal police more wiretapping and enforcement powers.

The draft legislation, created by the Bush administration and backed by Rep. Lamar Smith, already enjoys the support of large copyright holders such as the Recording Industry Association of America. Smith, a Texas Republican, is the chairman of the U.S. House of Representatives subcommittee that oversees intellectual property law.

[Excerpt by Declan McCullagh for RISKS]

4B4 EULA (End-user license agreements)

Category 4B4 EULA (End-user license agreements)

2007-02-06 Effector Online http://www.eff.org/deeplinks/archives/005104.php

MICROSOFT'S VISTA: READ THE FINE PRINT!

After numerous delays, Microsoft has launched its new Vista operating system and proclaimed the "Wow starts now." Thanks for filling us in, Microsoft, but what is there to be wowed about? Maybe Microsoft's talking about the collective gasp among consumers who are looking at the litany of restrictions buried within Vista's End User License Agreement (EULA). As law professor Michael Geist explains in a recent editorial, "In the name of shielding consumers from computer viruses and protecting copyright owners from potential infringement, Vista seemingly wrestles control of the 'user experience' from the user." For instance, Vista's EULA limits the numbers of copies that can be made (allowing only one for backup purposes). The anti-virus program that comes with Vista reserves the right to delete any programs it deems dangerous without permission, even though this could mean the removal of legitimate and useful software (or prevent other software from working). And the EULA warns users that "you may not work around any technical limitations of the software." And that's not all -- read the whole editorial for more: http://www.michaelgeist.ca/content/view/1640/159/
For this post and related links: http://www.eff.org/deeplinks/archives/005104.php

4B5 Trademarks

Category 4B5 Trademarks

2006-06-09 http://www.pingwales.co.uk/2006/06/19/SpamTM.html

WELSH SOFTWARE FIRM WINS BATTLE OVER "SPAM" TRADEMARK

A small Welsh firm, NetBop Technologies of Swansea, has won the right to use the word "spam" in its anti-junk e-mail product name, BopSpam. The firm was opposed in March 2005 by Hormel Foods Company, which owns the trademark "SPAM" for its luncheon meat. The UK Patent Office ruled in favor of NetBop and Hormel dropped its opposition in February 2006.

Category 4B5 Trademarks

2007-02-06 Effector Online http://www.eff.org/deeplinks/archives/005110.php

PORK BOARD SAVES OWN BACON, APOLOGIZES TO BLOGGER FOR TRADEMARK MISUSE.

The National Pork Board has apologized for threatening to sue "The Lactivist" blog for using the slogan "the other white milk." This is no joke, though the Board's legal theory was laughable. After warning blogger Jennifer Laycock that using the slogan on a T-shirt infringed and diluted the Pork Board's trademark on "the other white meat," perhaps the Board expected the blogger to cave immediately. Instead, Laycock took her case to the court of public opinion, blogging about the letter and asking her readers to contact the Pork Board to complain about it. Laycock and her readers were particularly offended by the letter's implication that Laycock was an advocate of adult breastfeeding. The Pork Board was hit with calls and emails. Doubtless realizing that an entity devoted to marketing a food product should not risk alienating mothers, the Pork Board promptly contacted Ms. Laycock to apologize. Kudos to the Pork Board for realizing the error of its ways. But it's a shame that it didn't spend a little more time investigating before sending off an improper cease and desist letter. Like Chicago Auto Show, the Pork Board decided to shoot first and ask questions later. Laycock refused to be intimidated, but other bloggers and parodists may not have the knowledge or resources to fight back to defend non-infringing uses.
For this post and related links: http://www.eff.org/deeplinks/archives/005110.php

Category 4B5 Trademarks

2007-02-28 Effector Online http://www.eff.org/news/archives/2007_02.php#005134

FIGHT OVER GOOGLE'S 'SPONSORED LINKS' THREATENS INTERNET FREE SPEECH. EFF ASKS JUDGE TO UPHOLD KEY TRADEMARK RULING.

