INFOSEC UPDATE 2002 Student Workbook

Norwich University eProtectIT Conference March 20-22, 2002



M. E. Kabay, PhD, CISSP
Assoc. Prof. Information Assurance
Dept. of Computer Information Systems, Division of Business
Norwich University

mkabay@compuserve.com

01 Introduction

Category 01

Introduction

2002-03-14

M. E. Kabay, PhD, CISSP

Welcome to the 2001 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).

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

2002-03-14

The taxonomy 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 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
- 1 Introduction
- 2 Taxonomy of INFOSEC Issues
- 3 Sources of Information
- 4 Copyright
- 5 Using IYIR
- 6 The INFOSEC UPDATE Course
- 7 Acknowledgements
- 8 About the Editor
- 10 Computer Crimes (cases, indictments, convictions, sentences)
- 11 Breaches of confidentiality, data leakage, covert channels
- 12 Wiretapping, interception (not jamming; not govt/law enforcement)
- 12.1 Wiretapping
- 12.2 Interception
- 13 Data diddling, data corruption, embezzlement
- 13.1 Data diddling
- 13.2 Data corruption & destruction
- 13.3 Embezzlement
- 13.4 Obsolescence
- 14 Viruses, virus-hoaxes, Trojans (assembly level or macro: not ActiveX or Java)
- 14.1 Viruses
- 14.2 Worms
- 14.3 Virus/worms
- 14.4 Trojans
- 14.5 Virus hoaxes
- 15 Fraud (not embezzlement), extortion, slamming
- 15.1 Fraud
- 15.2 Extortion
- 15.3 Slamming
- 16 INFOWAR, industrial espionage, hacktivism
- 16.1 Industrial espionage
- 16.2 Industrial information systems sabotage
- 16.3 Infrastructure protection
- 16.4 Military & government perspectives on INFOWAR
- 16.5 Hacktivism
- 17 Penetration, phreaking (entering systems, stealing telephone service)
- 17.1 Penetration
- 17.2 Web vandalism
- 17.3 Phreaking
- 18 Theft of equipment (laptops, ATMs, computers, cables, network components)
- 19 Counterfeits, forgery (including commercial software/music piracy)
- 19.1 Software piracy
- 19.2 Music
- 19.3 Movies / TV
- 19.4 Books / e-books
- 19.5 Games
- 19.6 Credit-cards, other tokens
- 19.7 Legal or business documents

- 19.8 Plagiarism
- 19.9 Products (hardware, clothing etc.)
- 1A Criminal hacker scene (conventions, meetings, testimony, biographies, publications)
- 1A1 Conventions and meetings
- 1A2 Testimony in court or committees
- 1A3 Biographical notes on individual criminals
- 1A4 Publications
- 1A5 Organizations
- 1B Pornography, Net-harm, cyberstalking, gambling, online auctions
- 1B1 Adult pornography
- 1B2 Child pornography
- 1B3 Pedophilia, kidnapping, Net-adoption fraud
- 1B4 Stalking
- 1B5 Gambling
- 1B6 Auctions
- 1B7 Hate groups, speech
- 1B8 Traffic in women, slavery
- 1B9 Non-virus hoaxes, urban myths
- 1C Spoofing
- 1C1 Impersonation
- 1C2 Identity theft
- 1C3 Pseudonymity
- 1D Law Enforcement & Forensics (technology, organizations, proposals, litigation, rulings, judgements)
- 1D1 Organizations, cooperation
- 1D2 Technology
- 1D3 Litigation, legal rulings, judgements
- 1D4 Government funding
- 1E4 Government funding
- 20 Emerging Vulnerabilities & Defenses
- 21 Quality assurance failures (general)
- 22 Quality assurance (security products)
- 23 Availability issues (not denial-of-service attacks)
- 24 Internet tools
- 24.1 Java
- 24.2 Javascript
- 24.3 ActiveX
- 24.4 HTML
- 24.5 E-mail & instant messaging / chat
- 24.6 Web-site infrastructure, general Web security issues
- 25 Computer / remote control, jamming (not interception), RFI, HERF, EMP/T
- 25.1 Remote control, reprogramming, auto-updates
- 25.2 Jamming
- 25.3 RFI, HERF, EMP/T
- 25.4 Health effects of electronic equipment (phones, screens, etc.)
- 26 Operating systems, network operating systems, TCP/IP problems (alerts)
- 26.1 Windows 9x/Me/XP
- 26.2 Windows NT/2K
- 26.3 UNIX flavors
- 26.4 TCP/IP & HTTP
- 26.5 LAN OS
- 26.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11
- 26.7 SWDR (Software-defined radio)
- 26.8 MAC OS
- 27 Tools for evaluating vulnerabilities
- 28 Denial of service
- 28.1 DoS attacks
- 28.2 DDoS attacks
- 28.3 DoS countermeasures
- 29 Peer-to-peer networking
- 2A Firewalls & other perimeter defenses
- 2B Intrusion detection systems
- 2C Addiction, cyber-syndromes, sociology

- 2D Port scanning
- 2E Online voting & legal proceedings
- 2F Spyware
- 2G Scumware
- 30 Management & Policy
- 31 The state of information security
- 31.1 Surveys, studies, audits
- 31.2 Estimates, guesses, predictions, forecasts
- 32 Censorship, indecency laws, 1st amendment (law)
- 32.1 USA
- 32.2 Non-USA
- 33 Acceptable-use policies, spam & anti-spam (laws, technology)
- 33.1 Acceptable use
- 33.2 Spam
- 33.3 Antispam
- 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
- 38 Consumer privacy, profiling, trade in personal information
- 38.1 Consumer profiling
- 38.2 Trade in personal information
- 38.3 Industry efforts for privacy protection
- 40 Cryptography, Law & E-commerce
- 41 Cryptanalysis techniques
- 42 Crypto algorithm weakness, brute-force attacks, implementation flaws
- 42.1 Weaknesses
- 42.2 Brute-force attacks
- 42.3 Implementation flaws
- 43 I&A products (tokens, biometrics, passwords, Kerberos)
- 43.1 Tokens
- 43.2 Biometrics
- 43.3 Passwords
- 43.4 Kerberos
- 44 Encryption algorithms, products
- 44.1 Algorithms
- 44.2 Products
- 45 E-commerce security, digital signature, products, digital cash, e-payments
- 45.1 Digital signatures / certificates
- 45.2 Digital cash
- 45.3 Micropayments
- 45.4 E-payments / e-wallets
- 45.5 Watermarks
- 45.6 Other e-commerce security measures
- 46 Cryptography exports from US
- 47 Key escrow / recovery laws
- 48 Foreign crypto & computer crime laws (not cases or sentences)
- 49 Privacy, government surveillance, legislation, agreements
- 49.1 International agreements on security, privacy, Net law
- 49.2 EC legislation & regulation
- 49.3 US legislation & regulation
- 49.4 Other legislation & regulation
- 49.5 Law enforcement
- 49.6 Surveillance & anonymity
- 4A Evolution of Net law: framing, pointing, linking, jurisdiction
- 4A1 Framing
- 4A2 Pointing, linking, metatext

- 4A3 Jurisdiction
- 4A4 Blocking
- 4A5 Archives
- 4A6 Libel
- 4B Intellectual property: patents, copyrights (law)
- 4B1 Copyright
- 4B2 Patents
- 4B3 Reverse engineering
- 4B4 EULA (End-user license agreements)
- 4B5 Trademarks
- 4C Security paradigms, risk management, site-security certification, professional certification
- 4C1 Paradigms, security standards
- 4C2 Risk management methodology & tools
- 4C3 Certification of site security, privacy protection
- 4C4 Professional certification in security, auditing
- 4D Funny / miscellaneous

O3 Sources of Information

Category 03 2002-03-14

Sources of Information

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, editors of the daily _NewsScan_ and biweekly _Innovation_ e-publications. In addition, I have been quoting (with attribution) many of the contributors to Peter G. Neumann's RISKS Forum Digest. Lately, the Daily Report from NIPC (National Infrastructure Protection Center) have proven valuable in supplementing the material at hand. I also naturally continue to write my own abstracts of interesting articles when necessary. These articles are pointed to by a range of news sources; for details, see the paper at < http://www2.norwich.edu/mkabay/overviews/infosec_ed.htm > or < http://www2.norwich.edu/mkabay/overviews/infosec_ed.pdf > .

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

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

The NIPC Daily Report is available to InfraGard members and law enforcement agencies. For details, see < http://www.nipc.gov/ >.

04 Copyright

Category 04 2002-03-14 Copyright

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

05 Using IYIR

Category 05 2002-03-14

Using IYIR

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!

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 2002-03-14

The INFOSEC UPDATE Course

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

Day 1:

AM: Computer Crime Update PM: Emerging Vulnerabilities

Day 2:

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

For full details, see section 2 on Taxonomy.

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

07 Acknowledgements

Category 07 2002-03-14

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 stand out for their kindness in so generously allowing me to quote them verbatim in so many hundreds of stories. Thanks guys – I simply could not do this without your help. My colleagues at TruSecure Corporation were always supportive and encouraging; I thank my favorite curmudgeon, David Kennedy, Director of Resarch for TruSecure, for many years of continuing friendship. And finally, as always, I thank my wife, Deborah Black, light of my life, for all her support despite the amount of time that this project subtracts from our time together.

O8 About the Editor

Category 08 2002-03-14

About the Editor

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/index.htm > and click on my CV link.

M. Kabay began programming in assembler at age 15 in 1965. In 1976, he received his PhD from Dartmouth College in applied statistics and invertebrate zoology. In 1979, he joined a compiler team for a new 4GL and RDBMS in the U.S. and then joined Hewlett-Packard Canada in 1980, winning the Systems Engineer of the Year Award in 1982. He has published over 350 technical papers in operations management and security, has published a 1996 textbook on security, and is Technical Editor of the 4th Edition of the Computer Security Handbook (Wiley, 2002). He returned to academia in July 2001 and is now Associate Professor, Information Assurance, Dept. of Computer Information Systems, Norwich University, Northfield, VT 05663-1035 USA where he is also the Director of the Master's Program in Information Assurance.

V: 802-479-7937

E: mkabay@compuserve.com

W: http://www2.norwich.edu/mkabay/index.htm

Breaches of confidentiality, data leakage, covert channels

Category 11 Breaches of confidentiality, data leakage, covert channels

2001-01-23 confidentiality Web data leakage customer information privacy fraud

RISKS 21 21

Monty Solomon wrote in RISKS, "A security breach at Travelocity recently exposed the personal information of up to 51,000 online travel company's customers who had participated in a site promotion. Customer names, addresses, phone numbers, and e-mail addresses were revealed because of an inadequately protected directory -- possibly for up to a month. This resulted from new servers cutover from San Francisco to Tulsa. [Source: Troy Wolverton, CNET News.com, 22 Jan 2001

http://news.cnet.com/news/0-1007-200-4564919.html]"

Category 11 Breaches of confidentiality, data leakage, covert channels

2001-02-16 proprietary document formats hidden information concealed data confidentiality Web

RISKS 21 25

Paul Henry noted that the well-known problem of hidden information in MS Word documents continues to be a source of breaches of confidentiality. Writing in RISKS, he explained, "I received an MS Word document from a software start-up regarding one of their clients. Throughout the document the client was referred to as 'X', so as not to disclose the name. However I do not own a copy of Word, and was reading it using Notepad of all things, and discovered at the end the name of the directory in which the document was stored -- and also the real name of the client! I checked on a number of other word documents I had for hidden info, especially ones from Agencies who are looking to fill positions -- and yes, again I was able to tell who the client was from the hidden information in the documents."

Mr Henry concluded, "Risks: What potentially damaging information is hidden in published documents in Word, PDF and other complex formats? Mitigation: Use RTF when you can -- no hidden info, no viruses."

Category 11 Breaches of confidentiality, data leakage, covert channels

2001-03-12 confidential arrest records law enforcement Web site privacy accuracy

completeness

RISKS 21 27

Dan Graifer noted that "Fairfax County police are posting their arrest records online. Everything from speeding tickets to homicide. . . .[These] are never updated to indicate the disposition of the cases, nor is that information available elsewhere." In addition, Mr Graifer reported, all the original crime reports in MS Word format were also available online.

Category 11 Breaches of confidentiality, data leakage, covert channels

2001-04-11 appropriate use confidentiality MS-Word document history data leakage QA

quality assurance modem penetration

RISKS 21 35

Tsotomu Shimomura revealed that there was a back door in the Alcatel ADSL modem that would allow anyone to "penetrate a computer system linked to the Internet by Alcatel 1000 ADSL and Speed Touch Home modems." The interesting consequence was that Alcatel posted a statement about the problem on their Web site. Unfortunately for Alcatel, someone chose to post a MS-Word document in which all the changes were still accessible, including the following embarrassing dialog reported to RISKS by Mike Bristow:

- > (When and where will the firewall software be available? CERT has
- > said that they don't believe that installing a firewall is the
- > answer. What are you doing to provide a legitimate fix?)

Category 11 Breaches of confidentiality, data leakage, covert channels

2001-05-04 banking financial information social engineering industrial espionage

confidentiality breach

NIPC Daily Report

About a dozen of the nation's leading banks will discuss on 4 May how to protect themselves from using information brokers who trick other banks into turning over confidential details about individuals' finances. One recommendation on the agenda is that banks insist that brokers sign contracts promising they will not use illegal pretext calls to get data about debtors' assets. Federal regulators have urged national banks to boost efforts to protect customers against information brokers and identity thieves. The banks' apparent sense of urgency on pretext calling shows how deep an impact privacy issues have had on the financial services industry in recent years. The financial institutions want to find a way to improve security and detect fraud, while providing easy telephone and Internet access for their customers.

Category 11 Breaches of confidentiality, data leakage, covert channels

2001-05-04 covert channel confidentiality e-mail appropriate use spreadsheet ignorance

novice user awareness education training Powerpoint presentation

RISKS 21 39

Christopher Auger contributed an interesting scenario to RISKS about unintended disclosures. Seems that a sales director created a new organization chart on a worksheet in one of her existing Excel files. She told her secretary to forward the new chart to the entire company. Unfortunately, the secretary sent the entire Excel file, including two other worksheets. One worksheet contained highly sensitive Personnel Department information including employee salaries and sometimes disparaging remarks about specific employees. The other worksheet included a detailed plan for firing a specific, veteran salesman. The unintended disclosures caused an uproar and provided fuel for a lawsuit by the intended victim of her machinations.

Category 11 Breaches of confidentiality, data leakage, covert channels

2001-05-11 proprietary document formats hidden information concealed data confidentiality

RISKS 21 40

According to Clive Page, writing in RISKS, MS-Word can generate two completely disparate texts if one uses UNIX utilities to read the files. In one case, he found a quote for equipment when he read the file using MS-Word but a quote for different equipment addressed to a different client when he used his non-Windows utilities.

Category 11 Breaches of confidentiality, data leakage, covert channels

2001-06-05 privacy Web confidentiality adolescent harassment arrest

NewsScan

STUDENTS CHARGED WITH WEB HARASSMENT [5 Jun 2001]

Two high school students in Chappaqua NY have been charged with sexual harassment for operating a Web site that published the secrets of several dozen girls at the school. If convicted the two teenagers could be sentenced to as much a year in jail and a \$1,000 fine. One student at the school said: "You hang out with your friends and you make stupid comments but no one acts on it. No one makes a Web site." A police official said: "In many cases, there was information put out that was very sensitive, very private and information that caused a lot of anguish. All of these girls felt exploited by it." (AP/USA Today 5 Jun 2001)

http://www.usatoday.com/life/cyber/tech/2001-06-05-web-sex-gossip.htm

Category 11 Breaches of confidentiality, data leakage, covert channels e-mail vulnerability holes bug confidentiality

NewsScan

E-MAIL SECURITY BREACHES: EVERYONE IS VULNERABLE

The e-mail of Dennis Tito, the investment banker who paid to become the first tourist in space, was insecure for more than a year – as were the communications of his entire company, Wilshire Associates. . . . Although there is no evidence that anyone took advantage of the breaches, they allowed access by outsiders to confidential company business, including financial data, passwords, and the personal information of employees. However, security experts say Wilshire's problem is not an isolated one, and warn that American companies are not taking computer security issues seriously. Peter G. Neumann, principal scientist in the computer science lab at SRI International, says that the security breach discovered at Wilshire is just "one of thousands of vulnerabilities known forever to the world. Everybody out there is vulnerable." (Washington Post 22 Jun 2001)

http://washingtonpost.com/wp-dyn/articles/A7642-2001Jun15.html

Category 11 Breaches of confidentiality, data leakage, covert channels

2001-07-05 confidentiality compromise e-mail CC BCC error medical information drug

prescription

RISKS 21 51

The drug company Eli Lilly sent out an e-mail reminder to renew their prescriptions for Prozac to 600 clients – and used CC instead of BCC, thus revealing the entire list of names and e-mail addresses to all 600 recipients.

Category 11 Breaches of confidentiality, data leakage, covert channels

2001-09-10 privacy miniature wireless camera broadcast voyeurs peeping Tom spying

surveillance law enforcement police

NewsScan

LITTLE BROTHER MAY BE WATCHING YOU (WITH X10 VIDEOCAMS)

A company called X10 Wireless Technology is marketing its tiny color video cameras for their use in keeping an eye on your kids or even engaging in voyeuristic activity. One ad for the \$79.99 device displays a bare-backed woman and the headline "Quit Spying on People! (we never told you to do that)." The technology uses radio frequencies for communication among devices within a 100-foot radius, and represents a development that one attorney says "is outstripping everything we once contemplated about privacy." X10 devices have been found planted secretly in such places as college shower rooms, attorneys' offices, and corporate meeting rooms. (San Jose Mercury News 10 Sep 2001) http://www.siliconvalley.com/docs/news/svfront/027254.htm

Category 11 Breaches of confidentiality, data leakage, covert channels

2001-10-08 covert channel confidentiality e-mail appropriate use spreadsheet ignorance novice user awareness education training Excel spreadsheet paste unformatted

8

RISKS 21 69

Will Middelaer noted another risk from Excel and Outlook that creates a covert channel for inadvertent data disclosure. Writing in RISK, he recounted how he and a colleague were puzzled at the size and lengthy opening of a simple e-mail message "composed of one short sentence of plain text followed by (what I thought was) a two column by ten row grid of excel cells. I put the cells into the e-mail by highlighting them in Excel, then copying and pasting them into an e-mail. What I did not know was that the e-mail message actually contained the entire 12,000 plus cells of the spreadsheet including formatting and formulas. Though it appears to contain only the 20 cells that I intended to send him, double clicking the cells in the e-mail launched Excel, which opened with a complete version of the spreadsheet from which I had selected the cells to send him. The only piece of information missing seems to be the name of the file, as it opens with a generic name."

A later posting indicated that this is a feature, not a bug: it's in the Microsoft Knowledge Base, where the text reads, "This is by design. . . . "

[MORAL: use PASTE UNFORMATTED or PASTE PICTURE when trying to send only an excerpt from an Excel spreadsheet.]

Category 11 Breaches of confidentiality, data leakage, covert channels

2001-11-20 confidentiality Web disclosure credit card subscribers error

RISKS 21 77

Declan McCullagh of Wired News and moderator of the Politech list, reported, "If you subscribe to any of Ziff-Davis' computer magazines, you may want to double-check your credit-card bill next month. Ziff-Davis Media, which publishes such popular tech titles such as Yahoo Internet Life and PC Magazine, accidentally posted the personal information of about 12,500 magazine subscribers on its website. On 19 Nov 2001, ZD removed the data, which included hundreds of credit-card numbers, and said its engineers had taken steps to prevent additional security leaks." http://www.wired.com/news/ebiz/0,1272,48525,00.html

Breaches of confidentiality, data leakage, covert channels Category 11

2001-11-26 confidentiality search engine data leakage

NewsScan

SEARCH ENGINES DIG TOO DEEP

Search engines increasingly are unearthing private information such as passwords, credit card numbers, classified documents, and even computer vulnerabilities that can be exploited by hackers. "The overall problem is worse than it was in the early days, when you could do AltaVista searches on the word 'password' and up come hundreds of password files," says Christopher Klaus, founder and CTO of Internet Security Systems, who notes that a new tool built into Google to find a variety of file types is exacerbating the problem. "What's happening with search engines like Google adding this functionality is that there are a lot more targets to go after." Google has been revamped to sniff out a wider array of files, including Adobe PostScript, Lotus 1-2-3, MacWrite, Microsoft Excel, PowerPoint, Word, and Rich Text Format. Google disavows responsibility for the security problem, but the company is working on ways to limit the amount of sensitive information exposed. "Our specialty is discovering, crawling and indexing publicly available information," says a Google spokesman. "We define 'public' as anything placed on the public Internet and not blocked to search engines in any way. The primary burden falls to the people who are incorrectly exposing this information. But at the same time, we're certainly aware of the problem, and our development team is exploring different solutions behind the scenes." (CNET News.com 26 Nov 2001) http://news.cnet.com/news/0-1005-200-7946411.html?tag=lh

12.2 Interception

Category 12.2 Interception

2001-01-08 man-in-the-middle attack pager interception malicious teenager adolescent

criminal hacker phreak medical information

RISKS 21 19

Terry Carroll reported to RISKS as follows on a case of a teenager-in-the middle-attack:

AP reports that a Virginia teenager obtained a pager used by the Inova Fairfax Hospital, in Fairfax Virginia. According to the article, he then "gained access to the hospital's paging system" (the article is not clear on whether this was a hack, or what) and forwarded a physician's number to his pager.

When the physician was paged, the allegedly boy returned the calls and gave the nurses medical orders, including authorizing prescriptions and minor medical procedures (such as blood tests and oxygen administration). According to the Washington Post, he is believed to have issued "about a dozen orders."

. . .

- < http://news.findlaw.com/ap/o/1110/1-4-2001/20010104042024690.html>; also,
- < http://www.washingtonpost.com/wp-dyn/articles/A14467-2001Jan3.html>.

An earlier report by the Post notes that:

The court papers and hospital say that on the overnight shift of Dec. 7-8, the youth ordered 12 treatments for six patients. His orders allegedly included prescribing the blood thinner heparin and asking for blood tests and oxygen for patients.

In each case, the orders were medically "appropriate under the circumstances," said Russell Seneca, chief of surgery at the hospital.

< http://www.washingtonpost.com/wp-dyn/articles/A13455-2000Dec15.html>

<

Category 12.2 Interception

2001-02-06 e-mail interception privacy confidentiality bug vulnerability

NewsScan

E-MAIL WIRETAPS

The University of Denver-based Privacy Foundation has begun calling attention to a new method of privacy invasion that allows someone to listen in on e-mail discussions. It can be defeated by disabling the Java programming language in Microsoft Outlook, Outlook Express, or Netscape 6 mail, and it doesn't affect people who use Eudora, America Online e-mail, or Web-based e-mail programs such as Hotmail or Yahoo Mail. Microsoft says the latest version of Outlook Express is not affected and Netscape says it will soon release a software patch that will eliminate the problem. (Atlanta Journal-Constitution 6 Feb 2001)

Category 12.2 Interception

2001-03-28 potential interception hospital medical information privacy

NewsScan

DIGITAL HOSPITAL

Each bed in HealthSouth's new \$100-125 million hospital in Birmingham, Alabama, will have an Internet connection that doctors and nurses can use to access and update patient records. The hospital will open in 2003, and HealthSouth is considering building similar facilities in ten other U.S. cities. The company's chief executive says HealthSouth is "making reality out of something that many people have talked about but no one has attempted." (AP/USA Today 27 Mar 2001)

http://www.usatoday.com/life/cyber/tech/2001-03-27-hospital.htm

Category 12.2 Interception

2001-06-04 cellular phone security encryption mobile interception

NewsScan

CELL PHONE SECURITY

Rohde & Schwarz, based in Munich, Germany, is offering wireless customers in that country a cell phone that features military-grade privacy. The TopSec cell phone is being marketed to corporate executives and government officials who want to discuss sensitive issues without worrying about electronic eavesdroppers. "They're especially aimed at companies who want to be sure they're not being spied on by their competitors," says a Rohde & Schwartz spokesman, who adds that they've sold "a few hundred" TopSec models so far. He estimates the world market at 20,000 to 30,000 customers. The \$3,000 device, which is a modified Siemens S35i phone with security features added, is believed to be the first mass-marketed mobile phone that offers high-quality service with a high level of encryption. The company has no immediate plans to market the phone in the U.S., but experts believe it's only a matter of time until such phones will be available in North America and elsewhere. (AP 4 Jun 2001) http://news.excite.com/news/ap/010604/17/crypto-cell-phone

Category 12.2 Interception

2002-01-24 ISP Internet service provider credit-card fraud snooping e-mail interception

accusation trial prosecution

RISKS 21 89

In Brisbane, Australia (reports Peter Deighan in RISKS), the Australian Competition and Consumer Commission began legal proceedings against the owners of an Internet service provider called Dataline.net.au for allegedly intercepting emails, collecting credit-card numbers, and debiting customers' credit cards without authorization. http://203.6.251.7/accc.internet/digest/view media.cfm?RecordID=574

Category 12.2 Interception

hotel Internet access proxy rerouting undocumented cache snooping interception

confidentiality profiling SMTP server e-mail

RISKS 21 91

Christian Holz discovered that the "STSN Internet Access, common at hotels.... re-route packets based on the service used(!)." Specifically, when he tried to reach his own SMTP server, he found that in fact his traffic was being rerouted—without notification or permission—to STSN's SMTP server. He concluded, "The risk: Obvious, if they can re-direct based on the service used, they could possibly see a lot of passwords by providing proxy-services for common services. In addition with the hotel-guest information, this could give an interesting profile of hotel guests. I wonder what information they can get their hands on if they have this services in Capitol-Hill hotels."

13.1 Data diddling

Category 13.1 Data diddling

2001-01-09 employee background check vetting sabotage data diddling criminal hacker

RISKS 21 19

Brian Randell noted in RISKS that some 18 months after an employee was caught in Jun e 1999 attempting to hack sensitive data to sabotage a nuclear power station, strict new security measures were imposed on all such facilities. Apparently the perpetrator had two prior criminal convictions but no one bothered to check his background before hiring him.

Category 13.1 Data diddling

2001-11-26 embezzlement stock fraud accountants data diddling theft trial guilty plea bargaining sentencing fines imprisonment

US Department of Justice

82

The < www.cybercrimes.gov > Web site of the US Department of Justice announced "Former Cisco Systems, Inc. Accountants Sentenced for Unauthorized Access to Computer Systems to Illegally Issue Almost \$8 Million in Cisco Stock to Themselves." Highlights of the press release:

- * "...[F]ormer Cisco Systems, Inc., accountants Geoffrey Osowski and Wilson Tang were each sentenced...[on 26 Nov 2001] to 34 months in prison for exceeding their authorized access to the computer systems of Cisco Systems in order to illegally issue almost \$8 million in Cisco stock to themselves."
- * "...[In] plea agreements with the government, Mr. Osowski and Mr. Tang each pled guilty to one count of computer fraud in violation of Title 18, United States Code, Section 1030(a)(4), agreed to the forfeiture of assets that the government had seized from the defendants (including stock already liquidated for \$5,049,057, jewelry and an automobile), and agreed to pay restitution in the amount of the difference between \$7,868,637 and the amount that the government will recover from the sale of the seized items."
- * "In pleading guilty, Mr. Osowski and Mr. Tang admitted that between October 2000 and March 27, 2001, they participated together in a scheme to defraud Cisco Systems in order to obtain Cisco stock that they were not authorized to obtain. As part of the scheme, they exceeded their authorized access to computer systems at Cisco in order to access a computer system used by the company to manage stock option disbursals, used that access to identify control numbers to track authorized stock option disbursals, created forged forms purporting to authorize disbursals of stock, faxed the forged requests to the company responsible for controlling and issuing shares of Cisco Systems stock, and directed that stock be placed in their personal brokerage accounts. The two defendants admitted that the first time that they did this, in December 2000, they caused 97,750 shares of Cisco stock to be placed in two separate Merrill Lynch accounts, with 58,250 of the shares deposited in an account set up by Mr. Osowski and 39,500 shares deposited in an account set up by Mr. Tang. In February 2001, they caused two additional transfers of stock, in amounts of 67,500 shares and 65,300 shares, to be transferred to brokerage accounts in their names. The total value of the Cisco stock that they took on these three occasions (at the time that they transferred the stock) was approximately \$7,868,637."

13.2 Data corruption & destruction

Category 13.2 Data corruption & destruction

2001-06-10 QA quality assurance incompatibility date formats platform operating system

spreadsheet data corruption

RISKS 21 47

MS-Excel on Macintosh computers uses a different date format ("1904 system") from Excel on Windows computers ("1900 system"). As a result, opening a Windows MS-Excel spreadsheet using Mac MS-Excel automatically converts all dates (and without notification). The resulting dates are exactly four years and a day earlier than the intended dates. RISKS correspondent Tom Walker noticed the well-known bug ("feature") during a legal proceeding where the error could have caused serious damage to the interests of several thousand employees. However, he wrote, "The fact that the data was presented in the course of an adversarial process was probably crucial to the error having been detected. I am wondering why there aren't more reports out there of encounters with this problem. Is this bug flying under the radar?"

Category 13.2 Data corruption & destruction

2001-07-11 QA quality assurance nuclear materials database data loss corruption

RISKS 21 50

Several correspondents to RISKS commented on news that the nuclear-material-tracking software supplied to Russia by Los Alamos National Laboratory has serious bugs that cause data losses. The same software is in use in the USA as well. Since the nuclear laboraties in the USA are claimed no longer toi keep paper trails of their nuclear supplies, the data losses have serious implications for nuclear safety and world peace.

Category 13.2 Data corruption & destruction

2001-07-12 QA quality assurance government records accounting database data loss

corruption

RISKS 21 50

James Paul commented on a serious government systems failure in Fiji: "A programming error resulted in the deletion of all Fiji Government accounts for the year 2000 and the postponement of official audits. There is reportedly some speculation about a cover-up of "mismanagement or abuse of taxpayer funds", although the simple solution of a screw-up seems likely. The information system dates from the mid-1970s. Presumably the various 52 government ministries and departments can retransmit the relevant data. [Source: Computer error deletes all Fiji Government accounts, Agence France-Presse, 11 Jul 2001, from the *Fiji Times*, 12 Jul 2001] "

Category 13.2 Data corruption & destruction

2001-08-07 data destruction downtime availability disaster disk format bank closure delay

customer relations

RISKS 21 58

Nicolai Langfeldt wrote from Norway to report on a massive failure of the Norwegian banking system. His report in RISKS includes the following summary:

EDB Fellesdata AS runs the computer services of about half of Norway's banks. On Thursday 2 Aug 2001, they apparently installed about 280 disks in their Hitachi storage. Then, instead of initializing the new disks, they initalized _all_ their disks -- thereby wiping out the entire warehouse. EDB Fellesdata itself declines to make any statements in the case pending further contact with their customers, the banks. They are considering lawsuits, but if one of their own employees made a "user error", they may have a hard time of it.

Talk about a lot of eggs in one basket, one can only imagine how many terrabytes of database this is, considering the number of disks, and how long it takes to restore from backup, and how many transactions were waiting to be processed from _other_ banks once the restore is done. Apparently the computers were running by Sunday, card services and ATMs were available on Monday, but Internet banking and automatic-phone-banking access is limited. They have announced that updated account balances will not be available until Wednesday, the 7th day after the mishap. The concerned banks' customers could pay their bills by visiting a local branch office the whole time, but apparently the transactions had not been processed because creditors have been warned that money may be late in arriving (but presumably retro-credited once the transaction is processed?).

Category 13.2 Data corruption & destruction

2002-01-15 data destruction sabotage evidence recovery forensic analysis reconstruction e-

mail files data investigation

NewsScan

DATA-RECOVERY EXPERTS LOOKING FOR MISSING ENRON E-MAIL [15 Jan 2002]

Lotus Notes e-mail messages ordered destroyed by a auditor whom Andersen has fired are now being searched by data-recovery experts using the same techniques used to look for suspected spy transmission and for Clinton White House correspondence sent by e-mail. A representative of Ontrack Data International says, "The general practitioner doesn't know that once you hit delete and get it out of your inbox that it's not gone. That is why this is a very fertile area for key evidence in litigation." Agencies such as the NSA, CIA and FBI go one extra step to keep deleted material from being recovered; they accomplish this through the use of software that repeatedly overwrites free space on hard drives. (AP/San Jose Mercury News 16 Jan 2002)

http://www.siliconvalley.com/docs/news/svfront/085710.htm

13.4 Obsolescence

Category 13.4 Obsolescence

2001-07-28 data loss archives format medium programs programmers documentation tape

RISKS 21 56

Valuable data from the mid-1970s collected by the Viking probes to Mars were lost over the years because no one bothered to convert the data to the next generation of medium and application program. By the time University of Southern California neurobiologist Joseph Miller asked for some records in 1999, the tapes were unreadable and uninterpretable.

Category 13.4 Obsolescence

2001-08-10 backward compatibility de facto standard archives data loss

RISKS 21 59

PDF documents created with Adobe Acrobat in 1998 were not readable using Acrobat 5.0 in 2001.

14 Viruses, virus-hoaxes, Trojans (assembly level or macro: not ActiveX or Java)

Category 14 Viruses, virus-hoaxes, Trojans (assembly level or macro: not Activ worldwide virus worm infection data top ten infectors malware

Symantec Antivirus Research Center (SARC)

In January, David Banes, Editor of the the Symantec Antivirus Research Center (SARC) Newsletter, summarized the findings of the year 2000 infection rates. The top ten malware types were as follows:

- 1. Wscript.KakWorm
 - www.sarc.com/avcenter/venc/data/wscript.kakworm.html
- 2. W95.MTX
- www.sarc.com/avcenter/venc/data/w95.mtx.html
- 3. VBS.LoveLetter
 - www.sarc.com/avcenter/venc/data/vbs.loveletter.a.html
- 4. W95.Hybris.gen
 - www.sarc.com/avcenter/venc/data/w95.hybris.gen.html
- 5. VBS.Stages.A
- www.sarc.com/avcenter/venc/data/vba.stages.a.html
- 6. W32.HLLW.Qaz.A
- www.sarc.com/avcenter/venc/data/qaz.trojan.html
- 7. Happy99.Worm
- www.sarc.com/avcenter/venc/data/happy99.worm.html
- 8. W32.Navidad
- www.sarc.com/avcenter/venc/data/w32.navidad.html
- 9. VBS.Network
 - www.symantec.com/avcenter/venc/data/vbs.network.html
- 10.W32.FunLove.4009
 - www.symantec.com/avcenter/venc/data/w32.funlove.4099.html

Category 14 Viruses, virus-hoaxes, Trojans (assembly level or macro: not Activ 2002-03-10 worldwide virus worm infection data top ten infectors malware

Trend World Virus Tracking Center

The new Trend World Virus Tracking Center < http://wtc.trendmicro.com/wtc/ > shows the top ten viruses observed in the wild through "actual virus infections detected by HouseCall, our free on-line virus scanner for PCs, and by the Trend Virus Control System (TVCS), our central management solution for network administrators." Viewers can easily select geographical areas and time periods of the last 24 hours, 7 days, or 30 days as well as details of each virus or worm. For example, as of 10 March 2002, the top ten infectors worldwide in the previous 30 days were as follows (showing the number of infected computers logged in parentheses) and a brief description of some of the malware types from Trend Micro's links to its comprehensive Virus Encyclopedia:

PE_NIMDA.A-O (233,321) [This is a fast-spreading Internet worm and file infector in pure and original form. It arrives as an embedded attachment, README.EXE file, in an email that has an empty message body and, usually, an empty subject field. It does not require the email receiver to open the attachment for it to execute. It uses a known vulnerability in Internet Explorer-based email clients to execute the file attachment automatically. This is also known as Automatic Execution of Embedded MIME type. The infected email contains the executable attachment registered as content-type of audio/x-wav so that when recipients view the infected email, the default application associated with audio files is opened. This is usually the Windows Media Player. The embedded EXE file cannot be viewed in Microsoft Outlook.]

WORM_SIRCAM.A (113,409) [This Worm is a high-level program created in Delphi that propagates via email using SMTP commands. It sends copies of itself to all addresses listed in an infected user's address book and in temporary Internet cached files. It arrives with a random subject line, and an attachment by the same name. This Worm also propagates via shared network drives.]

PE NIMDA.A (74,724) [

PE_MAGISTR.B (64,199) [This variant of PE_MAGISTR.A has polymorphic capabilities. It obtains email addresses from *.WAB, *.DBX, and *.MBX files found in the infected system's disk and then sends emails with its infected files as attachments. It may also include non-viral files such as .DOC, .GIF, and .TXT files as attachments to the emails it sends out. This destructive variant trashes the Hard Drive and deletes certain files.]

PE_FUNLOVE.4099 (56,146) [This virus infects all Win32 type Portable Executable (PE) files such as .EXE, .SCR, and .OCX in both Windows 9x and Windows NT 4.0. platforms. It searches for all Shared Network Folders with write access and then infects the files within them. To infect NT system files, the virus patches the integrity checking.]

PE NIMDA.E (46,722)

PE MAGISTR.A (37,346)

WORM_BADTRANS.B (36,157) [This memory-resident Internet worm is a variant of WORM_BADTRANS.A. It propagates via MAPI32, has a Key Logger component, and arrives with randomly selected double-extension filenames. It does not require the email receiver to open the attachment for it to execute. It uses a known vulnerability in Internet Explorer-based email clients (Microsoft Outlook and Microsoft Outlook Express) to automatically execute the file attachment. This is also known as Automatic Execution of Embedded MIME type.]

JS_EXCEPTION.GEN (31,733) [This Java Script (JS) Trojan changes the infected user's Internet Explorer startup page. One of this Trojan's samples (Coolsite samples) is a mass-mailer. It exploits security vulnerabilities in the Microsoft Virtual Machine. Some variants have non-destructive payloads that change the button caption, modify the appearance of Internet Explorer, and redirect links to a certain Web site.]

WORM.KLEZ.E (28,057) [This destructive mass-mailing worm propagates copies of itself across network drives. Upon execution, it drops two executable files, WINK*.EXE and WQK.EXE, in the Windows System folder. It also creates registry entries that allow it to run at system startup.

This worm terminates processes, and occasionally deletes files associated with certain antivirus programs. On the sixth (6) day of every odd-numbered month (January, March, May, July, September, November) it overwrites files with the following extensions: TXT, HTM, HTML, WAB, DOC, XLS, CPP, C, PAS, MPEG, MPG, BAK, MP3, JPG.]

14.1 Viruses

Category 14.1 V

Viruses

2001-01-05

php Hypertext Preprocessor scripting language virus malware

Central Command

From the Central press release:

Central Command, a leading provider of PC anti-virus software and computer security services, and its partners today announced the discovery of PHP.NewWorld, the first virus using the Hypertext Preprocessor (PHP) scripting language to infect computer systems.

PHP (www.php.net) is one of the most popular scripting languages used in the development of e-commerce and heavy content websites. It gained its popularity thanks to its user-friendly programming features, and the incorporation of cross platform compatibility between Windows, Linux, and UNIX environment features included within the language.

"Although PHP.NewWorld is currently not a major threat, it marks a new step toward new virus generation," said Steven Sundermeier, Product Manager at Central Command, Inc.

....PHP.NewWorld is spread to a system when executing an infected script.... PHP.NewWorld looks for .php, .hm, .html or .htt files in the C:\Windows directory. All files found with these extensions will become infected. When a user executes a .php file, the virus body will be executed from an external file and will take full control. In the case that the string "NewWorld.PHP" is identified as already existing, the infection routine will not be launched again. Thus, a file will not get infected twice. PHP.NewWorld has no activation date. The virus is not able to spread out from the infected system.

. . . .

Category 14.1 Viruses

2001-04-09 Logo programming language concept virus

Central Command

Here is the text of Central Command's announcement about a new concept virus:

Central Command... announced the discovery of I-Worm.LogoLogic.A, the world's first virus written using the popular Logo programming language.

"This is a proof of concept virus that utilizes a new development platform to spread, the SuperLogo programming language by Logotron. This language is popular in educational institutions and is a tool used to first expose future programming students to application development," said Steve Sundermeier, Product Manager at Central Command Inc.

Technical details

I-Worm.LogoLogic.A works only with default installations of Microsoft Windows 95 or 98 and mIRC: it assumes that the folders "C:\Windows" and "C:\Program Files" and "C:\MIRC" (default) or "D:\MIRC" or "E:\MIRC" exist. The virus requires the SuperLogo interpreter to be installed.

When executed, the virus overwrites the C:\MIRC\SCRIPT.INI with a small mIRC script that helps the propagation of the virus body (logic.lgp). The script also joins the channel #gigavirii and announces the infection, displaying the following message in the channel (a verse from "Livin' a Lie" a song written by Milk Inc., a Belgian pop band):

"Livin' a lie, tell me why I run and hide. Livin' a lie, you'll never know me deep inside."

After the mIRC infection, the virus drops a file in the Windows startup folder (C:\Windows\Start Menu\Programs\Startup\startup.vbs) that will spread the virus by e-mail. The script sends the virus to the first 80 e-mail addresses in the Microsoft Outlook and Outlook Express address book, with the following content:

Subject: Hey friends! Message: Hello! Look at my new SuperLogo program! Isn't it cool? Attachment: logic.lgp

It also overwrites C:\Windows\WINSTART.BAT and displays the following message: "You think Logo worms don't exist? Think again!"

When the infection routine is finished, the virus displays the message in the SuperLogo window: Logic, the Logo worm (c) Gigabyte

"We have no infection reports of this virus and nor do we consider it to be spreading at this time. This seems to be another demonstration by virus writers on their abilities," said Marius Gheorghescu virus researcher at Central Command's Emergency Virus Response Team.

Category 14.1 Viruses

2001-05-02 virus prevalence report wild frequency study top ten

NIPC Daily Report

UK anti-virus vendor Sophos has compiled its monthly listing of the top ten virus reported for April 2001. The April virus chart from the Sophos shows that W32/Magistr-A (Magistr) was first with 27.4% percent, followed by VBS/Kakworm (Kakworm) with 14.0 percent and W32/Hybris-B (Hybris variant) with 12.6 percent, respectively. In fourth was W32/Apology-B (Apology variant) with 9.3 percent, followed by W32/FLCSS (FunLove) with 5.1 percent. The W95/CIH-10xx (CIH or Chernobyl virus was in sixth 2.8 percent, W32/Badtrans-A (Badtrans) was followed by 2.8 percent. The ninth virus was WM97/Marker-C (Marker variant) with 2.3 percent and tenth was W32/Bymer-A (Bymer) with 2.3 percent. (Source: M2 Presswire, 2 May)

Category 14.1 Viruses

2002-01-10 macro virus .NET proof-of-concept demonstration

NewsScan

NEW "PROOF-OF-CONCEPT" VIRUS [10 Jan 2002]

A Czech programmer has created a "proof-of-concept" virus called W32/Donut to alert security antivirus vendors and Microsoft managers of software vulnerabilities in executable files created for Microsoft's .NET Web services technology. A spokesman for Symantec, a major vendor of security software, says that the virus "does not have any significant chance to become widespread. However, it shows that virus writers are paying close attention to the new .NET architecture from Microsoft and are attempting to understand the framework that eventually will be available on most systems." (Reuters/USA Today 10 Jan 2002)

http://www.usatoday.com/life/cyber/tech/2002/01/10/microsoft-dot-net-virus.h tm

14.2 Worms

Category 14.2 Worms

2001-02-12 encrypted Visual Basic worm infection malware

Central Command

VBS.SST.A, aka Calamar, Kalamar.A and Anna Kournikova worm is a Visual Basic Script worm that spread rapidly worldwide starting in February 2001. Central Command described it as follows:

"The worm travels via an email message with the following text:

Subject line: Here you have, ;0) Message body: Hi: Check This!

File attachment: AnnaKournikova.jpg.vbs

The worm attempts to trick users into executing the file attached to the e-mail message by pretending to be a jpeg graphic image of the Russian tennis player Anna Kournikova.

On January 26th the worm attempts to connect to a website www.dynabyte.nl

The worm modifies the systems registry by creating an entry named HKEY CURRENT USER\software\OnTheFly

When the worm is activated it emails itself to every address in the Outlook address book."

A week later, Trend Virus reported, "Several variants of the "Anna Kournikova" virus a.k.a. VBS_KALAMAR.A have emerged in the wild. These variants are similar to the previous virus and are detected by Trend antivirus, however, they differ in their subject header and message body. Like VBS_KALAMAR.A, these variants were also created using the VBSWG virus construction kit. Trend provided protection against Anna Kournikova before it began to spread, and Trend customers who had updated their pattern file and scan engine on a regular basis did not have to worry about this fast-spreading virus."

Category 14.2 Worms

2001-03-09 Visual Basic VBS worm generator

Viruslist.com

Viruslist.com issed the following warning: "As it became known on March 9, a computer hacker going by the pseudonym of [K]alamar--who belongs to a cyber-hooligans group from Argentina and is known to be the author of the script-virus generator "Vbs Worms Generator", which was used to create the infamous "Kournikova" virus-has released a new version of his program. Kaspersky Lab immediately responded to the discovered threat and already has integrated a new universal anti-virus module."