San Francisco - The Electronic Frontier Foundation (EFF) asked the U.S. 2nd Circuit Court of Appeals last week to uphold an important ruling allowing anyone to purchase Google's "sponsored links" tied to trademarks, arguing that the practice is legal under trademark law and provides a vital means for online speakers to connect with audiences on the Internet. Google's "sponsored links" feature allows customers to buy advertisements attached to certain search terms. When a Google user types those terms into the search engine, the sponsored links appear along with the search results. However, a company named Rescuecom filed a lawsuit against Google over the program, claiming that selling sponsored links for the term "Rescuecom" infringed its trademark. In an amicus brief filed with the appeals court last week, EFF argues that the sponsored links are not an infringing use, and in fact promote a vibrant public sphere by helping online speakers reach a broader audience. An example cited in the brief is that of "The Coalition of Immokalee Farmworkers," a group critical of McDonald's business practices. The coalition bought sponsored links attached to searches for "McDonald's" in order to stimulate debate and mobilize support. "The Internet has brought together speakers of many kinds - - some competing with trademark owners, others criticizing them, still others simply referring to them while discussing other subjects or products," said EFF Staff Attorney Corynne McSherry. "Services like Google's 'sponsored links' help people with something to say reach those who might be interested in hearing it." Rescuecom has asked the court to hold that trademark law regulates virtually any use of search keywords that are also trademarks. This would give trademark holders a legal sword to wield against critics and competitors, as well as the intermediaries upon which those critics and competitors rely to spread their message. But courts have historically taken care to ensure that trademark restrictions do not allow markholders to interfere with Constitutionallyprotected free speech. "On the Internet, trademarks aren't just identifiers. They are essential navigation tools and vehicles of expression," said EFF Staff Attorney Jason Schultz. "Quashing this speech goes against both the law and the public interest." A judge dismissed Rescuecom's case against Google last year, but the company is appealing the decision.
For the full brief filed in Rescuecom v. Google: http://www.eff.org/legal/cases/rescuecom_v_google/EFF_amicus.pdf
For this release: http://www.eff.org/news/archives/2007_02.php#005134

Category 4B5 Trademarks

2007-04-11 DHS Daily OSIR; Associated Press http://www.nytimes.com/aponline/technology/AP-Keyword-Law.html

UTAH PLANS TO CREATE TRADEMARK REGISTRY.

Utah plans to set up a trademark registry to prevent rival advertisers from capturing the attention of people who type a search query on another company or its products. The new law would allow any company to create an "electronic" trademark and stop rivals from using those marks to make their advertisements appear on search engines and other Websites that use keyword-triggered advertising. The electronic mark registry, set to take effect June 30, follows unsuccessful attempts by Utah in recent years to regulate advertising spyware and pornography on the Internet. Utah legislators said they believe the law can withstand a court challenge because it only lets companies enforce their marks in the courts, leaving state government out of the fray. Experts, however, doubt that makes the law constitutional. The Utah law "tries to stop keyword advertising across the world," said Eric Goldman, a professor at Santa Clara (CA) University School of Law, who said the U.S. Constitution reserves regulation of interstate commerce to the federal government alone.

4C1 Paradigms, security standards

Category 4C1 Paradigms, security standards

2006-05-15 DHS Daily OSIR; MarketWatch
http://www.marketwatch.com/News/Story/Story.aspx?guid=%7B827 2BEEA-DB72-4956-843D-212CC0C14446%7D&siteid=google

ELECTRIC INDUSTRY READIES RELIABILITY STANDARDS

Mandatory reliability standards for the electricity industry, as required by the Energy Policy Act in 2005, are expected to be in place ahead of next summer, more than three years after blackouts shut down major portions of the U.S. power system. The industry believes it can have the reliability rules in place "well before the summer of 2007," said Rick Sergel of the North American Electric Reliability Council (NERC), at a hearing before the Senate Energy and Natural Resources Committee on Monday, May 15. The Federal Energy Regulatory Commission (FERC) is reviewing NERC's application to become the Electric Reliability Organization, the organization that will oversee the reliability rules. Discussions continue over how much deference regions of the country should be given to impose region-specific requirements on power grid operators and users. Sergel said some regional difference may be necessary to reflect physical differences in electricity infrastructure. Debate has also ensued over who will be required to comply with the rules. NERC plans to compile a registry of all owners, operators, and end users whose actions or inactions can have a material impact on the reliability of the bulk power system.