Category 14.2 Worms

2001-08-06 worm patch vulnerability

NewsScan

"CODE RED II" WORM TARGETS NT AND 2000

Web site administrators who are running Microsoft's Windows NT or 2000 operating systems are being urged to download a software patch from the Microsoft site to protect against a new "worm" called Code Red II. Individual users have little to worry about for now: there is no direct risk to people running the Windows 95, 98, or Me operating systems or those using Macintoshes. (AP/USA Today 6 Aug 2001) http://www.usatoday.com/life/cyber/tech/2001-08-05-code-red2.htm

Category 14.2 Worms

2001-08-09 e-mail enabled worm virus Web defacement

NewsScan

FIGHTING THE "CODE RED" WORM [30 Jul 2001]

Representatives from the White, the FBI, Microsoft and others are engaging in a public information campaign to alert computer users of the dangers of the "Code Red" worm that exploits a flaw in Windows NT and 2000 operating systems and defaces Web sites with the words "hacked by Chinese." The vandals have left this message on hundreds of thousands of computers connected to the Internet, and the government-funded Computer Emergency Response Team predicts that the worm will start spreading again this week and "has the potential to disrupt business and personal use of the Internet." Microsoft has a patch for problem on its Web site. (AP/San Jose Mercury News 30 Jul 2001) http://www.siliconvalley.com/docs/news/svfront/004342.htm

NO PERSONAL DATA COMPROMISED BY CODE RED'S HIT ON HOTMAIL [9 Aug 2001]

Microsoft says that the "Code Red" worm struck some of servers running its MSN Hotmail service, which provides e-mail access to 110 million people, but that no personal information was breached. Code Red attacks only Windows NT and Windows 2000 software used on Web servers, and does not affect Windows 95, 98, or Me. (CNet/New York Times 9 Aug 2001)

http://partners.nytimes.com/cnet/CNET 0-1003-200-6826572.html

Category 14.2 Worms

2001-11-27 e-mail enabled worm keystroke capture logging audit confidentiality

NewsScan

NEW "WORM" CAN CAPTURE KEYSTROKES [27 Nov 2001]

A malicious program called Badtrans is moving around the Internet and worming itself into vulnerable computers and using a keystroke logger to surreptitiously record passwords, credit data, and other information. A virus manager at the security firm McAfee says that the worm "does no damage to files but does drop a backdoor trojan on the machine which would allow a hacker to come back and access personal information." Badtrans spreads through Microsoft's Outlook or Outlook Express e-mail programs and arrives with an attachment that can be executed simply by reading or previewing it and doesn't need to be double-clicked or opened separately. (Reuters/San Jose Mercury News 27 Nov 2001)

http://www.siliconvalley.com/docs/news/svfront/034639.htm

14.3 Virus/worms

Category 14.3

Virus/worms

2001-04-01

Windows shares virus/worm modem autodial data destruction

SANS

SANS issued an alert about a new type of worm on (unfortunately) 1 April 2001. The text reads as follows:

At 8:00 am on Saturday, April 1 (This is not an April Fool's joke!) the FBI announced it had discovered malicious code wiping out the data on hard drives and dialing 911. This is a vicious virus and needs to be stopped quickly. That can only be done through wide-scale individual action. Please forward this note to everyone who you know who might be affected.

The FBI Advisory is posted at http://www.nipc.gov/nipc/advis00- 038.htm

The 911 virus is the first "Windows shares virus." Unlike recent viruses that propagate though eMail, the 911 virus silently jumps directly from machine to machine across the Internet by scanning for, and exploiting, open Windows shares. After successfully reproducing itself in other Internet-connected machines (to assure its continued survival) it uses the machine's modem to dial 911 and erases the local machine's hard drive. The virus is operational; victims are already reporting wiped-out hard drives. The virus was launched through AOL, AT&T, MCI, and NetZero in the Houston area. The investigation points to relatively limited distribution so far, but there are no walls in the Internet.

		D (
 Action	1:	Detense.	

Verify that your system and those of all your coworkers, friends, and associates are not vulnerable by verifying that file sharing is turned off.

* On a Windows 95/98 system, system-wide file sharing is managed by selecting My Computer, Control Panel, Networks, and clicking on the File and Print Sharing button. For folder-by-folder controls, you can use Windows Explorer (Start, Programs, Windows Explorer) and highlight a primary folder such as My Documents and then right mouse click and select properties. There you will find a tab for sharing.

* On a Windows NT, check Control Panel, Server, Shares.

For an excellent way to instantly check system vulnerability, and for detailed assistance in managing Windows file sharing, see: Shields Up! A free service from Gibson Research (http://grc.com/)

	•	ъ .	
 Action	2:	Forensics	

If you find that you did have file sharing turned on, search your hard drive for hidden directories named "chode", "foreskin", or "dickhair" (we apologize for the indiscretion - but those are the real directory names). These are HIDDEN directories, so you must configure the Find command to show hidden directories. Under the Windows Explorer menu choose View/Options: "Show All Files". If you find those directories: remove them. And, if you find them, and want help from law enforcement, call the FBI National Infrastructure Protection Center (NIPC) Watch Office at 202-323- 3204/3205/3206. The FBI/NIPC has done an extraordinary job of getting data out early on this virus and deserves both kudos and cooperation. You can help the whole community by letting both the FBI and SANS (intrusion@sans.org) know if you've been hit, so we can monitor the spread of this virus.

	Moving	Forward	
--	--------	---------	--

The virus detection companies received a copy of the code for the 911 Virus early this morning, so keep your virus signature files up- to-date. We'll post new information at www.sans.org as it becomes available.

Category 14.3 Virus/worms

2001-06-11 e-mail enabled worm child pornography evidence police law enforcement

NewsScan

SOFTWARE "WORM" SEARCHES YOUR COMPUTER FOR PORNOGRAPHY

A new computer virus called VBS.Noped.a now circulating invades computer memories in a hunt for picture files with pornographic-sounding names and reports them to the police. The virus (a "worm") arrives from an unknown source as an e-mail attachment with the subject line: "FWD: Help us ALL to END ILLEGAL child porn NOW." If it finds suspected pornography, it sends a message to the police saying: "This is Antipedo2001. I have found a PC with known child pornography files on the hard drive. I have included a listing below and included a sample for your convenience." An executive of the National Center for Missing and Exploited Children has repudiated the rogue effort and says his group "does not support unlawful means even to achieve meritorious ends." (New York Times 11 Jun 2001) http://www.nytimes.com/2001/06/11/technology/11VIRU.html

Category 14.3 Virus/worms

2001-09-25 hoax e-mail enabled virus worm social engineering

NewsScan

PHONY "PEACE" MESSAGE CARRIES COMPUTER VIRUS [25 Sep 2001]

Beware of an e-mail virus circulating with the subject line "Peace Between America and Islam" and containing an attachment labeled "WTC.exe." The message reads in part "Let's Vote To Live in Peace," and continues: "AmerRiCa... Few Days WiLL Show You What We Can Do!! It's Our Turn. ZaCkER is So Sorry For You." (Los Angeles Times 25 Sep 2001)

http://www.latimes.com/technology/la-000076747sep25.story?coll=la%2Dheadline s%2Dtechnology

Category 14.3 Virus/worms

2001-11-01 e-mail enabled worm virus Trojan dropper file infector junk e-mail spam

NewsScan

NEW VIRUS: NIMDA [19 Sep 2001]

Saying it has no connection to the terrorist event of last week, U.S. Attorney General John Ashcroft reported the existence of a new computer virus called Nimda, which spreads in a variety of ways, including e-mail with "readme.exe" attachments, as well as infected Web sites that generate a stealth file called readme.eml. The virus can crash mail servers by creating massive loads of junk messages. (San Jose Mercury News 19 Sep 2001) http://www.siliconvalley.com/docs/news/svfront/worm091901.htm

On the 25th of September, Peter Håkanson reported that all public hospitals in Gothenburg Sweden were crippled by NIMDA. He wrote in RISKS 21.67, "The hospitals in "Västra Götaland" sweden (west coast, population 1M) were isolated fron Internet during 23 Sep 2001. Some of internal networks had to be partitioned to prevent nimda spreading further. Reservations and computer-based medical records were unavailable." http://www.vgregion.se

NEW VERSION OF THE NIMDA VIRUS [1 Nov 2001]

A new version of the Nimda computer virus, Nimda.E, has been detected on computer networks this week; however, the federally funded computer security organization Computer Emergency Response Team says the CERT has not seen a significant surge in the virus since it was first identified. On Tuesday, Nimda.E disrupted access to the Internet by New York Times employees, but the newspaper's computer operations are now back to normal. (New York Times 1 Nov 2001)

http://partners.nytimes.com/2001/11/01/technology/01VIRU.html

Category 14.3 Virus/worms

2002-05-04 worm e-mail enabled virus Outlook address books flooding spam

NIPC Daily Report

On 4 May, an outbreak of the "W32.Magister" computer virus [worm] has apparently struck businesses in Europe, the U.S., and elsewhere. Businesses reported receiving dozens of unsolicited e-mail. Replies and requests to be removed from any mailing lists involved only resulted in a flood of additional e-mail. Companies in the Netherlands, France, New Zealand, the U.K. and the U.S. were similarly affected, including such large multinationals as Unilever and Diageo. Many of the recipients were businesses in the food industry that subscribed to an e-mail newsletter service from Foodnavigator.com. The culprit appears to be the W32.Magistr.24876@mm virus. The virus infects Windows Portable Executable files. It then gathers e-mail addresses from Outlook and Outlook Express mail folders, Windows address books, and the sent items file in Netscape, and sends out multiple e-mail messages. According to the Symantec Anti-virus Research Center, the virus was first discovered on 13 March, and there have been at least 50 confirmed infections affecting more than ten sites since then. (Source: Newsbytes, 5 May)

15.1 Fraud

Category 15.1 Fraud

2001-03-02 securities fraud Internet Web SEC investigation prosecution

NewsScan

SEC REMINDS INVESTORS: THE NET CAN BE A DANGEROUS PLACE

The Security and Exchange Commission (SEC) finished its fifth nationwide Internet fraud sweep by charging 23 companies and individuals with using spam e-mail messages, electronic newsletters and message boards, and other Internet media to pump up stock prices and defraud investors. The SEC's enforcement officer called the new cases "a sobering reminder for investors that, on the Internet, there is no clearly defined border between reliable and unreliable information." (New York Times 2 Mar 2001)

http://partners.nytimes.com/2001/03/02/technology/02NET.html

Category 15.1 Fraud

2001-05-24 Internet wire fraud money laundering investigation arrests law enforcement

police

NewsScan

FBI ARRESTS DOZENS FOR INTERNET FRAUD

The Federal Bureau of Investigation has in the past ten days charged 88 individuals with Internet crimes, including wire and mail fraud and money laundering. A government prosecutor said: "Internet fraud -- whether it's in the form of securities and other investment schemes, online auction and merchandising schemes, credit card fraud and identity theft -- has become one of the fastest-growing and most pervasive forms of white-collar crime." (Bloomberg News/The Washington Post, 24 May 2001)

http://washingtonpost.com/wp-dyn/articles/A67744-2001May23.html)

Category 15.1 Fraud

2001-06-18 fraud Internet Web ISP misrepresentation

NewsScan

NET ACCESS SCAM [18 Jun 2001]

The Federal Trade Commission is suing Illinois company New Millennium Concepts for using its Web site, Rhinopoint.com, to scam 59,000 customers. The alleged scam involved taking \$10 to \$16 signup fees from customers promised reduced Internet access charges for agreeing to complete monthly marketing surveys. The FTC charges that the company "rarely sent the promised surveys, even more rarely reimbursed consumers for their Internet access costs, but collected initial setup fees and personal information from tens of thousands of consumers anyway." (AP/USA Today 18 Jun 2001) http://www.usatoday.com/life/cyber/tech/2001-06-18-net-access-scam.htm

Category 15.1 Fraud

2001-07-03 pyramid fraud Ponzi Internet victims charges

NewsScan

ANATOMY OF AN INTERNET SCAM [3 Jul 2001]

Federal investigators have charged 53-year-old mid-westerner Donald A. English with perpetrating an Internet-based "Ponzi" scheme that bilked tens of thousands of small investors out of \$50 million. In a Ponzi scheme, early investors are paid phony "profits" from the money taken from other investors who follow them, after hearing about the huge, fast profits. Since no money is really being earned, the pyramid eventually collapses, when the supply of new investors diminishes. Many of the investors in English's operation, which was called EE-Biz Ventures, were people who are elderly or sick. One of them wrote: "I need at the least a full refund of the \$3,000 spent if you do not intend to pay anyone back. Remember, I have cancer and am unable to work for the next six months." (New York Times 3 Jul 2001) http://partners.nytimes.com/2001/07/03/business/03PONZ.html

Category 15.1 Fraud

2001-09-14 online fraud scam bogus charities appeals

NewsScan

SCAM ARTISTS SHOULD NOT DISCOURAGE ONLINE RELIEF EFFORTS

Though the problem's not widespread, there have been some e-mail marketing campaigns soliciting funds for bogus relief efforts. To make online donations to the Red Cross, use one of the official partnership sites the Red Cross has established with Amazon, AOL, Yahoo, or other respected organizations. (Wall Street Journal 14 Sep 2001) http://interactive.wsj.com/articles/SB1000433930241803420.htm (sub reg'd)

Category 15.1 Fraud

2001-10-18 fraud Web advertising exploitation monitoring anthrax medication

NewsScan

ANTHRAX WEB ADS MONITORED FOR ILLEGAL CLAIMS

The National Association of Boards of Pharmacy is monitoring Web sites that promote anti-anthrax drugs or suggest stockpiling them. The group's executive director says, "Most of the ads we've seen, we feel are illegal. They are offering medication without a valid prescription. We believe they are just capitalizing on all of the anthrax and bioterrorism fears." However, the Association acknowledges that there are online pharmacies that are completely legitimate and can be used to fill valid prescriptions made by certified physicians." (Reuters/USA Today 18 Oct 2001) http://www.usatoday.com/life/cyber/tech/2001/10/18/anthrax-web-site-claims.htm

Category 15.1 Fraud

2002-02-25 online fraud credit card charges debit checking lawsuit

NewsScan

AOL ACCUSED OF CHARGING FOR UNWANTED GOODS [25 Feb 2002]

America Online has been named in a lawsuit for allegedly charging thousands of customers for merchandise, such as books and stereos, that they did not order. The suit, which is seeking class-action status, claims that AOL "unlawfully charged and collected money for this unordered merchandise and shipping and handling charges from credit card, debit card and checking accounts." The plaintiffs are seeking unspecified damages, the refund of unauthorized payments, and the consumers' retention of the unauthorized merchandise at AOL's expense. Meanwhile, an AOL spokesman said the "allegations are without merit and we intend to vigorously contest this lawsuit in court." (AP 25 Feb 2002) http://apnews.excite.com/article/20020226/D7HTDUH80.html

15.2 Extortion

Category 15.2 Extortion

2001-03-02 credit card theft international blackmail extortion

NewsScan

CREDIT CARD THEFT RING

The FBI says an organized ring of hackers based in Russia and the Ukraine has stolen more than a million credit card numbers from 40 sites in 20 states over the last few months, and attempted to blackmail the targeted businesses by threaten to embarrass them publicly. The intrusions have been made using a well-known vulnerability that existed in the Windows NT operating system. Free patches to prevent intrusion can be found at www.microsoft.com. (Washington Post 9 Mar 2001)

http://washingtonpost.com/wp-dyn/articles/A43993-2001Mar8.html

Category 15.2 Extortion

2001-03-09 patent intellectual property extortion lawsuits threats

NewsScan

TINY COMPANY CRITICIZED FOR 'PATENTMAIL'

A little-known company called TechSearch has found a new gimmick for making money off the Net -- it's using a 1993 patent that covers a basic process for sending files between computers to demand license payments from big-name companies, including The Gap, Walgreen, Nike, Sony, Playboy Enterprises and Sunglass Hut. Other less-willing contributors include Audible, Encyclopaedia Britannica and Spiegel, which were threatened with litigation when they refused to pay up. "We chose to settle the lawsuit rather than move forward with potentially costly litigation," says a Britannica spokeswoman. Following complaints that the patent is invalid, the U.S. Patent and Trademark Office reached an initial decision late last month to void it, but TechSearch has amassed a collection of 20-some other patents that it can use to extract payments. It's filed several lawsuits against major electronics firms based on a 1986 patent on "plug and play" technology, and has initiated litigation with several distance learning providers based on a 1989 patent that broadly covers computer-based educational techniques. TechSearch founder Anthony Brown says his methods, although aggressive, are perfectly legal, and the company's law firm says it's won \$350 million in settlements in a string of jury verdicts over the last six years. Critics have labeled the company's techniques "extortionate" and "patentmail." (Wall Street Journal 9 Mar 2001)

http://interactive.wsj.com/articles/SB984094820806670333.htm (sub req'd)

16.1 Industrial espionage

Category 16.1 Industrial espionage

2001-04-17 industrial espionage sabotage revenge credit card fraud disgruntled employee

firing

NewsScan

FIRED WORKER TO BARKSDALE: NO MORE BALOGNA

In the process of cleaning out her desk after being fired by the Barksdale Group, the high-tech investment company named after Netscape founder Jim Barksdale, a 30-year-old administrative assistant allegedly stole secrets worth \$1.5 million and used a company credit card to purchase \$100,000 worth of jewelry -- plus two TV sets, some leather chairs and sofas, a microwave, a cruise, cookware, several watches, three cameras, purses and a rug. A police sergeant commented: "She clearly had problems. Maybe it was being in that environment, working with all those very wealthy people, around all that money and, every lunch, having to pull out a bologna sandwich." (San Jose Mercury News 17 Apr 2001)

http://www.siliconvalley.com/docs/news/svfront/barks041701.htm

Category 16.1 Industrial espionage

2001-05-04 industrial espionage accusation arrest

NIPC Daily Report

Federal authorities on 4 May arrested two Chinese scientists working for Lucent Technologies and a man described as their business partner, charging them with stealing product designs from the telecommunications equipment giant and passing them to a Chinese government-owned company in Beijing. According to a criminal complaint filed by the U.S. attorney in Newark, the scientists stole computer code used in equipment that routes telephone calls and computer data over the Internet. They allegedly planned to develop an identical product in a joint venture with a major Chinese equipment manufacturer, Datang Telecom Technology Co. Newark, U.S. Magistrate Judge Stanley Chesler explained the charge against them, conspiracy to commit wire fraud, which carries a maximum sentence of five years in prison. (Source: Washington Post, 4 May)

Category 16.1 Industrial espionage

2001-05-04 industrial espionage software theft international arrests

NewsScan

LUCENT WORKERS CHARGED WITH SELLING SECRETS TO CHINESE

Federal authorities arrested two Lucent scientists and a third man yesterday, charging them with stealing software associated with Lucent's PathStar Access Server and sharing it with a firm majority-owned by the Chinese government. The software is considered a "crown jewel" of the company. Chinese nationals Hai Lin and Kai Xu were regarded as "distinguished members" of Lucent's staff up until their arrests. The motivation for the theft, according to court documents, was to build a networking powerhouse akin to the "Cisco of China." The men face a maximum five years in prison and a \$250,000 fine. (*USA Today*, 4 May 2001

http://www.usatoday.com/life/cyber/tech/2001-05-03-lucent-scientists-china.htm

Category 16.1 Industrial espionage

2001-05-29 Echelon espionage electronic intelligence ELINT SIGINT industrial espionage

international

NewsScan

EUROPEANS SAY THEY WANT PROTECTION FROM U.S. SPY NETWORK [29 May 2001]

A new European Parliament report says that, despite U.S. denials, a U.S.-led intelligence-gathering computer network called Echelon does in fact exist, and is used primarily to intercept private and commercial communications rather than military intelligence. Other countries allegedly cooperating in Echelon include Britain, Canada, Australia and New Zealand. The EU report urges countries in that alliance to make more use of encryption software to protect the security of any business and personal communications of a sensitive nature. (AP/New York Times 29 May 2001) http://www.nytimes.com/aponline/business/AP-EU-Echelon.html

Category 16.1 Industrial espionage

2001-07-05 industrial espionage employee termination breach confidentiality investigation

awsuit

NewsScan

LAWSUITS CHARGE EX-EMPLOYEES WITH DIVULGING COMPANY SECRETS [5 Jul 2001]

Data storage firm EMC has filed lawsuits against former employees it suspects of stealing company secrets and aiding its competitor, Network Appliance. "We prefer not to compete against our own technology," says an EMC spokesman, while a lawyer for Network Appliance responds that EMC's lawsuits are simply a strategy to impede the progress the company's business rivals: "The litigation started when there was a war in this industry for talent." (San Jose Mercury News 5 Jul 2001)

http://www.siliconvalley.com/docs/news/svfront/039513.htm

16.2 Industrial information systems sabotage

Category 16.2 Industrial information systems sabotage

2001-10-11 physical damage insects hardware circuit computers microprocessor mother

boards potential sabotage

NewsScan

DEBUGGING COMPUTERS

Entomologists are warning of the growing risks of insect invasion for electronic hardware, but so far few U.S. manufacturers are taking note. "...Modern (circuit) boards of comprised of fiberglass, epoxy and copper, and we're not aware that insects are particularly (attracted to them," says a spokeswoman for circuit board manufacturer RB Design. But she may be mistaken, according to Lisa Spurlock, a spokeswoman for the Entomological Society of America. "Subterranean termites attack the plastic insulation around electric cables, gnaw on electrical wiring and cause short circuits." Manufacturers in Japan are taking the threat more seriously. Matsushita Electronic Components is mass-producing circuit boards coated with a special semi-transparent insecticidal film designed to repel cockroaches, and Panasonic says it has already installed the insect-repelling boards in tens of thousands of rice cookers and refrigerators for Japanese customers. (Wired.com 11 Oct 2001)

http://www.wired.com/news/technology/0,1282,47361,00.html

Category 16.2 Industrial information systems sabotage

2001-10-31 critical infrastructure protection information warfare penetration criminal

hacker court case decision penalty punishment imprisonment jail

RISKS 21 74

According to a report on the Australian Broadcasting Corporation Web site, Vitek Boden, a computer hacker who hacked into the sewage control computer and intentionally released caused thousands of litres of raw sewage into creeks and parks on the lower Queensland Coast (and the grounds of the local Hyatt Regency), has been jailed for two years by a Maroochydore District Court jury [summarized by Peter G. Neumann in the RISKS Forum Digest].

http://www.abc.net.au/news/newslink/nat/newsnat-31oct2001-96.htm

16.3 Infrastructure protection

Category 16.3 Infrastructure protection

2001-03-23 infrastructure protection terrorism criminal hacking sabotage information

warfare

NewsScan

CONDOLEEZA RICE WARNS OF TERRORIST DISRUPTIONS TO THE NET

National Security Advisor Condoleeza Rice wants to heighten awareness by both private and government organizations of the threat that cyberterrorism poses to national stability: "Today, the cyber-economy is the economy. Corrupt those networks, and you disrupt this nation. It is a paradox of our times that the very technology that makes our economy so dynamic and our military forces so dominating also makes us more vulnerable... A clear willingness to show that you are prepared to confront the problem is what keeps it from happening in the first place." (USA Today 23 Mar 2001)

http://www.usatoday.com/life/cyber/tech/2001-03-23-rice-cyberterrorism.htm

Category 16.3 Infrastructure protection

2001-05-02 infrastructure protection information warfare e-mail Web criminal hackers

defacement

NIPC Daily Report

Hackers have knocked a Transportation Department Web site offline, leaving the department unable to post railroad decisions or use e-mail. The Surface Transportation Board's Web site was hacked on 1 May, spokesman Dennis Watson said, and federal investigators have been notified. The board is responsible for oversight of the nation's railroad industry, and sends out rulings on mergers and other railroad activities daily. The site also contains news releases, economic statistics and past decisions. It is not known whether any information on the site was altered or destroyed.responsible for the attack, or from what country it originated. Watson said technicians do not know when the site will be back online. (Source: Associated Press, 2 May)

Category 16.3 Infrastructure protection

2001-06-21 critical infrastructure protection terrorists criminal hackers

NewsScan

COMPUTER SECURITY: A FAST-MOVING TARGET

Lawrence K. Gershwin, the top science and technology advisor to the Central Intelligence Agency has told a Congressional committee that he doesn't "feel very good about our ability to anticipate" network attacks on U.S. computers, because hackers are developing tools and techniques faster than the CIA can keep up. But so far (and probably for the next 5 to 10 years) individual terrorists do not appear to represent a major treat against the U.S. phone system or financial networks. "Terrorists really like to make sure that what they do works. They do very nicely with explosions, so we think largely they're working on that." However, without being able to "feel very good about our ability to anticipate," that sense of security could disappear at any time. (AP/San Jose Mercury News 21 Jun 2001) http://www.siliconvalley.com/docs/news/svfront/082074.htm

Category 16.3 Infrastructure protection

2001-07-17 technology council regulation export coordination security

NewsScan

BUSH TEAM PONDERS TECH EXPORT COUNCIL [31 Jan 2001]

The Bush administration is deliberating whether to create a federal Chief Information Officer -- a technology "czar" -- or to create a technology export council instead. The Tech Czar position has been proposed as a means to coordinate ecommerce policy at home and promote the industry abroad, but a council would focus on tech-related security issues as they apply to both the online industry and the national defense. The council would also address the thorny problems associated with aerospace and computer exports, and encryption standardization. (eWEEK 31 Jan 2001) http://www.zdnet.com/eweek/stories/general/0,11011,2680725,00.html

COORDINATING BOARD FOR INFRASTRUCTURE PROTECTION [13 Jun 2001]

Rejecting the idea of having a single security czar, the Bush Administration is planning to create a coordinating board to manage the government's initiatives focused "critical infrastructure protection" (CIP), which guards information systems that are critical to national security. The board's chairman will report directly to the national security adviser, currently Condoleezza Rice. Paul Kurtz of the National Security Council explains: "We can't have a single government agency or single government entity handling this problem. The idea is a dispersed solution that allows coordination across agencies... We can't fight for each particular agency's needs. We can help, but we need to have each agency take responsibility for their security." (USA Today 13 Jun 2001) http://www.usatoday.com/life/cyber/tech/fcw2.htm

BUSH TO ENLARGE CYBERSECURITY GROUP [17 Jul 2001]

The Bush Administration plans to expand the office responsible for cybersecurity, replacing a single official with a group of about 21 officials from various federal agencies, including the National Security Agency, the Central Intelligence Agency, the Federal Bureau of Investigation, and the departments of State, Defense, Justice, Energy, and Treasury. The group will report to Condoleeza Rice, the National Security Advisor. The former head of the Justice Department's computer crimes division, Mark Rasch, warns sardonically: "The bad news is, nobody will do anything about critical infrastructure protection until there's a global catastrophic failure. The good news is, there will be a global catastrophic failure." (AP/USA Today 17 Jul 2001)

http://www.usatoday.com/life/cyber/tech/2001-07-17-bush-cybersecurity.htm

Category 16.3 *Infrastructure* protection

911 World Trade Center Pentagon terrorist attacks infrastructure law 2001-09-20

enforcement policy military investigation Internet Web communications

NewsScan

PHONE CARRIERS OVERWHELMED BY PANICKED CALLERS [11 Sep 2001]

Long-distance, local and wireless carriers struggled to cope with unprecedented call volumes yesterday in the wake of the U.S. attacks. Telecom companies reported between two and 10 times the number of phone calls made on an average Tuesday, and between the hours of 9 a.m. and 12 noon many customers encountered busy signals, dead air or taped recordings saying the circuits were overloaded and to try later. Cingular Wireless reported the number of attempted calls ballooned by 400% in Washington, DC and 1,000% in its New Jersey switching center. AT&T said its network handled, on average, four million calls every five minutes, while Verizon Wireless was forced to move in portable cell antennas to boost network capacity. Meanwhile, customers of VoiceStream, which is one of the few U.S. wireless companies to use the GSM mobile standard, were able to contact friends and family using text messaging, which was unaffected by call volumes and network outages. (Financial Times 11 Sep 2001) http://news.ft.com/news/industries/telecom

INTERNET PLAYS HUGE ROLE IN DISASTER COMMUNICATIONS [11 Sep 2001]

Various Internet chat rooms were created vesterday to provide information and discussion about the terrorist events that strained traditional communications facilities, and Web sites were inundated with traffic. Major news sites (CNN, FoxNews, MSNBC, YahooNews, and ABCNews) were slowed down, as were the sites of the airlines involved in the disaster, American Airlines and United Airlines. Statistics from Keynote Systems, which monitors Web performance, give some indication of how various sites were able to cope during the day: Nytimes.com, 9 a.m. 0% availability, 10-11 a.m. 43% availability; ABCNews.com, 9 a.m. 0% availability, 11 a.m. 5% availability; USAToday.com, 9 a.m. 18% availability (took 47 seconds to connect); MSNBC.com, 9 a.m. 22% availability (38 seconds to connect); CNN.com, 9-10 a.m. 0% availability. (CNet News.com 11 Sep 2001)

http://news.cnet.com/news/0-1005-200-7129241.html?tag=mn hd

FBI TARGETS E-MAIL FOR CLUES [12 Sep 2001]

The FBI has served major U.S. Internet service providers with search warrants in connection with an e-mail address believed to be connected to Tuesday's terrorist attacks. "They wanted to know what we have on our network, and our logs about this [e-mail] address, if that address has flowed through our network at any time," said an executive at Earthlink. The address does not belong to Earthlink, but the company was told to expect more warrants as the investigation continues. "They said they're going to all the ISPs," he said. Earthlink said that agents did not install the Carnivore e-mail surveillance device on its servers, relying instead on Earthlink's own computer logs. Meanwhile, AOL and Yahoo officials said their companies were cooperating fully with the FBI and an MSN spokesman would only say that the company works regularly with law enforcement officials. (AP 12 Sep 2001) http://news.excite.com/news/ap/010912/17/tech-attacks-internet-warrants

SECURITY AND PRIVACY ISSUES: THE BALANCING ACT GROWS HARDER [12 Sep 2001]

The technologists, who generally are strong privacy advocates, are struggling to decide what to do to maintain data privacy without hampering law enforcement efforts to stop terrorists. An executive of a security services company in New Jersey says: "Yesterday changed the way we live and there's a whole new dimension in the debate over privacy versus security. More people seem to be willing to compromise but no one seems to have figured out just yet what's reasonable." And a security director at an Internet service provider admits: "As much as I don't like the intrusive nature of online surveillance technology, I really want to find the guys who did this [Tuesday's terrorist attacks in New York and Washington]." But Joseph Turow, a University of Pennsylvania professor of privacy and new media insists: "The question is whether you overreact in pursuit of a handful of terrorists and in the process change the constitutional protections of millions of American citizens." (Washington Post 13 Sep 2001) http://www.washingtonpost.com/wp-dyn/articles/A21207-2001Sep12.html

PROTECTING THE NATION FROM CYBER ATTACKS [12 Sep 2001]

Although computer security observers have noticed no signs of unusual network activities since Tuesday's terrorist attacks, the FBI's National Infrastructure Protection Center held an emergency meeting yesterday to consider the situation. Computer security consultant Donn Parker says, "Terrorists attacked our financial and political centers Tuesday. The logical next step is to attack our computer infrastructure. That would shake Americans' daily lives." (USA Today 13 Sep 2001)

http://www.usatoday.com/life/cyber/tech/2001/09/13/cyber-attack-next.htm

BUSINESSES TURN ATTENTION TO DATA RETRIEVAL [12 Sep 2001]

In the wake of Tuesday's terrorist attack on Manhattan, businesses are scrambling to find programmers and system

administrators to assist in retrieving the financial and corporate data that form the lifeblood of the information economy. Bill Miller, CTO for Storage Networks, says he has confidence the ability of financial markets to recover their data, but that the attacks go beyond the scope of his clients' disaster mitigation planning. Meanwhile, recovery efforts are hampered by the lack of a facility in which to do business. "Most of our customers are not planning on showing up downtown for another two weeks," says Sanjay Kumar, CEO of Computer Associates. "The real question is, 'Where do these people go to work?'" Last night, for instance, CA bussed 40 network-design specialists from Atlanta to CA headquarters in Islandia, NY to assist in data recovery efforts. (Wall Street Journal 13 Sep 2001) http://interactive.wsj.com/archive/retrieve.cgi?id=SB1000336758447443683.djm (sub req'd)

THE IMPORTANCE OF REMOTE BACKUP OF CRITICAL DATA [12 Sep 2001]

Financial companies like Morgan Stanley, devastated by the attack on the World Trade Center buildings in which they were headquartered, were still able to resume operations because they used backup software and data replication software to transfer all data through instantaneous telecommunications to equivalent computing facilities located in New Jersey. (Reuters/Yahoo News 12 Sep 2001)

http://dailynews.yahoo.com/

FBI WARNS OF POSSIBLE CYBER-ATTACKS [14 Sep 2001]

Corporate systems administrators are beefing up security on their networks in response to an FBI Terrorist Threat Advisory that calls for IT professionals to "implement appropriate security measures -- both physical and cyber." Many security firms say the nation's corporate systems have a long way to go and some firms, such as RedSiren Technologies, are providing additional security measures to their clients for free. Among the recommendations RedSiren is making to clients is to review critical logs for suspicious activity in an effort to prevent corporate computers being used for distributed-denial-of-service attacks and other malicious acts. The FBI advisory will expire Oct. 11. (ZDNet 14 Sep 2001)

http://dailynews.yahoo.com/h/zd/20010914/tc/net admins redouble efforts to p revent cyber-attacks 1.html

EXPERTS PREDICT CYBERATTACKS [18 Sep 2001]

Although cyberattacks were not launched after last week's terrorist events in New York and Washington, a number of security expects are expecting a wave of such attacks once the U.S. commences military action against the terrorists. John Gartner, director of Gartner's Internet security research group, says, "There is no doubt that we'll see big attacks coming. It's time to plan for that now." (Interactive Week/USA Today 18 Sep 2001) http://www.usatoday.com/life/cyber/zd/zd5.htm

DISASTER GIVES BOOST TO DATA STORAGE FIRMS [18 Sep 2001]

Data storage companies such as EMC; data back-up companies such as Veritas Software and Comdisco; and IT data center managers such as IBM and EDS are expected to see a rise in business in the coming months, as businesses scramble to safeguard their data assets. In addition, companies that provide services such as Web site hosting could see a boost from customers eager to locate critical parts of their IT systems outside of their own facilities. Although many corporations have slashed their information technology budgets for the year, even before last week's attacks the focus has been shifting away from new equipment purchases and toward data protection and management. "There has been a rebalancing of IT spending by large corporations towards data storage systems," says Veritas CEO Gary Bloom. (Financial Times 18 Sep 2001)

http://news.ft.com/news/industries/infotechnology

PEOPLE WANT NEWS, NOT SEX, IN CYBERSPACE [19 Sep 2001]

Sex, a long-time Top 10 search engine term, has dropped down to No. 17 in popularity following last week's attacks. "Popular search terms last week turned almost exclusively to disaster-related information," says a spokesman for AltaVista. In addition to sex, almost all the perennial favorites like Pamela Anderson Lee, Britney Spears and Backstreet Boys were knocked off the list. Replacing them were news-related search terms, including CNN, news, World Trade Center, BBC and Pentagon. Google and Yahoo confirmed the same pattern on their search engine sites, with Yahoo saying its traffic had surged to at least 10 times normal levels since last week, and the overwhelming number of users seeking information about the attacks. (Reuters 19 Sep 2001) http://news.excite.com/news/r/010919/20/net-attack-internet-dc

FEDS TRACK TERRORISTS' PAPERLESS TRAIL [20 Sep 2001]

Federal agents are retracing the steps of the 19 hijackers involved in last week's attacks, who apparently used a pay-peruse public Internet terminal at a Kinko's store in Hollywood, Fla. to access online ticket sites. According to an FBI document obtained by Der Spiegel magazine, some of the hijackers even entered their frequent flier numbers as they purchased their electronic tickets. A spokesperson for Travelocity confirmed that at least two of them had used the service to book flights, but declined to say whether they had booked their seat assignments on their desired planes, as some in the media have speculated. A research librarian in Delray Beach, Fla., also confirmed that one of the 19 men named by the FBI had used a computer at her library in late August. (Wired.com 20 Sep 2001)

http://www.wired.com/news/politics/0,1283,46991,00.html

TECHNOLOGY REPLACEMENT COSTS ENORMOUS [20 Sep 2001]

Billions of dollars will be spent to replace technology destroyed in the terrorist attacks last week, and some computer manufacturers have ramped up production of PCs to a night-and-day basis to meet the need. Industry analyst Astok Kumar says: "Basically, Dell and Compaq will pick up most of the business and it will give the industry a much-needed shot in the arm." One individual involved with the reconstruction process said: "It's just staggering to me. We spent thousands of dollars just to get these bankers up and running over this weekend, and this is just temporary. It is not replacing their equipment." (New York Times 20 Sep 2001)

http://www.nytimes.com/2001/09/20/nyregion/20COMP.html

Category 16.3 Infrastructure protection

2001-10-15 GOVNET government restricted network critical infrastructure protection

hardened

NewsScan

BUSH ADMINISTRATION WANTS ITS OWN INTERNET [11 Oct 2001]

The Bush Administration, citing security concerns, has proposed a new Internet-like network be created to handle sensitive government information. The new network, dubbed GOVNET, is the brainchild of Richard Clarke, the newly appointed presidential adviser for Cyberspace Security. "Planning for this network has been going on for several months," says Clarke. The General Services Administration, which will play a key role in deploying the self-contained network, has posted a Request for Information on its Web site, calling on the high-tech industry to create potential blueprints for GOVNET. "There will be no interconnections or gateways to the Internet or other public or private networks," says the RFI, which also calls for immunity to cyber-attacks and full encryption using the standard recommended by the National Security Agency. (ZDNet News 11 Oct 2001) http://news.excite.com/news/zd/011011/07/should-the-government

'GOVNET' WOULD BE A MISTAKE, EXPERTS SAY [15 Oct 2001]

The Bush administration's proposed "Govnet" -- an independent government computer network that is separate from the Internet -- would be costly and would fail to create a safe haven from hack attacks and viruses, according to security experts. While the concept is theoretically feasible, it would be very difficult to execute. For instance, inside government offices, employees could easily pass viruses from the public Internet to Govnet via floppy disks, unless the floppy disk drive were locked shut. And if the Govnet fiber optic cable is run through the same conduits used by the Internet, it would be susceptible to the same sorts of physical attacks. "The thought is if we can have complete control over it, it will be bulletproof," says one security expert. "But this is farfetched unless they assume there's not going to be any kind of human intervention or place where someone is going to connect in through a PC." Experts recommend that instead of creating a new network from scratch, the government should improve its security practices and use existing security technologies. One possibility would involve virtual private network technology, which enables businesses to use the Internet securely by encrypting data communications before they are sent over the public network and decrypting them at the receiving end. (Reuters/SiliconValley.com 15 Oct 2001) http://www.siliconvalley.com/docs/news/svfront/002314.htm

Category 16.3 Infrastructure protection

2002-01-17 critical infrastructure protection terrorism

NewsScan

FBI WARNS OF TERRORIST ATTACKS ON GOVERNMENT INFOSYSTEMS [17 Jan 2002]

The FBI's infrastructure-protection team has alerted law-enforcement officers and high-tech companies of the possibility of new terrorist attacks on or through utility, municipal, or state information systems. The warning was not specific with regard to time frame or geographic area and its urgency-level was not as high as previous general alerts issued by the government to all Americans. (AP/USA Today 17 Jan 2002) http://www.usatoday.com/life/cyber/tech/2002/01/17/net-warning.htm

Category 16.3 Infrastructure protection

2002-01-31 critical infrastructure protection law enforcement terrorists targets Web Internet

esearch

NewsScan

FBI SAYS TERRORISTS HAVE USED INTERNET TO FIND NEW TARGETS

The National Infrastructure Protection Center (NIPC), which is the FBI's top cyber-security unit, says that al-Qaeda terrorists were apparently using the Internet to seek targets among American dams and water-supply systems and to acquire information about certain insecticides and pest-control products. Information obtained by the NIPC indicates that the terrorists had sought information on the supervisory control and data acquisition networks that control water supplies and wastewater facilities. (AP/USA Today 31 Jan 2002)

http://www.usatoday.com/news/attack/2002/01/31/terrorists-net.htm

16.4 Military & government perspectives on INFOWAR

Category 16.4 Military & government perspectives on INFOWAR
2001-05-02 military information warfare defacement attacks

NIPC Daily Report

The Air Force has experienced a steady increase in the number of attacks against its information systems, and experts agree that the number of attacks is only going to increase. One reason is the availability, ease of use, and sophistication of publicly available computer-attack software. To combat these threats, the Air Force Office of Special Investigations brings to bear a number of capabilities, including computer crime investigators who specialize in combating crimes against computers and information systems and counterintelligence investigations.

Category 16.4 Military & government perspectives on INFOWAR

2001-05-02 information warfare international Germany hacker attacks CERTs cooperation

NIPC Daily Report

The German government is planning an early warning system to protect the country's Internet resources against potential international hacker attacks. According to ministry spokesman, Dirk Inger, The Interior Ministry wants to build a network of the Computer Emergency Response Teams (CERTs). Cooperation between CERTs should help prevent major damage from coordinated attacks on German networks, without the necessity of publicizing every hacker attack. German security experts have warned about the potential vulnerability of the country's networks, especially after a recent series of hacker attacks accompanying increased political tension between China and the U.S. (Source: Federal Computer Week, 2 May)

Category 16.4 Military & government perspectives on INFOWAR

2001-05-06 international information warfare conflict political Web vandalism defacement

criminal hackers DoS denial of service

NIPC Daily Report

The ROK Ministry of Information and Communication warned domestic organizations to take precautionary measures against U.S. and Chinese hackers using Korean Internet sites as a stop over to attack each other's computer systems in a cyber war. The ministry warned against the possibility that U.S. and Chinese hackers will try to launch denial of service (DOS) attacks on each other's sites by way of the sites of Korean government agencies, universities, and private institutions. The ministry and the Korea Information Security Agency (KISA) has launched a special task force against possible attacks from U.S. and Chinese hackers. The Ministry and KISA advised operators of domestic Internet sites to report to the "cyber 118" anti-hacking squad if signs of unusually excessive loads of communications are found. (Source: Seoul Yonhap, 6 May)

Category 16.4 Military & government perspectives on INFOWAR

2002-02-14 information warfare critical infrastructure protection counterattack response

military action policy prediction

NewsScan

RESPONSE TO CYBERATTACK ON U.S. COULD INCLUDE MILITARY ACTION

White House technology advisor Richard Clarke told a Senate Judiciary subcommittee that a cyberattack on the United States would be answered "in any appropriate way: through covert action, through military action, any one of the tools available to the president." Clarke pointed out that a serious cyberattack is almost inevitable from the nation's enemies, because it is cheaper and easier than a physical attack. Senator Charles Schumer (D, NY) pointed out the potentially serious consequences of a successful attack over the Internet: "A well-planned and well-executed cyberattack wouldn't just mean the temporary loss of e-mail and instant messaging. Terrorists could gain access to the digital controls for the nation's utilities, power grids, air traffic control systems and nuclear power plants." (AP/USA Today 14 Feb 2002) http://www.usatoday.com/life/cyber/tech/2002/02/14/cyberterrorism.htm

16.5 Hacktivism

Category 16.5 Hacktivism

2001-05-10 information warfare hactivism vandalism international Web defacement

NewsScan

CHINESE HACKERS DECLARE A TRUCE

Boasting that its members have defaced a thousand U.S. Web sites since Chinese-American tensions mounted after the collision in April of a U.S. surveillance airplane and a Chinese jet fighter, the Honker Union of China at Chinabyte has declared the cyberwar over and said that "any attacks from this point on have no connection to the Honker Union." (Reuters/New York Times 10 May 2001)

http://www.nytimes.com/2001/05/10/technology/10HACK.html

Category 16.5 Hacktivism

2001-07-17 hactivist hacktivist Web vandalism information warfare

NewsScan

HACKER GROUP DECLARES "ARMS RACE" AGAINST WEB CENSORSHIP

A hacker group called Hactivismo has developed anti-censorship software called "Peekabooty" to circumvent attempts to deny citizens of any country access to political information, pornography, or other restricted material. The group cited censorship activities conducted by the United Arab Emirates, Saudia Arabia, Myanmar, China, and North Korea. Oxblood Ruffin, a leader of the group, said: "We believe that access to information is a basic human right guaranteed by law. It is going to be an arms race." Hactivismo will use a distributed privacy network to go around sites that use software filters to block access." (Reuters/San Jose Mercury News 17 Jul 2001)

http://www.siliconvalley.com/docs/news/svfront/047040.htm

Category 16.5 Hacktivism

2001-09-19 hacktivism retaliation Web vandalism law enforcement police

NewsScan

FBI WARNS AGAINST VIGILANTE HACKTIVISIM [19 Sep 2001]

A 60-member network of computer hackers calling themselves the Dispatchers has vandalized 200-300 Web sites in the Middle East, including the official Web site of the Presidential Palace of Afghanistan and a site of its ruling Taliban party. The FBI wants the vandalism stopped and says: Those individual who believe they are doing a service to this nation by engaging in acts of vigilantism should know that they are actually doing a disservice to this country." (USA Today 19 Sep 2001)

http://www.usatoday.com/life/cyber/tech/2001/09/19/hack-attack-launched.htm

17.1 Penetration

Category 17.1 Penetration

2001-01-26 criminal hacker indictment trial intrusion

NewsScan

HACKER INDICTED FOR NETWORK VANDALISM

Twenty-one-year-old Jerome Heckenkamp has been indicted by federal prosecutors for allegedly hacking into computers at eBay, Exodus, Juniper, eTrade, Lycos, and Cygnus and causing a total of more than \$900,000 in damage, in events that took place in 1999 while he was a student at the University of Wisconsin. He has pleaded innocent of all charges and says the break-ins were done by someone else using his computer. (AP/San Jose Mercury News 25 Jan 2001)

http://www.mercurycenter.com/svtech/news/breaking/ap/docs/786396l.htm

Category 17.1 Penetration

2001-04-05 government audit security systems failures critical operations vulnerability fraud

misuse disruption availability penetrations

RISKS 21 36

A report by the U.S. General Accounting Office on security at 24 agencies found widespread security failures. A brief summary by Peter G. Neumann in RISKS stated, "During the year 2000, 155 federal computer systems (some with sensitive information) were taken over by unauthorized users who gained full administrative privileges. The military recorded 715 serious attacks in that period."

Category 17.1 Penetration

2001-07-03 criminal hacker ISP Internet service provider international court lawsuit

prosecution trial judgement penalties fines

RISKS 21 50

Dave Stringer-Calvert summarized a case of hacking gone drastically wrong in the UAE: "A computer whizzkid has been fined £2,000 (\$2,600) for hacking into the United Arab Emirates' only Internet provider and causing the whole country's system to crash. Lee Ashurst, 22, originally from Oldham in Greater Manchester, was convicted of misusing equipment, services or facilities provided by Emirates Telecommunications Corp Etisalat. Ashurst, who works for a construction company in the Gulf, is now facing a compensation claim of more than £500,000 (\$650,000) from Etisalat after the Dubai Court of First Instance transferred his case to the civil courts. He was working as a computer engineer at a Dubai construction firm in May last year (00) when he began hacking into Etisalat's systems. According to the Gulf News newspaper, the court was told the entire United Arab Emirates internet system crashed on several occasions over a month."

http://63.108.181.201/2001/07/03/eng-wenn/eng-wenn_001056_76_4245186652988.html

Category 17.1 Penetration

2001-11-20 Web confidentiality penetration disclosure compromise criminal hacker credit

card pornography

RISKS 21 78

The Playboy.com Web site was penetrated by a criminal hacker who stole some customer information, including credit card data. According to an article in CNET News, "Playboy.com also said it reported the incident to law enforcement officials and hired a security expert to audit its computer systems and analyze the incident."

Category 17.1 Penetration

2001-12-05 court ordered penetration financial system trial judge hacker intrusion data

diddling modification account alterations

RISKS 21 82

Under court order, an expert security specialist easily penetrated a financial system run by the US Department of the Interior and was apparently never detected when he created a false account and modified an existing account. The hack was authorized by U.S. District Judge Royce C. Lamberth as part of a lawuit against the DoI for mishandling 300,000 trust accounts for American First People.

Category 17.1 Penetration

2002-02-27 penetration confidentiality cracking criminal hacker consultant Social Security

Number SSN vulnerabilities holes demonstration ethics professional standards

NewsScan

SECURITY CONSULTANT SAYS HE HACKED NYT COMPUTERS [27 Feb 2002]

Adrian Lamo, a 20-year-old part-time security consultant in San Francisco, claims to have hacked the Web site of the New York Times and browsed through the names and Social Security numbers of the newspaper's employees, customers, and editorial contributors. Lamo says he notified the newspaper of what he had done – and that the Times has patched up the security holes but has not acknowledged that he penetrated its system. (AP/San Jose Mercury News 27 Feb 2002)

http://www.siliconvalley.com/mld/siliconvalley/2752998.htm

In September, an article in the New Scientist reported, "A computer security expert has revealed how he altered news articles posted to Yahoo!'s web site without permission. The incident highlights the danger of hackers posting misleading information to respected news outlets. Freelance security consultant Adrian Lamo demonstrated that, armed only with an ordinary Internet browser, he could access the content management system used by Yahoo!'s staff use to upload daily news. He added the false quotes to stories to prove the hole was real to computer specialist site Security Focus. Yahoo! has issued a statement saying the vulnerability has been fixed and security is being reviewed. But experts say that the incident demonstrates a serious risk. "Just think how much damage you could do by changing the quarterly results of a company in a story," says J J Gray, a consultant with computer consultants @Stake." http://www.newscientist.com/news/news.jsp?id=ns99991329

17.2 Web vandalism

Category 17.2 Web vandalism

2001-05-03 Web server vulnerability exploit criminal hacker international defacement

NIPC Daily Report

Computer intruders managed to gain control of three international Microsoft home pages on 3 May, replacing the company s data with a simple message taunting the software giant. Microsoft s UK, Mexico and Saudi Arabia sites were replaced with messages from the hacker group Prime Suspectz. The defacements come two days after Microsoft revealed its flagship Web server software had a serious vulnerability, but it is not known if the intruders used that vulnerability to attack the Microsoft sites. In a related development, a computer hacker published code on 2 May that makes taking advantage of the new Microsoft flaw easy for any ill-intentioned computer programmer. (Source: MSNBC, 3 May)

Category 17.2 Web vandalism

2001-05-04 information warfare criminal hacker attacks Web sites defacement probing

scanning international vulnerabilities

NIPC Daily Report

According to the Xinhua News Agency, Chinese Internet operators and administrators have been warned to be aware of hacker attacks and reminded of the need for Internet security by an official with the Computer Network and Information Security Management Office. Nearly 14% of all hacker attacks that happened in April across the world were targeted at Chinese mainland Web sites, said the official. Among the several hundreds of Chinese Web sites attacked, 54% were commercial, 12% official and 19% education and scientific research Web sites. According to Internet experts, in April, there was an increase in reports of probing and scanning by would be intruders seeking to find security cracks in systems that could be compromised. An average of 100 sites a day have seen some form of attack. A Xinhua Web report said as many as 700 official and non-governmental Web sites from both countries were hacked from 30 April to 1 May, 600 were from the Chinese mainland and Taiwan, and the other 100 or so were from the U.S. (Source: Beijing China Daily, 4 May)

Category 17.2 Web vandalism

2001-05-05 Web defacement criminal hacker gang group

NIPC Daily Report

A hacker group calling itself Prime Suspectz defaced three Microsoft sites on 3 May, although the software company managed to get the sites back to normal within hours. That makes nine times that Microsoft Web sites have been hacked in the last 20 months. The latest Microsoft sites to be defaced-Microsoft Mexico - join previously defaced Microsoft sites in Brazil, New Zealand and Slovenia.incidents. COMMENT: Please remember that these sites are hosted by ISPs within the victim country and not maintained by Microsoft. (Source: Newsbytes, 5 May)

Theft of equipment (laptops, ATMs, computers, cables, network components)

Category 18 Theft of equipment (laptops, ATMs, computers, cables, network co

2001-11-14 laptop computer theft loss airport X-ray scanner inspection confusion label

NewsScan

PROTECTING LAPTOPS AT AIRPORT SECURITY CHECKPOINTS

Travelers going through airport security checkpoints these days need to take their computer laptops out of their cases and place them separately on the conveyor belts of the airport X-ray machines. To protect the machines from damage, airline experts suggest you take the following steps: request a plastic tub for your laptop before placing it on the conveyor belt; position the laptop in the middle of the belt and behind the carrying case, so that the case can serve as a cushion if the machine slides forward; and tape your name onto the laptop itself, so that it doesn't get confused with other laptops with the same general appearance. (Washington Post 14 Nov 2001) http://www.washingtonpost.com/wp-dyn/articles/A25015-2001Nov13.html

Category 18 Theft of equipment (laptops, ATMs, computers, cables, network co

2001-11-29 burglary theft physical security data loss confidentiality industrial espionage

financial data insider job

RISKS 21

In Auckland, New Zealand, sensitive data about the investments of 25,000 investment clients were stolen on magnetic tapes. News reports indicated that only the tapes were taken, with the thieves leaving behind laptop computers and other valuables. Richard A. O'Keefe, reporting to RISKS on this incident, noted, "Without knowing anything about the people involved, or having any expertise beyond that common to all readers of detective stories, I must say that it looks uncommonly like an insider job."

19.1 Software piracy

Category 19.1 Software piracy

2001-11-15 Windows XP counterfeit operating system decryption vulnerability copy

protection copyright intellectual property software piracy

RISKS 21 76

A few hours after its release, Windows XP was hacked and its copy protection mechanisms defeated. According to an article from a London paper, "Black market copies of the supposedly uncrackable Windows XP... are already on sale for 5 pounds."

Category 19.1 Software piracy

2001-11-16 software piracy counterfeit seizure investigation law enforcement police

intellectual property

NewsScan

FEDS MAKE RECORD COUNTERFEIT SOFTWARE SEIZURE [16 Nov 2001]

California law enforcement officials made the largest seizure of counterfeit software in U.S. history, estimated to be worth about \$100 million. The products, which originated in Taiwan, included about 31,000 high-quality copies of Microsoft's Windows Millennium Edition and 2000 Professional operating systems and tens of thousands of copies of Symantec security software. "They look so good that the purchaser would not know it was counterfeit," said Los Angeles County Sheriff Lee Baca. Some of the bogus discs even carried the "Do not make illegal copies of this disc" warning. Authorities have arrested three people on bribery conspiracy and smuggling charges, and another has been charged with state violations of counterfeiting a registered trademark. (AP 16 Nov 2001) http://news.excite.com/news/ap/011116/20/counterfeit-software

Category 19.1 Software piracy

2001-12-19 software piracy industrial espionage copyright intellectual property organized

crime international universities academia executives investigation international

cooperation law enforcement police

NewsScan

CUSTOMS SERVICE EXPANDS SOFTWARE PIRACY INVESTIGATION [19 Dec 2001]

The U.S. Customs Service, which is conducting what is described as the largest criminal investigation into software piracy ever pursued by the federal government, is expanding "exponentially" its questioning of employees and students at some of the nation's top universities. Included in the Operation Buccaneer sweep are Duke University, the Massachusetts Institute of Technology, the University of California at Los Angeles, and the Rochester Institute of Technology. Executives at several software companies have also been questioned as law enforcement officials work to shut down a multibillion-dollar international piracy ring that has produced counterfeit versions of everything from the newly launched Windows XP operating system to such recent Hollywood fare as "Harry Potter and the Sorcerer's Stone." Customs officials say some of the software appears to have been stolen by executives and other insiders at the affected companies. No arrests have been made so far, and officials are trying to persuade more suspects to cooperate in exchange for leniency. "We have people here who have never contemplated spending any time in prison who all of a sudden are coming to the realization that, wait a minute, I'm in trouble here," says Special Agent Alan Doody, who's heading up the operation. (New York Times 19 Dec 2001)

http://www.nytimes.com/2001/12/19/technology/19PIRA.html

Category 19.1 Software piracy

2002-02-28 music software piracy intellectual property theft shoplifing data storage

connectivity

NewsScan

HAVE IPOD, WILL SHOPLIFT?

It turns out that Apple's new iPod device is well-suited to electronic shoplifting, with its roomy 5GB hard drive capable of serving as portable storage for very large files, such as the latest Mac OS. A CompUSA shopper describes watching a young man equipped with an iPod walk over to a nearby display Macintosh, plug his iPod into the machine with a FireWire cable, and copy Microsoft's new Office for OS X suite, which retails for \$500. The whole process took less than a minute. "Watching him, it dawned on me that this was something that was very easy to do," said witness Kevin Webb. "In the Mac world it's pretty easy to plug in and copy things. It's a lot easier than stealing the box." And while the iPod has a built-in anti-piracy mechanism that prevents music files from being copied, there are no such protections for software. "This is the first we have heard of this form of piracy," said a Microsoft product manager. "And while this is a possibility, people should be reminded that this is considered theft." (Wired.com 28 Feb 2002)

http://www.wired.com/news/mac/0,2125,50688,00.html

Music 19.2

Category 19.2 Music

2001-02-23 music peer-to-peer networking copyright infringement bootleg intellectual

property rights infringement lawsuit judgement lawsuits

NewsScan

RECORD INDUSTRY TAKES AIM AT 'OPEN NAPSTER' CLONES

With legal victory over Napster on the horizon, the record industry has begun to take action against hundreds of Napster clones that also offer free music downloading via the Internet. Since [the 19th of February 2001], the Recording Industry Association of America has sent about 60 legal notices to the ISPs that provide Web connections for "Open Napster" servers -- computers that run Napster-like software, but aren't affiliated with Napster. One expert estimates that there are 350 such servers operating globally, although the number varies daily. Legal observers say the issues against Open Napster operators are clear-cut, but battling these guerilla operations is difficult. It's likely that smaller versions of Napster will continue to pop up on the Internet, because all it takes to run an Open Napster site is a PC and a fast Internet connection. (Wall Street Journal 23 Feb 2001)

http://interactive.wsj.com/articles/SB98289811070492178.htm (sub req'd)

Category 19.2 Music

2001-03-05 music sharing copyright intellectual property service alternative

NewsScan

PAID MUSIC SERVICES READY TO PICK UP WHERE NAPSTER LEFT OFF

A handful of file-sharing startups -- including U.K.-based Wippit, and U.S. firms CenterSpan Communications and Ipingpong -- are hoping to establish their paid music download services before Napster can follow through with plans to retool itself into a fee-based system by summer. An early version of Wippet is already in public trials, and later this month CenterSpan plans to start its own public tests of a new, secure file-sharing system based on technology it acquired from the now-defunct Scour. Meanwhile, Ipingpong plans to sweeten the pot by offering financial rewards to users based on the amount of music they ship to friends. "Napster has certainly opened up the [music] industry's minds," says Wippit's CEO, who says he approached an industry executive six months ago who "actually laughed in my face, saying, 'This can't happen.'" (Los Angeles Times 5 Mar 2001) http://www.latimes.com/business/20010305/t00001951.html

Category 19.2 Music

2001-04-10 music peer-to-peer networking copyright infringement bootleg intellectual

property rights infringement lawsuit judgement award error

NewsScan

OOPS -- MP3.COM JURY DROPS A ZERO

Jurors who ordered MP3.com to pay Tee Vee Toons \$300,000 for violating its copyrights have told the trial judge they goofed -- they meant to award something closer to \$3 million. "The total was supposed to be between \$2 and \$3 million," said U.S. District Judge Jed Rakoff. "This matter is far from obvious in how it should be adjudicated." News that the jurors had essentially dropped a zero in arriving at the announced award of \$296,873 stunned both sides. Tee Vee Toons, the largest U.S. independent music label, had sought damages of \$8.5 million, but MP3.com said at this point there was no basis for upsetting the award, noting that one of the jurors was a math teacher. Rakoff said he would issue a ruling in several weeks. (Bloomberg/Los Angeles Times 10 Apr 2001) http://www.latimes.com/business/20010410/t000030496.html

Category 19.2 Music

2001-08-21 music peer-to-peer networking copyright intellectual property rights

infringement lawsuit

NewsScan

MP3 SUED FOR "VIRAL" COPYRIGHT INFRINGEMENT [21 Aug 2001]

A new lawsuit brought by a group of independent songwriters and music publishers against the MP3.com service is demanding copyright infringement damages for "viral" uses of the material, including every bootleg track exchanged through any of the underground file-swapping services that were created after MP3 set the stage for massive piracy activities. An attorney for the plaintiffs says: "If a song has been downloaded hundreds of thousands of times on Napster, and at least a portion of that is attributable to MP3.com, the magnitude of damages that should be assessed would be many, many times what they would be liable for under direct infringement." (San Jose Mercury News 21 Aug 2001)

http://www.siliconvalley.com/docs/news/svfront/mp3082101.htm

Category 19.2 Music

2001-09-06 music piracy copyright intellectual property peer-to-peer

NewsScan

MORE PEOPLE TRADING BOOTLEGGED MUSIC THAN EVER

An estimated 15 million people downloaded illicit music online this summer, surpassing the song-swapping binge that followed the federal appeals court ruling against Napster in February. In the wake of that ruling, a new generation of file-swapping sites has arisen to fill the void. "It's like playing whack-a-mole: You kill one of these guys and another one pops up to take its place," says a Gartner Dataquest researcher. The fastest growing of these new services -- MusicCity's Morpheus and KaAaA, have logged 3 million users since Napster installed song-filtering technology in June, according to Jupiter Media Metrix. And a host of other sites -- Aimster, AudioGalaxy, iMesh and BearShare -- are expanding at a slower pace. "Not only are these services less centralized -- and more difficult to police, but whereas Napster was only an MP3 application, consumers now have been introduced to the wonderful world of porn and movie pirating," says a Jupiter analyst. The sustained popularity of these underground services is eroding CD revenues, with sales of albums and singles down 5.4% for the second quarter this year. Gartner predicts CD sales will continue to decline dramatically, with revenue off 20% by 2005. "No amount of wishful thinking on the part of the music industry will stop this." (Silicon Valley 6 Sep 2001) http://www.siliconvalley.com/docs/news/sytop/music090601.htm

Category 19.2 Music

2001-10-09 music copyright intellectual property distribution channel alternative agreement

NewsScan

MUSIC PUBLISHERS, RECORDING INDUSTRY INK LICENSING DEAL

The National Music Publishers' Association, Harry Fox Agency and the Recording Industry Association of America (RIAA) have signed a licensing agreement that will pave the way for a new generation of online music subscription services backed by the Big Five record labels. Under the terms of the agreement, all RIAA member labels and their licensees – including the new online services – will have access to every musical work authorized to be licensed by the Harry Fox Agency. Harry Fox will issue licenses for subscription services offering on-demand streaming and limited downloads, or downloads that can be played only for a designated period of time or number of times. To get the ball rolling, the RIAA will pay Harry Fox \$1 million toward royalties to be determined. Once rates are determined, royalties will be payable on a retroactive basis, but if the two sides don't settle on a rate within the next two years, the recording industry will pay \$750,000 a year until a rate is set. (Wall Street Journal 9 Oct 2001) http://interactive.wsj.com/articles/SB1002623694407861800.htm (sub req'd)

Category 19.2

Music

2001-10-30

music peer-to-peer networking copyright infringement bootleg intellectual property rights infringement lawsuit judgement

NewsScan

NAPSTER RULING [11 Feb 2001]

A California federal appeals court [ruled on February 12, 2001] on whether to shut down Napster or allow it to keep operating while its legal case continues. Napster lost the first round in its battle with the recording industry last July when a lower court ruled that the file-swapping service was guilty of "wholesale" copyright violation and ordered it to cease trading copyrighted material pending a full trial. The appeals court prevented that order from taking effect until it had a chance to review the injunction. If Napster wins its case, the ruling could unleash any number of other ventures that have been awaiting a decision on whether a "personal use" exception to copyright law extends to downloadable music. But even if it loses, the peer-to-peer file-sharing technology on which it's based is here to stay. Meanwhile, Napster has teamed up with recording giant Bertelsmann, which has offered it much-needed capital if it switches to a subscription-based service that pays artists' royalties. (AP 11 Feb 2001) http://news.excite.com/news/ap/010211/22/napster-lawsuit

NAPSTER RIVALS SEE OPPORTUNITY IN RULING [13 Feb 2001]

[The] appeals court decision [on February 12, 2001] prohibiting Napster from facilitating the sharing of copyrighted music files was welcomed by Napster rivals, who believe that record labels will now become more receptive to licensing agreements with them. Analysts say the recording industry's legal battle with Napster has stymied the online music distribution industry, and with the conclusion of the protracted court case in sight, may be more willing to negotiate deals with sites that present an alternative to Napster, which has been labeled a haven for "electronic shoplifting." Shares in RealNetworks, MP3.com, Liquid Audio and EMusic.com all rose on yesterday's news. "Now it's the time for the industry to move forward to build great businesses that respect the legitimate interests of consumers, artists and rights holders," says RealNetworks chairman and CEO Rob Glaser. (Reuters/InfoWorld 13 Feb 2001) http://www.infoworld.com/articles/hn/xml/01/02/13/010213hnnapriv.xml?p=br&s=6

NAPSTER OFFERS \$1 BILLION TO RECORD COMPANIES; "NOT ENOUGH" [21 Feb 2001]

Online music-swapping service Napster, which is still embroiled in lawsuits for infringing on copyrights, is proposing to pay record companies \$1 billion over five years to end the dispute. The five major companies would divide up \$150 million annually (according to what percentage of their works are exchanged by Napster users) and an additional \$50 million would be directed to independent music companies and artists. Music industry executives and analysts dismissed the offer as insufficient. Napster also announced details of its plan to convert its operation into a subscription-based activity. Users probably will be charged a fee of \$5.95 to \$9.95 for computer downloads of an unlimited number of music files, plus an additional fee for downloads to their own compact disks. (New York Times 21 Feb 2001) http://partners.nytimes.com/2001/02/21/technology/21NAPS.html

NAPSTER RULING MAY COME [2 March 2001]

With a federal judge about to rule (maybe today) on whether online music-swapping service Napster must shut down for ignoring copyright laws, some analysts are worried that the downfall of Napster would have a serious negative impact on the Internet itself. Ford Cavallari of the research firm Adventis says: "We believe that if you take Napster out of the mix, you basically stunt the growth of DSL and cable modems." And computer manufacturing companies have been busy selling computers configured specifically for people who want to download free music and create custom CDs. Cavallari estimates that Napster's 64 million users account for 3% of all Internet traffic. Some of those users are now convinced that "it doesn't make sense to pay" the piper anymore: they can call the tune without paying. (Washington Post 2 Mar 2001)

http://washingtonpost.com/wp-dyn/articles/A10875-2001Mar1.html

NAPSTER HOPES TO SURVIVE ORDER TO CURB COPYRIGHT ABUSE [6 March 2001]

Online music-swapping service Napster is now under a court order from U.S. District Judge Marilyn Hall Patel in San Francisco to delete from its database any song protected by copyright. It will have three business days to accomplish the task of removing a huge inventory of songs identified by the five major record companies suing it for copyright infringement. Copyright law professor Peter Jaszi of American University predicted: "What is likely to happen is that the recording companies will blanket Napster with a very, very large number of file names." To stay alive, Napster is making efforts to evolve its free service into one that charges a subscription fee and pays royalties for copyrighted material. (Washington Post 7 Mar 2001)

http://washingtonpost.com/wp-dyn/articles/A32654-2001Mar6.html

NAPSTER ACCUSED OF EVADING JUDGE'S ORDER [28 March 2001]

The Recording Industry Association of America (RIAA) is complaining that online music-swapping service Napster has

failed to remove from its database 675,000 copyrighted songs it is required by court order to shield from its users. RIAA president Hilary Rosen said: "Amazingly, every single one of the copyrighted works that was originally contained in our law suit is still readily available on Napster. Napster's filter fails to do even that which Napster claims it should dolet alone all of the things we believe Napster should do." The parties to the dispute will appear in court again in mid-April. (San Jose Mercury News 28 Mar 2001) http://www.siliconvalley.com/docs/news/svfront/nap032801.htm

MEDIATOR NAMED IN LAWSUIT AGAINST NAPSTER[10 Apr 2001]

U.S. District Court Judge Marilyn Hall Patel has picked A.J. "Nick" Nichols to serve as a mediator to evaluate the technical issues in the recording industry's lawsuit against online music-swapping service Napster. The industry says that Napster has failed to observe a court order requiring it to keep copyrighted music off its site, whereas Napster claims it is doing everything that is technically possible. Nichols has a Ph.D. in engineering from Stanford University and has previously served as mediator in a lawsuit between Sun and Microsoft. (WSJ/AP/San Jose Mercury News 10 Apr 2001) http://www.siliconvalley.com/docs/news/svfront/078061.htm

NAPSTER LICENSES RELATABLE SOFTWARE [20 Apr 2001]

Napster has harnessed a new tool in its efforts to remove copyrighted music from its service. Relatable's TRM software identifies songs by mapping their sound patterns – a process that the company says will work regardless of the file format or quality. "TRM will help ensure that the millions of music files transferred through the new Napster system will be accurately monitored, and it will enable the appropriate allocation of royalties," says Relatable CEO Pat Breslin. (AP 20 Apr 2001)

http://news.excite.com/news/ap/010420/16/napster

SONGBIRD TARGETS NAPSTER LISTINGS [10 May 2001]

New software written by a 20-year-old Internet entrepreneur enables artists and record labels to quickly identify songs available on Napster even if the song's title or artist's name is garbled. Songbird, as the software's called, improves on Napster's own efforts to identify copyrighted material because it can simultaneously tap into some 90 different Napster servers rather than checking one server at a time, says creator Travis Hill. Songbird was recently demonstrated at the International Federation of Phonographic Industries headquarters in London, and was able to ferret out 40 Janet Jackson files listed under such names as anetJ acksonJ. The software is available on www.iapu.org. (Wall Street Journal 10 May 2001) http://interactive.wsj.com/articles/SB989427592571440686.htm (sub req'd)

NAPSTER STRIKES DEAL WITH MAJOR RECORD LABELS [6 Jun 2001]

Napster has inked a deal to license music from three major record companies once it starts operating as a legal service later this summer. The agreement between Napster and MusicNet, the online music collaboration backed by AOL Time Warner, Berteslmann and EMI Group, marks Napster's latest step toward legitimacy. Under the deal, Napster users would pay one fee to access Napster's database of songs from independent record labels, and an additional fee to access MusicNet's content. The exclusive arrangement could give MusicNet a significant edge over rival service Duet, which is backed by Sony and Vivendi Universal. (Los Angeles Times 6 Jun 2001) http://www.latimes.com/business/20010606/t000047089.html

NAPSTER, THE MOVIE [6 Jun 2001]

The film production arm of Liberty Media Group, cable TV organization, is working on a movie called "Napster" to tell the story of the music-swapping software that turned the recording industry upside down. Napster, which was created in 1999 by Shawn Fanning, a Northeastern University dropout with "nappy" hair, allows a community of users to share music files over the Internet, including songs protected by copyright. Outraged, the music industry lodged numerous lawsuits against Napster, though it now appears there will be an accommodation between Napster and the industry. The big record labels are planning use Napster to offer consumers a paid subscription service. (Reuters/USA Today 6 Jun 2001)

http://www.usatoday.com/life/cyber/tech/review/2001-06-06-napster-movie-reut.htm

NAPSTER STRIKES ROYALTIES DEAL WITH EUROPEAN RECORD LABELS [27 Jun 2001]

In another step toward legitimacy, Napster announced it has signed a commercial deal with groups representing 150 European independent record labels. The non-exclusive deal with the UK's Association of Independent Music (AIM) and Europe's Independent Music Companies Association marks a minor victory for Bertelsmann, which has backed Napster's efforts to move from renegade status to a legitimate fee-based service. Meanwhile, the independent labels hailed Tuesday's deal as a victory for collective licensing. "The majors are busy creating an (online) duopoly of their own. We don't know to what extent we will be closed out of their plans. It makes sense for us to have an alternative," said AIM vice-chairman Martin Mills. The European Commission has launched an antitrust investigation into PressPlay and MusicNet, the two online music services run by the big five record labels. (Financial Times 27 Jun 2001) http://news.ft.com/news/industries/media

Napster, struggling to comply with a federal court order to stop its users from illegally swapping copyrighted music, suspended operations over the weekend because its technological solution needs more work. The company has been using filtering software that identifies a song by its unique acoustic properties, but some number of pirated songs have been slipping through the filter. Analyst P.J. McNealy says: "We knew they had technical challenges. this is the first time that they've outwardly said, 'They're huge,' and they shut it down." (San Jose Mercury New 3 Jul 2001) http://www.siliconvalley.com/docs/news/svfront/nap070301.htm

NAPSTER ORDERED TO STAY CLOSED [12 Jul 2001]

Unconvinced by Napster's claim that its new filtering technology works "with 99% accuracy" to prevent customers from illegally swapping copyrighted music, Federal District Judge Marilyn Hall Patel has ordered Napster to shut down. An attorney representing the music publishers who'd filed the suit says: "Instead of being able to distribute infringing works while they figure out some way to stop doing it, Napster just has to stop distributing until they can do it legally. Which is sort of what we've been after for a year and a half." (San Jose Mercury News 12 Jul 2001) http://www.siliconvalley.com/docs/news/svfront/nap071201.htm

NAPSTER GETS REPRIEVE [19 Jul 2001]

Napster got a breather on Wednesday when a U.S. federal appeals court temporarily suspended a lower court decision ordering it to shut down while it implemented filters to block the trading of copyrighted material. The court decision offers Napster the chance to demonstrate the effectiveness of its new fingerprinting filters, which it says are capable of blocking over 99% of copyrighted songs from its service. U.S. District Court Judge Marilyn Hall Patel had said that anything less than 100% effectiveness failed to comply with her ruling ordering Napster to remove all copyrighted material from its site. Meanwhile, the Recording Industry Association of America says it's confident that Napster will be blocked once again after the Court of Appeals reviews the case. (Financial Times 19 Jul 2001) http://news.ft.com/news/industries/infotechnology

NAPSTER TO OFFER SUBSCRIPTION SERVICES BEFORE YEAR'S END [22 Aug 2001]

Napster's new chief executive, Konrad Hilbers, is promising that, as soon as his company fully complies with a court order to remove all copyrighted material from its site, he will start offering music-subscription services, to begin by the end of this year. "I'm very much a believer in what Napster stands for, which is the sharing of music among friends and private consumers when it comes to making available things like my children's Christmas carol singing or a garage band... It is quite obvious that we are challenging some of the music industry's business. (AP/USA Today 22 Aug 2001) http://www.usatoday.com/life/cyber/tech/2001-08-22-new-napster-services.htm

NAPSTER INKS PRELIMINARY DEAL WITH MUSIC PUBLISHERS [24 Sep 2001]

Napster has reached a preliminary settlement with U.S. songwriters and music publishers in a further step toward legitimizing its online music service. Napster has agreed to pay songwriters and publishers \$26 million in damages for past infringement, plus \$10 million in advance for future royalty payments. The company, though, is still facing court action by the record labels, and talks in those lawsuits are continuing. The agreement marks the first of what is likely to be several announcements from companies hoping to launch online music services before the end of the year. Such agreements are a prerequisite for two industry-backed services — Pressplay and MusicNet — to launch their membersupported sites this fall. Napster CEO Konrad Hilbers says his revamped service will be up and running before the end of the year, also. (Financial Times 24 Sep 2001) http://news.ft.com/news/industries/media

NAPSTER RELAUNCH HIT WITH DELAYS [30 Oct 2001]

Napster says it will postpone the launch of its new secure subscription-based service until next year, citing difficulties in obtaining record label licenses. The delay is a setback for Napster, which had hoped to beat the upcoming competition by several months. Industry-backed Pressplay and MusicNet both hope to launch their services before the end of the year, although they'll face several hurdles -- most notably, antitrust investigations in the U.S. and Europe. (Financial Times 30 Oct 2001) http://news.ft.com/news/industries/media

Category 19.2 Music

2001-11-14 music copyright intellectual property distribution channel alternative agreement

NewsScan

EMI TO OFFER NEW SUBSCRIPTION SERVICE EMI

Recorded Music has cut a deal with Liquid Audio that will provide EMI a way to launch a subscription service for consumers who want to permanently download song tracks off the Internet, burning copies to CDs, and transferring music compilations to portable players. Gerry Kearby of Liquid Audio says: "People can go out, for a pre-prescribed amount of money a month and download a bunch of songs, own those songs and burn them to CD — not just rent them like the other services. For the first time, it brings the consumer much closer to the experience that they learned to love with Napster — in a legitimate way." The new service will begin by focusing on EMI's Christian music catalog, offering subscribers access to an online jukebox of thousands of Christian songs for \$14 a month; jazz, classical and other genres are expected to be added to the service at a later date. (San Jose Mercury News 14 Nov 2001) http://www.siliconvalley.com/docs/news/svfront/audio111401.htm

Category 19.2 Music

2001-12-03 music copyright intellectual property marketing prediction

NewsScan

BERTELSMANN THINKS THE DAY OF FREE MUSIC IS OVER [13 Feb 2001]

"I don't think in the long term there will be any free services left out there," says the e-commerce chief executive of Bertelsmann, the German media conglomerate that forged a deal last year with Napster and laid out plans to develop a fee-based music swapping service on the Internet. "When we closed the alliance with Napster, we never focused on the lawsuit. We focused on the new membership-based service. Whatever is happening on the legal front has no impact on our position." (Reuters/San Jose Mercury News 13 Feb 2001)

http://www.mercurycenter.com/svtech/news/breaking/internet/docs/843771l.htm

[The company certainly put its money where its mouth is, as shown in the next item:]

BERTELSMANN BUYS MYPLAY.COM [30 May 2001]

German media giant Bertelsmann is acquiring Myplay.com for \$30 million in an strategy aimed at building up its Webbased music business. Myplay operates an online music storage locker, which enables users to manage and store their song collections online. It also owns technology used to create digital subscription services. The purchase continues the trend of large media companies acquiring Internet music startups. Bertelsmann also backs Napster, the file-swapping service, and is part of MusicNet, a venture formed by RealNetworks, AOL Time Warner and EMI. (Financial Times 30 May 2001)

http://news.ft.com/news/industries/media

BMG TO TEST PROTECTIVE CDs [31 Jul 2001]

Bertelsmann's BMG Entertainment is testing a new type of compact disc that enables consumers to make a limited number of digital copies, but prevents unlimited "ripping" of songs. Listeners can e-mail songs to others, but the recipients will have to pay a fee to listen to them. The CDs use technology from SunnComm, based in Phoenix, Ariz. BMG's test is the latest sign that the era of free music is drawing to a close. (Wall Street Journal 31 Jul 2001) http://interactive.wsj.com/archive/retrieve.cgi?id=SB996530381990482524.djm

BERTELSMANN LICENSES NAPSTER TECHNOLOGY [23 Oct 2001]

Bertelsmann, which has backed Napster with funding, says it will use Napster's new secure technology for the German group's BeMusic operations as part of a licensing arrangement between the two companies. BeMusic's holdings consist of Web retailer CDNow, record club BMG Direct, and myplay Inc, a digital music locker business. The technology's underlying architecture, which does not include Napster's peer-to-peer functionality, will serve as the platform for BeMusic's offerings. (Reuters 23 Oct 2001)

http://dailynews.yahoo.com/h/nm/20011023/tc/tech bertelsmann_napster_dc 1.html

LISTEN UP: NEW ONLINE MUSIC SERVICES READY FOR LAUNCH [3 Dec 2001]

Several online music sites are ready for launch, offering musical selections for a monthly subscription fee. Rhapsody, created by the independent music firm Listen.com, will be presented as a streaming service available for \$5.95 to \$7.95 a month (visit www.listen.com if you want to see how it works). Tomorrow, MusicNet (backed by EMI, RealNetworks, AOL Time Warner, and Bertelsmann's BMG) will begin a similar service priced at about \$9.95 a month. Later this month, Pressplay (jointly owned by Vivendi Universal's Universal Music and Sony Music) will join the competition for your mind and heart and ears. (Reuters/San Jose Mercury News 3 Dec 2001) http://www.siliconvalley.com/docs/news/svfront/013946.htm

Category 19.2 Music

2001-12-12 music sharing copyright intellectual property service alternative

NewsScan

REALNETWORKS IN TALKS WITH 3 MAJOR RECORD LABELS

RealNetworks is negotiating license rights with three major record companies - Warner Music Group, BMG Entertainment and EMI Group - to use their music in its planned subscription service, tentatively called MusicNet. As part of the deal, RealNetworks is offering the companies the option of an ownership interest in MusicNet. Other possibilities include making MusicNet available to other online services, and giving Napster an opportunity to license the service. If RealNetworks can sign a deal with Warner, BMG and EMI, the resulting service would present a strong challenge to the Duet subscription music service now being developed by Sony and Universal Music Group. (Wall Street Journal 30 Mar 2001)

http://interactive.wsj.com/articles/SB985905203900372337.htm (sub req'd)

MICROSOFT LAUNCHES MUSIC SERVICE [4 Apr 2001]

Microsoft is jumping on the music bandwagon with the first public test of MSN Music, its free Web-based service designed to help listeners discover new songs and artists. Users can specify styles and characteristics of music that they'd like to listen to, and a string of songs is then streamed to their PCs. The result is comparable to a custom-tailored radio channel -- users do not have the capability to listen to a particular song on demand. The distinction is important -- by not allowing users to download songs, Microsoft is relieved of the burden of negotiating individually with record labels for copyright licenses. Microsoft's announcement comes on the heels of the launch of MusicNet, a joint venture of AOL Time Warner, EMI Group, Bertelsmann and RealNetworks. (Wall Street Journal 4 Apr 2001) http://interactive.wsj.com/articles/SB986337880412283670.htm (sub req'd)

AOL TIME WARNER UNVEILS ONLINE MUSIC SERVICE [12 Dec 2001]

AOL Time Warner has launched its long-awaited MusicNet online music subscription service, which it will offer for \$9.95 a month. AOL's move into the online music space is being closely watched by experts who see it as a natural leader in the nascent market. "AOL beginning to sell digital music subscriptions is critically important and potentially cataclysmic for a lot of retailers out there in the long run," says a Jupiter Media Metrix analyst. Meanwhile, RealNetworks just launched its service, dubbed RealOne, last week and AOL rival Microsoft's MSN service is poised to launch its competing Pressplay service in the next few weeks. MusicNet is jointly owned by AOL's Warner Music, RealNetworks, EMI and Bertelsmann. Pressplay is owned by Vivendi Universal and Sony. (Wall Street Journal 12 Dec 2001)

http://interactive.wsj.com/archive/retrieve.cgi?id=SB1008087024649633040.djm (sub req'd)

Category 19.2 Music

2001-12-19 music peer-to-peer networking copyright intellectual property rights

infringement lawsuit judgement service alternative

NewsScan

VIVENDI, SONY PLAN A DUET [23 Feb 2001]

Vivendi Universal and Sony are teaming up to launch an online "virtual jukebox" music service this summer. Duet, as it's called, will challenge the recently announced deal worked out between Napster and Bertelsmann to offer a subscription-based Napster service. "It is an alternative to Napster which will allow us to monitor exactly which titles have been listened to and downloaded," says the head of Vivendi's Universal Music France. "It is over a secure network that prevents the item from getting distributed all over the Internet and provides better sound quality." Sony and Vivendi will have equal ownership of Duet and will offer a subscription service and a pay-per-listen option. (Reuters/Los Angeles Times 23 Feb 2001)

http://www.latimes.com/business/20010223/t000016279.html

YAHOO JOINS DUET WITH VIVENDI AND SONY [6 Apr 2001]

Yahoo has inked a deal with Vivendi Universal and Sony to deliver music over the Net. The new alliance, which calls for Yahoo to provide worldwide distribution for Duet, the online music platform being developed by Universal and Sony Music, will add a much-needed channel to Vivendi's U.S. distribution network. The alliance comes only days after the three other big music companies – AOL Time Warner, Bertelsmann and EMI – launched their MusicNet initiative with RealNetworks. "We're really jazzed about this," says Jeff Mallett, Yahoo's president and COO. "It provides our 100 million registered users with access to the premier entertainment destination." (Financial Times 6 Apr 2001) http://news.ft.com/news/industries/internet&e-commerce

VIVENDI MAKES A PLAY FOR MP3.COM [21 May 2001]

Vivendi Universal, the world's second largest media group, is buying online music distributor MP3.com for \$372 million in cash and shares. The amount is considerably less than MP3's peak valuation, but values the company at 3.1 times its estimated 2001 earnings. The purchase is Vivendi's third and most substantial move this year in terms of opening up new U.S. distribution channels. In March, Vivendi and Sony announced their Duet collaboration, an online music distribution service, and last month Vivendi announced a separate music deal with Yahoo. (Financial Times 21 May 2001)

http://news.ft.com/news/industries/internet&e-commerce

VIVENDI AND AOL CHARGED WITH CD PRICE-FIXING [1 Aug 2001]

The Federal Trade Commission has accused Warner Music (a unit of AOL Time Warner) and PolyGram (now a part of Vivendi) of colluding in 1998 to fix prices on CDs, cassettes and videos of opera singers Placido Domingo, Luciano Pavarotti, and Jose Carreras, knowns as "The Three Tenors." Neither company has admitted wrong-doing, but AOL has settled the case and Warner "has made the business decision to resolve this matter amicably rather than engage in protracted adversarial proceedings." (Washington Post 1 Aug 2001) http://www.washingtonpost.com/wp-dyn/articles/A12775-2001Jul31.html

VIVENDI PUTS A LOCK ON ITS MUSIC CDs [26 Sep 2001]

Vivendi Universal's Universal Music Group, the world's biggest music company, says it is preparing to roll out "a number of releases" on CDs that contain technology preventing consumers from making digital copies. The move is the most aggressive to date among U.S. record labels to block copying onto computers and other devices. A company spokesman declined to say exactly what technology would be used, but said it "will not impede the consumer experience." Meanwhile, Sony Music Entertainment reported it has used copy protection on some promotional releases of its new Michael Jackson single that were sent to radio stations last month, but doesn't plan to use on commercial releases of the singer's new album. However, the company affirmed that its "goal is to implement copy protection on a broader basis to deter digital piracy." BMG Entertainment said it's conducting trials of copy-protection on promotional CDs in the U.S. and Warner Music is "looking closely at the technology" and doing market research on the concept. No comment was available from EMI. (Wall Street Journal 26 Sep 2001) http://interactive.wsj.com/archive/retrieve.cgi?id=SB1001427903167857240.djm (sub req'd)

PRESSPLAY SET TO LAUNCH TOMORROW [19 Dec 2001]

The long-awaited online music service backed by Sony and Vivendi Universal will launch tomorrow, offering a tiered service priced between \$9.95 and \$24.95 a month for users who want to access music through their computers. Pressplay, which will offer 14-day free trials, has differentiated itself from rival MusicNet by allowing some users to "burn" a limited number of songs based on which tier of service is selected. The \$24.95 Platinum Plan allows users to "stream" 1,000 songs, download 100 songs, and "burn" 20 songs a month. Subscribers are limited to no more than two songs from a particular artist each month. The pressplay service will be available through MSN Music, Roxio and

Yahoo. (Wall Street Journal 19 Dec 2001)

http://interactive.wsj.com/articles/SB1008716795123839160.htm (sub req'd)

Category 19.2 Music

2002-01-10 music copyright intellectual property marketing distribution subscription

NewsScan

NAPSTER GETS READY FOR REBIRTH AS SUBSCRIPTION SERVICE [10 Jan 2002]

Napster, the Internet file-swapping service that was plagued by lawsuits accusing it of violating the intellectual property rights of music producers and artists, has launched a new six-week trial in which 20,000 volunteers will swap music files legally. The company will offer 50 downloads per month for about \$5-10, and will be using improved file identification technology. A Napster spokesman says the company is "close to getting all major label content." (AP/New York Times 10 Jan 2002)

http://www.nytimes.com/aponline/technology/AP-Napster.html

Category 19.2 Music

2002-01-11 DVD DeCSS decryption copyright infringement intellectual property piracy

lawsuit trial indictment DMCA international jurisdiction

NewsScan

TEENAGER "DVD-JON" CHARGED AS CRIMINAL FOR BREAKING DVD CODE [11 Jan 2002]

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

http://www.siliconvalley.com/docs/news/svfront/034227.htm

Category 19.2 Music

2002-01-23 music piracy peer-to-peer networking downloads copyright intellectual property

alternative distribution lawsuits trademark infringement

NewsScan

PRESSPLAY DEBUTS, AIMSTER RESURFACES AS MADSTER [23 Jan 2002]

Pressplay, the online music distribution service backed by Sony and Vivendi Universal, announced its launch this week following about a month of public testing. U.S.-based subscribers will be able to receive up to 300 streamed tunes on demand, as well as up to 30 downloads each month for \$9.95. Heavy users can opt for a \$24.95 deal that provides 1,000 songs and 100 downloads. Unlike rival MusicNet, pressplay subscribers will be able to burn a limited number of songs onto their own CDs. Meanwhile, renegade music-downloading Web site Aimster has resurfaced under a new moniker -- Madster, named after company founder John Deep's daughter Madeleine. Aimster had been under siege by AOL Time Warner, which that the "Aimster" name and Internet domain infringed on its trademarked AIM instant messaging software. (Newsbytes 23 Jan 2002)

http://www.newsbytes.com/news/02/173858.html

Category 19.2 Music

2002-01-24 music peer-to-peer networking copyright infringement bootleg intellectual

property rights infringement lawsuit judgement

NewsScan

NAPSTER LAWSUIT ON HOLD WHILE PARTIES RECONSIDER SETTLEMENT [24 Jan 2002]