NERC testimony: ftp://www.nerc.com/pub/sys/all_updl/docs/testimony/Sergel-%20testimony0515.pdf
FERC testimony:
http://www.ferc.gov/EventCalendar/Files/20060515151838-SENR%
20EPAct%2005%20Electric%20Reliability%20Provisions%20(Moot)% 2005-15-06.pdf

---

Category 4C1 Paradigms, security standards

2006-05-17 DHS Daily OSIR; Federal Computer Week http://fcw.com/article94546-05-17-06-Web

NIST RELEASES STANDARDS FOR SECURING DOMAIN NAMES

The National Institute of Standards and Technology (NIST) released new guidelines for securing the Domain Name System (DNS) on Tuesday, May 16. The publication details threats and how best to approach them as well as specific recommendations on secure configurations for domain names and their associated mechanisms.

NIST guidelines: http://csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf

---

Category 4C1 Paradigms, security standards

2006-07-13 DHS Daily OSIR; Washington Technology
http://www.washingtontechnology.com/news/1_1/homeland/28931-1.htm

NEW STANDARD PROPOSED FOR INFORMATION SHARING.

The federal government should develop an “authorized use” standard to improve information sharing against terrorism, according to a new report from the Markle Foundation Task Force on National Security in the Information Age. The 100-page report, Mobilizing Information to Prevent Terrorism, was released on Thursday, July 13, and is the third from the task force addressing how to share information for national-security purposes while also protecting privacy and civil liberties. Under the proposed authorized use standard, access would be granted based on how the information will be used, rather than on nationality or location of collection. Report: http://www.markle.org/downloadable_assets/2006_nstf_report3.pdf

---

Category 4C1 Paradigms, security standards

2006-08-31 DHS Daily OSIR; Platts Energy Bulletin
http://www.platts.com/HOME/News/7683435.xml?sub=HOME&p=HOME/News&?undefined&undefined

NERC SUBMITS CYBERSECURITY GRID STANDARDS FOR FERC APPROVAL.

The North American Electric Reliability Council (NERC) submitted 16 new and 11 revised reliability standards to the Federal Energy Regulatory Commission (FERC) late Wednesday, August 30. "The largest number of them are what we refer to as the cybersecurity standards," said Stan Johnson, NERC's manager for situation awareness and infrastructure security. The commission approved NERC to be the electric reliability organization (ERO) in July after Congress in the Energy Policy Act of 2005 ordered the agency to supervise an electric reliability organization that develops standards and enforces the country's new mandatory reliability system. In its application to be the ERO, NERC in April submitted 102 existing voluntary reliability standards. FERC staff released a report in May citing deficiencies in those standards. "These are additional standards that had been in progress and have been working through the drafting teams and were not included in the 102," Johnson said. Cybersecurity standards relate to the control systems and "the possibility of hackers getting into the control systems" and compromising the reliability of the bulk power system," Johnson said.

4C2 Risk management methodology & tools

Category 4C2 Risk management methodology & tools

2006-10-31 EDUPAGE; Federal Computer Week http://www.fcw.com/article96645-10-31-06-Web

USERS POPULATE THE VULNERABILITY DATABASE

A database of computer vulnerabilities created by the National Institute of Standards and Technology (NIST) has proven extremely popular, both for reporting new problems and for researching existing ones. Since its debut one year ago, the National Vulnerability Database receives hits at the rate of 25 million per year and has grown from 12,000 vulnerabilities to 20,000, with new ones being reported regularly. According to Peter Mell, senior computer scientist at NIST, who created the database, "I think 20,000 is just the tip of the iceberg." The database categorizes vulnerabilities by product and version number, directing users to resources to fix the problems. The database uses the Common Vulnerability Scoring System to rate the severity of each vulnerability recorded. Alan Paller, director of research at the SANS Institute, noted that a significant portion of the most recently reported problems affect Web-based applications.

4C4 Professional certification in security, auditing

Category 4C4 Professional certification in security, auditing

2006-04-27 RISKS; The Register http://www.theregister.co.uk/2006/04/26/law_change_for_pis

GEORGIA LAW REQUIRES LICENSING FOR DIGITAL FORENSICS SPECIALISTS?