U.S. Federal District Judge Marilyn Patel has granted a request by Napster and four record companies to suspend for 30 days the lawsuit brought by the record industry charging Napster, the Internet music-swapping service, with illegal distribution of copyrighted material. The four record companies joining Napster in the request were AOL Time Warner, BMG, Vivendi Universal and Sony; a fifth company, EMI, declined to participate in the request. Napster is gradually transitioning itself from a free to a paid-subscription service, and Hilary Rosen of the Recording Industry Association of America says of Napster: "We understand they have limited their repertory to licensed music. Resolving the lawsuit may now be feasible." (New York Times 24 Jan 2002)

http://partners.nytimes.com/2002/01/24/technology/ebusiness/24NAPS.html

Category 19.2 Music

2002-02-28 music peer-to-peer networking copyright intellectual property rights

infringement lawsuit judgement service alternative

NewsScan

SONY LICENSES MUSIC TO SONG-SWAPPING SERVICE [28 Feb 2002]

Peer-to-peer music-swapping service CenterSpan Communications says it's clinched a deal to distribute Sony Music Entertainment songs, marking the first time a major record label has licensed its content to a file-sharing outfit. CenterSpan bought the file-swapping Web site Scour.com after it declared bankruptcy in 2000. The pact calls for CenterSpan to pay Sony about \$2 million in cash plus 283,556 shares and a warrant to buy 189,037 additional shares at \$8.11 per share. A CenterSpan spokesman said the company is also talking to other record labels and movie studios, as well as online music subscription services such as Pressplay. "The deal continues the experimental phase the music industry is going through as it tries to figure which digital distribution model is going to work," says a GartnerG2 analyst. (Reuters 28 Feb 2002)

http://story.news.yahoo.com/news?tmpl=story&cid=581&u=/nm/20020228/tc nm/media centerspan sony dc 1

19.3 Movies / TV

Category 19.3 Movies / TV

2001-04-16 music video DVD movies film copyright intellectual property new technology

volume distribution

NewsScan

DIGITAL FOUNTAIN GUSHES CONTENT

Digital Fountain has developed new technology that packages streaming video and audio in a different way for Internet transmission, making its server hardware as much as 30 times more efficient than existing hardware in broadcasting movie and music files. When coupled with multicasting software, a single machine can deliver files on demand to an almost unlimited audience. The technology uses "meta-content" packets that provide mathematical snapshots that represent random chunks of files. Unlike the conventional process, which requires that all of a file's packets be received in the correct order, Digital Fountain's technology enables a server to receive the packets in any order—missing packets don't slow the process. One Digital Fountain server can pump DVD-quality video simultaneously to 4,000 users, a load that could require up to 30 conventional servers. (Wall Street Journal 16 Apr 2001) http://interactive.wsj.com/articles/SB987369482760951166.htm (sub req'd)

Category 19.3 Movies / TV

2001-11-01 copyright intellectual property television video lawsuit

NewsScan

NETWORKS SUE PERSONAL DIGITAL RECORDER MAKER [1 Nov 2001]

Three major television networks -- NBC, ABC and CBS -- are suing SONICblue Inc., maker of ReplayTV personal digital video recorders, saying that new ReplayTV 4000 would violate their copyrights by allowing users to distribute programs over the Internet. In a joint statement, the broadcasters said the device "violates the rights of copyright owners in unprecedented ways" and "deprives the copyright owners of the means by which they are paid for their creative content and thus reduces the incentive to create programming and make it available to the public." The company, which has not yet released the ReplayTV 4000, said the device limits to 15 the number of times a user can send any particular show to another ReplayTV 4000 owner, or so-called "TV buddy." The product also supports a digital rights copy protection technology that broadcasters could use to restrict consumers from sending shows over the Internet. Analysts say the lawsuit marks the networks' preemptive strike against a technology that is expected to flourish over the next few years and that could spark the same controversial issues as Napster's music-sharing technology. (AP 1 Nov 2001)

http://news.excite.com/news/ap/011101/00/tech-networks-replaytv

Category 19.3 Movies / TV

2002-02-06 video online distribution copyright alternative

NewsScan

VIVENDI PLANS ONLINE VIDEO SERVICE

Vivendi Universal is launching MP4.com -- a Web site that features a collection of short videos, including animated flicks, feature film-related content, movie trailers and games -- in a few weeks. MP4.com piggybacks on the concept of MP3.com, a music-aggregation site that Vivendi acquired last May. The move into online video follows Sony's debut last September of Screenblast, a site that offers would-be film and animation makers the publishing tools to create video, animation and music. The target user group is 18- to 24-year-olds, an age cohort most likely to have access to broadband connections in dorms or on college campuses. "The concept of MP4 is good if Vivendi can afford the bandwidth and the streaming costs that could attract a big audience," says a digital media researcher at Raymond James Financial. In recent years, a number of similar endeavors have failed to find a viable business model, with Pop.com, AOL Time Warner's Entertaindom, Digital Entertainment Network, Pseudo Programs, CMGI's iCast, and Icebox all falling victim to the dot-com debacle. (CNet News.com 6 Feb 2002) http://news.com.com/2100-1023-831091.html

Category 19.3 Movies / TV

2002-02-20 video online distribution copyright alternative

NewsScan

MGM AND CINEMANOW PLAN VIDEO-ON-DEMAND OVER THE NET

MGM is teaming up with CinemaNow of Marina del Rey, Calif., to become the first major Hollywood studio to offer video-on-demand via the Internet. The companies will offer both downloadable and "streamed" versions of "What's the Worst That Could Happen?" and "The Man in the Iron Mask" to any consumer with a high-speed Internet connection and a Windows-based computer. "Our intention in the next two years is to find out as much as we can about how consumers want VOD delivered, what they think about it, [and] how much they want to pay," says MGM Home Entertainment marketing VP Blake Thomas. MGM had previously joined with four other Hollywood studios in the "Movielink" joint venture, but that effort and its rival, Movies.com, have become bogged down in an antitrust probe by the Justice Department. The MGM movies will be available at two streaming speeds: 300 kbps, which is described as a near-VHS-quality picture, and 700 kbps, which is between VHS and DVD quality. Prices will range from \$2.99 to \$5.99, depending on location and Internet connection. (Los Angeles Times 20 Feb 2002) http://www.latimes.com/technology/la-000012921feb20.story?coll=la%2Dheadlines%2Dtechnology

19.4 Books / e-books

Category 19.4 Books / e-books

2001-08-21 copyright intellectual property library distribution

NewsScan

LIBRARY PACT SIGNALS NEW CHAPTER IN E-BOOK LENDING

California State University system is working with NetLibrary to provide simultaneous access to electronic books for multiple borrowers -- a significant change in how subscription models generally work. Previously, a single copy of an e-book could be borrowed by only one reader at a time -- just like a print version. Under the new rules, half of the 1,500 e-books owned by Cal State will be available to multiple readers at the same time, at no extra cost. Libraries need to exert more influence in the ongoing debate over the fledgling e-book industry, says Evan Reader, of the CSU Chancellor's office. "They accept what's put on the plate. We don't want to do that." The Cal State system has 23 campuses and 370,000 students. "I suspect (NetLibrary) went along with it because of our size," says Reader. (Wired.com 21 Aug 2001)

http://www.wired.com/news/culture/0,1284,46160,00.html

Category 19.4 Books / e-books

e-book piracy facsimile scanner peer-to-peer distribution copyright intellectual

property

NewsScan

DIGITAL PIRACY SPREADS FROM MUSIC TO BOOKS

Book publishers are beginning to see the same kind of piracy tactics recently experienced by the recording industry, and Internet monitoring firm Envisional predicts that the illegal downloading of books could become as big a problem as Napster. Envisional found nearly 7,300 copyrighted titles available for free through file-sharing networks such as Gnutella, including more than 700 individual copies of J.K. Rowling's Harry Potter books. In most cases, the book has been scanned and converted into downloadable text, but in a few instances hackers had cracked the copyright protection codes to e-books and made them available. Envisional says the files it found are simply the tip of the iceberg. "It's a relatively conservative estimate of the number of illegal books out there," says an Envisional executive. (Financial Times 23 Aug 2001)

http://news.ft.com/news/industries/internet&e-commerce

19.7 Legal or business documents

Category 19.7 Legal or business documents

2001-03-23 digital certificates fraud impersonation counterfeit

NewsScan

MICROSOFT WARNS OF HACKER THREAT

Microsoft says that hackers have gained possession of two digital certificates that would allow them to distribute malicious code masquerading as official Microsoft software. Digital certificates serve as proof that software code was written by a particular company and is safe. Microsoft said the criminals tricked VeriSign into issuing two of the certificates back in January, and the software giant is warning users to be suspicious of any program that arrives with a certificate claiming Microsoft's authority. The firm is working on a downloadable patch to fix the problem, but it won't be ready for about a week. "Anything that says it was issued on the 29th and 30th of January is bogus. Do not trust it," says a Microsoft spokesman. (MSNBC 22 Mar 2001)

http://www.msnbc.com/news/548228.asp

19.8 Plagiarism

Category 19.8 Plagiarism

2001-05-08 penetration identification authentication I&A term paper plagiarism pattern

recognition

RISKS 21 39

Richard Kaszeta, a seasoned systems administrator in a college department, commented on a report about how a University of Virginia professor used a computer to catch 122 plagiarists using the professor's own home-grown program. "The program basically compares papers and looks for phrases shared between papers." However, noted Mr Kaszeta, "The risk is that some of the students are probably innocent, merely being guilty of having their own papers copied without their knowledge. Indeed, some of the students claim towards the end of the article that exactly that has happened. Unfortunately, the technology of online composition and submission of papers (as typically done at most Universities) lacks sufficient security, encryption, and authentication standards."

Category 19.8 Plagiarism

2001-06-28 plagiarism cheating dishonesty software biometric identification schools

NewsScan

SCHOOLS ADOPT HIGH-TECH ANTI-CHEATING TOOLS [11 Jun 2001]

Secondary and post-secondary schools are increasingly trying to defeat high-tech cheaters by using high-tech tools to search out plagiarism, exam manipulation, and other forms of dishonesty. Some examples: software from turnitin.com will be used at 1,800 schools to compare term papers with text on the Internet and in publications; more than 100 schools will use software that prevents students from using e-mail or the Web to cheat on computer-based tests; national testing centers will use thumbprint scanners and digital cameras to monitor students and prevent imposters from taking tests under other names. The tools seem to work: an anti-plagiarism service tested at UCLA this year detected "significant instances of plagiarism" in student papers and lab reports submitted. (USA Today 11 Jun 2001) http://www.usatoday.com/life/cyber/tech/2001-06-11-tech-tools-nab-cheaters.h tm

THEIR CHEATIN' TECHNO HEARTS: HS STUDENT PLAGIARISM [28 Jun 2001]

According to a survey of 4,500 high school students by Rutgers management professor Donald McCabe, who has studied cheating on college campuses, plagiarism from Web sites is even worse a problem at the secondary level than at the university level. More than half of the high school students surveyed admitted either downloading and reusing an entire paper from the Web or at least copying parts of a paper without citation. Of college students surveyed, only 10-12% have admitted doing such things. But plagiarists often get caught, and the Internet sometimes taketh away what the Internet hath given... as can happen when a teacher enters the five or so words from a student paper and plugs them into a search engine. Then the game is over. (New York Times 28 Jun 2001) http://partners.nytimes.com/2001/06/28/technology/28CHEA.html

1A3 Biographical notes on individual criminals

Category 1A3 Biographical notes on individual criminals

2001-01-19 criminal hacker trial plea guilty distributed denial of service DDoS

NewsScan

MAFIABOY PLEADS GUILTY

A 16-year-old Montreal network vandal has pled guilty to 56 charges related to attacks last February on a number of major Web sites around the world, including Amazon, CNN, eBay, Yahoo and Dell, in a rampage causing US\$1.7 billion in damage according to FBI estimates. The young man said "I would be very surprised if it would that high," and showed no remorse. An officer of the Canadian Mounted Police said: "He was fairly proud of what he did, how he committed the crimes and what tools he used. He bragged that the FBI. was unable to catch him, that the FBI were fools, and that he would commit these crimes again. He boasted that he would make lots of money with the case and that he would become famous." The boy has quit school and taken a job as busboy in a steakhouse; because he is a minor, the maximum penalty he faces is two years in prison and a \$650 fine. (New York Times 19 Jan 2001) http://www.nytimes.com/2001/01/19/technology/19CANA.html

Category 1A3 Biographical notes on individual criminals

2001-02-14 worm writer excuses exculpation culture psychology

NewsScan

HACKER DEFENDS HIS VANDALISM, BLAMES THE VICTIMS

Defending his vandalism as an attempt to do good, a 20-year-old Dutch student arrested for creating the so-called Anna Kournikova computer virus that jammed Internet traffic throughout the world justified his action by saying he "never wanted to harm the people" whose computers he infected. He claims he intended only to issue them a warning to tighten their Internet security, and insisted that "after all it's their own fault they got infected." (AP/New York Times 14 Feb 2001)

In September, a contributor to RISKS 21.67 reported, "The 20-year-old creator for the Kournikova virus, J. de W. from Sneek, was sentenced to 150 hours of community service by the court of Leeuwarden this Thursday. The prosecution demanded the maximum of 240 hours of community service. In February De W. released on the Internet the so-called wormvirus, which spread itself as an e-mail message. The virus was activated by clicking the e-mail which was titled Anna Kournikova (the tennis player). This lead to inconvenience of Internet users all over the world. When determining the sentence, the court took into consideration that the boy had no previous run-in with justice, that he turned himself in, and that material damages were limited. The American investigation service FBI reported an amount of [\$166,827] in damages."

http://www.volkskrant.nl/nieuws/nieuwemedia/1001567916953.html (in Dutch).

Category 1A3 Biographical notes on individual criminals

2001-10-21 criminal hacker phreak opinion surveillance terrorism privacy

NewsScan

MITNICK SAYS TERRORISTS AREN'T "SUBTLE LITTLE HACKERS"

Infamous phone-system hacker Kevin Mitnick, who served more than four years of jail-time for breaking into telephone company computer systems, is critical of new antiterrorist legislation that makes government surveillance easier. "Terrorists," says Mitnick, "have proved that they are interested in total genocide, not subtle little hacks of the U.S. infrastructure, yet the government wants a blank search warrant to spy and snoop on everyone's communications." Mitnick, forbidden from using information technology without the permission of his probation officer, now plays a CIA computer expert in the TV spy drama "Alias." (Observer 21 Oct 2001) http://www.observer.co.uk/international/story/0,6903,577846,00.html

Category 1A3 Biographical notes on individual criminals

2002-03-04 criminal hacker virus writer subculture personality teenager adolescent rebellion

reputation woman girl female stereotype e-mail enabled worm

NewsScan

GIRLS JUST WANT TO HAVE HACKER FUN [4 Mar 2002]

An unidentified hacker who claims to be a 17-year-old girl says she was motivated to write the "Sharpei" worm to dispel the notion that there aren't any female virus writers and to annoy Microsoft, rather than to have it spread to actual computer users. Going by the name "Gigabyte," she says on her Web site that she's a high-school senior who takes kick-boxing classes and likes techno and trance music. A consultant for Sophos, the U.K. based security company that reported the worm says, "I just don't know what she's accomplishing by this. She's neither hurting nor helping people." The worm was written to spread via Outlook Express e-mail, with a subject line reading, "Important: Windows Update." (Reuters/New York Times 4 Mar 2002)

http://www.nytimes.com/reuters/technology/tech-tech-feminist.html

1**B**1 Adult pornography

Category 1B1 Adult pornography

2001-01-12 pornography technology innovation

NewsScan

PORN INDUSTRY A FORCE IN DRIVING INNOVATION

The world's oldest profession has been instrumental for years in driving technological innovation. The porn industry was an early force in popularizing Polaroid cameras, VCRs, and CD-ROMs, and became the first industry to make money on the Web. Now it's turning its eye toward DVD technology and has begun making DVD movies that resemble video games, allowing viewers to watch and play along. "The technology fits our product," says one cutting edge DVD producer. Meanwhile, the interactive technology now pioneered by porn purveyors likely will find its way into mainstream Hollywood studios before too long: "It has a great children's application, says David Crawford, DVD production manager for Wicked Pictures. "You can tell a nice little fairy tale and have this be the frame of it. The idea is great, whether the content is for adults or children." (Los Angeles Times 9 Jan 2001)

http://www.latimes.com/news/columns/colone/20010108/t000002277.html

Category 1B1 Adult pornography

2001-03-07 pornography children peer-to-peer networking legislation effectiveness

NewsScan

KIDS AND PORN ON THE WEB

The constitutionality of the Child Online Protection Act of 1998 has yet to be decided by the U.S. Supreme Court, but its effectiveness may be in as much doubt as its wisdom, because Napster-like free swapping services may develop that will make the law largely irrelevant, since it makes Web site operators responsible for ensuring that their patrons are adults. But Herb Lin, a senior scientist at the National Research Council, says: "Right now, the so-called adult online industry is in it for the money. But what happens when a different community starts exchanging pornography on the Net and no money changes hands at all, just like Napster?" The technology already exists for doing just that. (San Jose Mercury News 7 Mar 2001)

http://www.siliconvalley.com/docs/news/svfront/porn030701.htm

Adult pornography Category 1B1

2001-08-07 pornography Internet Service Provider ISP commercial

NewsScan

EUROPEAN ISPs TURN TO PORN FOR PROFITS

Cash-strapped European ISPs are branding their own adult content, aiming for the tried-and-true profits found in pornography and sex-related products. "What's triggering the move towards (adult content) is the steady revenue streams it generates. Sex sells," says Yankee Group European Internet strategies director Scott Smith. Freenet.de, Germany's No. 2 ISP, is preparing a mid-August launch of Fundorado.de, a site hawking hardcore videos, photos and sex chat rooms for about \$8 a month. And on Monday, Freenet.de's biggest domestic rival T-Online announced it was teaming up with Barcelona-based Private Media Group to break into the adult content business, while last month, GMX.de -- a German free e-mail service -- said it would develop a similar venture. Meanwhile in the UK, struggling etailer Lastminute.com quietly introduced an auction specializing in sex toys last week. "The old revenue stream was click-throughs and e-commerce. Companies are being urged to develop new business models to convince investors there is value in an ISP or portal business," says Kai Kaufman, an analyst with Dresdner Kleinwort Wasserstein in London. A recent study by Netvalue indicated that 33% of German Internet users regularly access adult sites, and a 1998 Datamonitor report predicted that Internet pornography would represent a \$2.8-billion business by 2003. (Reuters 7 Aug 2001)

http://news.zdnet.co.uk/story/0,,t269-s2092680,00.html

Child pornography 1B2

Category 1B2 Child pornography

2001-01-23 child pornography computer-generated images law jurisprudence

NewsScan

SUPREME COURT TO HEAR CASE ON COMPUTER-GENERATED CHILD PORN

The U.S. Supreme Court has agreed to hear a case that challenges the 1996 federal "Child Pornography Prevention Act," which makes engaging in child pornography a crime even when the images depicting minors engaging in sexually explicit acts are generated entirely by computer, without the participation of real children. A lower court overturned the law, ruling that it "criminalizes the use of fictional images that involve no human being" and are "entirely the product of the mind." However, both Congress and the U.S. Justice Department have taken the position that the law protects real children by reining in a pornography industry that desensitizes viewers and thus puts children at risk of exploitation. (New York Times 23 Jan 2001) http://partners.nytimes.com/2001/01/23/national/23SCOT.html

COURT TO REVIEW "VIRTUAL PORNOGRAPHY" CASE [29 Oct 2001]

Tomorrow the U.S. Supreme Court will begin reviewing arguments in a case about "virtual" pornography, and will be required to answer the question whether child pornography is child pornography even when the "minors" shown engaging in sex are not real children but rather computer-generated images that only appear to be children. The Free Speech Coalition, backed by the American Civil Liberties Union, considers the case a "no-brainer," and FSC lawyer Louis Sirkin insists that "when "you don't have a child, you don't have a crime. It'd be like charging someone for murder by turning on a computer and making something that looked like murder." The government, however, maintains that the law restricting virtual child pornography is needed to protect real children from pedophiles and others seeking to harm them. Robert Flores, an attorney in favor the law, says: "If the Supreme Court does not uphold the statute, it will negatively impact on all child pornography investigations. It's just not the case that the First Amendment protects all fantasy." (San Jose Mercury News 29 Oct 2001) http://www.siliconvalley.com/docs/news/svfront/pornlw102901.htm

COURT HEARS ARGUMENTS ON "VIRTUAL" CHILD PORNOGRAPHY [31 Oct 2001]

The U.S. Supreme Court heard arguments yesterday to decide whether "virtual" child pornography could be outlawed because it "conveys the impression" that it depicts real children engaged in sex acts, even though the images of sex acts are created entirely through computer video graphics. Government lawyers took the position that virtual child pornography was as effective as actual child pornographer in putting children at danger from predators. Lawyers defending computer-generated pornographer as an exercise of Constitution-protected free speech said the Child Pornography Prevention Act would have "radical and tragic consequences," in that "visual messages of adolescent sexuality will be barred regardless of their artistic or scientific merit." Justice Scalia asked: "What great works of art would be taken away from us if we couldn't see minors copulating?" When the attorney offered the movie "Lolita" as an example, Scalia said, "With all due respect, this is not the Mona Lisa or the Venus de Milo." (New York Times 31

http://partners.nytimes.com/2001/10/31/national/31SCOT.html

Category 1B2 Child pornography

2001-03-27 child pornography international investigation arrests

NewsScan

ARRESTS FOLLOW RAID ON RUSSIAN CHILD PORN SITE

Operation Blue Orchid, a joint criminal investigation by Moscow city police and the U.S. Customs Service, has shut down a Russian child pornography Web site and brought about the arrest of nine people, with more under investigation. Four people have been arrested in the U.S. and 15 search warrants have been issued. The site sold videotapes of children participating in sexual acts. (AP/USA Today 26 Mar 2001)

http://www.usatoday.com/life/cyber/tech/2001-03-26-net-porn.htm

Category 1B2 Child pornography

2001-05-31 virtual child pornography violent video games legislation proposal

RISKS 21 45

Marcus de Geus reported on proposals to ban virtual child pornography in the Netherlands:

"The Dutch Minister of Justice, Korthals, has announced measures that will make it illegal to produce or possess child pornography created by means of electronic image manipulation. The proposed legislation appears to be aimed at preventing the production and possession of artificially rendered images that could be interpreted as representations of children involved in sexual acts. Current Dutch law states that the production or possession of pornography is a criminal offence if it involves the physical (ab)use of (real) persons under a certain age. [Based on a report in an e-mail message from Radio Nederland Wereldomroep.]"

The correspondent noted that on the same basis of reasoning (child porn is bad therefore virtual child porn should be banned), it would be possible to ban violent video games (wholesale slaughter is bad therefore virtual wholesale slaughter is bad).

[MK adds: PLEASE don't shower me with abuse for reporting this line of argument.]

Category 1B2 Child pornography

2001-07-30 child pornography mandatory reporting law enforcement police integrity

authenticity presumption innocence guilt proof evidence exculpation credibility

RISKS 21 57

Brien Webb pointed out some risks of a new law in South Carolina which requires "that private technicians tell police if they find child pornography when servicing computers." Webb writes in RISKS, "Think of the possibilities. You're servicing computers, and you get the idea to have some fun. You take a client's computer, roll the date back, access some child pornography web site(s), reset the date, and call the cops. Carrying it one step further, imagine that this as a political 'dirty trick.' It might just be the mayor or some legislative representative who gets victimized. Who would believe any protestations of innocence?"

http://www.washingtonpost.com/wp-srv/aponline/20010727/aponline203146 000.htm

Category 1B2 Child pornography

2001-08-08 child pornography investigation Web international indictment

NewsScan

CRACKDOWN ON INTERNET CHILD PORNOGRAPHY [8 Aug 2001]

More news about the world of netporn: A two-year investigation by the U.S. Postal Inspection Service and other federal agencies has resulted in the indictment of subscribers to a child porn site operated by a Texas couple charged with running the largest commercial child pornography business ever uncovered. The couple provided a credit card verification service that, for \$29.95 a month, let customers visit sites that offered graphic pictures and videos of children engaging in sex acts with adults and with each other. The sites were operated by webmasters in Russia and Indonesia. (AP/USA Today 8 Aug 2001)

http://www.usatoday.com/life/cyber/tech/2001-08-08-child-porn.htm

1B4 Stalking

Category 1B4 Stalking

2001-06-14 data consolidation Web publication privacy public records tracking tracing

stalking real estate taxes addresses location

RISKS 21 49

The Washington Post Web site consolidated records from tax records and property tax appraisals and posted the resulting detailed database for the Washington DC metropolitan area. Nick Laflamme commented in RISKS that the unprecedented level of detail, comprehensive coverage and ease of access raise concerns over privacy issues. The situation also makes it v assier than ever before for stalkers to locate victims' addresses.

Category 1B4 Stalking

2001-08-27 privacy database automobile registration license plate stalking electronic access

directory commercial telephone

RISKS 21 63

Ulf Lindqvist summarized a report frm the Swedish newspaper *Aftonbladet* of Aug 27, 2001 < http://www.aftonbladet.se/vss/nyheter/story/0,2789,84644,00.html > that described "a new type of directory service" allowing one to supply "the license plate number of a car" for immediate access to "the name, address and phone number of the person registered as owner of that car." Lindqvist pointed out that rapid access to such a service (e.g., using a mobile phone) might exacerbate the consequences of road rage.

[MK: the potential dangers of increasing temptation for stalkers is another source for concern.]

1B5 Gambling

Category 1B5 Gambling

2001-05-30 online gambling state law legislation prohibition international jurisdiction

RISKS 21 45

On May 30, 2001 the California legislature passed a bill making it illegal to play illegal games online. According to a summary in RISKS, "The bill would fine first-time transgressors \$25 per transaction (not conviction) and \$100 per transaction thereafter. Companies (anywhere) convicted of catering to Californians could be liable for \$1000 per transaction and 90 days in jail. The bill supposedly specifically allows prosecutors to go after offshore corporations." http://www0.mercurycenter.com/breaking/docs/064216.htm

Category 1B5 Gambling

2001-07-25 online gambling legislation proposal casinos betting gaming fraud

NewsScan

NEW EFFORT TO CURB ONLINE GAMBLING

After three unsuccessful attempts at reining in the \$1.6-billion Internet gambling industry, members of Congress are trying again, this time with a package bill that attempts both to ban online gambling completely and to block the ability of online casinos to collect bets through credit cards, checks or electronic fund transfers. In the past, gambling companies have evaded credit card restrictions by passing off gambling transactions as non-gambling purchases. The congressmen introducing the current legislation are Representatives Bob Goodlatte, Jim Leach, John LaFalce and Senator Jon Kyl. Goodlatte says that Internet gambling "is sucking billions of dollars out of the country. It's unregulated, untaxed, illegal and offshore, and we need legislation to address that problem." (AP/Salon 25 Jul 2001) http://www.salon.com/tech/wire/2001/07/25/gambling/index.html

Category 1B5 Gambling

2001-07-26 online gambling betting gaming marketing video games

NewsScan

ADVERTISERS TURN TO ONLINE GAMING TO BOOST BRANDING

Traditional corporations, including General Motors, Honda and PepsiCo, are turning to online videogames to get their message out, targeting the 145 million consumers who are active computer and videogame players, according to a study by the Interactive Digital Software Association. "Forget your image of a gamer being a teenage punk with a skateboard and loud music," says the president of an advertising agency that specializes in targeting the 18-34 age group. IDSA's survey found that 42% of frequent game players are older than 35, while 30% are in the 18-34 range. The online games cost advertisers between \$150,000 and \$500,000 to create, depending on the graphics, says one game developer, who predicts the next wave will include other media, including cell phones and pagers. One scenario under discussion involves a player receiving pages during the day instructing him or her to log on to the game because the player's character is in danger. (Wall Street Journal 26 Jul 2001)

http://interactive.wsj.com/articles/SB996102206258182085.htm (sub req'd)

Category 1B5 Gambling

2001-08-02 privacy personal information geographical location surveillance online gambling

gaming taxation law enforcement police investigation

NewsScan

GEO-LOCATION SOFTWARE FINDS PEOPLE ON THE NET

"Geo-location software" is the next wave in collecting information from online users, tracing the connection route to locate the city where a user is logging on. The software is raising new questions among privacy advocates, who worry that geo-location capabilities infringe on both a user's anonymity and his or her access to information. "Right now oppressive governments around the world are not able to keep information away from their citizens as they had (before the Internet)," says David Sobel, general counsel for the Electronic Privacy Information Center. One industry likely to benefit from the technology is online gambling, which is expected to generate \$6 billion worldwide by 2003. Legitimate gambling sites could restrict access to only residents of states and countries where such activities are legal. In June, the state of Nevada moved forward on legislation to consider making online gambling legal within state borders. (Financial Times 2 Aug 2001)

http://news.ft.com/news/industries/infotechnology

Category 1B5 Gambling

2001-09-10 online gambling penetration hacking data diddling code modification algorithms

corrupted illegal winnings

RISKS 21

Peter G. Neumann summarized an article about a hacked online-gambling site:

"The article is on risks in on-line gambling, and particularly CryptoLogic, Inc., a Canadian on-line casino games developer that has been hacked. One of their sites had been "fixed" so that craps and video slot players could not lose, with winnings totalling \$1.9 million. Every dice throw turned up doubles, and every slot spin generated a perfect match. Whether it was an insider attack or a penetration is not clear from the article. (We noted the likelihood of hacking of Internet gambling sites in RISKS-19.27, 1 Aug 1997, not to mention my 1995 April Fool's piece in RISKS-17.02.) Interesting question: which laws against hacking will apply to subversions of illegal Internet gambling parlors? Who gets to prosecute remote attacks on off-shore operations?

http://news.excite.com/news/r/010910/11/net-tech-gambling-hacking-dc

Category 1B5 Gambling

2001-09-10 online gambling international

NewsScan

BRITISH TV TO OFFER REAL-TIME GAMBLING

Two British digital television platforms are planning to launch real-time interactive gambling services in an effort to boost revenues and attract the loyalty of couch-potato bettors. Both Telewest and ITV Digital will use SportXction software developed by U.S. software maker Interactive Systems Worldwide. SportXction allows bets to be placed at key points in television programming — in particular during sports events where, for example, a player is about to take a penalty shot in soccer or serve in tennis. The UK's interactive TV industry is betting on gambling to help it win back some of the billions of pounds spent on subsidizing and selling digital TV to British consumers. "Many broadcasters now realize that their future success will be based upon incremental revenues generated from new, compelling and distinctive services," says Global Interactive Gambling CEO Cees Zwaard, whose company is partnering with Telewest on its interactive gambling venture. (Reuters 10 Sep 2001)

http://news.excite.com/news/r/010910/12/net-media-britain-tvbetting-dc

Category 1B5 Gambling

2002-01-14 online gambling legalization interactive TV handheld

NewsScan

COMPANIES GAMBLE ON ONLINE WAGERING

A growing number of companies are developing online gambling technologies, betting that cyberwagering will be legalized in the U.S. in the not-too-distant future. Interactive Systems Worldwide has designed interactive-television gambling software for German media firm Kirch Group that will enable European sports fans to bet from their own living rooms, and Interactive chairman Barry Mindes expects it will be available for this year's soccer World Cup. Interactive Systems is now working on a handheld gambling device and is hoping to introduce an online "contest" concept in the U.S. based on the gambling software. Under current U.S. law, online gambling is prohibited but TV viewers can enter contests to win prizes such as a car. Mindes envisions users answering a list of questions posed by an advertiser to rack up credits that could then be used for playing the game. (Wall Street Journal 14 Jan 2002) http://interactive.wsj.com/articles/SB1010960972280769280.htm (sub req'd)

Category 1B5 Gambling

2002-01-31 online gambling gaming mobile telephone Internet

NewsScan

MOBILE GAMING SET TO BOOM

Almost half of all European mobile phone customers will be using their handsets to play games by 2005, according to a recent Forrester Research report, as users take advantage of snazzy new handsets and upgraded wireless networks. "The increase in wireless bandwidth and better phones will attract more firms to offer mobile games. Just as an increase in Internet-ready PCs pushed more companies to offer Web services, a bigger audience for mobile games will make firms like Eidos Interactive and Electronic Arts follow in the footsteps of Riot Entertainment and Picofun," says the report. As more games become available, the number of mobile game users is anticipated to rise from 5 million currently to 130 million by 2005. And while most of these players will be young, older gamers are expected to join the fun next year as classic 1970s- and '80s-era games, such as Pong, Frogger and Space Invaders, are revamped for the mobile platform. However, in order to capitalize on this new source of revenue, "operators must curb their greed," warns the report, saying that to ensure developers to continue to produce the games, operators must share their revenues with them. Forrester predicts that over the next five years, ad agencies will begin to acquire their own game development groups to create games for advertising and branding purposes. Television and film studios will also jump into the mix, with mobile games based on shows such as "Who Wants to Be a Millionaire?" (ElectricNews 31 Jan 2002) http://www.electricnews.net/news.html?code=5909714

1B7 Hate groups, speech

Category 1B7 Hate groups, speech

2001-01-03 hate speech auction censorship filtering

NewsScan

YAHOO TO BE PROACTIVE IN POLICING COMMERCIAL POSTINGS

Yahoo has adopted a new "proactive" monitoring program that will use software to accomplish an initial review of all commercial postings on its auctions, classified sections, and shopping areas. If the software detects any postings that appears to violate the site's policies hateful or violent material, it will give the senders the opportunity to revise their submissions or appeal the rejection to a human reviewer. Yahoo has been under pressure from human rights groups to take a more proactive stance against auctions of Nazi memorabilia and similar kinds of activities, and believes its new monitoring process will show that it has "thought about these issues in good faith." The monitoring will apply only to the commercial side of Yahoo and not to its discussion groups or home pages: "There we want to promote inclusiveness. We don't want Yahoo deciding who can or cannot speak in public debates." (New York Times 3 Jan 2001)

http://partners.nytimes.com/2001/01/03/technology/03YAHO.htm

1B9 Non-virus hoaxes, urban myths

Category 1B9 Non-virus hoaxes, urban myths

2001-08-02 hoax chain e-mail credit information privacy false news misinformation

NewsScan

FALSE CREDIT SCARE FROM MESSAGE MAKING THE ROUNDS

The Federal Trade Commission has posted a consumer alert warning against the "half-truths and misinformation" in a widely circulated anonymous e-mail message that's falsely warning consumers that major credit bureaus in the U.S. are now allowed to release people's credit information to anyone who requests it. The head of Associated Credit Bureaus, a trade association, says: "We want to make it perfectly clear that a consumer credit report is provided only to legitimate businesses for the purpose of making a determination on the extension of credit and other consumer benefits... One of the great things about the Internet is the ability to disseminate information at the click of a button. The downside is that things can be picked up and relayed – and keep going and going." (AP/Washington Post 2 Aug 2001)

http://washingtonpost.com/wp-dyn/articles/A21402-2001Aug2.html

Category 1B9 Non-virus hoaxes, urban myths

2001-10-10 securities fraud pump-and-dump scam bogus fraudulent press release ISP liability

policy investigation

NewsScan

YAHOO WON'T CHANGE CHATROOM POLICY [10 Oct 2001]

Trading in shares of Viasource Communications and Extreme Networks was halted Monday after a bogus document resembling a PR Newswire release was posted in a Yahoo Finance chatroom. Yahoo took the release off the message board as soon as it was contacted by PR Newswire. A spokeswoman said, "All of our message boards are considered unmoderated pieces of public forum. We don't proactively monitor the content of our boards." Citing Yahoo's user-privacy policy, she did not comment on whether Yahoo intended to pursue an investigation to determine who posted the press release. (Wall Street Journal 10 Oct 2001)

http://interactive.wsj.com/articles/SB1002654113365462080.htm

Category 1B9 Non-virus hoaxes, urban myths

2002-01-30 securities fraud Web marketing gullibility scam SEC government regulators hoax

lesson

NewsScan

SEC PLAYS LITTLE HOAX TO WARN INVESTORS OF WEB SCAMS

The Securities and Exchange Commission is a principal agency behind the hoax site www.mcwhortle.com, which purports to provide testimonials from investment analysts and financial exports for an outfit called McWhortle Enterprises, but which greets visitors with the warning: "If you responded to an investment idea like this... You could get scammed!" (AP/San Jose Mercury News 30 Jan 2002)

http://www.siliconvalley.com/docs/news/svfront/046980.htm

1C1 Impersonation

Category 1C1 Impersonation

2001-05-11 jamming emergency radio broadcasts impersonation intrusion penetration law

enforcement police investigation arrest

RISKS 21 39

The Rocky Mountain News for 11 May 2001 reported on a case of dangerous hacking:

> A 16-year-old boy using a handheld radio and a computer allegedly sent Denver police cruisers and a helicopter to fake emergencies and called officers off legitimate 911 calls for more than a month before getting caught.

Police said Thursday that the teen managed to hack into the department's computer-controlled radio system, program his radio to transmit on the department's frequency from his Southwest Denver home and then took on the alias of Jerry Martinez, a fictitious Denver police officer.

The teen enjoyed chatting with police helicopters flying overhead as well as reporting non-existent emergencies and accidents.

Eventually, police dispatchers caught on. When he called requesting license-plate information, they kept him talking for an hour and a half while the FCC physically located him using "special equipment". The final straw came a couple days later when an informant talked him into modifying another radio to transmit on police frequencies. The teen was charged with a dozen misdemeanors and a dozen felonies.

Category 1C1 Impersonation

2001-06-27 e-mail SMTP headers IP address reverse lookup electoral fraud forgery

impersonation criminal prosecution charges no contest nolo contendere plea Internet MS-Word properties sheet GUID globally-unique identifier

RISKS 21 50

A report from a RISKS correspondent (name not supplied) told a story of technobumbling in the political fray of Minnesota:

Christine Gunhus, wife of former U.S. Senator Rod Gram (R-MN) pled "no contest" to charges of criminal violations of Minnesota election code. She used a pseudonymous Hotmail e-mail account to send disparaging propaganda about her husband's rival -- but failed to notice that the "X-Originating-IP:" header shows the IP address of the sender. A simple reverse IP lookup identified "the AT&T WorldNet user who repeatedly used the 'Katie Stevens" Hotmail account by connecting from Gunhus' home number. In addition to the compromising headers, the e-mail included MS-Word documents as attachments, and those documents listed Christine Gunhus as an author. The Globally Unique Identifiers (GUIDs) in the attached Word documents; "[the] GUID includes the Ethernet MAC address. Prosecutors last August obtained a search warrant to seize Gunhus' computer, from which they could extract the MAC address if the Ethernet card was still the same."

The correspondent adds an interesting comment about the effects of such stupid dirty tricks on anonymous or pseudonmous speech: "The Minnesota Civil Liberties Union reasonably argues that a criminal law that bans sending pseudonymous messages is unconstitutional. A Supreme Court decision, McIntyre v. Ohio Elections Commission < http://www.epic.org/free_speech/mcintyre.html >, says that a prohibition on the distribution of anonymous campaign literature violates the First Amendment. The state law seems to be ecumenical in its application: A Republican has used it to attack the Sierra Club < http://www.fcregister.com/ziegler11 6 00.htm >.

Cluebot story (with links):

http://www.cluebot.com/article.pl?sid=01/06/15/0135212&mode=nocomment

Minnesota Public Radio story on original affidavit:

http://news.mpr.org/features/200009/08 radila grams/index.shtml

Category 1C1 Impersonation

2001-08-07 bank credit card fraud countermeasures identification authentication I&A

mutual protocol failure design spoofing impersonation

RISKS 21 59

Michael Bacon identified a problem in the credit-card fraud countermeasures used by his bank. Called by someone claiming to be the bank's fraud department to check on unusual buying patterns, he requested a method of verifying _their_identity before revealing his authentication information. Apparently no one had ever thought of checking to see if the caller were legitimate bank employees. He settled the problem in an imaginative way: "After much discussion and calling two supervisors, we agreed that they would tell me the last two purchases I had made on that card (approximately 1 hour and 20 minutes beforehand respectively from two different stores). If they could, then they were probably from the bank, and I would authenticate myself to them." He added, "The RISKS are clear. You supply some 'secret' data to the bank so that they can authenticate you when you call them. But there is no simple way to authenticate the bank when it calls you. You can't ask for the number and call them back, because you have no way of authenticating the number given. They're ex-directory, so you can't confirm it through Enquiries, and they withhold the number so the CLI doesn't show! If you blindly supply the data (as clearly many people do), then you may be divulging to a crook the 'secrets' necessary to authenticate yourself to the bank. The bank has not thought to provide any means of authenticating themselves. I suspect this to be endemic."

Category 1C1 Impersonation

2002-01-24 spoofing forgery impersonation voting information warfare

RISKS 21 89

Nick Brown wrote about a case of e-mail spoofing that backfired because of a spelling mistake. As he reported in RISKS, "An e-mail was sent from the account of the mayor, telling members of a city commission to vote in favour of a plan to extend a local hypermarket. The official, public policy of the city council and the mayor is to oppose this extension. The mail to one member of the commission bounced, because the recipient's name was incorrectly spelled. An assistant to mayor Fabienne Keller, who has access to her mailbox, noticed the "undeliverable" reply and determined that the mail had been sent at a time when the mayor could not have sent it. The general manager of the hypermarket is under police investigation for illegal entry into a computer system, forgery, use of forged documents, and attempted fraud."

[French references:]

 $http://www.dna.fr/cgi/dna/motk/idxlist_light?a = art\&aaaammjj = 200201\&num = 18041610\&m1 = keller\&m2 = mairie\&m3 = 200201\&num = 18041610\&m1 = keller\&m3 = 200201\&num = 200201\&num$

 $http://www.dna.fr/cgi/dna/motk/idxlist_light?a = art\&aaaammjj = 200201\&num = 19049910\&m1 = keller\&m2 = mairie\&m3 = 200201\&num = 19049910\&m1 = keller\&m3 = 200201\&num = 19049910\&m1 = 200201\&num = 19049910\&m1 = 200201\&num = 19049910\&m1 = 200201\&num = 19049910\&m1 = 200201\&num = 200201\&$

1C2 Identity theft

Category 1C2 Identity theft

2001-01-17 identity theft bogus accounts fact-checking background quality assurance design

NewsScan

IDENTITY THIEVES MAY HAVE OPENED AN ACCOUNT FOR YOU

Fraud investigators are reporting that one of the common strategies used by identity thieves is to open a new account with a utility company under the name of the person whose identity they are trying to assume. The address on the account could be anywhere, because utility companies typically check only names and credit worthiness. Another trick used by scam artists is to generate bogus credit card numbers and then attach the real names and addresses of the people whose identity they plan to steal. By doing this they are relying on the fact that the verification process of online merchants is usually restricted to name, address, and phone number, and doesn't reveal until later the fact that the credit card number is a work of fiction. (USA Today 16 Jan 2001) http://www.usatoday.com/life/cyber/tech/ctj001.htm

Category 1C2 Identity theft

2001-02-28 identity theft personal information confidentiality impersonation fraud

international

RISKS 2

Keith A Rhodes wrote in RISKS about a system penetration at Indiana University that raised fears of identity theft: "A user browsing from Sweden stored music and video files on a server at Indiana University that had apparently been left unprotected after a crash. IU realized it had a problem when huge increases were noted in network traffic. In the process, they also noted that a file of over 3,100 student names and SSNs had been copied from the server. Associate Vice President Perry Metz contacted the Social Security Administration about what might be an appropriate reaction, and said that they told him ``it's unlikely and unusual for someone who has your Social Security number to be able to do anything with it. Normally, financial institutions require additional information.'' [Is that reassuring to RISKS readers? Sources: Swedish hacker breaches IU server; Culprit stored music, video files on system and also downloaded private student data, AP item 28 Feb 2001, and article by John Meunier, *Herald-Times*, 28 Feb 2001; PGN-ed]"

Category 1C2 Identity theft

2001-03-20 identity theft impersonation fraud public records confidentiality Web

RISKS 21 29

RISKS moderator Peter G. Neumann wrote a brief summary of a recent arrest with implications for theft of identity; his item started with the punning title, "Identity theft: Forbes-ing a head?" His comments were as follows:

>In RISKS, we have for many years been warning about the burgeoning increase in identity theft. The following case could foster a broader awareness of the depth of the problem, but then again most folks still seem to have their heads in the sand - unless they have already been burned.

Abraham Abdallah was arrested on 7 Mar 2001, a 32-year-old Brooklyn NY high-school dropout working as a busboy, and already a convicted swindler. Although he was arrested as he was picking up equipment for making bogus credit cards, he is suspected of already having stolen millions of dollars. In his possession were SSNs, addresses, and birthdates of 217 people whose names appeared in a Forbes Magazine itemization of the 400 richest people in the U.S. He reportedly also had over 400 stolen credit-card numbers, and had used computers in his local library to access of the Web for information gathering. He is being held on bail of \$1M. His activities were detected after an e-mail request to transfer \$10M from a Merrill Lynch account, whereupon authorities found mailboxes he had rented in various names and other evidence. His defense attorney said Abdallah is innocent, and that prosecutors had ``made an unfair leap from possession of this information to an inference that there was an attempt to take money.'' [PGN-ed from a variety of sources, including an AP item by Tom Hays

http://www0.mercurycenter.com/premium/business/docs/forbes21.htm; Thanks to Dave Stringer-Calvert and to Michael Perkins at Red Herring]<

Category 1C2 Identity theft

2001-03-21 identity theft impersonation government documents national identifier driver's

license public access confidentiality

RISKS 21 29

Peter V. Cornell reported in RISKS on the recent declaration of the California driver's license and ID card as the primary identification document for the state. Mr Cornell wrote, "Courtesy of the California legislature, *anyone* who has a fake California drivers license with YOUR correct data, but with *his* picture and *his* version of your signature, can steal your money in many different ways. For example, if he knows your Social Security Number, bank, and account number, (easily obtained online or by mail theft) he can walk into any branch office and receive cash. Tens of thousands have been stolen from my (no longer existent) Wells Fargo accounts. . . . With that fake drivers license, that fraudster becomes YOU. All he need do is write a bad check drawn on another bank's bogus name account set up for that purpose, with the victim (you) as payee. He then walks into (in my case) a Wells Fargo branch and, impersonating the victim, cashes the check. When the check bounces, Wells Fargo (probably others, too) simply debits the victims account."

In addition, writes the correspondent, "The banking industry has arranged the law (California Commercial Code Sections 4401-4407 and 3101-3119) to ensure that the customer takes the hit. So that, among other conveniences, THE LAW allows banks to rely *solely* on the CDL data to confirm the identity of a customer with no risk exposure whatsoever. 'IF THE CUSTOMER PROVES' means you must sue the bank. They have it written so you'd lose anyway, but the amounts, however painful, are not nearly enough to pay a lawyer."

In riposte, attorney John Noble contributed a detailed rebuttal of Cornell's description of the California Commercial Code. He wrote, in part, "Mr. Cornell's description of the CA Commercial Code leaves out the good parts. An account may be debited if the item was 'properly paid,' i.e. 'authorized' in fact. If the item was not authorized, the customer need only notify the bank within a reasonable time after receiving his statement to have the account recredited -- the burden is on the bank to prove that the endorsement was genuine, which is impossible. Banks typically ask the customer to sign an affidavit; and they pull the video sequence of the transaction at the teller window to confirm that the customer did not cash the check himself (the unlikely exception to the impossibility of proving the endorsement was genuine). Mr. Cornell points to Code provisions that require the victim to "prove" that the bank failed to exercise 'ordinary care.' But the provision only applies to losses caused by the customer's failure to review his bank statement and report an unauthorized debit within a reasonable time. In effect the bank is strictly liable for unauthorized debits during the first 6-8 weeks on little more than the customer's insistence that they were unauthorized. But if the customer doesn't look at his statement and report the unauthorized transactions disclosed on the statement, the bank's liability is cut off and the customer is stuck with the additional losses. The reasons for this are obvious. Only the customer is in a position to know that the debit was unauthorized. If he doesn't look at his statements, and the same guy is cleaning him out month after month, whose fault is that? In addition, the law has to take into account the possibility that the customer is having his own checks cashed by a third party. . . . The moral of the story: review your bank statements -- it's part of the deal."

Category 1C2 Identity theft

2001-03-25 identity theft social security number SSN fraud driver's license theft law

enforcement justice system probation

RISKS 21 31

Tom Goltz described a theft of his identity in some detail in RISKS:

>I am white. I have held a California driver's license in the past, but that license has been inactive for over two years since I established residency in another state.

In October of last year, a black male obtained a fake California driver's license with my name on it and his picture. The driver's license ID # he used belongs to a white female. The address is a Commercial Mail Receiving Agency in Costa Mesa CA, which the state doesn't normally allow. The fake also contained two spelling errors.

This person used this ID and my social security number to open a dozen different credit accounts in my name at various locations around the Los Angeles area. He was using a cell phone with a phone number based in the 603 area code as his residence phone.

If anyone had bothered to look, just about everything about this guy screamed fraud, yet he managed to steal \$15,000 worth of merchandise (mostly jewelry).

Out of all these people who were supposed to be checking this information, only TWO found problems. One was a used car dealer who became suspicious when the check this guy gave for the down payment proved to be bogus. They refused to give the guy the car, but didn't bother to pursue the matter with the police. The other was store security at a Costco in Las Vegas, who tracked me down in New Hampshire and informed me that I had a problem. They detained the man, and turned him over to the police.

Sadly, the most he's going do is a couple of years probation - he didn't actually steal anything in Las Vegas, and the identity theft, although a crime in NV is not sufficient to assure jail time by itself. I discussed the matter of extraditing the varmint to California with Las Vegas police, but they told me that it was unlikely that California would bother for something that would only net the offender probation there as well. According to the LV police detective, in California, you have to be charged with stealing over \$50,000 before you'll do any jail time.

It's no wonder this crime is exploding...it's low risk, extremely profitable, and trivial to implement.

Oh yes...how did he get my name and social security number? He told the Las Vegas police that he purchased the information on the street for \$500.

Category 1C2 Identity theft

2001-05-11 social security number SSN drivers license permit state federal law identity theft

privacy government legislation court ruling judgement

RISKS 21 39

Brett Glass published a chilling report in RISKS about changes in federal law that _require_ applicants for state drivers' permits to submit their Social Security Numbers. Glass wrote, "What I found out was chilling. Not only does Federal Law -- thanks to the striking of a single word from a huge statute -- require that drivers submit their Social Security numbers when applying for licenses. It also requires that all of the information maintained about a driver by a state -- including that number -- be revealed to virtually all comers. Here are the details of these onerous laws, along with additional information about the laws in my particular state (which are typical of state laws throughout the country). I'll also describe the way in which one state is fighting the Federal laws that would require it to compromise its citizens' privacy and subject them to trivially easy identity theft."

It seems that changes in welfare reform legislation removed the word "commercial" from existing requirements that applicants for commercial drivers' licenses submit their SSN. In addition, amendments to the "Drivers' Privacy Protection Act"

now require that "ALL of the information you submit to your state's DMV/DOT [be] available to *anyone* who claims that it's needed for any business purpose. If I wanted your driving records and SSN, all I'd have to do is walk into the courthouse and claim that you owed me a dollar." Athough the amended act "was challenged by the Alabama Attorney General on states' rights grounds and was ruled unconstitutional by a Federal district court" it was upheld by the Supreme Court of the United States.

Mr Glass provides much more extensive documentation and detail in his report.

Category 1C2 Identity theft

2001-05-31 identity theft social security number abuse

NewsScan

IDENTITY THEFT

Identity theft is an increasing problem in the Information Age, and brokerage companies sometimes unwittingly sell dossiers to people using fake credit card and posing as other people. In one scam, thieves used an e-mail account and a stolen credit card number to purchase reports containing Social Security numbers, employment information and driving records, and were able to use this information to plunder bank accounts. One victim of identity theft said: "What has taken me a lifetime to build -- my trust, my integrity and my identity -- has been tainted. I don't know if I'm dealing with a 14-year-old messing around with a computer or if I'm dealing with organized crime." The Social Security Administration's inspector general says the power of the Social Security number makes it a valuable asset subject to limitless abuse, and calls that misuse has developed into "a national crisis." (Washington Post 31 May 2001) http://washingtonpost.com/wp-dyn/articles/A77996-2001May25.html

Category 1C2 Identity theft

2001-08-09 national identification number cellular phone wireless transmission eavedropping encryption password access code identity theft

NewsScan

FINLAND MULLS PUTTING NATIONAL IDs ON CELL PHONES

The Finnish government is considering using SIMs – the subscriber information modules inside every cell phone – to take the place of its national identity card, and eventually even a passport. Under the plan, the computer chip embedded in every SIM would store personal information, transforming the SIM into a person's legal proof of identity. Of course the drawback would be what would happen if you lost your phone – about 9,000 cell phones are left on the London Underground alone every year. The solution, according to Roger Needham, manager of Microsoft's British research lab, is to store the information on secure servers accessible via a WAP connection to the Web. The SIM in this case would store only a personal identifier – an encryption key – that the owner would have to punch in a PIN to use. The Finnish government is already taking the initiative with a national technical standard called FINEID. Currently FINEID uses a smart card and a card reader attached to a PC, but the plan is to migrate to an SIM, says Vesa Vatka of the Finnish Population Register Center in Helsinki. (New Scientist) http://www.newscientist.com/hottopics/tech/yourphoneisyou.jsp

Category 1C2 Identity theft

2001-11-09 national identity card civil liberties anonymity privacy

NewsScan

CYBERSECURITY CHIEF NOT INTERESTED IN NATIONAL ID CARD

Bush Administration cybersecurity chief Richard Clarke is showing little interest in a proposal from Oracle's Larry Ellison to create a national identity card as part of the nation's response to the dangers posed by terrorists. Clarke says that no one he's talked to in the administration thinks it's a good idea, and civil liberties groups have uniformly opposed the plan. (ZDNET/USA Today 9 Nov 2001)

http://www.usatoday.com/life/cyber/zd/zd1.htm

1C3 Pseudonymity

Category 1C3 Pseudonymity

2001-07-20 pseudonymity risks marriage love affairs strangers husband wife fracas

embarrassment rage

RISKS 21 55

An unexpected risk of Internet pseudonymity was reported to RISKS by Gary Stock:

A married couple in China ended up brawling after realising they had unwittingly courted each other over the internet. The pair from Beijing sneaked online to flirt with their mystery girlfriend and boyfriend at a chat website called the Green, Green Schoolyard. After a month, the man arranged to meet up with his ideal new friend only to discover it was actually his wife. He had known only her user name, I Want You. They each agreed to carry a certain newspaper to identify themselves, but were shocked when they came face-to-face and started fighting in the street. Passers-by eventually alerted security guards who had to separate the two, reports Norway's main news agency NTB.

http://www.ananova.com/news/story/sm 354103.html?menu=news.weirdworld.rockyrelationships

[MK adds: ironically, the two seemed to be ideally mated already -- each person's exciting new dream date was already their own spouse.]

1D1 Organizations, cooperation

Category 1D1 Organizations, cooperation

2001-01-16 cooperation alliance technology hacking ISAC

NewsScan

TECH ALLIANCE TO SHARE DATA ON HACK ATTACKS

Nineteen big-name companies, including AT&T, Microsoft, Oracle, Cisco, IBM and Hewlett-Packard, are banding together to launch a private, nonprofit alliance to share sensitive data about cyber-attacks and vulnerabilities in their hardware and software products. "The overriding goal is to protect ourselves from cyber-hazards, whether they be deliberate attempts or accidental events," says Guy Copeland of Computer Sciences Corp., a board member of the new Information Technology Information Sharing and Analysis Center (IT-ISAC). "We've known that each of us have a little bit of the picture... By sharing the information, we can be that much smarter." Other technology firms will be invited to join the alliance for \$5,000 a year. Three similar private alliances to deter cyber-attacks exist already, covering the banking, telephone and electrical industries, and more are planned for oil and gas companies and the transportation sector. (Wall Street Journal 16 Jan 2001)

http://interactive.wsj.com/articles/SB97959775829133953.htm

Category 1D1 Organizations, cooperation

2001-04-25 international cooperation law enforcement police fraud laws consumer

information investigations

NewsScan

COUNTRIES TEAM UP TO FIGHT E-FRAUD

Thirteen countries have agreed to back a project aimed at stifling cross-border Internet fraud and improving consumer confidence in e-commerce. A multilingual Web site -- www.econsumer.gov -- will provide information on consumer protection laws in the 13 countries and offer consumers a way to file complaints online. The cooperating governments will use a parallel, but secure, site to share complaint data and information on e-commerce fraud investigations. The 13 countries are: Australia, Canada, Denmark, Finland, Hungary, Mexico, New Zealand, Norway, South Korea, Sweden, Switzerland, the U.K., and the U.S. The plan is also backed by the Organization for Economic Cooperation and Development. (Financial Times 25 Apr 2001)

http://news.ft.com/news/industries/internet&e-commerce

Category 1D1 Organizations, cooperation

2001-11-08 international agreement convention cybercrime investigation fraud child

pornography cooperation law enforcement investigation extradition

NewsScan

EUROPEAN COUNCIL ADOPTS FIRST CYBERCRIME TREATY

The 43-nation Council of Europe has adopted a convention on cybercrime that criminalizes activities such as fraud and child pornography committed over the Web and sets up global law enforcement procedures for conducting computer searches, intercepting e-mail messages, and extraditing criminal suspects. The convention marks the first treaty on criminal offenses committed via the Internet. It will enter into force once five states, including at least three Council of Europe member nations, have ratified it. States will have that opportunity at a conference on cybercrime to be held in Budapest on November 23. (Reuters 8 Nov 2001)

http://news.excite.com/news/r/011108/13/net-europe-cybercrime-dc

Category 1D1 Organizations, cooperation

2002-01-14 ISP Internet service providers association group security cooperation

collaboration information sharing critical infrastructure protection law

enforcement investigation

NewsScan

ISPs FORM A NEW ASSOCIATION

Several Internet companies have banded together to form a new group that will focus on compliance and liability issues. The U.S. Internet Service Provider Association (US ISPA) will replace the Commercial Internet eXchange, which is folding. Founding members of the new group including AOL, Cable & Wireless, Earthlink, eBay, Teleglobe, Verizon Online and WorldCom. US ISPA vice president Tom Dailey says the group will examine such issues as online security, liability and compliance with the new antiterrorism law, the USA-Patriot Act, and the Council of Europe Convention on Cybercrime. In addition, the US ISPA will raise "a variety of other policy and legal issues of concern to ISPs, such as Internet privacy, content regulations and intellectual property." (Wall Street Journal 14 Jan 2002) http://interactive.wsj.com/articles/SB1011053572133523720.htm (sub req'd)

1D2 Technology

Category 1D2 Technology

2001-07-05 e-mail archives evidence forensic investigation law enforcement

NewsScan

IT'S A SLOW WEEK: SHOULD YOU CLEAN OUT YOUR INBOX?

One person interviewed about his e-mail usage admitted to having 2,465 messages sitting in his inbox: "I know you can put these things in files and have them organized, but it never seems worth the trouble." Ned Kock of Temple University's e-collaboration center agrees that mailbox organization places an additional burden on busy people: "In using e-mail, you have six main tasks. You open the system. You download the messages. You read the messages. You reply. You file them. You shut off the system. We as a species are optimized for face- to-face communication, so only two of these the reading and replying are vaguely associated with that. The others are just overhead. They carry no social interest at all. There is an excitement to reading and replying, but filing takes cognitive effort without an immediate reward. So despite its being important in the long run to be organized, it is human nature to avoid it." Our conclusion? The choice is yours: follow your dream... or your nature. (New York Times 5 Jul 2001) http://partners.nytimes.com/2001/07/05/technology/05MAIL.html

Category 1D2 Technology

2001-07-25 e-mail interception Carnivore ISP filtering law enforcement investigation privacy

civil liberties

NewsScan

FBI's CATCH-22 (OR CATCH-374) NAME FOR CARNIVORE [8 Feb 2001]

The FBI's plans for its Carnivore system for "wiretapping" the Internet have been under continuous criticism from privacy advocates, and House majority leader Dick Armey of Texas has said the technology raises strong concerns that the government is "infringing on Americans' basic constitutional protection against unwarranted search and seizure." Some defenders of Carnivore, have suggested that the controversy is largely because of the catchy name chosen for the system, which was called Carnivore because it could get to the "meat" of a criminal investigation. One official said ruefully: "If they called it Device 374, nobody could remember what Device 374 was." (New York Times 8 Feb 2001) http://partners.nytimes.com/2001/02/08/technology/08CARN.html

CARNIVORE TO GET NEW PRIVACY PROTECTIONS [19 Apr 2001]

Justice Department sources are saying that Attorney General John Ashcroft, a strong defender of individual privacy rights, will heed FBI Director Louis Freeh's advice to allow the government to continue using the Carnivore e-mail surveillance system but will require various new safeguards - such as tightening the "audit trail" to make sure the system is not being abused by law enforcement officials and developing a more precise definition of what e-mail may be inspected. (Los Angeles Times 19 Apr 2001)

http://www.latimes.com/business/cutting/todays.topstory.htm

FBI JUSTIFIES ITS INTERNET SURVEILLANCE METHODS [4 May 2001]

Documents obtained by the Associated Press under the Freedom of Information Act show that the FBI used the Carnivore or Etherpeek surveillance tools 24 times from October 1999 to August 2000 to monitor Internet e-mail and other communications traffic as part of criminal investigations of such activities as network vandalism, drug probes, extortion, and intellectual property theft. One agent wrote to a superior: "We got bank accounts, where money was hidden and other information. Some of the data sent was instrumental in tying several of the conspirators to the crime." The agent's superior told the agent that the kind of information he was providing would be "very helpful in fighting the idea that we are randomly looking at everyone's e-mail." (AP/USA Today 4 May 2001) http://www.usatoday.com/life/cyber/tech/2001-05-04-carnivore.htm

DICK ARMEY CONTINUES OPPOSITION TO CARNIVORE

In a letter to Attorney General John Ashcroft, House majority leader Dick Armey (R-Texas) is urging the Justice Department and the FBI to consider abandoning its DCS-1000 system (popularly known as "Carnivore"), which monitors large amounts of Internet traffic in search of communications to or from the target of an investigation. Armey noted that the Supreme Court has just ruled that the police must discontinue use of thermal-imaging technology to look inside a suspect's house, and argued that the same privacy principles apply to Carnivore. (New York Times 14 Jun 2001) http://partners.nytimes.com/2001/06/14/technology/14CARN.html

CONGRESS AGAINST CARNIVORE [25 Jul 2001]

The U.S. House of Representatives has passed a bill that would require federal law-enforcement officials to provide a detailed accounting each year of how they made use of the system known as Carnivore (renamed DCS 1000), which allows criminal investigators with a search warrant to monitor the e-mail traffic to and from a suspect's computer. The FBI would be called on to reveal which officials and which courts authorized its use, which specific laws were invoked to justify its use, and what benefits were gained from that use. (Reuters/USA Today 25 Jul 2001) http://www.usatoday.com/life/cyber/tech/2001-07-25-carnivore.htm

Category 1D2 Technology

2001-09-04 computer forensics digital evidence law enforcement police investigation

NewsScan

BITS OF EVIDENCE

A growing number of consultants now specialize in helping law firms prepare for trail by sorting through electronic documents and e-mail messages found either on a defendant's own computer or on file server systems. Computers can identify documents by date, authors, recipients and keywords, and can frequently yield information the author thought had been erased. Attorney Michael Epstein says: "You know for a paper document, it's either there or it isn't. With e-mail, it's a little different." He provides the example of a lawsuit bought by one company against its former employees, whose denials of working for themselves on company time were refuted by evidence of their personal activities obtained by restoring files erased from the computers they had used at work. (New York Times 4 Sep 2001) http://partners.nytimes.com/2001/09/04/technology/04DISC.html

Category 1D2 Technology

2001-12-05 e-mail content filtering terrorism key word search law enforcement policy

technology Carnivore denial-of-service attack false positives flooding saturation

useless defeat

RISKS 21 82

Fredric L. Rice contributed a depressing analysis to RISKS about why Carnivore and similar content-based e-mail scanning will inevitably be defeated. He pointed out that it would be trivially simple to flood the system with vast numbers of messages containing machine-generated gibberish fitting the profiles used by Carnivore to spot possible involvement in terrorism. In addition, any activist who actually did get picked up the by the FBI because of a real e-mail could simply post the suspect e-mail on the Web, thus providing a template for yet more chaff. The author concluded, "I can't see anything coming out of the struggle besides a pile of useless software running on ISP's servers fingering innocent people and failing to point at a single bad guy."

Category 1D2 Technology

2002-01-09 biometric face recognition I&A identification authentication failure removal law

enforcement police

RISKS 21

Nick Brown wrote in RISKS, "...[A] highly-publicised facial recognition system has been quietly dropped by law enforcement officials in Tampa, Florida, following a large number of false positives (including males identified as females, and vice versa) and a total of zero matches against known criminals, leading to zero arrests. Aside from the already-discussed civil liberties RISKs of such systems, it seems we need to add the possibility that the taxpayers may not be getting value for money, with or without their knowledge (the withdrawal of this kind of thing tends to be done with rather less media coverage than its introduction). One wonders if this will have any effect on plans to introduce such systems into airports to 'detect' terrorists."

http://www.aclu.org/issues/privacy/drawing blank.pdf

Category 1D2 Technology

2002-01-20 content filtering analysis lying dissimulation dishonesty untruth law

enforcement investigation forensic

NewsScan

SOFTWARE UNCOVERS E-MAIL UNTRUTHS

SAS Institute has developed software that it says can sift through e-mails and other electronic text to discern falsehoods. "The patterns in people's language change when they are uncertain or lying," says Peter Dorrington, business solutions manager at SAS. "We can compare basic patterns in words and grammatical structures versus benchmarks to detect likely lies." For instance, over-use of the word "or" and too many adjectives can be giveaways, according to Aldert Vrij's book, "Detecting Lies and Deceit." SAS says its software can also be used to detect inaccuracies in resumes and job applications. (Financial Times 20 Jan 2002)

http://news.ft.com/news/industries/internet&e-commerce

Category 1D2 Technology

2002-02-20 paper snail mail conversion e-mail law enforcement surveillance investigation

privacy security confidentiality vulnerability

NewsScan

NEW SERVICE DELIVERS PAPER MAIL ELECTRONICALLY

PaperlessPOBox offers a service that delivers 100% of your mail electronically, whether it starts out that way or not. Customers who sign up have their snail mail forwarded to an outside P.O. Box address, where it is picked up by PaperlessPOBox, scanned, and transmitted to users' e-mail accounts on the same day. The user receives exact replicas of whatever mail was sent, including hand-written notes and photos. "Personal notes translate very well," says PaperlessPOBox President David Nale. "We use state-of-the-art scanners." The service is targeted toward business travelers who have difficulty keeping up with overflowing mail boxes and received a boost last fall during the anthrax scare when people were fearful of contamination via paper mail. (Reuters 20 Feb 2002) http://story.news.yahoo.com/news?tmpl=story&cid=581&u=/nm/20020220/tc nm/column nettrends dc 14

Category 1D2 Technology

2002-02-21 consumer profiling audit trail logging tracking music video surveillance law

enforcement police investigation family parental control supervision

NewsScan

MICROSOFT TRACKS USERS' SONGS, MOVIES

The newest version of Microsoft's MediaPlayer software, which comes free with the Windows XP operating system, is designed to create a log of the songs and movies that users play. When a CD or DVD movie is played, the MediaPlayer 8 software stores that information in a file on the user's PC, in addition to transmitting an identifier number unique to each user on the computer. That function creates the possibility that information on user habits could be tracked and sold for marketing purposes. Privacy experts say the log file could be used by investigators, lawyers, snooping family members, or companies interested in finding out an individual's personal entertainment habits. Microsoft said the program creates the log so that a user does not have to repeatedly download the same track, CD or movie information, and that the ID number was created simply to enable MediaPlayer users to have a personal account on the Web site dealing with software. The company says it has no plans to share that information with others. (AP/Miami Herald 21 Feb 2002)

http://www.miami.com/mld/miamiherald/2712422.htm

1D3 Litigation, legal rulings, judgements

Category 1D3

Litigation, legal rulings, judgements

2001-02-20

surveillance technology privacy search seizure constitution law enforcement

NewsScan

TECHNOLOGY TESTS THE BOUNDARIES OF YOUR HOME The Constitution's Fourth Amendment protecting citizens against unwarranted search and seizure will be debated this week in the U.S. Supreme Court, which is considering a case in which police used a thermal scan of a private house to determine if excessive heat from the building suggested that it was being used to grow marijuana under high-intensity lights. An ACLU executive protests that "if the government is free to use technology inside our homes, there really won't be anything left of the right to privacy," and an attorney for the man whose house was targeted argues: "Since we don't permit police to break into people's homes, should we permit them to use technology to accomplish the same thing?" The police, however, justify the thermal scan as no different in principle from having an officer watching a house from the outside. (AP/USA Today 19 Feb 2001)

http://www.usatoday.com/life/cyber/tech/review/2001-02-19-thermal.htm

Category 1D3

Litigation, legal rulings, judgements

2001-05-03

monitoring legal roadblocks prevention government interference auditing criminal hackers honeypot warrant

NIPC Daily Report

A late-term change in the Clinton administration's approach to prosecuting cybercrime has made it much more difficult for NASA to track and prosecute hackers who attempt to penetrate its computer networks, a NASA network-protection office official said 30 April. "NASA lost 90% of its ability to track and pursue (suspected computer) intruders because of changes in policy" by the Justice Department, according to a director from NASA's network and advanced technologies protection office. Apparently, over the last year-and-a-half, the Justice Department's Computer Crime and Intellectual Property section began prohibiting federal agencies from electronically monitoring the actions of hackers who break into their systems. Under federal wiretapping statutes, system administrators of private computer networks may do such monitoring, but law enforcement officials are normally prohibited from doing so without a warrant. (Infosec News, 3 May)

Category 1D3 Litigation, legal rulings, judgements

2001-12-12 encryption organized crime police law enforcement investigation keystroke

logging surveillance data capture password wiretap virus logger Magic Lantern

NewsScan

ENCRYPTION AND ORGANIZED CRIME [30 Jul 2001]

When Phil Zimmerman created the encryption software known as PGP ("Pretty Good Privacy") he knew that his program would be used not only by honest citizens but also by criminals, and he says "I felt bad about that," but notes that "the fact that criminals use cars doesn't mean that the rest of us shouldn't have cars." Criminal use of PGP is now being examined in a federal case against Nicodemo S. Scarfo Ir., accused of running gambling and loan sharking operations for the Gambino crime family. The defendant's lawyers are arguing that federal law enforcement officials acted unconstitutionally when they evaded the privacy protections of PGP by surreptitiously installing on Scarfo's personal computer some technology that recorded every keystroke made, including his password. Their position is that this action amounted to a wiretap, for which they should have obtained a special court order, called a "Title III" order. But assistant U.S. attorney Ronald Wigler says that "letters do not become 'electronic communications' subject to Title III merely because they happen to have been typed on a computer." (New York Times 30 Jul 2001) http://partners.nytimes.com/2001/07/30/technology/30TAP.html

PRIVACY ADVOCATES OBJECT TO "KEY LOGGING" TECHNOLOGY [14 Aug 2001]

Privacy advocates are strenuously criticizing the use by federal law enforcement officials of "key-logging" technology to monitor the communications of "Little Nicky" Scarfo, a reputed Philadelphia mob boss. Rather than obtain a courtapproved wiretap order, the officials used a simple search warrant (much easier to obtain) in order to plant on Scarfo's computer a yet-to-be-explained technology that monitors every keystroke, including e-mail. Mark Rasch of the security consulting firm Predictive Systems says: "The logical consequence of the government's argument is that the government will never need to get a wiretap order for a computer. With the technology that's available today, the government can remotely install software on a computer to capture all keystrokes and transmit that report to its agents in real time." (Washington Post 14 Aug 2001)

http://washingtonpost.com/wp-dyn/articles/A55606-2001Aug9.html

FBI TARGETS SUSPECTS' PCs WITH SPY VIRUS [21 Nov 2001]

The FBI is working on software that could insert a computer virus into a suspect's computer capable of reading encrypted data. The software, known as "Magic Lantern," installs "keylogging" software that can capture keystrokes typed on a computer. The virus can be sent via e-mail and once on the targeted PC, it waits for a suspect to launch the Pretty Good Privacy encryption program and then logs the passphrase used to start the program, essentially giving agents access to the keys needed to decrypt files. The Magic Lantern software is part of the FBI's "Enhanced Carnivore Project Plan," which operates under the umbrella project name of Cyber Knight. Electronic Privacy Information Center attorney David Sobel says privacy issues arise when keylogging results in "overly broad" searches, since it would be possible to observe every keystroke typed by the suspect, even if a court order specified only encryption keys. The FBI has already used a less-sophisticated version of the software to build the high-profile racketeering case against Nicodemo Scarfo, but had to manually turn the system on and off in order to comply with the court order. (MSNBC/Wall Street Journal 21 Nov 2001) http://interactive.wsj.com/articles/SB10062942834030720.htm (sub req'd)

FBI CONFIRMS DEVELOPMENT OF KEYSTROKE-CAPTURING EAVESDROP TECHNOLOGY [12 Dec

The FBI has confirmed that it has under development a technology that could use the Internet to plant Trojan Horse software in a criminal or terrorist suspect's PC that would capture passwords to access the suspect's e-mail and other documents. An FBI official said, "Like all technology projects or tools deployed by the FBI it would be used pursuant to the appropriate legal process." (Reuters/Yahoo 12 Dec 2001)

http://dailynews.yahoo.com/htx/nm/20011212/tc/tech magiclantern dc 1.html

Category 1D3 Litigation, legal rulings, judgements

2002-02-20 law enforcement e-mail interception forensics inspection authority warrant court

order lawsuit jurisprudence wiretapping

NewsScan

DO THE POLICE NEED A COURT ORDER TO INSPECT A SUSPECT'S E-MAIL? [20 Feb 2002]

In a case involving the admissibility of Internet evidence used to convict he a man for solicitation of a 15-year-old girl he met in a chat room, the Pennsylvania Supreme Court will decide whether police authorities need a court order (as they would if they wanted to set up a telephone wiretap operation) before looking at a suspect's e-mail and instant messages. The lower court took the position that the wiretapping law did not apply because the police did not intercept the messages but looked at them after they had been received, and it suggested that the defendant had given implied consent to the inspection of his messages: "Any reasonably intelligent person, savvy enough to be using the Internet, would be aware that messages are received in a recorded format, by their very nature, and can be downloaded or printed." (AP/USA Today 20 Feb 2002)

http://www.usatoday.com/life/cyber/tech/2002/02/20/internet-wiretap.htm

Quality assurance failures (general)

Category 21 Quality assurance failures (general)

2001-01-02 Y2K quality assurance bug denial of service

NewsScan; RISKS 21 18

Y2K BUG BELATEDLY BEDEVILS NORWAY'S TRAINS

The Y2K glitch hit Norway's national railroad company a year later than expected, when none of the company's 16 new airport express trains or 13 high-speed long-distance Signatur trains would start on the morning of Dec. 31. The company performed a quick work-around by resetting the computers to Dec. 1, 2000, and the trains were able to start up on ignition. "We didn't think of trying out the date 31/12/00," says a spokesman for Adtranz, the German producer of the new trains. "Now we have one month to find out what went wrong so we can fix the problem for good." (AP/San Jose Mercury News 1 Jan 2001)

http://www0.mercurycenter.com/svtech/news/breaking/ap/docs/797241l.htm

Category 21 Quality assurance failures (general)

2001-01-03 Y2K+1 QA quality assurance palm computerorganizer

RISKS 21 18

Philip Berman reported in RISKS that his Sharp YO-550 Electronic Organizer was unable to function correctly with any system date of 2001 or later.

Category 21 Quality assurance failures (general)

2001-01-03 QA quality assurance Y2K+1 credit card availability

RISKS 21 18

The national chain of 7-Eleven convenience stores were hit by a belated Y2K bug ("Y2K+1!) when all their credit-card processing software failed on the 1st of January 2001.

Category 21 Quality assurance failures (general)
2001-04-16 quality assurance bug flaw software

NewsScan

ULTIMATETV USERS ARE BUGGED BY GLITCH

Users of Microsoft's UltimateTV are complaining about a glitch in the system that severely restricts their useable recording time. Subscribers are entitled to as many as 35 hours of digital recording time, but the bug can reduce that time to as little as five hours. Other functions – including the interactive features and Internet access – are not affected. Microsoft WebTV Networks acknowledged that a "small number of subscribers" had lost storage space on their systems, and warned users not to press "erase" before pressing "stop" first. "We believe it is a software bug that is exacerbated by some fairly obscure pattern of usage by the subscriber." Meanwhile, the company says a software correction will be distributed directly to the hardware via satellite in the next few months. (Hollywood Reporter 15 Apr 2001)

http://hollywoodreporter.com/hollywoodreporter/convergence/

Category 21 Quality assurance failures (general)
2001-04-17 automated loo toilet WC QA quality assurance

RISKS 21 35

Article by Lester Haines, 17 Apr 2001, quoted in RISKS by Gareth Randell: <From < http://www.theregister.co.uk/content/28/18312.html >]

A 51-year-old woman was subjected to a harrowing two-hour ordeal [on 16 Apr 2001] when she was imprisoned in a hitech public convenience. Maureen Shotton, from Whitley Bay, was captured by the maverick cyberloo during a shopping trip to Newcastle-upon-Tyne. The toilet, which boasts state-of-the-art electronic auto-flush and door sensors, steadfastly refused to release Maureen, and further resisted attempts by passers-by to force the door. Maureen was finally liberated when the fire brigade ripped the roof off the cantankerous crapper. Maureen's terrifying experience confirms that it is a short step from belligerent bogs to Terminator-style cyborgs hunting down and exterminating mankind.

Category 21 Quality assurance failures (general)

2001-04-25 QA quality assurance availability real-time process control failure bug design

RISKS 21 36

Peter G. Neumann, moderator of RISKS, reported on quality assurance failures in the Washington Metro: "Washington D.C. Metro's \$20 million central computer system crashed at 5:15 p.m. during the evening rush hour on 24 Apr 2001. The central system provides real-time graphics to the downtown control center. Similar malfunctions occurred in 1998 and 1999 (e.g., RISKS-20.60). In the 15 months following its installation, this BDM system crashed 50 times, according to the Metro. Coincidentally, a six-car train that had broken down 8 minutes earlier was stuck in the tunnel between Friendship Heights and Bethesda, and had to be towed out."

Category 21 Quality assurance failures (general)

flaw testing

2001-06-06 QA quality assurance e-commerce Web shopping cart software bug data entry

error refund

RISKS 21 46

Steve Loughran, writing in RISKS, reported that the shopping cart software for a particular Web site allowed him to enter negative quantities into an order form, resulting in apparent refunds. He was too honest to continue with the order to find out if he really would get a check.

Category 21 Quality assurance failures (general)

2001-08-12 system failure crash availability communications network phone software error

bug flaw QA quality assurance notification

RISKS 21 60

Andre Oppermann reported from Switzerland on a massive mobile telephone network failure. Writing in RISKS, he summarized the events as follows:

On Friday, July 27th 2001, the whole Swisscom Mobile GSM network, serving 3.3 million customers (70% market share in Switzerland), broke down for 10 hours from approx. 12:30 until 22:30 GMT+0200.

Two independent software errors in the primary and backup network signaling processors (the SS7 network) caused a halt for the processing of all signaling in a GSM network. This includes call setup, call receiving, SMS (short message service), logging onto network and basically everything else. The central GSM systems (HLR, VLR, NMC and so on) stayed up but were unable to communicate with the base stations in the field.

The primary system suffered a complete failure (software error) and as designed the backup system took over. While it was working fine first the backup system got loaded more and more, judging from the description something like a missing free() call, and eventually broke down too half an hour later.

The newspaper "Le Monde" was reporting insider information last week saying that these signaling processors are made by Alcatel and that Alcatel found out about the software errors two weeks before (and probably also had a fix) but "forgot" to inform Swisscom Mobile about it. Alcatel is now facing a Swiss Franc 30 million liability case. This is the loss Swisscom Mobile has because of lost revenues, not including public image damages.

In one thing I have respect for Swisscom; They did a pretty good job with public relations and informed the media and public very openly about their technical problem(s). Now, two weeks later, Swisscom Mobile also issued a, thought written for the non technician but pretty detailed, press release of the cause and events of this network failure.

. . . .

Category 21 Quality assurance failures (general)

2001-11-06 QA quality assurance installation format data destruction disk drive underlying

assumptions

RISKS 21 74

A minor programming bug (missing quotation marks) in the new version of the iTunes media player for Macintosh computers resulted in total deletion of all the data on the unfortunate victims' disk drives.

In a later issue of RISKS, a commentator made the point that actually, it wasn't a minor programming bug that caused the error, it was bad quality assurance. Another writer explained the underlying problem: on the Mac, spaces can be used within file names. However, writes the contributor, "With the new Unix-based OSX, long-time mac users are discovering the hard way that spaces are used as delimiters in scripts and in parsing, so filenames containing spaces can have unintended results. Most Unix code samples and docs assume that no one ever puts spaces in their file names, so the samples never show quotes being used, and some docs don't mention this need either. Just about every programmer making the Mac switch from OS 9 to 10 finds this out the hard way, just not as publicly and catastrophically. The risk-changing the underlying behavior of familiar software, and not being aware of all the assumptions behind that underlying behavior."

Another followup explained that "According to a well-placed friend within Apple, the failure was a bit more complex than described. He says that the bug in the script was actually discovered prior to the software being posted, but that the corrected version somehow did not end up being posted (classic version management issue.) Furthermore, the fact that broken script had been posted was discovered in the middle of the night, but the folks responsible for the server did not pull it down until hours later, thus increasing the collateral damage (classic people management issue.)"

Category 21 Quality assurance failures (general)

2001-12-04 data entry keystroke error QA quality assurance bounds checking limits

reasonableness check losses stock market trading share price fall

RISKS 21 81

According to the _Wall Street Journal_, "Dentsu Inc., one of the world's biggest advertising companies, was making its trading debut Friday on the Tokyo Stock Exchange after completing one of the year's biggest initial public offerings – a deal arranged by UBS Warburg, a unit of Switzerland's UBS AG. . . . Before the Tokyo market opened Friday, a UBS Warburg trader entered what was intended to be an order to sell 16 Dentsu shares at 610,000 yen (\$4,924.53) each or above. Instead, the trader keyed in an order to sell 610,000 Dentsu shares at 16 yen apiece. . . . The order was canceled by 9:02 AM, but not before 64,915 shares, almost half of the 135,000 shares in the IPO, had been sold. The price of Dentsu shares, which had been bid up to 600,00 yen before the market opened, fell to 405,000 yen. Now, UBS Warburg is obligated to deliver the shares it sold, and will have to buy them on the open market."

George C. Kaplan, who contributed this item to RISKS, cogently pointed out, "The article doesn't say anything about sanity checks in UBS's trading software. These have their own risks, of course, but you'd think that an error of 4 orders of magnitude in the selling price would at least merit an "Are you sure?" before the order went through. Once again, we see how computers let people make really big mistakes quickly."

Category 21 Quality assurance failures (general)

2001-12-21 buffer overflow vulnerability quality assurance remote control penetration

NewsScan

SECURITY PROBLEMS IN MICROSOFT AND ORACLE SOFTWARE [21 Dec 2001]

Two top companies have issued new statements acknowledging security flaws in their products: Microsoft (Windows XP) and Oracle (the 9i application server, which the company had insisted was "unbreakable." Resulting from a vulnerability called "buffer overflow," both problems could have allowed network vandals to take over a user's computer from a remote location. Microsoft and Oracle have released software patches to close the security holes, and a Microsoft executive says: "Although we've made significant strides in the quality of the software, the software is still being written by people and it's imperfect. There are mistakes. This is a mistake." (San Jose Mercury News 21 Dec 2001)

http://www.siliconvalley.com/docs/news/svfront/secur122101.htm

Category 21 Quality assurance failures (general)

2001-12-26 QA quality assurance buffer overflow programming flaws language design compiler

RISKS 21 84

Henry Baker and Peter G. Neumann began a discussion of buffer overflows as a root cause of quality assurance problems world wide. Some highlights from Baker's essay:

- * I'm no fan of lawyers or litigation, but it's high time that someone defined "buffer overflow" as being equal to "gross criminal negligence".
- * If buffer overflows are ever controlled, it won't be due to mere crashes, but due to their making systems vulnerable to hackers. Software crashes due to mere incompetence apparently don't raise any eyebrows, because no one wants to fault the incompetent programmer (and his incompetent boss). So we have to conjure up "bad guys" as "boogie men" in (hopefully) far-distant lands who "hack our systems", rather than noticing that in pointing one finger at the hacker, we still have three fingers pointed at ourselves.

Highlights from Dr Neumann's response:

- * ...[A]n expressive programming language that prevents you from doing bad things would with very high probability be misused even by very good programmers and especially by programmers who eschew discipline; and use of a badly designed programming language can result in excellent programs if done wisely and carefully.
- * ... [I]t would be very helpful if designers of modern programming languages, operating systems, and application software would more judiciously observe the principles that we have known and loved lo these many years (and that some of us have even practiced!). Take a look at my most recent report, on principles and their potential misapplication, for DARPA's Composable High-Assurance Trustworthy Systems (CHATS) program, now on my Web site:

http://www.csl.sri.com/neumann/chats2.html

[This discussion went on for weeks and can be followed in subsequent issues of RISKS.]

Category 21	Quality assurance failures (general)		
2002-01-04	QA quality assurance automated teller machines ATM bank data corruption error bug		
RISKS		21	84

Paul van Keep reported to RISKS on a drastic programming error in the Netherlands just as the currency switched to

"About 51,000 customers who withdrew money from their ING Bank account on 1 & 2 Jan 2002 (through an ATM) have had the wrong amount debited from their account. The bank hasn't yet given an explanation for the error other than to suspect that it was related to the high stress their systems were under during the first few days of the new year. The amounts debited from customer accounts was a hundred times what they withdrew from the ATMs. This got some people into trouble when their balance went negative and they could no longer use their bank PIN card to pay with in shops. ING Bank corrected the error yesterday."

Category 21 Quality assurance failures (general)

2002-01-06 QA quality assurance Euro conversion

RISKS 21 86

Clive Page told RISKS readers of a serious quality assurance problem in England: "Although the UK is one of the three European Union countries not to have adopted the Euro, many large retailers in the UK announced that they would accept them, but would give change in pounds sterling. Among these was the Debenhams chain of department stores. . . Robert Sheilds, a 15-years old Luton schoolboy, decided he would like experience of using Euro, so he changed 10 pounds to Euro at a bank, and went on to his local branch of Debenhams to spend them. He found that they had programmed their tills as if there were 1.6 pounds to the Euro rather than 1.6 Euro to the pound, but none of the sales assistants was experienced enough to notice the error. So after his initial purchase, he still had more than 10 pounds in change. He tried to tell the store staff of their mistake, but they said the rate was programmed into the computer, and nobody had the authority to change it. So he carried on spending, and after two hours, ended up with 130 pounds of goods, and 20 pounds in cash. At this point the store manager asked him to leave, saying «I think you've had your fun». Richard then took a train to Bedford (about 20 miles away) to try his luck at another branch, but by this time staff had been alerted, and refused all Euro transactions."

Category 21 Quality assurance failures (general)

2002-01-10 QA quality assurance design support flaws features failures incompetence stupidity foolishness crash data corruption

RISKS 21 86

Rex Black wrote in to RISKS with an off-the-top-of-his-head list of obvious quality assurance and design failures and bloopers from his recent experience. Some key points summarized (not literal quotes) from his list:

- * Too many programs are written with no consideration of the possibility of data corruption in their data files. They ought to have recovery capabilities.
- * Products are designed so that there are sometimes no error or diagnostic messages at all when they fail.
- * Automatic updates of software can sometimes wipe out laboriously constructed configurations, making the updated version useless.
- * Long-established problems that are known to technical support fail to make into even the electronic read-me files for their products.
- * "The daily (or more often) crash that my Windows Me laptop computer subjects me to, generally without warning, usually losing a good fifteen minutes worth of work. I guess I should learn to save every thirty seconds?"

Mr Black ends with, "If experienced people like me have problems like this, imagine the average computer user who has no idea whatsoever about what is going on when her system screws up. And why should they have to understand a computer to use them? (Don Norman, in his book *The Invisible Computer*, discusses this situation at length.) Ultimately, a computer is a tool, nothing more, nothing less. I think we have a long way to go before we can claim levels of quality consistent with what the makers of almost any other tool could claim."

Category 21 Quality assurance failures (general)

2002-01-16 QA quality assurance data input bounds checking limits edits output verification

RISKS 21 87

Carl Fink contributed this gem to RISKS: "A Georgetown, TX man who had arranged for his water bill to be automatically debited from his bank account alertly noticed that his monthly bill was for over \$21,000. (If he hadn't noticed, the debit would have happened, causing him to bounce multiple checks before the error was corrected.) When he told the city of the problem, «They said there was absolutely nothing they could do to stop the automated debit, and it was out of their hands.» Their solution was to send a city employee with a check for \$21,000 to reimburse their customer!

http://www.austin360.com/statesman/editions/tuesday/metro state 1.html

Risks? Lack of sanity checking on a new billing system springs to mind. Lack of any way to correct errors is also quite prominent.