Some computer professionals will need to get a Private Investigator license just to continue doing their computer work. I imagine this will also apply to accountants and auditors, in fact anyone who analyses data that is on computer systems, on behalf of some other company, and perhaps people who work at software houses, computer retailers, whoever does repairs to computers, installations of new stuff. We will have to be asking suppliers of firewall, anti-virus, anti-spam, anti-spyware etc. if they have a PI license, otherwise it might be illegal to buy their products, and if there are no such suppliers, then it may be illegal to be protected against the cyber-criminals.

Companies will need to get an opinion from their lawyers, with respect to filing annual reports with the state and with government regulators. We are supposed to swear this data is correct under penalty of perjury, but it was derived by accounting and computer experts, not Private Investigators, but now it is illegal to get such data from people who are not Private Investigators? Does this also mean that Police Department personnel need to get a PI license before they may testify in court?

[Summary and analysis by Al Macintyre]

Category 4C4 Professional certification in security, auditing

2006-07-20 DHS Daily OSIR; Washington Technology
http://www.washingtontechnology.com/news/1_1/homeland/28965-1.html

FEMA CRAFTS CREDENTIALING SYSTEM FOR FIRST RESPONDERS.

FEMA crafts credentialing system for first responders Documentation for millions of police, firefighters, medical workers and other emergency personnel nationwide is being aggregated into a National Emergency Responder Credentialing System that the Department of Homeland Security (DHS) expects to make operational next year. At a future date, the new credentialing system may include a national identification card for emergency responders and a record-keeping system, according to a DHS fact sheet published on project. The little-publicized credentialing system is intended to assist in identifying which responders should be allowed to enter an incident scene immediately following a disaster or terrorist attack. It is designed to help prohibit unauthorized entry of volunteers who may not be qualified to assist. DHS Fact Sheet: http://www.fema.gov/pdf/emergency/nims/credent_faq.pdf

4C5 Academic/Industry/Vendor/Govt efforts

Category 4C5 Academic/Industry/Vendor/Govt efforts

2006-03-27 DHS Daily OSIR; http://www.washingtontechnology.com/news/1_1/homeland/28284-1.html

COUNCIL TO DRAW UP CYBER ATTACK RESPONSE.

Setting up a national IT disaster response apparatus is one possible topic to be addressed by the IT Sector Coordinating Council as it drafts a sector-specific plan for protecting the nation's computer networks against a terrorist attack or other disaster, according to the group's chairman. The goal is for private sector IT companies and government to work together to prevent and to respond to cyber attacks. The council wants ideas from the IT industry and from the Department of Homeland Security as it begins work on the sector-specific critical infrastructure protection plan at its Tuesday, April 4, meeting. The council expects to complete the plan by September.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2006-06-28 EDUPAGE; Wall Street Journal (sub. req'd)
http://online.wsj.com/article/SB115144422202392266.html

NEW RESEARCH CENTER WILL STUDY IDENTITY FRAUD

A new research center is being launched at Utica College in New York to study identity fraud and ways to fight the problem. The Center for Identity Management and Information Protection (CIMIP) is being developed by the Secret Service, the FBI, IBM, and LexisNexis. Norm Willox, chief executive of special services at LexisNexis, said that CIMIP will fill a gap in current efforts to understand and address identity fraud. Gary Gordon, professor of economic crime management at Utica College, will direct CIMIP, which will have access to Secret Service files to help researchers see the big picture and potentially spot patterns. James Burrus, acting assistant director of the FBI's criminal investigative division, noted that identity fraud also has implications for national security. "The FBI looks forward to the opportunity to apply CIMIP research to more effective law enforcement and protection," he said.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2006-10-26 DHS Daily OSIR; GovExec
http://www.govexec.com/story_page.cfm?articleid=35360&dcn=todaysnews

ACADEMIC URGES GOVERNMENT-RUN EMERGENCY COMMUNICATIONS NETWORK.