Category 21 Quality assurance failures (general)

2002-02-01 quality assurance security reliability development Microsoft oxymoron

NewsScan

GATES REFLECTS ON FUTURE HOPES AND PAST SINS [12 Nov 2001]

Microsoft Chairman Bill Gates says his two top priorities now are improving the reliability of his company's software and conquering the market for "tablet" computers, the laptop-size computers that can be used like a clipboard. The tablets can be written on with a special stylus, and the writing is then treated by Microsoft software as though the words had been typed. Gates says tablet PCs will overtake laptops by 2005. As for software reliability, Gates is repentant: "We're doing a little bit of mea culpa on this. These are areas where Microsoft needs to improve. It affects the way we develop code." (USA Today 12 Nov 2001)

http://www.usatoday.com/life/cyber/tech/review/2001-11-12-comdex-gates.htm

MICROSOFT MAKES SECURITY A TOP PRIORITY [16 Jan 2002]

Microsoft Chairman Bill Gates says it's time to shift away from focusing on features to ensuring more security and privacy. Calling the new initiative "Trustworthy Computing," Gates wrote in an e-mail to employees, "When we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize security right out of the box." Gates also emphasized that privacy should be a concern: "Users should be in control of how their data is used. It should be easy for users to specify appropriate use of their information, including controlling the use of e-mail they send." The new focus comes on the heels of a widely publicized security flaw in its flagship Windows XP program. (CNet News.com 16 Jan 2002)

http://news.cnet.com/news/0-1003-200-8509737.html?tag=mn hd

MICROSOFT HIRES SECURITY SPECIALIST [1 Feb 2002]

Microsoft has hired a top security expert who will oversee the development of company strategies to enhance the security of Microsoft's products, services and infrastructure. Scott Charney, a principal for PricewaterhouseCoopers' Cybercrime Prevention and Response Practice, called his new job "in a word, irresistible." Microsoft CTO Craig Mundie said Charney would be a valuable addition to the company: "As one of the industry's top computer security experts, Scott has wide-ranging experience in cybercrime and computer forensics, which will make him an essential member of Microsoft's Trustworthy Computing leadership team." (AP 1 Feb 2002) http://apnews.excite.com/article/20020201/D7HD1SFO0.html

Quality assurance (security products)

Category 22 Quality assurance (security products)

2001-04-23 hacker challenge firewall QA quality assurance promotion gimmick backfire

failure penetration

RISKS 21 36

Jay Anantharaman reported in RISKS on a hacker challenge gone wrong: "A team of computer hackers has gained 35,000 pounds for hacking into a computer system just twenty-four hours after the competition began. Argus Systems organised the competition – to break into a Web server locked down using its security product called PitBull – to promote its products and to coincide with the start of Infosec, the UK's premier computer security event. Undeniably, the stunt backfired and is an embarrassment for Argus Systems Group, as well for as security consultant firm Integralis and hardware vendor Fujitsu Siemens, which helped organise the stunt and have coordinated three similar competitions in the US and Germany without suffering setbacks."

Category 22 Quality assurance (security products)

2001-04-29 virus operations security production software infection QA quality assurance

embarrassment

RISKS 21 37

Dave Stringer-Calvert reported in RISKS that Microsoft security fixes were infected with FunLove virus upon release. "A virus infection of security fix files on Microsoft's partner and premier support Web sites has forced the software giant to suspend certain downloads for more than a fortnight. Microsoft issued an alert on Monday, which states that various Hotfix files on its Premier Support and Microsoft Gold Certified Partners Web sites are infected with the FunLove virus. A copy of the notice said Microsoft has stopped access 'in order to protect customers' to an unspecified number of files, and expects to be able to restore access later today [29 Apr 2001]. Customers were advised to contact their technical account manager in the interim."

Category 22 Quality assurance (security products)

2001-06-13 bug tracking database error QA quality assurance incorrect data corruption

transcription dissemination validation validity integrity

RISKS 21 49

Uwe Ohse was able to compare his original bug posting about a particular problem with the version of his report in the SecurityFocus Vulnerability Database; to his distaste, he "found a number of errors in the database entry. The vulnerability in question is a local one, not a remotely exploitable bug. The bug database got it exactly the other way round. The database entry states the bug exists in version 1.0, but not in 1.0.1 to .3. This is wrong - the bug exists in version 1.1.0 (i don't know about older versions). There are other minor incorrect information."

Category 22 Quality assurance (security products)

2001-07-20 password change programming design error rejection false negative logic

RISKS 21 53

A RISKS correspondent reported on a flaw with general applicability for all security systems: don't change the rules on password composition when receiving existing passwords.

Philip Bragg explained that the original password for a digital certificate allowed non-alphanumeric characters; however, after a software change, the Web site form that asks users to log on with their old (or new) passwords explicitly forbids non-alphanumeric characters in the input field. Interestingingly, entering a bad password leads to an error message, whereas entering the correct password leads to "a mostly blank and useless page." Mr Bragg notes, "If the system knows I am using the correct passphrase why won't it let me renew my certificate?"

Web designers take note.

Category 22 Quality assurance (security products)

2002-03-10 buffer overflows vulnerabilities ICAT CVE

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported 240 vulnerabilities involving buffer overflows out of a total of 1241 for the period from 1 Jan 2001 to 10 Mar 2002. This represents about 19% of all vulnerabilities logged for that period. Overall, for the entire period since the CVE began recording vulnerabilities in 1995, buffer overflows are named in 737 of the 3677 vulnerabilities or about 20% of the total.

Availability issues (not denial-ofservice attacks)

Category 23 Availability issues (not denial-of-service attacks)
2000-12-28 availability outage infrastructure

RISKS 21 18

Glenn C. Lasher Jr. reported in RISKS' "On Thursday, 28 November 2000, 17 of the 21 telephone exchanges in the City of Schenectady NY were taken out of service by a water-main break (for those not familiar with the North American phone system, exchanges uniformly contain a range of 10,000 phone numbers). The Central Office serving downtown Schenectady is located on the block between Franklin and State Streets and Jay and Clinton Streets. The water main break was on Clinton St, and caused the closure of Clinton and State Streets. The break occurred at 3 AM, and the phones went out around 9 AM.

The cellular telephone networks appear to be unable to cope with the additional traffic. I received a frantic call from my wife, who called me at work from her cell phone to tell me the house phone was out. The signal quality was extraordinarily bad, as is the nature of CDMA digital when the cell is overloaded. One is left to assume that users of FDMA and TDMA-based phones may have been cut off completely, especially analog phone users, where the cells have a hard limit of 20 simultaneous calls."

The report continues with more details and an analysis of the situation that includes the following excellent points: "So, where do we begin on this one? Well, here are the RISKS:

- 1. Placement of mission-critical equipment below ground level leaves it susceptible to flooding. One might assume that an unusually heavy downpour might also have caused problems here.
- 2. This is a good example of network stress, looking at the behaviour of the cellular networks.
- 3. This is also a classic demonstration of a single point of failure. A problem in one location has cut off a critical service to an entire (although small) city. It does not matter if your service is through the IBOC (Verizon, in this area) or a CLEC (Sprint, AT&T, Met Tel, to name a few), all fo the equipment is owned and maintained by the IBOC and housed at the corner of Franklin and Clinton.
- 4. It is also a classic demonstration of diverse paths, as my Internet service continues to run. It does not pass through that same building, but is rather located a mile away on Eastern Parkway (or at least I believe that is the location). "

Category 23 Availability issues (not denial-of-service attacks)
2001-01-04 availability mystery down time bank crash ATM bank machines
RISKS 21 18

Ulf Lindqvist reported to RISKS, "As reported in various Swedish news media, The Swedish bank Nordbanken has suffered repeated computer outages during late December and early January. The outages, each with a duration of several hours, shut down ATMs, Internet bank services, debit card purchases and office teller services for Nordbanken's 3.5 million customers.

In an article on the Swedish CNN Web site (cnn.passagen.se) 4 Jan 2001, Nordbanken CEO Magnus Falk says that the bank still does not know what caused the outages, but that they are now able to restart their system faster the next time it crashes... "

Category 23 Availability issues (not denial-of-service attacks)

2001-01-10 automated teller machines ATM single point failure operations security backup

availability financial network

RISKS 21 20

Andre Oppermann reported in RISKS that "On the day before Christmas Eve, usually the day with the highest turnover of the year in all shops, the whole Swiss debit-card (EC-Card) processing system of Telekurs broke down for more than two hours. Also getting Money from ATM's and the processing of on-line MasterCard credit card payments, which is handled by the same company, was interrupted." The cause: "...[On] Saturday 23 Dec 2000 at 13:15, a tape robot in an automated tape library in the data center of Telekurs, the sole operator of all EC card transactions, drops a tape on the floor which in turn leads to an error propagation which shuts down the whole EC and MasterCard card processing for approximately two and a half hours until 15:25." Oppermann noted that this was another example of a single point of failure and of poor business continuity planning.

Category 23 Availability issues (not denial-of-service attacks)

2001-01-22 availability power fluctuation outage generators calibration

NewsScan

CAN SILICON VALLEY SURVIVE ENERGY CRISIS?

Rolling blackouts are wreaking havoc on the high-tech companies that form the bedrock of the Silicon Valley, and some are wondering how long they can rely on emergency back-up generators to keep their enterprises going. The blackouts have prompted talks between the Silicon Valley Manufacturing Group and state and local legislators regarding both short- and long-term fixes for the energy crisis. "What I've heard from many executives is, we want to stay and prosper in Silicon Valley," says Carl Guardino, president and CEO of the SVMG. "Yet at the same time, there's a very real recognition that if you do not have a reliable source of power and your products go down, it becomes extremely difficult to prosper." As one manufacturing firm COO puts it, "The loss of power for a few hours may not be a big problem, but recalibrating the equipment is." (EE Times 19 Jan 2001) http://www.techweb.com/wire/finance/story/INV20010119S0015

Category 23 Availability issues (not denial-of-service attacks)

2001-01-25 availability failure operations

NewsScan

MICROSOFT SITES DOWN 24 HOURS AS RESULT OF 'OPERATIONAL ERROR'

Various Microsoft Web sites, including MSN.com, MSNBC.com, and Microsoft.com, were down about 24 hours beginning Tuesday night, and a company spokesman emphasized that the problem was not with vandalism or with defects in Microsoft systems: "This was an operational error, and not the result of any issue with Microsoft or third-party products, nor the security of our networks." Security consultant Mark Loveless remarked: "If you look at how the Internet works at a really low level, it's a miracle anyone can get to anything. The thing is just so fragile." (Washington Post 25 Jan 2001)

http://washingtonpost.com/wp-dyn/articles/A43208-2001Jan24.html

Category 23 Availability issues (not denial-of-service attacks)

2001-03-10 availability theft backhoe attack single point of failure network

RISKS 21 27

Gregory Soo reported in RISKS on another network interruption (as abstracted by Peter G. Neumann), "Another copper-theft attempt shut down the Rogers@Home cable Internet service in Canada on 8Mar2001 for over 12 hours, although the thieves wound up only with fiber-optic cable carrying Internet traffic to a U.S. backbone. Over 300,000 Ontario subscribers were affected, because of an outdated backup system and a single-point vulnerability. [Source: Vito Pilieci, *The Ottawa Citizen*, 10Mar2001, Rogers@Home: First cut is the deepest. Rogers admits 'rather outdated' network vulnerable to bumbling thieves."

http://www.ottawacitizen.com/hightech/010310/5075158.html

The RISKS moderator added: "[Coppers, robbers, backups, backbones, backhoes, back to basics. PGN]"

A later report added that exposed communications were attacked by unidentified rodents while workers were trying to repair the damage caused by the stupid thieves who couldn't tell the difference between copper cable and fiber-optic cable. Apparently the rodent cut service to some 300,000 network subscribers in the Niagara peninsula.

Category 23 Availability issues (not denial-of-service attacks)
2001-03-21 undersea cable break availability accident costs

RISKS 21 30

According to _The Shanghai Daily_ of Mar 21, 2001, Korean-developed fishing nets that use anchors have been wreaking havoc with Chinese cybersurfers' access to the, ah, 'Net. The anchors rip through undersea cables when they are dragged up to several miles during strong tides; such accidents have repeatedly destroyedand then repaired at great expense. An article from _The Australian_, "The first serious break occurred on 9 Feb 2001 about 370km off China's coast, severing the main Internet link between China and the US. Although communications were partially restored during a repair process that stretched over two weeks, 22.5 million customers, including many in Shanghai, suffered slow service, the paper reported. On 9 Mar, the Internet backbone linking Taiwan and Shanghai was cut by a fishing net about 120km south of the city, affecting four million users. When that split was finally repaired on 19 Mar, authorities found another break in the undersea cable that will disrupt Internet services for a further two weeks. Each break costs about six million UN (\$1.4 million) to repair, in addition to unknown business losses resulting from the Internet disruptions."

Category 23 Availability issues (not denial-of-service attacks)

2001-03-27 antivirus software performance degradation operating system design quality

assurance

RISKS 21 32

Joaquim Baptista found that his Windows-based antivirus program was seriously interfering with processing on his Windows 2000 server. For example, "processing involving a 53MB RTF file consumed after 3 hours of CPU" until he turned off the antivirus. Then the process completed in 15 minutes. He pointed out that running virus-prone Windows and its necessary antivirus products can delay "the computation at least 24 times, and the Pentium 700 becomes less than a Pentium 30! Linux suddenly seems a lot cheaper!"

Category 23 Availability issues (not denial-of-service attacks)

2001-04-01 wireless communications spectrum shortage availability regulation

NewsScan

U.S. AGENCIES WARN OF SPECTRUM SHORTAGE

The U.S. Commerce Department, Defense Department and the Federal Communications Commission issued reports last week warning that there isn't enough radio spectrum to readily accommodate companies seeking to develop new wireless Internet services. The reports came in response to a request by the Clinton administration last year to review options for relocating some traditional government and industry uses of the radio spectrum to make way for so-called third generation (3G) wireless services. Officials at the Commerce Department and the Pentagon said they could identify only about 45 megahertz out of the 140 MHz studied, and that it would cost about \$2 billion in engineering and other changes to free it up. Meanwhile, the FCC examined 190 MHz now used by schools and fixed wireless providers, but said any change would disrupt those services. Commerce Secretary Donald Evans said he was committed to finding a solution to the spectrum impasse, but a Pentagon official said the wireless industry has yet to prove that it really needs more spectrum. (Wall Street Journal 2 Apr 2001) http://interactive.wsj.com/articles/SB986160719120388594.htm (sub req'd)

Category 23 Availability issues (not denial-of-service attacks)

2001-04-27 availability artificial intelligence AI

NewsScan

IBM PROJECT TO DEVELOP SELF-MONITORING SERVERS

IBM will devote one-fourth of its research & development budget to a project called eLiza, aimed at perfecting e-commerce server computers that, without intervention by human operators, will be able to detect and fix system problems, automatically install new software updates, perform load-balancing and security checks, and call on redundant systems to fill in for failing components. The company says that the new servers will be as easy to operate as a kitchen appliance, even though they will have processing power hundreds of times more power than the server computers of today. (AP/Washington Post 27 Apr 2001)

http://washingtonpost.com/wp-dyn/business/latestap/A9273-2001Apr27.html

Category 23 Availability issues (not denial-of-service attacks)

2001-07-06 availability network logon failure

NewsScan

PROBLEMS FOR MSN MESSENGER

Log-on problems were experienced this week by about one third of the more than 18 million people who use Microsoft Messenger, a free service that allows users to send instant text messages via the Internet to communicate individuals in their personal address books or "buddy lists." A Gartner Inc. analyst said philosophically: "They're certainly not the only ones who have had those kinds of problems. Computers and technology are not infallible." (San Jose Mercury News 6 Jul 2001)

Category 23 Availability issues (not denial-of-service attacks)

2001-07-19 availability accident fiber optic Internet backbone bandwidth throughput traffic

NewsScan

TUNNEL FIRE DERAILS INTERNET SERVICE

Derailed train cars burning in a Baltimore tunnel have seriously damaged the area's fiber-optic cables, slowing Internet service and other communications traffic in the Mid-Atlantic states, with a ripple effect across the country. WorldCom, PSINet and AboveNet all reported problems with service, but said they had not yet been able to quantify the severity of the problems. Keynote Systems, which measures Web site performance, said the delay experienced by Internet users was the worst it has ever seen. "What we're seeing is a problem in the handshake between the backbones which serve as the Internet's infrastructure," said a Keynote spokeswoman. "These backbone providers hand off traffic to travel between them across the country." Keynote reported major slowdowns as far away as Seattle and Los Angeles that may be attributable to the train wreck. (AP Jul 19 2001)

http://news.excite.com/news/ap/010719/18/train-derailment-communications

Category 23 Availability issues (not denial-of-service attacks)

2002-02-15 availability denial of service quality assurance service level agreement contractual obligation liability e-mail delivery reliability

NewsScan

COMCAST: 'NOT 100% READY' TO DEAL WITH CUSTOMER PROBLEMS [4 Jan 2002]

Internet service problems were experienced by about 10% of 71,000 Comcast Cable customers in North Jersey who had been transferred to Comcast's own network after the failure of one offered by Excite@Home. "These kinds of problems are very typical when you're launching something new... Our folks were dealing with a large amount of calls at a single point in time. There were some early folks we brought on that were not 100% ready for everything customers were asking," says a company spokesperson. (New York Times 4 Jan 2002) http://partners.nytimes.com/2002/01/04/technology/04COMC.html

COMCAST PROBLEMS AFFECT DELIVERY OF 300,000 MESSAGES [15 Feb 2002]

Comcast, the cable company and Internet service provider, said yesterday it would "work around the clock" to fix a technical problem that slowed delivery of 300,000 subscriber messages. Industry observers remember that when Excite@Home was on the way to declaring bankruptcy last year it had tried forcefully to make the point that cable companies Comcast and AT&T did not understand the complexity and costs of operating an Internet business. (New York Times 15 Feb 2002)

http://partners.nytimes.com/2002/02/15/technology/15PRIV.html

24.1 Java

Category 24.1 Java

Java cookies protocol vulnerability exposure confidentiality penetration patch

repair bug QA quality assurance

RISKS 21 76

A RISKS correspondent reported, "A flaw was discovered in the way Internet Explorer's about: protocol handles javascript requests, enabling a malicious web site to gain access to cookie information on the client's hard drive." http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=discussion&id=3513 http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-055.asp

Category 24.1 Java

2002-03-10 Java vulnerabilities ICAT CVE

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported the following vulnerabilities involving Java for the period from 1 Jan 2001 to 10 Mar 2002:

CAN-2000-1117: The Extended Control List (ECL) feature of the Java Virtual Machine (JVM) in Lotus Notes Client R5 allows malicious web site operators to determine the existence of files on the client by measuring delays in the execution of the getSystemResource method. Published Before: 1/9/2001 Severity: Low

CAN-2001-0068: Mac OS Runtime for Java (MRJ) 2.2.3 allows remote attackers to use malicious applets to read files outside of the CODEBASE context via the ARCHIVE applet parameter. Published Before: 2/12/2001 Severity: Medium

CAN-2001-0186: Directory traversal vulnerability in Free Java Web Server 1.0 allows remote attackers to read arbitrary files via a .. (dot dot) attack. Published Before: 5/3/2001 Severity: High

CAN-2001-0297: Directory traversal vulnerability in Simple Server HTTPd 1.0 (originally Free Java Server) allows remote attackers to read arbitrary files via a .. (dot dot) in the URL. Published Before: 5/3/2001 Severity: Low

CAN-2001-0307 Summary: Bajie HTTP JServer 0.78 allows remote attackers to execute arbitrary commands via shell metacharacters in an HTTP request for a CGI program that does not exist. Published Before: 5/3/2001 Severity: Medium

CAN-2001-0308: UploadServlet in Bajie HTTP JServer 0.78 allows remote attackers to execute arbitrary commands by calling the servlet to upload a program, then using a ... (modified ..) to access the file that was created for the program. Published Before: 5/3/2001 Severity: Medium

CAN-2001-0324: Windows 98 and Windows 2000 Java clients allow remote attackers to cause a denial of service via a Java applet that opens a large number of UDP sockets, which prevents the host from establishing any additional UDP connections, and possibly causes a crash. Published Before: 5/3/2001 Severity: High

CAN-2001-0926: SSIFilter in Allaire JRun 3.1, 3.0 and 2.3.3 allows remote attackers to obtain source code for Java server pages (.jsp) and other files in the web root via an HTTP request for a non-existent SSI page, in which the request's body has an #include statement. Published Before: 11/28/2001 Severity: Medium

CAN-2001-1008: Java Plugin 1.4 for JRE 1.3 executes signed applets even if the certificate is expired, which could allow remote attackers to conduct unauthorized activities via an applet that has been signed by an expired certificate. Published Before: 8/31/2001 Severity: High

CVE-2000-1099: Java Runtime Environment in Java Development Kit (JDK) 1.2.2_05 and earlier can allow an untrusted Java class to call into a disallowed class, which could allow an attacker to escape the Java sandbox and conduct unauthorized activities. Published Before: 1/9/2001 Severity: Medium

CVE-2001-0126: Oracle XSQL servlet 1.0.3.0 and earlier allows remote attackers to execute arbitrary Java code by redirecting the XSQL server to another source via the xml-stylesheet parameter in the xslt stylesheet. Published Before: 3/12/2001 Severity: High

CVE-2001-0137: Windows Media Player 7 allows remote attackers to execute malicious Java applets in Internet Explorer clients by enclosing the applet in a skin file named skin.wmz, then referencing that skin in the codebase parameter to an applet tag. Published Before: 3/12/2001 Severity: High

24.2 Javascript

Category 24.2 Javascript
2001-02-13 e-mail address capture spyware Web privacy JavaScript
RISKS 21 24

Stewart C. Russell reported to RISKS on unauthorized e-mail address capture while browsing:

> I was looking at an estate agent's (realtor's) website when I noticed the status line on my browser saying "Contacting < mailserver > " then "Message Sent". I looked through the site's HTML code and there was a little piece of JavaScript which appeared to send an e-mail message to the site's owner with no intervention from me. This service is provided by http://www.siteguest.com/, who describe it as "Caller ID for your web site".

Sure enough, in the next few days I started to get a number of e-mails from this realtor promising the best deals on houses. I'd prefer to choose who gets my e-mail address, and the behaviour of this particular individual has pretty much guaranteed no business from me.

The risk? The usual JavaScript and security warnings should be on, and that combining web and mail functions in one program is not always a good idea. <

Category 24.2 Javascript

2002-03-10 JavaScript vulnerabilities ICAT CVE

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported the following vulnerabilities involving JavaScript for the period from 1 Jan 2001 to 10 Mar 2002:

CAN-2001-0365: Eudora before 5.1 allows a remote attacker to execute arbitrary code, when the 'Use Microsoft Viewer' and 'allow executables in HTML content' options are enabled, via an HTML email message containing Javascript, with ActiveX controls and malicious code within IMG tags. Published Before: 6/27/2001 Severity: High

CAN-2001-0596: Netscape Communicator prior to 4.77 allows a remote attacker to execute arbitrary javascript via specially crafted GIF images. The javascript is embedded in the GIF file as a comment. Published Before: 8/2/2001 Severity: High

CAN-2001-0722: Internet Explorer 5.5 and 6.0 allows remote attackers to read and modify user cookies via Javascript in an about: URL. Published Before: 12/6/2001 Severity: Medium

CAN-2001-0723: Internet Explorer 5.5 and 6.0 allows remote attackers to read and modify user cookies via Javascript, aka the "Second Cookie Handling Vulnerability." Published Before: 11/14/2001 Severity: Medium

CAN-2001-0743: Paging function in O'Reilly WebBoard Pager 4.10 allows remote attackers to cause a denial of service via a message with an escaped 'character followed by JavaScript commands. Published Before: 10/18/2001 Severity: Medium

CAN-2001-0745: Netscape 4.7x allows remote attackers to obtain sensitive information such as the user's login, mailbox location and installation path via Javascript that accesses the mailbox: URL in the document.referrer property. Published Before: 10/18/2001 Severity: Medium

CAN-2001-0824: Cross-site scripting vulnerability in IBM WebSphere 3.02 and 3.5 FP2 allows remote attackers to execute Javascript by inserting the Javascript into (1) a request for a .JSP file, or (2) a request to the webapp/examples/directory, which inserts the Javascript into an error page. Published Before: 12/6/2001 Severity: High

CAN-2001-0828: A cross-site scripting vulnerability in Caucho Technology Resin before 1.2.4 allows a malicious webmaster to embed Javascript in a hyperlink that ends in a .jsp extension, which causes an error message that does not properly quote the Javascript. Published Before: 12/6/2001 Severity: High

CAN-2001-0829: A cross-site scripting vulnerability in Apache Tomcat 3.2.1 allows a malicious webmaster to embed Javascript in a request for a .JSP file, which causes the Javascript to be inserted into an error message. Published Before: 12/6/2001 Severity: High

CAN-2001-0898: Opera 6.0 and earlier allows remote attackers to access sensitive information such as cookies and links for other domains via Javascript. Published Before: 11/15/2001 Severity: Medium

CAN-2001-0919: Internet Explorer 5.50.4134.0100 on Windows ME with "Prompt to allow cookies to be stored on your machine" enabled does not warn a user when a cookie is set using Javascript, Published Before: 11/26/2001 Severity: High

CAN-2001-0987: Cross-site scripting vulnerability in CGIWrap before 3.7 allows remote attackers to execute arbitrary Javascript on other web clients by causing the Javascript to be inserted into error messages that are generated by CGIWrap. Published Before: 7/22/2001 Severity: High

CVE-2001-0148: The WMP ActiveX Control in Windows Media Player 7 allows remote attackers to execute commands in Internet Explorer via javascript URLs, a variant of the "Frame Domain Verification" vulnerability. Published Before: 6/2/2001 Severity: High

CVE-2001-0149: Windows Scripting Host in Internet Explorer 5.5 and earlier allows remote attackers to read arbitrary files via the GetObject Javascript function and the htmlfile ActiveX object. Published Before: 6/2/2001 Severity: High

24.3 ActiveX

Category 24.3 ActiveX

2002-03-10 ActiveX vulnerabilities ICAT CVE

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported the following vulnerabilities involving ActiveX for the period from 1 Jan 2001 to 10 Mar 2002:

CAN-2000-1105: The ixsso.query ActiveX Object is marked as safe for scripting, which allows malicious web site operators to embed a script that remotely determines the existence of files on visiting Windows 2000 systems that have Indexing Services enabled. Published Before: 1/9/2001 Severity: Medium

CAN-2001-0365: Eudora before 5.1 allows a remote attacker to execute arbitrary code, when the 'Use Microsoft Viewer' and 'allow executables in HTML content' options are enabled, via an HTML email message containing Javascript, with ActiveX controls and malicious code within IMG tags. Published Before: 6/27/2001 Severity: High

CAN-2001-0538: Microsoft Outlook View ActiveX Control in Microsoft Outlook 2002 and earlier allows remote attackers to execute arbitrary commands via a malicious HTML e-mail message or web page. Published Before: 8/14/2001 Severity: High

CAN-2002-0022: Buffer overflow in the implementation of an HTML directive in mshtml.dll in Internet Explorer 5.5 and 6.0 allows remote attackers to execute arbitrary code via a web page that specifies embedded ActiveX controls in a way that causes 2 Unicode strings to be concatenated. Published Before: 3/8/2002 Severity: High

CVE-2001-0090: The Print Templates feature in Internet Explorer 5.5 executes arbitrary custom print templates without prompting the user, which could allow an attacker to execute arbitrary ActiveX controls, aka the "Browser Print Template" vulnerability. Published Before: 2/16/2001 Severity: High

CVE-2001-0091: The ActiveX control for invoking a scriptlet in Internet Explorer 5.0 through 5.5 renders arbitrary file types instead of HTML, which allows an attacker to read arbitrary files, aka a variant of the "Scriptlet Rendering" vulnerability. Published Before: 2/16/2001 Severity: Medium

CVE-2001-0148: The WMP ActiveX Control in Windows Media Player 7 allows remote attackers to execute commands in Internet Explorer via javascript URLs, a variant of the "Frame Domain Verification" vulnerability. Published Before: 6/2/2001 Severity: High

CVE-2001-0149: Windows Scripting Host in Internet Explorer 5.5 and earlier allows remote attackers to read arbitrary files via the GetObject Javascript function and the htmlfile ActiveX object. Published Before: 6/2/2001 Severity: High

CVE-2001-0434: The LogDataListToFile ActiveX function used in (1) Knowledge Center and (2) Back web components of Compaq Presario computers allows remote attackers to modify arbitrary files and cause a denial of service. Published Before: 7/2/2001 Severity: High

HTML 24.4

Category 24.4 HTML

2001-01-23 cross-site scripting vulnerability Web

RISKS 21 22

Michael Sims reported cross-site scripting vulnerabilities on the News.com (CNET) Web site. Users were able to insert arbitrary headlines on the Web site; e.g., Sims wrote, "http://news.cnet.com/news/topic/0-1003-249-0.html?title = CNET%20Editors%20Agree:%20Slashdot%20is%20a%20better%20news%20site%20than%20News.com&topics and the contraction of the contractioopic=slashdot"

Sims wrote, "CNET was notified six hours before this e-mail was sent to RISKS; they have not replied at this time or taken any corrective action."

Category 24.4 HTML

2001-10-02 html malicious code programming Web site hijacking misspellings

cybersquatting fraud court case injunction diversion advertising pornography

NewsScan

COURT SHUTS DOWN THOUSANDS OF WEB SITES

A U.S. court shut down more than 5,500 Web sites operated by John Zuccarini of Andalusia, Penn., after it determined that the sites illegally diverted Web surfers from their intended destinations and forced them to download pop-up ads for pornography and gambling. Zuccarini had registered many misspellings of popular sites, including 41 variations on "Britney Spears," in a strategy to corral sloppy typists and bombard them with the unwanted ads. Visitors to Zuccarini's sites often could not leave without shutting down their systems, because the "back" button on their Web browsers was rigged to trigger more ads. (Reuters/Los Angeles Times 2 Oct 2001)

http://www.latimes.com/technology/la-000078749oct02.story?coll=la%2Dheadline s%2Dtechnology

Category 24.4 HTML

2001-12-11 html malicious code programming Web site hijacking flaw vulnerability browser

NewsScan

MICROSOFT FIXING SECURITY FLAW IN INTERNET EXPLORER [11 Dec 2001]

Finnish security researcher Jouko Pynnonen of Oy Online Solutions says that Microsoft is working on a software patch to fix a security vulnerability in Internet Explorer versions 5, 5.5, and 6, which would make it possible for a malicious intruder to exploit ordinary Web page code to bypass the browser's system for securely handling downloaded files. A Microsoft spokesperson declined to discuss the status of the browser patch at this time. (Newsbytes 11 Dec 2001)

http://www.newsbytes.com/news/01/172878.html

Category 24.4 HTML

2002-01-28 Web page hijacking URL user ID misleading trickery dissimulation spoofing

browser

RISKS 21 89

Rob Graham spotted a dangerous application of syntax in a URL that looked like this:

< http://www.microsoft.com&item=3Dq209354@hardware.no/nyheter/feb01/Q209354 %20%20HOWTO.htm >

The naïve users would assume that the URL is part of the microsoft.com domain; in fact, this syntax means that a user ID and password (the part in front of the @ sign) is being passed to the URL following the @ sign.

[MK notes: In testing this in March 2002 using MS IE6, I was taken directly to the "hardware.no" site, where a message read "This page has been removed after request from Microsoft. . . . " In contrast, using my preferred browser, Opera 6.01, I received a pop-up warning from the browser alerting me to the fact that the string "www.microsoft.com&item=3Dq209354" was in fact a user ID and password and asking if it was OK to proceed. Bravo Opera!]

Category 24.4 HTML

2002-03-10 HTML vulnerabilities ICAT CVE

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported the following vulnerabilities involving ActiveX for the period from 1 Jan 2001 to 10 Mar 2002:

CAN-2000-0898: Small HTTP Server 2.01 does not properly process Server Side Includes (SSI) tags that contain null values, which allows local users, and possibly remote attackers, to cause the server to crash by inserting the SSI into an HTML file. Published Before: 1/9/2001 Severity: Medium

CAN-2000-1172: Buffer overflow in Gaim 0.10.3 and earlier using the OSCAR protocol allows remote attackers to conduct a denial of service and possibly execute arbitrary commands via a long HTML tag. Published Before: 1/9/2001 Severity: High

CAN-2001-0322: MSHTML.DLL HTML parser in Internet Explorer 4.0, and other versions, allows remote attackers to cause a denial of service (application crash) via a script that creates and deletes an object that is associated with the browser window object. Published Before: 6/2/2001 Severity: Medium

CAN-2001-0365: Eudora before 5.1 allows a remote attacker to execute arbitrary code, when the 'Use Microsoft Viewer' and 'allow executables in HTML content' options are enabled, via an HTML email message containing Javascript, with ActiveX controls and malicious code within IMG tags. Published Before: 6/27/2001 Severity: High

CAN-2001-0389: IBM Websphere/NetCommerce3 3.1.2 allows remote attackers to determine the real path of the server by directly calling the macro.d2w macro with a NOEXISTINGHTMLBLOCK argument. Published Before: 7/2/2001 Severity: Medium

CAN-2001-0484: Tektronix PhaserLink 850 does not require authentication for access to configuration pages such as _ncl_subjects.shtml and _ncl_items.shtml, which allows remote attackers to modify configuration information and cause a denial of service by accessing the pages. Published Before: 6/27/2001 Severity: Medium

CAN-2001-0519: Aladdin eSafe Gateway versions 2.x allows a remote attacker to circumvent HTML SCRIPT filtering via a special arrangement of HTML tags which includes SCRIPT tags embedded within other SCRIPT tags. Published Before: 8/14/2001 Severity: Medium

CAN-2001-0520: Aladdin eSafe Gateway versions 3.0 and earlier allows a remote attacker to circumvent filtering of SCRIPT tags by embedding the scripts within certain HTML tags including (1) onload in the BODY tag, (2) href in the A tag, (3) the BUTTON tag, (4) the INPUT tag, or (5) any other tag in which scripts can be defined. Published Before: 8/14/2001 Severity: Medium

CAN-2001-0521: Aladdin eSafe Gateway versions 3.0 and earlier allows a remote attacker to circumvent HTML SCRIPT filtering via the UNICODE encoding of SCRIPT tags within the HTML document. Published Before: 8/14/2001 Severity: Medium

CAN-2001-0523: eEye SecureIIS versions 1.0.3 and earlier allows a remote attacker to bypass filtering of requests made to SecureIIS via the escaping of HTML characters within the request, which could allow a remote attacker to use restricted variables and perform directory traversal attacks on vulnerable programs that would otherwise be protected by SecureIIS. Published Before: 8/14/2001 Severity: Medium

CAN-2001-0538: Microsoft Outlook View ActiveX Control in Microsoft Outlook 2002 and earlier allows remote attackers to execute arbitrary commands via a malicious HTML e-mail message or web page. Published Before: 8/14/2001 Severity: High

CAN-2001-0726: Outlook Web Access (OWA) in Microsoft Exchange 5.5 Server, when used with Internet Explorer, does not properly detect certain inline script, which can allow remote attackers to perform arbitrary actions on a user's Exchange mailbox via an HTML e-mail message. Published Before: 12/6/2001 Severity: High

CAN-2001-0835: Cross-site scripting vulnerability in Webalizer 2.01-06, and possibly other versions, allows remote attackers to inject arbitrary HTML tags by specifying them in (1) search keywords embedded in HTTP referrer information, or (2) host names that are retrieved via a reverse DNS lookup. Published Before: 12/6/2001 Severity: High

CAN-2001-0837: DeltaThree Pc-To-Phone 3.0.3 places sensitive data in world-readable locations in the installation directory, which allows local users to read the information in (1) temp.html, (2) the log folder, and (3) the PhoneBook folder. Published Before: 12/6/2001 Severity: Medium

CAN-2001-0874: Internet Explorer 5.5 and 6.0 allow remote attackers to read certain files via HTML that passes information from a frame in the client's domain to a frame in the web site's domain, a variant of the "Frame Domain Verification" vulnerability. Published Before: 12/13/2001 Severity: Medium

CAN-2001-0901: Hypermail allows remote attackers to execute arbitrary commands on a server supporting SSI via an attachment with a .shtml extension, which is archived on the server and can then be executed by requesting the URL for the attachment. Published Before: 11/19/2001 Severity: High

CAN-2001-0925: The default installation of Apache before 1.3.19 allows remote attackers to list directories instead of the multiview index.html file via an HTTP request for a path that contains many / (slash) characters, which causes the path to be mishandled by (1) mod_negotiation, (2) mod_dir, or (3) mod_autoindex. Published Before: 3/12/2001 Severity: Medium

CAN-2001-0948: Cross-site scripting (CSS) vulnerability in ValiCert Enterprise Validation Authority (EVA) 3.3 through 4.2.1 allows remote attackers to execute arbitrary code or display false information by including HTML or script in the certificate's description, which is executed when the certificate is viewed. Published Before: 12/4/2001 Severity: High

CAN-2001-1013: Apache on Red Hat Linux with with the UserDir directive enabled generates different error codes when a username exists and there is no public_html directory and when the username does not exist, which could allow remote attackers to determine valid usernames on the server. Published Before: 9/12/2001 Severity: Medium

CAN-2001-1019: Directory traversal vulnerability in view_item CGI program in sglMerchant 1.0 allows remote attackers to read arbitrary files via a .. (dot dot) in the HTML_FILE parameter. Published Before: 9/8/2001 Severity: Medium

CAN-2002-0022: Buffer overflow in the implementation of an HTML directive in mshtml.dll in Internet Explorer 5.5 and 6.0 allows remote attackers to execute arbitrary code via a web page that specifies embedded ActiveX controls in a way that causes 2 Unicode strings to be concatenated. Published Before: 3/8/2002 Severity: High

CAN-2002-0024: File Download box in Internet Explorer 5.01, 5.5 and 6.0 allows an attacker to use the Content-Disposition and Content-Type HTML header fields to modify how the name of the file is displayed, which could trick a user into believing that a file is safe to download. Published Before: 3/8/2002 Severity: High

CAN-2002-0025: Internet Explorer 5.01, 5.5 and 6.0 does not properly handle the Content-Type HTML header field, which allows remote attackers to modify which application is used to process a document. Published Before: 3/8/2002 Severity: Medium

CVE-2000-0897: Small HTTP Server 2.01 allows remote attackers to cause a denial of service by repeatedly requesting a URL that references a directory that does not contain an index.html file, which consumes memory that is not released after the request is completed. Published Before: 1/9/2001 Severity: Medium

CVE-2000-1187: Buffer overflow in the HTML parser for Netscape 4.75 and earlier allows remote attackers to execute arbitrary commands via a long password value in a form field. Published Before: 1/9/2001 Severity: High

CVE-2001-0002: Internet Explorer 5.5 and earlier allows remote attackers to obtain the physical location of cached content and open the content in the Local Computer Zone, then use compiled HTML help (.chm) files to execute arbitrary programs. Published Before: 7/21/2001 Severity: High

CVE-2001-0028: Buffer overflow in the HTML parsing code in oops WWW proxy server 1.5.2 and earlier allows remote attackers to execute arbitrary commands via a large number of " (quotation) characters. Published Before: 2/12/2001 Severity: High

CVE-2001-0089: Internet Explorer 5.0 through 5.5 allows remote attackers to read arbitrary files from the client via the INPUT TYPE element in an HTML form, aka the "File Upload via Form" vulnerability. Published Before: 2/16/2001 Severity: Medium

CVE-2001-0091: The ActiveX control for invoking a scriptlet in Internet Explorer 5.0 through 5.5 renders arbitrary file

types instead of HTML, which allows an attacker to read arbitrary files, aka a variant of the "Scriptlet Rendering" vulnerability. Published Before: 2/16/2001 Severity: Medium

CVE-2001-0130: Buffer overflow in HTML parser of the Lotus R5 Domino Server before 5.06, and Domino Client before 5.05, allows remote attackers to cause a denial of service and possibly execute arbitrary commands via a malformed font size specifier. Published Before: 3/12/2001 Severity: High

CVE-2001-0149: Windows Scripting Host in Internet Explorer 5.5 and earlier allows remote attackers to read arbitrary files via the GetObject Javascript function and the htmlfile ActiveX object. Published Before: 6/2/2001 Severity: High

CVE-2001-0154: HTML e-mail feature in Internet Explorer 5.5 and earlier allows attackers to execute attachments by setting an unusual MIME type for the attachment, which Internet Explorer does not process correctly. Published Before: 5/3/2001 Severity: Medium

CVE-2001-0243: Windows Media Player 7 and earlier stores Internet shortcuts in a user's Temporary Files folder with a fixed filename instead of in the Internet Explorer cache, which causes the HTML in those shortcuts to run in the Local Computer Zone instead of the Internet Zone, which allows remote attackers to read certain files. Published Before: 6/27/2001 Severity: Medium

CVE-2001-0340: An interaction between the Outlook Web Access (OWA) service in Microsoft Exchange 2000 Server and Internet Explorer allows attackers to execute malicious script code against a user's mailbox via a message attachment that contains HTML code, which is executed automatically. Published Before: 7/21/2001 Severity: High

CVE-2001-0457: man2html before 1.5-22 allows remote attackers to cause a denial of service (memory exhaustion). Published Before: 6/27/2001 Severity: Medium

24.5 E-mail & instant messaging / chat

Category 24.5 E-mail & instant messaging / chat

2001-07-23 e-mail bounce management ISP SMTP header

RISKS 21 56

Robert J. Woodhead suggested a useful improvement in list server software. Writing in RISKS, he explained that AOL bounce messages fail to include the _original_ destination address, making it impossible to fix mailing lists when someone redirects messages to another e-mail address. He wrote, "If mail servers added an "Original-Recipient:" header if they have to forward the e-mail (and there isn't already one in the headers), life would be immeasurably easier for bounce management. A standard for bounce reporting that made life easy for nonhumans would also seem to be an obvious idea."

Category 24.5 E-mail & instant messaging / chat

2002-01-04 denial-of-service DoS attack vulnerability servers instant messaging chat

NewsScan

AOL FIXES BUG IN INSTANT MESSENGER

AOL Time Warner says it has patched the software on its central servers to fix a problem in the free, downloadable version of the Windows versions of its Instant Messenger (AIM) software that could have allowed a network vandal to flood a victim's computer with data. (San Jose Mercury News 4 Jan 2002) http://www.siliconvalley.com/docs/news/svfront/aol010402.htm

Category 24.5 E-mail & instant messaging / chat

2002-03-10 e-mail chat vulnerabilities ICAT CVE

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported the following vulnerabilities involving e-mail or chat for the period from 1 Jan 2001 to 10 Mar 2002:

CAN-2001-0581: Spytech Spynet Chat Server 6.5 allows a remote attacker to create a denial of service (crash) via a large amount (> 100) of connections to port 6387. Published Before: 8/22/2001 Severity: Medium

CAN-2001-0615: Directory traversal vulnerability in Faust Informatics Freestyle Chat server prior to 4.1 SR3 allows a remote attacker to read arbitrary files via a specially crafted URL which includes variations of a '...' (dot dot) attack such as '...' or '....'. Published Before: 8/14/2001 Severity: Medium

CAN-2001-0616: Faust Informatics Freestyle Chat server prior to 4.1 SR3 allows a remote attacker to create a denial of service via a URL request which includes a MS-DOS device name (e.g., GET /aux HTTP/1.0). Published Before: 8/14/2001 Severity: Medium

CAN-2001-0726: Outlook Web Access (OWA) in Microsoft Exchange 5.5 Server, when used with Internet Explorer, does not properly detect certain inline script, which can allow remote attackers to perform arbitrary actions on a user's Exchange mailbox via an HTML e-mail message. Published Before: 12/6/2001 Severity: High

CAN-2001-0792: Format string vulnerability in XChat 1.2.x allows remote attackers to execute arbitrary code via a malformed nickname. Published Before: 10/18/2001 Severity: High

CAN-2001-0857: Cross-site scripting vulnerability in status.php3 in Imp Webmail 2.2.6 and earlier allows remote attackers to gain access to the e-mail of other users by hijacking session cookies via the message parameter. Published Before: 12/6/2001 Severity: Medium

CAN-2001-0945: Buffer overflow in Outlook Express 5.0 through 5.02 for Macintosh allows remote attackers to cause a denial of service via an e-mail message that contains a long line. Published Before: 12/3/2001 Severity: Medium

CVE-2000-1148: The installation of VolanoChatPro chat server sets world-readable permissions for its configuration file and stores the server administrator passwords in plaintext, which allows local users to gain privileges on the server. Published Before: 1/9/2001 Severity: Medium

CVE-2001-0154: HTML e-mail feature in Internet Explorer 5.5 and earlier allows attackers to execute attachments by setting an unusual MIME type for the attachment, which Internet Explorer does not process correctly. Published Before: 5/3/2001 Severity: Medium

24.6 Web-site infrastructure, general Web security issues

Category 24.6 Web-site infrastructure, general Web security issues

2001-03-16 e-commerce electronic data interchange EDI vulnerabilities weakness audit

government tax confidentiality integrity penetration

RISKS 21 28

Dave Stringer-Calvert, writing in RISKS, reported a finding by the GAO of lax security in IRS electronic filing systems:

"Even as the IRS was assuring taxpayers last year that electronic filing of tax returns was secure, serious shortcomings existed that could have allowed hackers to view and even change information on returns, a government watchdog agency said. The General Accounting Office found no evidence that hacking had occurred, but it said its investigators were able to gain unauthorized access to the tax agency's electronic filing system, which will handle a third of all federal returns this year. The GAO cited the IRS for lax security controls and for not requiring encryption of electronic returns. The report also said the IRS sent out \$2.1 billion in refunds to taxpayers whose returns were not properly authorized."

Category 24.6 Web-site infrastructure, general Web security issues
2001-05-01 buffer overflow QA quality assurance Web server

NIPC Daily Report

Microsoft has released security bulletin MS01-023 regarding a security flaw that could allow a hacker to gain complete control of a Web site running IIS 5.0 server software for Windows 2000. The security vulnerability results because the ISAPI extension contains an unchecked buffer in a section of code that handles input parameters. This could enable a remote attacker to conduct a buffer overrun attack and cause code of their choice to run on the server. Such code would run in the Local System security context. This would give the attacker complete control of the server. Additional information regarding this vulnerability can be found at

http://www.microsoft.com/technet/security/bulletin/MS01-023.asp. (Source: Microsoft Corporation, 1 May)

Category 24.6 Web-site infrastructure, general Web security issues

2001-05-02 criminal hacker tool exploit Web servers vulnerabilities rootkit patch

NIPC Daily Report

A hacker, using the name "Dark Spyrit," released a program on 2 May designed to exploit the security hole in Windows 2000 Web servers. The program will give anyone with limited technical knowledge the ability to completely control a Windows 2000 server running version 5 of Microsoft's Internet Information Server (IIS) Web software. The creation of the exploit code for the flaw came as no surprise to Microsoft. "Customers who have applied the patch don't have to worry," the company said in a statement. "Customers who haven't applied the patch should take this as a reminder to do so immediately." (Source: ZDNet News, 3 May) (NIPC Comment: The NIPC issued Advisory 01-011 on 2 May, reporting the vulnerability in Microsoft s Internet Information Services (IIS) 5.0. www.nipc.gov/warnings/advisories/2001/01-011.htm.)

Category 24.6 Web-site infrastructure, general Web security issues
2001-06-12 distributed computing Web design denial of service availability saturation
RISKS 21 48

Steve Loughran noted in RISKS that the SETI@home screensaver that does computations for the Search for Extraterrestrial Intelligence project inadvertently caused a problem when Internet access to the SETI@home site became inaccessible. Seems the screensaver repeatedly attempted to "phone home" and saturated the Network Address Translation (NAT) pool of addresses. Mr Loughran noted, "The article closes by saying the problem was "solved" by increasing the number of available NAT addresses, although of course that didn't fix the problem, merely caused it to 'go away'. A real solution would be to have the screen-saver software implement incremental backoff and other mechanisms designed to gracefully handle a complete loss of remote server access. One would hope that the authors of the next generation of distributed computation applications take heed of the lessons of the current batch."

However, a staff member from SETI@home noted later, "One of the risks of developing any software is that problems experienced by users will be associated with the design of the software, not the failure of other components. The GUI version of SETI@home, upon connection failure, retries the connection twice at 45 second intervals. After the third failure the program waits 60 minutes before retrying. The UNIX version waits 60 minutes between connection failures. Apart from this report, I am unaware of any TCP/IP implementation that is unable to support 3 connection attempts per hour."

Category 24.6 Web-site infrastructure, general Web security issues
2001-08-31 cross-site scripting vulnerability Web hack e-commerce digital cash e

08-31 cross-site scripting vulnerability Web hack e-commerce digital cash e-wallet e-mail patch

NewsScan

HOTMAIL HACKABLE WITH ONE LINE OF CODE [31 Aug 2001]

Security consultant Jeremiah Grossman was able to break through Microsoft's Hotmail and Passport protection schemes with just one line of code. Microsoft has patched the code, but Grossman says he could do it again in eight hours of work. His hacking experiment used a "cross-site scripting" technique that attaches invasive code onto programs used to make Web pages more interactive. Grossman calls them "a breeding ground for new types of Web security vulnerabilities," and Shawn Hernan of the Computer Emergency Response Team at Carnegie Mellon University says that "it's easy to dream up very, very bad scenarios." (USA Today 31 Aug 2001) http://www.usatoday.com/life/cyber/tech/2001-08-31-hotmail-security.htm

Category 24.6 Web-site infrastructure, general Web security issues

2001-12-06 Internet security architecture implementation failure penetration vulnerability

hacking intrusion

RISKS 21 81

Peter G. Neumann summarized an article entitled, "Security hole at WorldCom left internal computer networks at risk" from the Associated Press:

"A security hole at WorldCom Inc. left internal networks at several of the nation's top companies (e.g., AOL Time Warner, Bank of America, CitiCorp, News Corp., JP Morgan, McDonald's Corp., Sun Microsystems) open to hackers. Adrian Lamo, a consultant in San Francisco, worked with WorldCom to fix the months-old problem over the weekend. There is no evidence that the security hole had been exploited, although it was possible to reconfigure or shut down corporate networks. Lamo: ``These networks were never designed to be connected to the Internet, They were private circuits running between locations.'' [Source: eponymous AP item, 05 Dec 2001, PGN-ed] "http://www.siliconvalley.com/docs/news/tech/080991.htm

Category 24.6 Web-site infrastructure, general Web security issues

2002-01-07 Web site design ActiveX operating system compatibility standards security

RISKS 21

Koos van den Hout noted in RISKS that the mcafee.com Web site "shows a pop-up asking me to enable an ActiveX plug-in.... The fact that I am using a different operating system for which an ActiveX plug-in isn't available at all has never crossed the mind of whoever designed that." As he continued his browsing, he found that when he used the text-based Lynx 2.8.2 browser for Unix, he was told to lower the security setting for his browser – in terms clearly indicating that the designer was taking MS Internet Explorer for granted.

Category 24.6 Web-site infrastructure, general Web security issues

2002-03-10 Web server vulnerabilities ICAT CVE

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported 76 vulnerabilities involving Web servers out of a total of 1241 for the period from 1 Jan 2001 to 10 Mar 2002. This represents about 6% of all vulnerabilities logged for that period. Overall, for the entire period since the CVE began recording vulnerabilities in 1995, Web servers are named in 199 of the 3677 vulnerabilities or about 5% of the total.

25.1 Remote control, reprogramming, auto-updates

Category 25.1 Remote control, reprogramming, auto-updates
2000-12-27 remote control upload update firmware device
RISKS 21 18

Andrew Klossner noted in RISKS that home electronics such as DVDs are being reprogrammed using automatic firmware upgrades from media (e.g., DVDs). The correspondent writes, "When the authoritarian software forbids me to skip past a twenty-second copyright notice, it makes me nostalgic for the old 12-inch laser disks."

[MK notes: This poses additional sources of troublesome problems when the software doesn't work right. Even if it isn't broke, someone at a distance may try to fix it anyway.]

Category 25.1 Remote control, reprogramming, auto-updates

2001-01-12 automated firing computer control weapons system military aircraft quality assurance

RISKS 21 20

Daniel P. B. Smith reported in RISKS that a new airborne laser is being designed to shoot down missiles. Smith quotes an article at < http://www.cnn.com/2001/US/01/12/airborne.laser/index.html> as follows:

>No trigger man

>

>No human finger will actually pull a trigger. Onboard computers will decide when to fire the beam.

>

> Machinery will be programmed to fire because human beings may not be fast enough to determine whether a situation warrants the laser's use, said Col. Lynn Wills of U.S. Air Force Air Combat Command, who is to oversee the battle management suite. The nose-cone turret is still under construction

> "This all has to happen much too fast," Wills said. "We will give the computer its rules of engagement before the mission, and it will have orders to fire when the conditions call for it."

>

> The laser has about only an 18-second "kill window" in which to lock on and destroy a rising missile, said Wills.

>

> "We not only have to be fast, we have to be very careful about where we shoot," said Wills, who noted that the firing system will have a manual override. "The last thing we want to do is lase an F-22 (fighter jet)."

[MK: Readers are invited to decide if, given the current state of software quality assurance worldwide, they would be willing to entrust the safety of their family to an automobile equipped with analogous control systems.]

Category 25.1 Remote control, reprogramming, auto-updates 2001-01-19 remote control automobile speed governor

RISKS 21 22

Steve Loughran noted in RISKS that the British government has sponsored tests of computer-controlled speed governors for automobiles; the system would rely on a GPS to locate the vehicle and an on-board database of speed limits. Loughran commented, "Just think how much fun you'll be able to have by a UK motorway in five years time from jamming the GPS signals. Or how much a 'chipped' database or speed limiter will be worth. A more rigorous trial would be to place the speed limited vehicles in the hands of well known violators of the speed laws to see how much effort it takes to disable -- the UK home secretary himself, for example." In addition, the prospect of being unable to take evasive action in an emergency should cause grave concern. Furthermore, given the dismal state of software quality assurance, few RISKS readers would be happy with such a system.

Category 25.1 Remote control, reprogramming, auto-updates

2001-01-26 remote control reprogramming smart cards access token

RISKS 21 22

Jeremy Epstein wrote an interesting report for RISKS on remote reprogramming: "DirecTV has the capability to remotely reprogram the smart cards used to access their service, and also to reprogram the settop box. To make a long story short, they were able to trick hackers into accepting updates to the smart cards a few bytes at a time. Once a complete update was installed on the smart cards, they sent out a command that caused all counterfeit cards to go into an infinite loop, thus rendering them useless."

Category 25.1 Remote control, reprogramming, auto-updates

2001-03-30 QA quality assurance automatic upgrade remote control ISP Internet service

provider long-distance modem database loss data corruption

RISKS 21 32

Microsoft Networks (MSN) upgraded its dialup lists automatically for users in the Research Triangle, NC area -- and wiped out several local access node numbers. Outraged users found out (too late) that their modems had switched to dialing access nodes in areas reached through long distance calls. About a month later, MSN reimbursed its customers for the long-distance calls their modems had placed due to MSN's errors.

Category 25.1 Remote control, reprogramming, auto-updates

2001-04-09 home appliance hacking remote control wireless

RISKS 21 35

Appliance hacking has been a subject of speculation for years, but more and more manufacturers are interested in controlling their domestic appliances at a distance. According to a report in RISKS, "IBM and Carrier, an airconditioning manufacturer, said they plan to offer Web-enabled air conditioners in Europe this summer that can be controlled wirelessly. Financial terms of the collaboration were not disclosed. Owners of the newfangled air conditioners will be able to set temperatures or switch the units on or off wirelessly using a website called Myappliance.com <

http://www.wired.com/news/business/0,1367,42918,00.html >. The press release quoted in RISKS indicates that the system will log information about device utilization and allow remote maintenance operations.

Category 25.1 Remote control, reprogramming, auto-updates

2001-04-10 remote control thermostat TCP/IP Internet access vulnerability risk

NewsScan

INTERNET THERMOSTAT

IBM and the Carrier Corp., which makes heating and air conditioning systems, is planning a pilot program this summer in Britain, Greece and Italy to test an Internet-based system that would allow people to use a Web site, myappliance.com, to control their home air conditioners from work or elsewhere. The system will allow troubleshooting to be done remotely and will make it easier to conserve electricity during peak demand periods. (AP/New York Times 9 Apr 2001)

http://www.nytimes.com/aponline/business/AP-Internet-Thermostat.html

Category 25.1 Remote control, reprogramming, auto-updates

2001-09-06 remote control encryption Windows PC access authorization

NewsScan

NEW SERVICE OFFERS REMOTE CONTROL OF YOUR PC

A new Web-based service called GoToMvPC enables users to control their desktop PCs in their homes or offices using any other Windows PC anywhere in the world that has Internet access. The service, a brainchild of Expertcity Inc., costs \$10 a month. Instead of lugging a laptop along on a trip, a user could sit down at an Internet café PC and access all files, e-mail, etc. on his or her PC at home. Alternatively, if a worker found that the file he or she needed over the weekend was on the computer at work, it could be retrieved using the service. The company says the system is highly secure and requires two passwords - one to log onto the service and another to gain access to each target PC. All of the data exchanged in each remote-control session is encrypted and Expertcity says the service will operate through many corporate firewalls. (Wall Street Journal 6 Sep 2001)

http://interactive.wsj.com/archive/retrieve.cgi?id=SB999723847321875907.djm (sub req'd)

Category 25.1 Remote control, reprogramming, auto-updates

2001-10-01 remote control airliners airplanes interception impersonation

RISKS 21 68

Steve Bellovin contributed an item to RISKS about remote control of airplanes:

"The Associated Press reported on a test of a remotely-piloted 727. The utility of such a scheme is clear, in the wake of the recent attacks; to the reporter's credit, the article spent most of its space discussing whether or not this would actually be an improvement. The major focus of the doubters was on security:

But other experts suggested privately that they would be more concerned about terrorists' ability to gain control of planes from the ground than to hijack them in the air.

I'm sure RISKS readers can think of many other concerns, including the accuracy of the GPS system the tested scheme used for navigation (the vulnerabilities of GPS were discussed recently in RISKS), and the reliability of the computer programs that would manage such remote control."

Category 25.1 Remote control, reprogramming, auto-updates

2001-12-20 remote control telemedicine telesurgery hacking vulnerability interception

disruption availability interruption

NewsScan

TELESURGERY REVOLUTION, PART III [20 Dec 2001]

In a discussion of "the telesurgery revolution" in The Futurist magazine, surgeon Jacques Marescau, a professor at the European Institute of Telesurgery, offers the following description of the success of the remotely performed surgical procedure as the beginning of a "third revolution" in surgery within the last decade: "The first was the arrival of minimally invasive surgery, enabling procedures to be performed with guidance by a camera, meaning that the abdomen and thorax do not have to be opened. The second was the introduction of computer-assisted surgery, where sophisticated software algorithms enhance the safety of the surgeon's movements during a procedure, rendering them more accurate, while introducing the concept of distance between the surgeon and the patient. It was thus a natural extrapolation to imagine that this distance--currently several meters in the operating room--could potentially be up to several thousand kilometers." A high-speed fiber optic connection between New York and France makes it possible to achieve an average time delay of only 150 milliseconds. "I felt as comfortable operating on my patient as if I had been in the room," says Marescaux. (The Futurist Jan/Feb 2002) http://www.futurist.com

Copyright © 2002 M. E. Kabay.

Category 25.1 Remote control, reprogramming, auto-updates

2002-01-08 remote control FPGA field-programmable logic array firmware

RISKS 21 87

J. P. Gilliver noted an alarming development in remote reprogramming -- an easy way to modify firmware: "... For example, IRL (Internet Reconfigurable Logic) means that a new design can be sent to an FPGA in any system based on its IP address." (From Robert Green, Strategic Solutions Marketing with Xilinx Ltd., in "Electronic Product Design" December 2001. Xilinx is a big manufacturer of FPGAs.) For those unfamiliar with the term, FPGA stands for field-programmable logic array: many modern designs are built using these devices, which replace tens or hundreds of thousands of gates of hard-wired logic.

The RISKs involved are left as an exercise to the readers."

Category 25.1 Remote control, reprogramming, auto-updates

2002-01-16 theft deterrent remote control explosion destruction tampering interception data diddling man-in-the-middle attacks criminal hackers vulnerability potential

NewsScan

EXPLODING CHIPS COULD FOIL THIEVES

Researchers at the University of California in San Diego have developed a way to blow up silicon chips using an electric signal – an innovation that could be used to fry electronic circuitry in devices after they're stolen or fall into the wrong hands. The American spy plane that was impounded in China last year is an example where such technology would have proven handy in destroying its secret electronics systems. Similarly, if a cell phone were stolen, the owner could alert the wireless carrier, which would send a signal to trigger a small explosion in the phone's chip, rendering it useless. The techniques uses a small amount of the oxidizing chemical gadolinium nitrate applied to a porous silicon wafer. (New Scientist 16 Jan 2002)

http://www.newscientist.com/news/news.jsp?id=ns99991795

Category 25.1 Remote control, reprogramming, auto-updates

2002-01-25 remote control firmware reprogramming update configuration change SMS

RISKS 21 89

In Switzerland, the mobile phone company Swisscom admitted that it reconfigured its customers' phones using a program embedded in a SMS (short message service) transmission. The message deleted roaming information. S. Llabres reported in RISKS, "... [I]nsiders believe that the modification of the roaming information was to direct traffic to networks owned by Vodafone -- which acquired a 25% share of Swisscom [in April] last year." Llabres commented astutely, "It would be interesting:

- * If there is any security mechanism protecting anyone from sending such "special" messages.
- * Which setting[s] on the mobile phone can be changed (or probably retrieved from the phone) without knowledge to the customer.
- * If the network provider must implement such features, I do not understand why this must happen unperceived by the customer. Why not send a message telling people what will happen?"

Category 25.1 Remote control, reprogramming, auto-updates

2002-02-15 remote control self-updating programs essay article summary

RISKS 21 92

Scott Schram "published an article addressing some risks of programs that update themselves. Rather than a bona-fide update, the auto-update feature could be used to send programs with undesired features. The activity of these updaters would not be detected by firewall tools, as they are expected to be periodically checking for updates and downloading them. Further, the most careful reverse-engineering of the updater would not reveal anything unexpected." http://schram.net/articles/updaterisk.html

25.2 Jamming

Category 25.2 Jamming

2001-11-21 RFI radio frequency interference jamming cellular mobile phones hospital

medical electronics

RISKS 21 78

Russell Stewart caught what appeared to be an interesting paradox about attempts to stop people from using mobile phones in hospitals: seems a Hong Kong company is offering radio-frequency jamming devices. As Mr Steward pointed out, "Hospitals? Now, I admit I know very little about jamming technology, but I know that, at the very least, it requires transmitting radio energy on the same frequency as the signal you are trying to jam. Presumably, it involves transmitting at a considerably higher power than that of the target signal. Now, as I understand it, hospitals' nocellphone policy is based on the fear that the phones' radio transmissions might interfere with hospital equipment. Are we to understand, then, that they intend to combat the problem by installing a device that, by definition, must transmit on the same frequencies at the same or considerably greater power?"

However, Markus Kuhn immediately responded to the list explaining that mobile-phone jamming does _not_ send a signal that competes with the phone-to-base-station signal; instead, one james cellular phones by competing with the base-station-to-phone signal, which is orders of magnitude weaker. In addition, wrote Mr Kuhn, "The no-cellphone policies in hospitals are today mostly based on the fear that clueless phone users might operate phones in the immediate vicinity (with a couple of centimeters) of critical equipment. As soon as the mobile phone is a few meters away, field strength will drop well bejond the 3 V/m levels against which medical equipment has to be EMC immunity tested by the manufacturers (EN 50082, IEC 601-1-2)."

25.3 RFI, HERF, EMP/T

Category 25.3 RFI, HERF, EMP/T

2001-01-09 avionics failure RFI radio frequency interference cellular phone

RISKS 21 20

A cellular (mobile) phone that had been left on in baggage stowed on a Slovenian Adria Airways plane disrupted the avionics and forced an emergency landing.

25.4 Health effects of electronic equipment (phones, screens, etc.)

Category 25.4 Health effects of electronic equipment (phones, screens, etc.)

2001-01-16 cellular phone mobile cancer research

NewsScan

STUDY LINKING CELL PHONE USE TO EYE CANCER CRITICIZED

An Essen (Germany) University Clinic study of 118 patients with uveal melanoma, a type of eye cancer, found that those cancer patients used cell phones and other such devices more often than 475 healthy individuals. Michael Foerster of the Free University in Berlin is one of the study's harshest critics: "The problem with the study is that it did not measure how much radiation the studied people had. With such a detailed energetic study, such results are biostatistical garbage." (Reuters/New York Times 15 Jan 2001)

http://partners.nytimes.com/reuters/technology/tech-germany-cellphon.html

Category 25.4 Health effects of electronic equipment (phones, screens, etc.)

2001-05-23 cell phone safety radiation

NewsScan

GAO AND CONGRESS CONSIDER CELL PHONE SAFETY

The U.S. General Accounting Office says that federal agencies such as the Federal Communications and the Food and Drug Administration have not been doing enough to make people understand that the safety of cell phones has not yet been conclusively determined. "It will likely be many more years before a definitive conclusion can be reached on whether mobile phone emissions pose any risk to human health." In another development, Congress is considering variations on legislation that would ban or restrict the use of a cell phone while driving an automobile. (AP/New York Times 23 May 2001)

http://www.nytimes.com/aponline/national/AP-Cell-Phone-Safety.html

Category 25.4 Health effects of electronic equipment (phones, screens, etc.)

2002-02-20 RFI radio frequency interference emissions wireless communications health

danger fraud lawsuit regulation

NewsScan

FTC SUES SELLERS OF CELL PHONE "RADIO SHIELD" [20 Feb 2002]

The Federal Trade Commission is suing two companies for selling devices purporting, without good evidence, to shield people from harmful radiation emitted by their cell phones. The small metallic devices were sold under such names as WaveShield 1000, NoDanger, and SafeTShield. The FTC said that by claiming that their products could "block up to 97% to 99%" of electromagnetic radiation," the companies were actually "using a shield of misrepresentation to block consumers from the facts." Among the facts missing in company sales materials is any mention of a 2001 General Accounting Office report indicating that "scientific research to date does not demonstrate that the radio frequency energy emitted from mobile phones has adverse health effects, but the findings of some studies have raised questions indicating the need for further investigation." (Newsbytes/Washington Post 20 Feb 2002) http://www.washtech.com/news/telecom/15264-1.html

26.1 Windows 9x/Me/XP

Category 26.1 Windows 9x/Me/XP

2001-11-15 Windows XP vulnerability administrator account root privilege default cost benefit analysis 80/20 rule Pareto principle

RISKS 21 76

By default, all user accounts created under Windows XP are have administrator (root) capability and have no passwords. Mark Wilkins offered an interesting explanation of what might be behind such a decision. Writing in RISKS, he described how he had worked on the design for a TV security system which originally kept all channel lock settings in place, allowing parents to selectively "allow or deny TV viewing according to those settings as they liked." However, the TV manufacturer reversed this policy so that "unlocking the TV caused ALL of the information about which channels or times were or were not permissible to be erased, requiring that they be re-entered next time." Mr Wilkins continued, "... support telephone calls on the issue of parental lock . . . nearly always asked 'My kids have locked me out of the television. What do I do?' Since those calls cost money to support a product for which the company had already been paid, they were to be minimized. The product had to be easy to unlock and hard to lock." He concluded, "I suspect this behavior in Windows XP is a similar matter."

26.2 Windows NT/2K

Category 26.2 Windows NT/2K

risk management insurance rates operating system stability hacking penetration

vulnerabilities

RISKS 21 44

According to an article in _InternetWeek_, hacking insurance will cost more for clients using Windows NT. Oleg Broytmann contributed this summary:

> "We saw that our NT-based clients were having more downtime" due to hacking, says John Wurzler, founder and CEO of the Michigan company, which has been selling hacker insurance since 1998. Wurzler said the decision to charge higher premiums was not mandated by the syndicates affiliated with Lloyd's of London that underwrite the insurance he sells. Instead, the move was based on findings from 400 security assessments that his firm has done on small and midsize businesses over the past three years. Wurzler found that system administrators working on open-source systems tend to be better trained and stay with their employers longer than those at firms using Windows software, where turnover can exceed 33 percent per year.<

http://www.zdnet.com/intweek/stories/news/0,4164,2766045,00.html

Category 26.2 Windows NT/2K

2001-10-08 wireless network security product management chip

NewsScan

IBM TO OFFER SECURITY SOFTWARE AND SERVICES FOR WIRELESS DEVICES

IBM is launching new security software and services for wireless devices, including the ability for a corporation to manage those devices the same way it uses firewalls and servers to manage other security exposures. The company has also begun to sell ThinkPad notebooks and NetVista desktop computers that include a security chip designed to protect against vandals trying to hack into them through a wireless network. (Reuters/San Jose Mercury News 8 Oct 2001)

http://www.siliconvalley.com/docs/news/svfront/020703.htm

26.4 TCP/IP & HTTP

Category 26.4 TCP/IP & HTTP

2001-05-01 vulnerability sequence number datagrams packets alert CERT/CC

NIPC Daily Report

On 1 May, CERT/CC released Advisory CA-2001-09, Statistical Weaknesses in TCP/IP Initial Sequence regarding a new vulnerability (CERT VU#498440, CVE CAN-2001-0328) which is present when using random increments to constantly increase TCP ISN values over time. Attacks against TCP initial sequence number (ISN) generation have been discussed for some time now. The reality of such attacks led to the widespread use of pseudo-random number generators (PRNGs) to introduce some randomness when producing ISNs used in TCP connections. Previous implementation defects in PRNGs led to predictable ISNs despite some efforts to obscure them. The defects were fixed and thought sufficient to limit a remote attacker's ability to attempt ISN guessing. It has long been recognized that the ability to know or predict ISNs can lead to manipulation or spoofing of TCP connections. What was not previously illustrated was just how predictable one commonly used method of partially randomizing new connection ISNs is in some modernTCP/IP implementations. Additional information regarding this advisory can be found at http://www.cert.org/advisories/CA-2001-09.html. (Source: CERT/CC, 1 May)

26.5 LAN OS

Category 26.5 LAN OS

2001-10-15 wireless networks wired LANs cache poisoning vulnerability penetration hacker

RISKS 21 69

Gary McGraw summarized a new class of wireless attacks in RISKS:

Bob Fleck, a security consultant at Cigital, working with Jordan Dimov, has discovered new class of wireless attacks that can be used to gain unauthorized access to normally-protected machines on a standard wire-based internal network. Wireless networks involve installation of a wireless Access Point on a normal internal network. This Access Point is usually connected to the wired network through a switch or a hub. The attacks discovered by Cigital are based on an adaptation of a well understood network attack from the non-wireless world known as ARP cache poisoning. This emphasizes the importance of re-considering old risks in light of new technologies, something that is especially important in software-based systems!

The new class of attacks encompasses: 1) the ability to monitor and manipulate traffic between two wired hosts behind a firewall 2) the ability to monitor and manipulate traffic between a wired host and a wireless host 3) the ability to compromise roaming wireless clients attached to different Access Points 4) the ability to monitor and manipulate traffic between two wireless clients

Previous wireless attacks have demonstrated that wireless traffic on an 802.11b network is vulnerable to monitoring and manipulation, even when it is "protected" with WEP encryption. This new class of attacks discovered by Cigital is based on abusing the Address Resolution Protocol (ARP) which binds internal IP addresses to ethernet addresses.

Mitigating the risks of these attacks is possible. The best fix involves placing a technical barrier between the wireless network and the normal wired network. This provides only a partial solution that leaves the wireless network in a compromised state, though it protects against the worst of the attack class Cigital discovered. Further risks can be mitigated through advanced design of any and all software applications that make use of the wireless network.

For more, see:

http://www.cigital.com/news/wireless-sec.html http://www.cigital.com/news/wireless/faq.html

26.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

Category 26.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2001-04-03 802.11 wireless local area networks bug flaw vulnerability eavesdropping spoofing

man-in-the-middle attack

NewsScan

FLAW IN STANDARD FOR LOCAL WIRELESS NETWORKS

Computer science researchers at the University of Maryland have found new security flaws in the 802.11 wireless standard used in many local area wireless networks deployed in corporations and in public areas such as airports and cafes. Researchers from Intel and the University of California at Berkeley had previously found weaknesses in the standard. William A. Arbaugh, in the Maryland group, said: "We're seeing a great proliferation of wireless activity now in products, and people have not paid close enough attention to security issues. When we began looking at this I was flabbergasted by what I found." The newly discovered flaw might be used by someone physically close to private wireless computer network to masquerade as a legitimate user. (New York Times 3 Apr 2001) http://partners.nytimes.com/2001/04/03/business/03FLAW.html

Category 26.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2001-05-03 wireless network interception intrusion spam penetration e-mail

RISKS 21 39

Thor Lancelot Simon commented on a bad implementation of wireless network access in a report in RISKS:

> A local university has deployed a large 802.11 wireless network without WEP or any other security measure. Given the complexity of distributing WEP keys to huge numbers of students, faculty, and staff, not to mention the need for periodic changes, and the notorious insecurity of WEP itself, this might seem to be a reasonable choice. They have decided to provide public access to their IP connectivity for those within radio range of their campus rather than tackle the very significant issues associated with restricting access.

The RISK? Their campus mail-handling machines will relay mail to any inside or outside destination if it's received from an address "inside" their campus network. The network architecture they've chosen for their wireless deployment dictates that anyone can walk onto their (large, urban) campus, or even just park his car outside, and spam away freely with hundreds of megabits per second of bandwidth to most points on the Internet.

Basically, their entire campus just became a "safe harbor" for anyone owning a laptop and wireless card to do nefarious things to outside hosts with, essentially, perfect, impenetrable anonymity. There's not even a billing record for a throwaway dialup account to trace back; just a MAC address that can be trivially changed and the knowledge that it was used *somewhere* on their campus to do Bad Things at some point in the past. <

In a followup posting to RISKS, Danny Burstein confirmed by direct experimentation that fears of abuse were perfectly justified. Burstein wrote, "Furthermore, any mail coming through them will have an envelope indicating it came from a well known and trusted source. Meaning not only would people be more likely to let it through their filters (whether computerized or the Mark One Eyeball method of glancing at the 'from' and 'subject' line), but they're also far more likely to open it."

In addition, wrote Burstein, "Getting back to spamming: this system doesn't block outgoing 'port 25' access, meaning a spammer could set up their own mail server and pseudo-anonymously engage in all sorts of socially deviant activities."

Category 26.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2001-06-07 wireless communications interception Bluetooth

NewsScan

PALM TO GET BLUETOOTH WIRELESS LINKS

New expansion cards will allow Palm m500 and m505 handheld computers to use Bluetooth short-range wireless technology to communicate with Bluetooth-enabled printers, mobile phones, and other devices. The cards will be priced below \$150. (San Jose Mercury News 7 Jun 2001)

http://www.siliconvalley.com/docs/news/svfront/023533.htmg

Category 26.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2001-08-12 wireless communications Internet access confidentiality vulnerabilities

NewsScan

WIRELESS INTERNET SPARKS SECURITY CONCERNS

Business travelers plugging into wireless Wi-Fi networks now found in airports and coffee shops should beware – those networks can easily be intercepted, according to security experts. "When you sit in an airport and use your laptop you might as well be broadcasting to anyone within listening distance," says a digital forensics specialist with Predictive Systems. No special software is required to intercept data off a Wi-Fi network, and eavesdropping on other's e-mail exchanges is easy to do, says one security expert. "Everyone who is touching the Internet should know that it is wide open to everyone," says MobileStar chief technology officer Ali Tabassi. "People should think of it as a pay phone or a cell phone, in a public place." (AP 12 Aug 2001)

http://news.cnet.com/news/0-1004-200-6853688.html?tag=mn_hd

Category 26.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2001-08-19 wireless network intrusion penetration confidentiality eavesdropping WEP

802.11 WiFi medical informatics privacy integrity safety

RISKS 21 62

Cryptographer Avi Rubin demonstrated the weakness (or absence) of wireless network security in a hospital in Morristown, NJ. Peter G. Neumann of RISKS summarizes what happened: "... Avi Rubin... noticed that his laptop wireless connection card was blinking, and then discovered that the hospital's wireless network was open to his laptop, using 802.11b (Wi-Fi) and automatically granting him access...."

Category 26.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2001-11-06 wireless security penetration firewall encryption

NewsScan

DRIVE-BY HACKING

An experiment conducted by BBC Online found that the "wifi" (wireless) computer networks in London's financial center have serious security gaps that would allow network vandals to drive, pedal a bike, or walk through the streets and pick up information from the networks almost at will. The problem will only be solved when companies take security seriously and protect wireless networks behind a firewall that allows only encrypted, authenticated traffic to pass from a wifi network to a wider corporate network. (BBC News 6 Nov 2001 http://news.bbc.co.uk/hi/english/sci/tech/newsid 1639000/1639661.stm

Category 26.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2002-01-25 wireless tunneling firewall network workstation

RISKS 21 89

Jeremy Epstein noted in RISKS that, "Wireless carriers including Sprint, Cingular, and Seven (a startup) are putting together products that tunnel through the firewall to allow you to access the e-mail, calendars, etc. on your desktop machine remotely from a wireless device. . . . "

http://www.infoworld.com/articles/hn/xml/02/01/28/020128hnport.xml

Category 26.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11

2002-01-28 wireless networks Wi-Fi vulnerability implementation installation problems

weakness ban

NewsScan

WIRELESS TECHNOLOGY CRITICIZED FOR VULNERABILITIES

Lawrence Livermore National Laboratory in California has banned all wireless networks, including Microsoft's Wi-Fi, because of security concerns. Wi-Fi supporters say the technology is secure when it's been properly installed, but experts say that only about 10% of all users install them correctly. (USA Today, 28 Jan 2002) http://www.usatoday.com/life/cyber/tech/2002/01/29/wifi.htm

28.1 DoS attacks

Category 28.1 DoS attacks

2001-01-26 criminal hacker Web vandalism DoS denial of service DNS domain name service

colocation

NewsScan

NETWORK VANDAL ATTACKS MICROSOFT SITES

Just a day after Microsoft's Web sites were down for an extended period of time because of the "human error" of a technician, they were victimized by the "human malice" of a network vandal who subjected them to a "denial of service" attack that flooded them with bogus communications, causing them to gridlock and reject legitimate communications from their customers. The company has called in the FBI for assistance. Computer security expert Abe Singer of the San Diego Supercomputer Center said that part of Microsoft's vulnerability to attack was due to the fact that its four domain-name servers are linked in a single network. "They had all their eggs in one basket and basically someone knocked down the basket." (Washington Post 26 Jan 2001) http://washingtonpost.com/wp-dyn/articles/A47581-2001Jan25.html

Category 28.1 DoS attacks

2001-05-24 DoS denial-of-service attack routine ho-hum yawn

NewsScan

CERT SUBJECTED TO "JUST ANOTHER ATTACK"

The Web site of the federally funded Computer Emergency Response Team (CERT) was clogged by a "denial of service" attack that lasted 30 hours this week. CERT, which is located at Carnegie Mellon University in Pittsburgh, has a mission of providing warnings about computer attacks and viruses. An official of the organization said: "We get attacked every day. This is just another attack. The lesson to be learned here is that no one is immune to these kinds of attacks. They cause operational problems, and it takes time to deal with them." (AP/USA Today, 24 May 2001) http://www.usatoday.com/life/cyber/tech/2001-05-24-cert-hacked.htm]

Category 28.1 DoS attacks

2001-10-31 DoS denial of service bandwidth saturation

NewsScan

DENIAL OF SERVICE ATTACK ON NEW YORK TIMES

Although the company's Web site was unaffected, the New York Times experienced a "huge amount of electronic transmissions on Tuesday" that disrupted operations and denied Times employees access to the Internet for several hours. The company's network administrator says the Times does not know whether or not the "storm of data" it received was sent maliciously, but that "there seems to be no innocent explanation" and that it appears to have been a "deliberate attack." (AP/Washington Post 31 Oct 2001)

http://www.washingtonpost.com/wp-dyn/articles/A16398-2001Oct31.html

Category 28.1 DoS attacks

2002-05-05 DoS denial of service government information warfare

NIPC Daily Report

The White House Web site reportedly suffered a brief but crippling denial of service attack that rendered the site inaccessible to users on 4 May. White House spokesperson Jimmy Orr confirmed that the White House site was rendered inaccessible due to a "denial of service" in the morning hours between 9 a.m. and 11:15 a.m. EDT. [Spokespersons could not attribute the denial of] service to an orchestrated attack, but did confirm that the White House was "looking into" the possible causes of the of the shutdown. Technicians were able to "unclog the clog" between Whitehouse.gov and its Internet service provider, making the site accessible to the general public. At no point did any malicious data reach White House servers. Security experts believe the Whitehouse.gov shutdown to be linked to the spate of Web site hacks and defacements launched by Chinese and pro-Chinese Internet vandals over the past few days. (Source: Newsbytes, 5 May)

28.2 DDoS attacks

Category 28.2 DDoS attacks

2001-02-02 DDoS distributed denial-of-service attack e-mail list

NewsScan

SECURITY EXPERTS TRICKED INTO HELPING LAUNCH ATTACK

Bugtraq – an Internet mailing list comprising about 37,000 security industry technicians – was used as the instrument for launching a denial-of-service attack against Network Associates, one of the world's largest Internet security companies. The bizarre incident began when a hacker sent a disguised string of code to Securityfocus.com, which manages the Bugtraq list. The hacker's message claimed the code was an example of a program that could exploit a recently discovered security hole in corporate security systems, but when Bugtraq members opened the code, it caused their computers to flood Network Associates' Web site with tens of thousands of messages, disabling the Web site for about 90 minutes. In another strange twist, Securityfocus admitted that it had forwarded the infected message to its members – after getting the code checked and okayed by Network Associates. Industry watchers say the attack could be motivated by revenge against Network Associates, which was the company that first publicized the corporate network vulnerability. (Financial Times 2 Feb 2001) http://news.ft.com/news/industries/infotechnology

Category 28.2 DDoS attacks

2001-05-03 information warfare DDoS distributed denial of service firewalls blocking defense

NIPC Daily Report

Attacks on Croatia's Internet space, particularly Croatian Telekom's (HT) Internet provider HThinet, which started 12 days ago, have been subsiding and are being successfully blocked, according to a HThinet network specialist. HT has been detecting and blocking attacks in cooperation with other Croatian Internet providers and its foreign partners Seabone and Deutsche Telekom. It has been established that the attacks have been coming from more than 1,000 addresses from all over the world. The attacks have been reported to the Croatian Interior Ministry, which cooperates with the Interpol on such cases. (Source: EUP, 3 May)

Category 28.2 DDoS attacks

2001-12-20 distributed denial-of-service attacks DDoS zombie passwords compromise bot

eggdrop

NewsScan

'EGGDROP' VANDAL SETS STAGE FOR DENIAL-OF-SERVICE ATTACKS [20 Dec 2001]

A software robot (or "bot") known as "eggdrop" has been used to invade the customer Web servers of CCBill, a credit card processing company in Tempe, Arizona, and the company has urged all of its customers to change their server passwords and search their systems for malicious software that might have been planted by stealth on their own systems. The fear is that the malicious intrusion could lead to a wider "denial-of-service" attack, in which computer servers are commandeered and then used to generate floods of bogus Internet traffic that denies service to legitimate traffic. (Reuters/New York Times 20 Dec 2001)

http://partners.nytimes.com/reuters/technology/tech-tech-hack.html

29 Peer-to-peer networking

Category 29 Peer-to-peer networking

2001-05-03 criminal hacker gang group tools civil disobedience censorship peer-to-peer

networking

NIPC Daily Report

A computer hacking group known for creating tools for hijacking computer systems is turning its hand to civil disobedience and plans to release an application that could hinder government and corporate censorship around the world. The tool, to be called Peekabooty, will be based on peer-to-peer network technology. This allows data to be distributed directly between computer systems and has attained fame through the emergence of music-sharing technologies such as Napster and Gnutella. of the Dead Cow, a team of computer hackers best known for producing security tools that exploit weaknesses in Microsoft software. (Infosec News, 3 May)

Category 29 Peer-to-peer networking

2001-08-01 peer-to-peer networking exposure risk commerce distributed computing

NewsScan

PEER-TO-PEER NETWORKING MOVES TO WALL STREET [9 Feb 2001]

Peer-to-peer networks have already proven their popularity for swapping music files, and now the same technology is invading Wall Street, with a number of startups "poised to revolutionize the investment management industry," according to an analyst at research firm TowerGroup. Two types of peer-to-peer models are emerging: one resembles Napster, in which computers share the files directly, and the other pools the resources of lots of computers to maximize the processing power. The first type enables Wall Street brokerages to deliver targeted information to clients and provides a platform for money managers to trade stock among themselves without the use of a broker. Meanwhile, distributed peer-to-peer computing networks can process complex calculations in record speed. The investment community "is a space that does not need religion when it comes to distributed computing," says Datasynapse CEO Peter Lee. "Every one of our clients was already doing it in some way, shape or form" through their own internal networks. (Investor's Business Daily 9 Feb 2001) http://www.investors.com/editorial/tech01.asp?v=2/9

PEER-TO-PEER MOVES INTO THE MAINSTREAM [13 Jun 2001]

Many people think "Napster" when they hear about "peer-to-peer" computing, but the technology, which enables users to share files and collaborate by linking their computers over the Internet, is moving into corporate America. A variety of companies, including Intel, GlaxoSmithKine, Raytheon, Ernst & Young, and First Union, are finding that peer-to-peer technology allows their workers to do business faster, better and cheaper. Employees can hold online meetings from any location, bypassing the bottleneck of corporate servers, and freelance workers and contractors can join an online group without compromising the company's security system. "The way people get things done is by working together in small or large groups," says a Garner Group research director. "With peer-to-peer, we move from personal to interpersonal computing." Garner estimates that by 2003 nearly one in three corporations will use peer-to-peer technology to distribute files among employees. (New York Times 13 Jun 2001) http://www.nytimes.com/2001/06/13/technology/13BURT.html

PEER-TO-PEER SCREENSAVERS [1 Aug 2001]

DALiWorld, a new peer-to-peer software program that debuted this week, is one of the first examples of how file-sharing technology is emerging as a foundation for a new generation of online games. "Traditional peer-to-peer software like Napster or Gnutella is just about moving files," says DALi CEO Todd Pappainoannou. "What we're talking about is shared, networked entertainment -- people interacting in the same virtual world from wherever they are." For the moment, DALi's major creation is software that allows you to create a virtual aquarium on your computer housing your own artificially intelligent fish, as well as others created by other users. Users can right-click on any fish swimming by to see where they've come from. Future plans call for evolving DALiWorld into a complex universe where players can create their own creatures, communicate with players from around the world, forage for food and even fiddle with the biochemistry of the virtual environment. (Wired.com 1 Aug 2001) http://www.wired.com/news/culture/0,1284,45726,00.html

Category 29 Peer-to-peer networking

2001-08-30 peer-to-peer distributed network parasitic computing servers

NewsScan

'PARASITIC' COMPUTING [30 Aug 2001]

Researchers at the University of Notre Dame have demonstrated "parasitic" computing -- using other people's servers to do your own processing. Although several projects have harnessed the power of distributed computing for a common research goal, the difference here is that the Notre Dame researchers didn't ask the other server owners' permission. The methodology exploits technical protocols that ensure reliable communication by, in effect, turning the Internet into a distributed computer. Servers can then be harnessed to perform computations on behalf of an uninvited users, solving complex mathematical problems while engaging in standard communications. (InfoWorld 30 Aug 2001)

http://www.infoworld.com/articles/hn/xml/01/08/30/010830hnparasite.xml

2C Addiction, cyber-syndromes, sociology

Category 2C Addiction, cyber-syndromes, sociology 2001-06-07 information overload study coping

NewsScan

INFORMATION OVERLOAD IS A STATE OF MIND

A new study titled "The Next Big Thing" found surprising anecdotal evidence that people who receive the greatest volume of electronic information reported a greater ability to cope, while the group that feels the most overwhelmed has the least amount of data to deal with. "We went into the survey expecting to find people were really struggling. We were surprised to find they were thriving," says the study's publisher, Josh Clark. "Anecdotally, there are people out there who are feeling overwhelmed, but practice makes perfect. The people who are most comfortable practice dealing with high volumes of information, and they are coping beautifully." The study's authors caution that because their response group was predominantly male with 42% working in the technology sector, its results cannot be extrapolated to the entire U.S. population. Nevertheless, the comparatively high response rates for the study mean the results are meaningful, and the results bear out what previous studies and empirical evidence has shown -- that simplicity is the key to success in the technology age. (Newsbytes 7 Jun 2001) http://www.newsbytes.com/news/01/166615.html

Category 2C Addiction, cyber-syndromes, sociology

2001-07-22 Internet cyberspace culture games children effects benefits harm obsession addiction

NewsScan

COMPUTER GAMES BOOST KIDS' ABILITIES

Computer games can boost children's coordination and ability to concentrate, putting them on a par in those categories with top-level athletes, according to a study by the UK government's Economic and Social Research Council. "People who play games regularly seem to develop a mental state that we have seen before only in serious athletes or professionals such as astronauts, whose life depends on concentration and coordination," says Jo Bryce, who led the research. "Their minds and bodies work together much better than those of most other people." Bryce found that although a minority of gamers become obsessive, the majority have a healthy mix of other interests and varied social lives. "Our subjects were averaging about 18 hours a week on computer games, which sounds a lot, but they were spending similar amounts of time reading and doing sport or socializing," says Jason Rutter of the Center for Research on Innovation and Competition at Manchester University. A recent study by Britain's Home Office also showed that those who regularly played computer games when young were more likely to be intelligent, to attend a university, and to get a better-than-average job. (The Sunday-Times 22 Jul 2001) http://www.sunday-times.co.uk/news/pages/sti/2001/07/22/stinwenws03005.html

Category 2C Addiction, cyber-syndromes, sociology

2001-07-23 psychology depression loneliness Internet user profile research study

NewsScan

SOME ARE HAPPY SURFERS, SOME ARE SAD

A new study by Carnegie Mellon University psychologist Robert Kraut, who claimed three years ago that Internet use led to depression, says that Internet use can no longer be correlated with depression or loneliness but can add to the stress people feel (as "just another thing on their to-do list"). Kraut 's research has convinced him that the Internet deepens the prevailing mood of both extroverts (who become livelier) and introverts (who become lonelier the more time they spend online, and look to the Internet less for social contact than for entertainment). The study findings are unsurprising to Vanderbilt University psychologist and e-commerce expert Donna Hoffman, who says that people are "going to use computers in a predictable way, based on the kind of person they are." (USA Today 23 Jul 2001) http://www.usatoday.com/life/cyber/tech/2001-07-23-web-depression-study.htm

2E Online voting & legal proceedings

Category 2E Online voting & legal proceedings 2001-01-11 online voting technology

NewsScan

TECH ALLIANCE TO DEVELOP NEW VOTING SYSTEM

Unisys, Microsoft, and Dell will jointly work on a project to create a new voting system that will integrate all election processes, from voter registration to ballot counting, and avoid the confusion and uncertainty experienced in the recent U.S. presidential elections. (Reuters/San Jose Mercury News 11 Jan 2001) http://www.mercurycenter.com/sytech/news/breaking/reuters/docs/833061l.htm

Category 2E Online voting & legal proceedings

2001-03-16 online elections voting problems report analysis

RISKS 21 28

Terry Carroll summarized in RISKS a recent report on online voting. "The National Science Foundation recently released a study that it commissioned from the Internet Policy Institute on problems associated with Internet voting. The NSF's press release on the study may be found at < http://www.nsf.gov/od/lpa/news/press/01/pr0118.htm>. The IPI has a page devoted to the study (including a link to the report itself) at < http://www.internetpolicy.org/research/results.html>."