A Carnegie Mellon University expert on Thursday, October 26, called for the development of a government-run communications network that would enable police, firefighters and other emergency responders from different jurisdictions to talk to each other. "A government system is feasible, and it would clearly be more cost effective than what we have today," Jon Peha, an engineering and public policy professor, said during the presentation of a paper on the issue at a forum sponsored by the New America Foundation. Peha said that after the disastrous communications failures on September 11, 2001, and during Hurricane Katrina, he could "not see why we should tolerate" the current decentralized emergency-response system, which gives the flexibility of local "first responder" agencies precedence over standardization and regional cooperation. Peha said a good starting place for a new system would be the congressionally mandated program to double the emergency broadcast bandwidth by reallocating 24 megahertz of prime spectrum from television to public safety as a part of the transition from analog to digital signals in 2009.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2007-05-21 DHS Daily OSIR; Washington Technology
http://www.washingtontechnology.com/online/1_1/30696-1.html

DHS CALLS FOR CYBERSECURITY WHITE PAPERS.

The Department of Homeland Security (DHS) is initiating an ambitious Cyber Security Research Development Center program that entails soliciting input from industry, government labs and academia on how to protect data against the latest threats and intrusions. The Science & Technology Directorate published a 43-page broad agency announcement seeking white papers on topics such as botnet and malware protection, composable and scaleable systems, cyber metrics, data visualization, routing security, process control security, real-time assessment, data anonymization and insider threat detection and management. White papers on technologies to address the threats and strengthen protections are due on June 27. Final proposals will be due on September 17.

4D Funny / miscellaneous

Category 4D Funny / miscellaneous

2007-04-01 Effector Online http://www.eff.org/cgi/tiny?urlID=5

RIAA TO PARENTS: PAY WHEN THEY'RE TODDLERS AND SAVE THE BOTHER LATER

The RIAA today sent a "settlement letter" to all parents of children under 3 years old offering a toddler settlement rate for online copyright infringement if they simply send payment to major record labels before their children learn to read. "Our goal is to make this easier for parents," said RIAA President Cary Sherman. "Everyone knows that in this era of increasing hard drive capacity and new digital media technologies, it is inevitable that every child in America will infringe copyright sooner or later. With our 'toddler settlement' rate, parents can avoid those pesky lawsuits. Consider it a way to invest your child's future." The toddler settlement requires parents to log everything their child ever does online and to make those logs available to the RIAA at regular intervals. "It can just become a part of every birthday celebration," added RIAA's counsel at Holme, Roberts and Owen. "Blow out the candles and send your Internet logs to Uncle RIAA!"
For this post: http://www.eff.org/cgi/tiny?urlID=5

[NOTE TO THE HUMOR-IMPAIRED: THIS IS AN APRIL-FOOL'S JOKE]

Category 4D Funny / miscellaneous

2007-04-01 Effector Online

NSA TO OPEN VIRTUAL "BLACK BOX" OFFICE IN SECOND LIFE

The National Security Agency announced today plans to open a virtual "office" in the popular online game Second Life. The office will consist of a large black box located in an undisclosed location. "We've already eavesdropped on most Americans' first lives," said NSA spokesperson Narc Informer. "Now we have a whole new world to listen in on." The government also plans to build a virtual secret courtroom to issue virtual carte blanche wiretapping orders and will eventually add a virtual offshore interrogation island for enemy combatant avatars to be held without trial.
For this post: http://www.eff.org/cgi/tiny?urlID=556

[NOTE TO THE HUMOR-IMPAIRED: THIS IS AN APRIL-FOOL'S JOKE]

Category 4D Funny / miscellaneous

2007-05-18 DHS Daily OSIR; eWeek http://www.eweek.com/article2/0,1895,2132447,00.asp

HUNDREDS CLICK ON 'CLICK HERE TO GET INFECTED' AD.

The fact that 409 people clicked on an ad that offers infection for those with virus-free PCs proves that people will click on just about anything. That was evidenced by the 409 people who clicked on an ad that offers infection for those with virus-free PCs. The ad, run by a person who identifies himself as security professional Didier Stevens, reads like this: "Drive-By Download. Is your PC virus-free? Get it infected here! drive-by-download.info." Stevens, who says he works for Contraste Europe, has been running his Google Adwords campaign for six months now and has received 409 hits. Stevens has done similar research in the past, such as finding out how easy it is to land on a drive-by download site when doing a Google search. Stevens says that he got the idea after picking up a small book on Google Adwords at the library and finding out how easy and cheap it is to set up an ad.