According to Carroll, "The NSF highlights the following findings with respect to the feasibility of Internet voting:
- Poll site Internet voting systems offer some benefits and could be responsibly deployed within the next several election cycles;

- The next step beyond poll-site voting would be to deploy kiosk voting terminals in non-traditional public voting sites;
- Remote Internet voting systems pose significant risk and should not be used in public elections until substantial technical and social science issues are addressed; and
- Internet-based voter registration poses significant risk to the integrity of the voting process, and should not be implemented for the foreseeable future.

Another item in the same issue of the RISKS Digest noted an amusing glitch in an online election. Sarr Blumson reported, "The college I attended is running the election for alumni appointed trustee with a Web voting option through election.com. So I went to cast my vote, and got in response:

Microsoft OLE DB Provider for SQL Server error '80040e14'

The log file for database 'electnet' is full. Back up the transaction log for the database to free up some log space. /dartmouth2001/confirmation.asp, line 92

It's happened twice. It let me vote successfully a few hours later; I'm assuming/hoping it only recorded my vote once. . "

Copyright © 2002 M. E. Kabay.

Category 2E Online voting & legal proceedings
2001-03-29 online Internet voting standards

RISKS 21 33

David Marston reported on a move by The Organization for the Advancement of Structured Information Standards (OASIS,

http://www.oasis-open.org) to address online voting by developing standards. He provided the following excerpt from published documents on that site:

"A new OASIS technical committee is being formed. The Election and Voter Services Committee has been proposed by Gregg McGilvray, election.com (chair); Oliver Bell, Microsoft; and Ed McLaughlin, Accenture.

Purpose: To develop a standard for the structured interchange of data among hardware, software, and service providers who engage in any aspect of providing election or voter services to public or private organizations. The services performed for such elections include but are not limited to voter role/membership maintenance (new voter registration, membership and dues collection, change of address tracking, etc.), citizen/membership credentialing, redistricting, requests for absentee/expatriate ballots, election calendaring, logistics management (polling place management), election notification, ballot delivery and tabulation, election results reporting and demographics.

Implementation: The standard under development by election.com, Inc. will be made available for review and revision and can be expanded upon as necessary. A phased approach will be used to implement the standard due to the number of aspects being considered by the standard."

Category 2E Online voting & legal proceedings
2001-11-10 online voting election paper ballots QA quality assurance failure programmer dishonesty

RISKS 21 74

In San Bernardino County, an election was screwed up by an untested and faulty computer program. The responsible programmer falsely claimed to have run quality assurance tests; his buggy program ignored some votes, reversed the meaning of votes on other cards, and even counted zero votes in one precinct. Geoff Kuenning, reporting for RISKS, quoted a significant passage from the Los Angeles Times: "County officials said the good news is that using a card-counting system means that ballots are still around to be recounted. If the same error had occurred with an electronic voting system, there would be no paper record "

Commentators responded to RISKS with the obvious remark that a programmer should never be the only person to test his or her own code. Others suggested that the programmers managers should have been fired for allowing such sloppy procedures.

Category 2E Online voting & legal proceedings
2001-12-03 online voting risks internation laws agreements regulations principles legal analaysis

RISKS 21 81

Lucas B. Kruijswijk published an analysis of several national constitutions and International law with respect to online voting. He wrote in his introduction, "After some research I made the conclusion that some kinds of voting are indeed violating International Law. This means that there is a risk that a judge may forbid some kind of voting methods, making the investment worthless."

Category 2E Online voting & legal proceedings

2002-01-09 cybercourt Internet connection legal system vulnerabilities interception man-in-

the-middle attack confidentiality reliability availability integrity data diddling

NewsScan

MICHIGAN GOVERNOR ESTABLISHES CYBERCOURT

Michigan Governor John Engler has signed into law a bill to create a virtual state court -- the first to operate in the U.S., according to Matt Resch, an Engler spokesman. A cybercourt exists at the College of William and Mary in Virginia, but isn't operational, says Resch. The court won't have a jury and will handle only business disputes involving at least \$25,000. District or circuit court judges will be assigned for three-year terms and will be specially trained to use the system. "In a world where we can go from idea to IPO at warp speed, we need a connected court that can keep up," says Engler. (AP 9 Jan 2002)

http://apnews.excite.com/article/20020109/D7GU9I300.html

Category 2E Online voting & legal proceedings

2002-01-26 online court proceedings judgements Web

RISKS 21 26

Tony Ford summarized a new official self-service litigation system available in England & Wales in a brief article in RISKS (quoted verbatim below):

Today's Daily Telegraph (a quality UK broadsheet newspaper) carries a *potentially* disturbing report describing a new service, "Money Claim Online", whereby individuals and law firms (solicitors) can issue most simple legal proceedings (where a sum less than UK pounds 100,000 is claimed, = USD 140K)) and enforce judgments via a Web browser. The new service has been set up without publicity by the Lord Chancellor's Department, which runs the courts system in England and Wales. It seems that the system is accessible to the public now, although it has not been officially launched.

People using the service are (oddly) referred to as "customers" and there is a Customer Help Desk ...

The newspaper report is also viewable at this Daily Telegraph link on-line: http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2002/01/26/nsue26.xml&sSheet=/news/2002/01/26/ixho me.html

The service can be seen on-line at: https://www.moneyclaim.gov.uk/csmco/index.html

No details are apparent of what measures are taken to validate the identity of the claiming party or prevent other gross miscarriages of justice but it would appear that the potential exists for significant trouble even though the site warns that "vexatious litigants" are not allowed to us it (these are people who have abused the litigation system in the past to such an extent that they have been declared "vexatious litigants", restricting their ability freely to issue legal proceedings).

PS: I am a lawyer myself, although I don't practise in this area .. but do work in-house for a large IT company ... these comments are offered purely in a personal capacity.

2F Spyware

Category 2F Spyware

2001-02-01 spyware prohibition control privacy consumer software

NewsScan

SPYWARE SECURITY BILL RESURFACES

U.S. Senator John Edwards (D-NC) has reintroduced legislation that would protect the privacy of individuals from software that monitors their surfing habits. The Spyware Control and Privacy Protection Act was originally filed in October 2000, but Congress failed to take action on it. The Act mandates that companies that use codes to track the activities of Internet users would have to notify Web site visitors of their surveillance actions in plain language. Businesses that gather data would be required to let users know what information has been gathered, provide a way to correct errors, and safeguard the data against unauthorized access by hackers. (InfoWorld.com 31 Jan 2001) http://www.infoworld.com/articles/hn/xml/01/01/31/010131hnedwards.xml?p=br&s=5

Category 2F Spyware

2001-06-15 spyware Java covert installation unauthorized software Internet server firewall

end-user license agreement EULA

RISKS 21 49

Bill Tolle reported in RISKS on covert installation of spyware. Mr Tolle accepted an offer for rebates from < www.ebates.com > and discovered that the service had installed "Javarun.exe" on his system; "the program was trying to access the Internet and was also trying to act as a server for the Internet. Fortunately, the firewall caught it and stopped it." The covert installation was apparently the result of his having forgotten to disable Java in Internet Explorer while he was signing up for the service. Nowhere in the end-user license agreement was there any indication that a subscription would involve installation of such spyware.

Category 2F Spyware

2001-07-31 spyware license usage environment software EULA end-user license agreement

contract

RISKS 21 56

Livestage Pro from Totally Hip Software "phones home" to report via the Internet on its license information, usage and computing environment using a covert http interaction. According to Michael F. Maggard, writing in RISKS, the company stonewalled, refusing to discuss the issue; however, one employee did express surprise in a public discussion group that anyone would object to such a proceeding. He pointed to an explicit clause in the end-user license agreement that specifically allows the company to "electronically verify their serial number."

Category 2F Spyware

2002-01-04 spyware music-sharing peer-to-peer unauthorized installation implementation

supervision QA quality assurance

NewsScan

USER WEB HABITS TRACKED BY SOME MUSIC-SWAPPING PROGRAMS

The Web surfing habits of people who used the LimeWire, Grokster and KaZaA music-sharing programs were surreptitiously tracked because those programs were linked to an online sweepstakes game called ClickTillUWin, in which players pick numbers and win cash prizes. The company that operates the sweepstakes game says it told outside distributors to get users' permission before installing the software, but in these cases that action was not taken. The three companies have posted new versions of their software without the tracking component, and LimeWire has issued an apology. (AP/USA Today, 4 Jan 2002)

http://www.usatoday.com/life/cyber/tech/2002/01/04/limewire-tracking.htm

2G Scumware

Category 2G Scumware

2001-04-04 scumware alteration Web interpretation conversion alteration text HTML

RISKS 21 36

Marc Roessler reported an interesting effect of using filtering proxies. A colleague of his reported problems in a published text document Roessler had posted on the Web; it turned out that his colleague's WebWasher Version 3.0 for Windows was changing redirected links to direct links. The plaintext file included examples of enquoted HTML, but the proxy filter did not take the file type or quoting into account; in fact, it altered the file type from "text/plain" to "text/html" thus forcing the browser to interpret HTML fragements as instructions.

Category 2G Scumware

2001-05-23 scumware unauthorized modification editing changes invisible data corruption

integrity arrogance word processing spreadsheet office software design flaw arrogant public relations dismissive

RISKS 21 42

Jonathan Arnold reported with outrage to RISKS about yet another scumware feature in MS Office XP. "When you type a hyperlink in FrontPage 2002, Word 2002, Excel 2002, PowerPoint 2002, or Outlook 2002 (using Word as your email editor), the Office application will alter what you've typed, without notifying you or giving you an opportunity to undo the "correction." In fact, in most cases, you can't override the 'correction' at all: you're stuck with FP, Word or Excel's version of what you typed."

Specifically, Microsoft describes as a "feature" the fact that it silently and irremdiably removes double slashes from all hyperlinks typed in its Office XP suite. The descriptor is left as intended, but the underlying hyperlink is modified. Challenged with this bizarre behavior, Microsoft responded essentially that no one should be using double slashes anyway and that its unauthorized changes are in the interest of "cleanliness and consistency."

Quoting Peter Deegan, the correspondent adds, "The company has gone too far in compulsory changes to the link with no warning to the user or any workaround to fix the Autocorrect. Adding injury to insult, there's no documentation on these changes in the help file. Microsoft has declined to provide details of any other compulsory changes made to hyperlinks in Office XP nor have they suggested any workaround for those affected, or some way to switch off this behavior. The Microsoft arrogance shows through: it's not a problem, so why bother fixing it? The fact that Microsoft has declined to detail what changes are arbitrarily made to links makes us even more concerned. Office XP users don't know what compulsory changes will be made to their links. Chances are they'll find out the way I did - the hard way."

Category 2G Scumware
2001-06-07 Scumware HTML URL redirection Web advertising pornography

RISKS 21 47

Justin Mason provided RISKS readers with an interesting (if distressing) example of scumware. Mr Mason used a free URL-redirection service to provide an easier entry into his Web site, which had a cumbersome URL. Some years later, having forgotten all about the redirection. To his horror, someone who wanted to reach his site reported (and Mr Mason confirmed) that entering the old URL resulted in a number of unclosable windows with advertisements, including pornography.

[MORAL: routinely check all the URLs you have placed with redirection services to be sure that you approve of how your site is being represented to unsuspecting viewers.

Category 2G Scumware

2001-06-07 scumware pop-up advertisements hiding

RISKS 21 47

Greg Searle reported in RISKS on yet another way of annoying Web users. A company called Fastclick provides code that hides pop-up windows behind the windows already on screen. These pop-ups remain in place and are revealed only after one minimizes or closes the other windows on screen – by which time it is difficult to determine where the pop-ups came from. The solution, such as it is, is to disable JavaScript; alternatively, if one can locate the offending sites, one can put them on a firewall's or brower's exclusion list.

Category 2G Scumware

2001-06-20 BIOS ROM firmware Internet connection links desktop browser scumware

RISKS 21 51

Merlyn Kline reported a novel example of scumware to RISKS as follows [identity of "Myrv" not clear]:

Myrv writes: "There is an interesting thread over at DSL Reports discussing Phoenix Technologies new BIOS. This BIOS contains the PhoenixNet Internet Launch System. ILS resides safely within ROM and is activated the first time a user launches a PhoenixNet-enabled PC with a Windows 98 Operating System. When the PhoenixNet ILS detects an Internet connection, it makes contact with the PhoenixNet server and delivers user-selectable services. These services are delivered to the user as hotlinks on the desktop and in the web browser or, as applications that PhoenixNet automatically packages, downloads and installs. It's 3 a.m., do you know who your motherboard's talking to?????"

http://slashdot.org/yro/01/06/19/2039216.shtml

Category 2G Scumware

2001-06-22 scumware adware junk e-mail spam

NewsScan

TOOL WRAPS E-MAIL MESSAGES WITH SPAM

Admail, a new technology marketed by Australian online marketing firm Reva Networks, enables advertisers to intercept e-mail messages as they enter the mail server and "wrap" them in advertising content tailored to the recipient's demographic profile. Reva Networks CEO Robert Pickup says the concept has proven more effective than other forms of online advertising. "Because the advertising is embedded within a regular e-mail and not a separate e-mail message from an advertiser, users are more likely to open the message and hence be exposed to the advertising offer." Pickup says he doesn't think consumers will be annoyed by the ads "as long as it's relevant to them." But Australian Consumer Association IT policy officer Charles Britton says he doesn't think that consumers will passively accept advertising with their personal e-mail: "Without some incentive, why would you want advertising in your e-mail?" (ZDNet Australia 22 Jun 2001)

http://dailynews.yahoo.com/h/zd/20010622/tc/tool_feeds_spam_to_your_e-mails_1.html

Category 2G Scumware

2001-06-28 scumware smart tags Windows XP

NewsScan

MICROSOFT OFFERS NEW VERSION OF ITS OFFICE SOFTWARE [31 May 2001]

Microsoft today is announcing Office XP, sixth version of the software it introduced ten years, and which now has been integrated with the Internet for interactive information retrieval and collaboration. For example, a word processing feature called "Smart Tags" will allow documents to link automatically to Internet databases, and Microsoft Word will be able to recognize an address, a parcel shipping number, or a flight number, etc., and look up further information about it. Some of these retrieval functions will be free from company Web sites but others (such as legal searches in the Lexis-Nexis database) will cost money. (New York Times 31 May 2001) http://www.nytimes.com/2001/05/31/technology/31SOFT.html

MICROSOFT PULLS CONTROVERSIAL SMART TAG FEATURE [28 Jun 2001]

Bowing to a wave of criticism, Microsoft says it will kill plans to include a Smart Tag feature in its forthcoming Windows XP operating system. The feature would have allowed Internet Explorer to turn any word on any Web site into a link to Microsoft's own sites and services, or to a site of Microsoft's choosing. The company continues to defend Smart Tags in principle, and plans to work toward including it in a future version of Windows or Internet Explorer, but group VP Jim Allchin said the decision was made to remove the Smart Tags because "we got way more feedback than we ever expected." Although many people view the public reaction against Smart Tags as excessive, Wall Street Journal columnist Walter Mossberg says, "...Microsoft's dominant Internet Explorer browser is like a television set, or a digital printing press, for the Web. Its function is to render — accurately and neutrally — all Web pages that follow standard programming... Microsoft has a perfect right to produce and sell its own Web content with its own points of view. But it is just plain wrong for the company to use the browser to seize editorial control and to steal readers from other sites." (Wall Street Journal 28 Jun 2001)

http://interactive.wsj.com/archive/retrieve.cgi?id=SB993679289461737795.djm (sub req'd)

Category 2G Scumware

2001-08-29 scumware adware popup banners overlay advertisements lawsuit

NewsScan

LEGAL FIGHT OVER POP-UP BANNERS [29 Aug 2001]

The Interactive Advertising Bureau (IAB) is planning a complaint with the Federal Trade Commission against software Gator.com, and Gator has sued IAB in a preemptive legal strike. The IAB is asking the FTC to stop the practice of superimposing new ads over the existing ads of other Web sites. Gator argues that its software – which generates ads relevant to the particular individuals surfing a Web site – "is going to revolution the industry. There are a lot of online media sites that are failing right now and it's because their advertising isn't working." IAB president Jeff McFadden says: "What they are doing isn't very smart. It's harmful to Web sites and their advertisers and it's not very fair to consumers." (Washington Post 29 Aug 2001)

http://washingtonpost.com/wp-dyn/articles/A11208-2001Aug29.html

Category 2G Scumware

2001-11-09 scumware Microsoft Visual Basic programming language undocumented

modification unauthorized inconsisten stupid arrogant swine detestable

reprehensible disgusting nauseating

RISKS 21 74

John Sullivan noted yet another example of the questionable design philosophy of programmers and product managers at Microsoft. His report in RISKS demonstrates that Visual Basic (VB6 SP5) alters dates without permission, without notification, and inconsistently.

Part of his report reads, "... I'd entered the start date as a literal date of the form #2001-11-08#.... When I came back to it today, I noticed it read #11/8/2001#.... Retyping it showed that the date was changed in front of my eyes:

#2001-11-08# becomes #11/8/2001# (2001-11-08) #11/8/2001# becomes #11/8/2001# (2001-11-08) #8/11/2001# becomes #8/11/2001# (2001-08-11) #15/11/2001# becomes #11/15/2001# (2001-11-15)

It changes as soon as the cursor left the line. So you type it, check it, find it correct, go off somewhere else, blam! The first has reduced the comprehensibility of the code. The second and third give no feedback that they're not conforming to the current locale. The last two show that VB is not even being consistent in its parsing."

Nick Brown replied in a later RISKS that perhaps the algorith is as follows:

- Find a number which could only be the month
- Find a number which could only be the day
- If there is ambiguity, assume the user typed the date in mm/dd order

Category 2G Scumware

2001-11-14 scumware copyright content intellectual property advertising TV commercials

moral rights consumers tampering alteration

NewsScan

TV 'TIME MACHINE' SPARKS CONTROVERSY [14 Nov 2001]

A machine that "squeezes" television programming so that broadcasters can fit in extra commercials is stirring controversy in the industry. The Time Machine is being marketed by Prime Image for \$93,000 and so far, 120 have been sold to local stations in the U.S., with another 70 going to stations in Mexico. The patented technology shears seconds off of programming by editing out repetitive video frames in real time. With most TV shows running at 30 frames per second, a missing frame here or there is undetectable to viewers, but the accumulated time enables a station to insert an addition 20- to 30-second commercial. People in the TV industry say there is nothing controversial about using such a device during a local news show, for instance, but the problem arises when the station is airing programming from an outside source, such as a professional sports organization, that has strict limits on local commercials. Many Hollywood execs aren't happy with the Time Machine's ability to tinker with content in order to beef up advertising. "Adding more commercials that take away from content is the wrong direction for the industry to go," says Gary Newman, president of News Corp.'s 20th Century Fox Television. (Wall Street Journal 14 Nov 2001) http://interactive.wsj.com/articles/SB1005695943407459080.htm (sub req'd)

Category 2G Scumware
2001-12-06 scumware autocorrect proper names MS Word XP
RISKS 21 82

Arnold Weissberg was practically spitting with outrage in his note to RISKS about yet another example of having Microsoft engineers tell the rest of the world how to type:

"I typed my last name into a document. I thought something funny had happened because it came out with one "s." I never misspell my last name. There was a line under the "W". Holding the mouse on this line I got the following choices:

- 1. Change back to "Weissberg"
- 2. Stop Automatically Correcting "Weissberg"
- 3. Control AutoCorrect Options

Now this is, as my grandmother would have said, real chutzpah. Telling me how to spell my own name! Talk about arrogance--what's next, "anglicizing" it? Like, auto correcting it to "Whitehill?" And if I try to change it back will it say, "I'm sorry, Arnold, I can't do that"? I think in this little example we can learn a lot about Microsoft's corporate attitudes toward the rest of the world--that is, no one is smart enough even to be trusted to spell their own name right. Much less choose what software they'd like to use."

[MK notes: Hey, this is progress - at least you get to turn off the correction!]

Category 2G Scumware

2001-12-07 scumware Microsoft Office Windows XP sensitive information debugging

memory dump program crash document

RISKS 21 82

David Farber noted yet another threat to sensitive information from Microsoft Office XP and Windows XP. Writing in risk, he contributed the following summary:

PROBLEM: Microsoft Office XP and Internet Explorer version 5 and later are configured to request to send debugging information to Microsoft in the event of a program crash. The debugging information includes a memory dump which may contain all or part of the document being viewed or edited. This debug message potentially could contain sensitive, private information.

PLATFORM:

- * Microsoft Office XP
- * Microsoft Internet Explorer 5.0 and later
- * Windows XP
- * Microsoft has indicated that this will be a feature of all new Microsoft products

DAMAGE: Sensitive or private information could inadvertently be sent to Microsoft. Some simple testing of the feature found document information in one message out of three.

SOLUTION: Apply the registry changes listed in this bulletin to disable the automatic sending of debugging information. If you are working with sensitive information and a program asks to send debugging information to Microsoft, you should click Don't Send.

http://www.ciac.org/ciac/bulletins/m-005.shtml

Category 2G Scumware

2002-01-11 scumware Lotus Notes unauthorized undocumented data modification

corruption diddling arrogance stupidity criminal negligence design flaw bug error expletive deleted

RISKS 21 88

Erling Kristiansen posted a note in RISKS discussing undocumented, unannounced data loss in Lotus Notes. The author's examples follow verbatim:

By the way, correcting the addresses in place and re-sending had a very strange effect: The corrected addresses, and only those, were turned into an X.400-like address with a number of attributes pointing to my local environment. I had to remove and re-type the "sick" addresses to have them accepted.

- * I copied and pasted about 100 addresses from a spreadsheet into the bcc: field of a mail. Everything looked OK, the pasted addresses appeared neatly in the address window, I could scroll through them, etc. But the message was only sent to the first address. No warning of any kind appeared that a good hundred addresses had been discarded. I only discovered the error because I had asked for delivery notification, and got very few. Had I not discovered this, only a handful of people would have been invited to a presentation. (there were a few other addressees that had not been pasted in those worked OK even though some were entered AFTER the skipped addresses).
- * Notes allows you to format messages, with facilities more or less equivalent to an HTML editor. If a message is sent outside the Notes domain, ALL formatting is removed, even things like indentation and paragraph numbers. So a nicely formatted message may become rather unreadable, even ambiguous (indentation may imply a lot about the meaning of a text). No warning is given that formatting information is being removed.

The RISKS correspondent concludes, "The RISK of all this is that Notes accepts instructions to do something, does not complain about the input, and then goes ahead and does something else than what could reasonably be expected. You can obviously check for any of these events, but they are rare enough, and different enough, that you don't really know when to expect a problem, and what to look for in order to make sure everything went as expected."

Category 2G Scumware

2002-01-18 scumware Microsoft Excel unauthorized undocumented data modification

corruption diddling arrogance stupidity criminal negligence design flaw bug error expletive deleted

RISKS 21 88

Geoffrey Brent, writing in RISKS, identified yet another Microsoft undocumented, unauthorized data modification. If you open two MS-Excel files and copy a cell containing a number and paste it into a cell in the other file, everything works fine. For example, 1.2345 gets copied as 1.2345 regardless of how many figures are showing in the cell. However, if you open file A, copy a number, _close file A_, and then paste the number into file B, you get a value that is identical to what was _visible_ rather than to what was entered in the original cell. Thus in the example above, 1.2345 in the source becomes 1.23 in the destination worksheet. [MK note: I tested this myself in Excel 2000 and it's true.]

^{*} I printed a mail message before I sent it. Some of the cc: addresses were quietly and permanently removed. (Did anybody say buffer overflow recently? Maybe it is more like buffer truncation, but certainly member of the same family)

^{*} Trying to reply to a mail I received, I discovered that 3 out of the about 10 cc: addresses in the incoming message had been truncated, rendering them invalid. No addresses were lost completely, but the amount of truncation that occurred suggests that a short address might be "truncated into extinction" if it is in the right place in the list of addresses. I checked the original RFC-822 header that is accessible. It was correct.

Category 2G Scumware

2002-01-28 scumwarescumware unauthorized modification editing changes invisible data

corruption integrity arrogance word processing spreadsheet office software

design flaw arrogant public relations dismissive

RISKS 21

Bear Giles reported that Microsoft Outlook has an erroneous algorithm for recognizing UUENCODED text within the body of a message. The designers incorrectly assumed that any line beginning with the word "begin" must be the start of UUENCODED text. The algorithm does not bother to check for any other evidence that this assumption is correct, with the result that perfectly ordinary text is relegated to an attachment and may easily be lost. In addition, malware writers have already figured out that they can send ordinary text messages and have Outlook obligingly convert embedded malicious code into an attachment _after_ it has gone through a firewall or e-mail filtereven if users don't permit attachments to get through.

Microsoft's breathtakingly arrogant workaround (not solution) for their own design error was to recommend that everyone on the planet either stop using the word "begin" or use the capitalized form "Begin" in all e-mail messages sent to Outlook users or potentially forwarded to Outlook users -- that is, in effect, in all e-mail messages the world over.

Category 2G Scumware

2002-01-29 scumware automated spelling correction software

RISKS 21 90

Automated spelling-correction software mangled several names in the HP'annual report; examples include "David and Lucite Packard Foundation" [from "Lucile"], "Edwin van Pronghorns" [from "Bronkhorst], "Eleanor Hewlett Limon" [from "Gimon"], and "Mary Hewlett Gaffe" [from "Jaffe"]. http://www.siliconvalley.com/docs/news/tech/085146.htm

Category 2G Scumware

2002-02-12 scumware Google search engine periods removed data modification corruption e-

mail address bounce

RISKS 21 91

Google appears to remove some periods even in e-mail addresses that appear in the summary lines for hits. Robert Marshall reported this problem to RISKS as follows (quoting verbatim):

I was searching for the work e-mail address for a friend using google. Let's say the name was Paul Consultant. Google gave me a hit with the correct company and the web page was such that his e-mail appeared in the google summary. So I cut and pasted it directly without having to visit the company web site. It appeared as PR.Consultant@relations.com.

When the e-mail bounced I investigated and the company web page has the mail as P.R.Consultant@relations.com, as does google's cache. It looks as if google is trying to cut down on the synposis by removing redundant '.'s

Unfortunately they aren't always redundant. Fortunately my e-mail bounced rather than going to an unrelated recipient.

31.1 Surveys, studies, audits

Category 31.1 Surveys, studies, audits

2001-01-04 survey CIO confidence security law enforcement

NewsScan

CIOs: "WHAT, ME WORRY?"

A national poll of 1,400 CIOs reveals that 90% have confidence in their network security, despite estimates that billions of dollars are lost every year to cybercrime. The survey, conducted by RHI Consulting, has raised eyebrows among security experts who point out that it's generally in a CIO's best interest to keep quiet when security breaches occur. A recent survey conducted by the Computer Security Institute indicated that more than half of the respondents said they did not report the intrusions to law enforcement out of fear of negative publicity or that rival companies would use the information to competitive advantage. In addition, many CIOs may feel that they must live with a "buffer of acceptable risk." "Just as credit card companies accept some level of loss as a cost of doing business, so some CIOs are saying, 'if I do a really solid job of protecting my systems, then I can live with the low-level pain that some break-ins cause,'" says one expert. Meanwhile, a 1999 survey found that Fortune 1000 companies lost more than \$45 billion in thefts of proprietary information that year. (InfoWorld 3 Jan 2001)

http://www.infoworld.com/articles/hn/xml/01/01/03/010103hncios.xml?p=br&s=2

Category 31.1 Surveys, studies, audits

2001-01-12 computer crime statistics exaggeration inflation

RISKS 21 21

S. Harris contributed an interesting analysis to RISKS of how very large figures get reported for losses due to industrial espionage. In response to another correspondent's question about how companies estimate the costs of breaches of confidentiality, he wrote the following:

>I can give a first hand account of a \$2 billion theft of proprietary information to illustrate how these exaggerated figures get manufactured. Back in 1989 I worked at a Toronto software development company that did lots of work with the Unix operating system, and licensed the Unix source code from AT&T for about \$60,000 a year.

Night after night someone was logging in to the computers from a dialup line to download chunks of the Unix source code. Somebody at the company noticed this, called in the police, who traced the connection to an ex-employee, raided his house and seized his home computer. Apparently the ex-employee, a software development manager, who had recently left the company, missed having access to the Unix source code and wanted to grab a copy of it for personal study. Satisfied that the source code had been recovered, and that this wasn't a case of espionage or sabotage, the company would have been happy to let the matter drop.

But the cops insisted on laying charges and it appears that they leaked the story to the media. All three Toronto newspapers (Toronto Sun, Toronto Star, and the Globe & Mail) reported that the police had foiled a \$2 billion theft!

Why wasn't this as a \$60,000 theft of a commercial source code license? Or at the very most a \$500 theft of an educational license, since the ex-employee's intended use was only to study it?

Well it seems that the police had called up AT&T and asked them "How much is Unix worth?" The answer was \$2 billion. AT&T gave Unix an asset value of \$2 billion on their books. The police equated a little mischief to the cost of acquiring total ownership of AT&T's Unix System Laboratories and all its intellectual property!

In this case, the large corporation gave an accurate estimate to a bogus question. It was law enforcement (and sloppy fact checking by the media) that twisted the story.

But you know, even the \$2 billion asset value seems suspect to me now because AT&T sold Unix to Novell in 1993 for just \$270 million (see http://www.att.com/press/0693/930614.ulb.html). Novell in turn sold it to SCO in 1995 for a paltry \$54 million (6M SCO shares at about \$9 each is \$54M, see

 $http://www.novell.com/company/ir/96annual/mandis.html). \ But if AT&T overestimated by tenfold, the police still exaggerated by 4 million fold. <$

Category 31.1 Surveys, studies, audits

2001-01-24 privacy marketing children study survey

NewsScan

ONLINE KIDS READY TO TELL YOUR SECRETS

Three out of four children are perfectly willing to divulge private family information online in exchange for incentives such as prizes, products or cash, according to a new report by eMarketer. Fifty-four percent of the children surveyed were willing to disclose the name of their parents' favorite store, while 26% were willing to tell e-tailers about their parents' weekend activities. According to the study, the information typically given by children online tends to be marketing oriented, rather than financial. "The information is not the really serious information like credit card or Social Security numbers," says eMarketer analyst Rob Janes. "It's more stuff that's of value to a marketer, such as product information, family activities, etc... Children and teens were very casual about revealing family information. It can't be extrapolated accurately to the entire population, but it's a good strong indicator of how kids will respond to information online. It's an issue that parents should address." (E-Commerce Times 24 Jan 2001) http://www.ecommercetimes.com/perl/story/6942.html

Category 31.1 Surveys, studies, audits

2001-02-12 privacy corporate governance administration position CPO

NewsScan

CHIEF PRIVACY OFFICER AN ACCEPTED POSITION IN TODAY'S ORGANIZATIONS

The position of CPO ("chief privacy officer") is being created at an increasingly large number of U.S., including some companies as IBM, AT&T, Eastman Kodak, DoubleClick, RealNetworks, Microsoft, U.S. Bancorp, and many others. Privacy expert Alan F. Westin says there are now at least 100 privacy chiefs in the United States, making \$125,000 to \$175,000 a year, and he expects that number will grow by 5 to 10 times just one year from now." Who becomes a CPO? Stephanie Perrin, the chief privacy officer of Montreal-based Zero-Knowledge Systems, explains: "Obviously, we're not going to just pick somebody from the legal department," because privacy is more than a matter of just following the law. "You have to have a fundamental commitment to - dare I say it? - morality. Privacy is not just good business. We are framing the information age, and it is important to take that job seriously. We really do look at privacy as a human right, and not just a luxury item for spoiled North Americans. We're talking about the global information infrastructure." (New York Times 12 Feb 2001)

http://partners.nytimes.com/2001/02/12/technology/12PRIV.html

Category 31.1 Surveys, studies, audits

2001-02-12 online gambling survey predictions

NewsScan

ONLINE GAMING TAKES OFF IN U.S.

Forty million households will be engaged in online gaming by 2004, up from 25 million in 2000, according to new research from IDC. Fueling the growth will be faster Internet connections, the arrival of next-generation game consoles, and new, nontraditional gaming platforms. Most online gaming business models are based on advertising revenue, but sites are seeking ways to create different types of advertising opportunities or to migrate free subscribers to a paid model. Meanwhile, NetValue reports that in Europe, the U.K. leads Germany, France, Spain and Denmark in online gaming, with one in five British Internet users visiting a game site in December. Spanish gamers spent an average of 27 minutes on each site, Danish and U.K. users 23 minutes, French and German users just 14 minutes, while U.S. users stayed online an average of 38 minutes. The most visited game site in the U.S. was uproar.com, while in the U.K., gamers flocked to gamesdomain.com. (NUA Internet Surveys 12 Feb 2001) http://www.nua.ie/surveys/?f=VS&art_id=905356444&rel=true

Category 31.1 Surveys, studies, audits

2001-03-10 CERT/CC Summaries general trends vulnerabilities attacks malicious software

malware

CERT/CC Summaries

The CERT/CC Summaries Web page < http://www.cert.org/summaries/ > lists (and links to) the following regularly-scheduled overviews for January 2001 through March 10, 2002:

CS-2002-01

February 28, 2002

Topics in this regularly scheduled CERT Summary include multiple vulnerabilities in SNMP, a buffer overflow vulnerability in Microsoft Windows UPnP, vulnerabilities in SSH implementations, and the W32/BadTrans Worm.

CS-2001-04

November 20, 2001

Topics in this regularly scheduled CERT Summary include the W32/Nimda Worm and active exploitation of vulnerabilities in SSH1 CRC-32 Compensation Attack Detector and in Microsoft DNS servers.

CS-2001-03

August 28, 2001

Topics in this regularly scheduled CERT Summary include self-propagating worms, active exploitation of vulnerabilities in Solaris in.lpd, BSD telnet daemon, and Microsoft IIS by intruders. We have also seen an increase in intruder activity directed at home users.

CS-2001-02

May 29, 2001

Topics in this regularly scheduled CERT Summary include a significant increase in reconnaissance activity, a number of self- propagating worms, and active exploitation of vulnerabilities in snmpxdmid, BIND and IIS by intruders

CS-2001-01

February 28, 2001

Topics in this regularly scheduled CERT Summary include multiple vulnerabilities in BIND, compromises via "ramen" toolkit, input validation problems in LPRng, and VBS/OnTheFly (Anna Kournikova) malicious code. There is also mention of the new Vulnerability Notes Database.

Category 31.1 Surveys, studies, audits

2001-04-03 survey privacy attitudes USA surveillance Internet

NewsScan

PEOPLE WANT PRIVACY FOR THEMSELVES, SURVEILLANCE FOR OTHERS

A Pew Internet & American Life Project survey of Internet users has found that Americans have distinctly mixed feelings about privacy on the Internet: they want it for themselves but they also want the government to use surveillance techniques to catch pornographers, con artists, and other criminals online. More than 90% of those surveyed expressed revulsion at child pornography online, and 62% want legislators to pass new laws protecting online privacy. According to project director Susannah Fox: "Americans are searching for an Information Age answer to the age-old question of how to balance their yearning to be protected from criminals and their yearning to prevent government authorities from abusing their investigative powers..." (Washington Post 2 Apr 2001) http://washingtonpost.com/wp-dyn/articles/A28560-2001Apr2.html

Category 31.1 Surveys, studies, audits

2001-04-10 survey study music intellectual property copyright sharing alternative

NewsScan

STUDENTS WILLING TO PAY FOR MUSIC

More than a third of students who download music from the Internet would be willing to pay \$8.50 a month for the privilege, according to a survey of 1,800 students on campuses ranging from Harvard to the University of Southern California. The typical student is interested in singles, live tracks, international music and new artists, and spends more time listening to tunes on his or her computer than on the radio. Boosting these figures is the fact that the typical student also has access to fast Internet connections and high bandwidth. "As broadband grows, more people will use computers for music and other entertainment," says an analyst with Mercer Management Consulting, which conducted the poll in conjunction with the National Association of Recording Merchandisers. "We don't feel this is going to erase CD purchasing completely. This is a new opportunity. There's a whole other batch of music record labels could sell to people... One of the biggest surprises to some of the retailers is that people sample music on Napster and then go out and buy it." (InformationWeek 9 Apr 2001)

http://www.techweb.com/wire/story/TWB20010409S0020

Surveys, studies, audits Category 31.1

2001-04-17 privacy policy compliance federal government Web report

NewsScan

FEDS LAX IN FOLLOWING PRIVACY GUIDELINES

Senator Fred Thompson (R., TN) says that a forthcoming study will show that dozens of federal Web sites are ignoring guidelines intended to protect the privacy of persons visiting them, and are not closely managing how the sites are operated. One agency, the National Aeronautics and Space Administration, was not even able to determine how many Web sites it operates. The report, which will be released within a few months, was assembled from 16 separate agency audits. http://www.cnn.com/2001/TECH/internet/04/17/internet.privacy.ap/index.html?s=10

Category 31.1 Surveys, studies, audits

2001-04-19 study COPPA Children's Online Privacy Protection Act enforcement evasion

NewsScan

CHILD PRIVACY LAW BEING EVADED [28 Sep 2001]

A study of the effectiveness of the rules the Federal Trade Commission issued to implement Children's Online Privacy Protection Act (COPPA) has found that most Web sites have failed to do what the law requires. One of its requirements is for sites must obtain "verifiable parental consent" involving any use of data from children under 13; another is that the privacy policy of the sites be clearly explained. The new study, which was authored by Joseph Turow of the University of Pennsylvania's Annenberg Public Policy Center, says that a large number of sites are skirting the intent of those requirements, and that most of the site policy statements were so long and complex that it took an average of 9.4 minutes to reach policy in search of its COPPA statements. (San Jose Mercury News 28 Sep

http://www.siliconvalley.com/docs/news/svfront/034390.htm

FTC FINES THREE KIDS SITES FOR PRIVACY VIOLATIONS [19 Apr 2001]

Three Web sites for young people -- GirlsLife.com, BigMail.com, and InsideTheWeb.com -- have agreed to pay \$100,000 to settle charges brought against them by the Federal Trade Commission for collecting personal data about children without proper permission from their parents. A survey of kids sites by the nonprofit Center for Media Education found that only 38% of those required to obtain parental permission did so adequately. (AP/USA Today 19 Apr 2001) http://www.usatoday.com/life/cyber/tech/2001-04-19-kids-sites-privacy-fine.htm

Category 31.1 Surveys, studies, audits

2001-05-01 audit review study survey Web weaknesses vulnerabilitiesl servers

NIPC Daily Report

At least 100 New Zealand Web sites have security flaws, claims an Auckland-based Internet security firm. Software Creations says this includes one in five of those using version 5 of Microsoft's Internet Information Server (IIS) and a third of those with version 4. The claim follows a "friendly hack" of the sites earlier this month by owner-operator Brett Moore using a year-old "web bug." The program enters a Web site and, depending on the code returned, tells a hacker if a system is at risk assess the sites using a simple program he developed in 20 minutes. He says it is similar toand took two hours to test the sites. (IDG News Service, 1 May)

Category 31.1 Surveys, studies, audits

2001-05-07 Web sites vulnerabilities audit weaknesses study survey

NIPC Daily Report

Out of three million Web sites tested worldwide, 80 percent have been given the thumbs down when it comes to security vulnerability, exposing a large number of organizations and governments to hackers, criminals and vandals. The study, by Unisys Australia Architecture Director, IT Security Consulting Services Ajoy Ghosh, randomly tested three million .com, .net, and .au domains for security holes, finding 80 percent of Web sites transacting on the Internet open to damage and theft as the correct technology is not in place. The study further revealed that Australian banks were among the Web sites most open to online attacks.

Category 31.1 Surveys, studies, audits

2001-05-29 music piracy copyright intellectual property youth culture survey study

NewsScan

YOUNGER USERS CRANK UP THE VOLUME ON ONLINE MUSIC

More than half of all young adult Web users (age 18 to 24) have downloaded tunes from the Internet, according to a survey of 7,688 Internet users from 30 countries. Research firm Ipsos-Reid found that 61% of users in that age group had downloaded music, up from 53% a year earlier. The study also found that 70% of males age 18 to 24 had downloaded music, compared with 48% of females. Meanwhile, another study conducted by Informa Media Group predicts that with the advent of big-label music subscription services, subscriptions likely will account for nearly 24% of online music sales worldwide by 2006. The study estimates total global music sales, online and off, will increase 26% to \$46.5 billion in 2006, led by the U.S. with 54% of the market. Europe and Asia-Pacific will follow, with 25% and 18% respectively. "We really are witnessing the dawn of the global music bazaar," says a senior researcher at Ipsos-Reid. "In a few years we're going to be seeing people from anywhere in the world acquiring music online from anywhere in the world -- a sort of musical ubiquity." (CNET News.com 29 May 2001) http://news.cnet.com/news/0-1005-200-6087379.html?tag=owv

Category 31.1 Surveys, studies, audits

2001-06-05 physical damage sabotage computers equipment rage

NewsScan

SURVEY REVEALS EPIDEMIC OF BATTERED PCs

A survey by British PC maker Novatech, intended to take a lighthearted look at techno-glitches, instead revealed the darker side of computing. One in every four computers has been physically assaulted by its owner, according to the 4,200 respondents. "The incidents of willful neglect have always been high," says the owner of a New York computer repair shop. "We've always had to deal with computers damaged by people who dumped their refreshing beverage on the computer's keyboard, or got tangled up in the cords, bringing the computer crashing down off their desk." But recently, more instances of intentional abuse are cropping up – broken keys "from people smacking down on the keyboard with an open hand or sometimes a fist," and more commonly, "a sharp slap delivered to the monitor or the hard drive case. If you smack a machine when the hard drive is spinning, you can kill the hard drive." Most likely to provoke abuse by British users were "oops" moments, like when sensitive e-mail is sent to the wrong recipient, or a cache of previously visited porn sites is revealed at the wrong time. But an Italian repair specialist said it was all part of the culture: "People here tend to express themselves very emotionally. It is not uncommon for them to hit their televisions, their scooters and their computers... And sometimes a fast smack does fix the problem, you know." A retired psychology professor from Budapest sums it up: "We treat our machines as if they are persons. We talk to them, we name them, we even somachine. And when the little god turns out to be evil we beat the machine to purge the demon." (Wired.com 5 Jun 2001)

http://www.wired.com/news/culture/0,1284,44284,00.html

Category 31.1 Surveys, studies, audits

2001-06-09 expectation of privacy workplace monitoring survey study

NewsScan

WORKPLACE PRIVACY "A CONTRADICTION IN TERMS"

A study by the American Management Association (AMA) has found that three out of four of the 1600 U.S. businesses it surveyed electronically monitor their employees in one way or another. Internet connections were monitored by 63%, telephone use by 43%, computer use (time logged on or keystroke counts) by 19%, video security surveillance by 38%. Although federal law generally prevents employers from monitoring of live conversations, it does not apply when the communication is stored and retrieved, such as through voice mail, e-mail, or Web monitoring. The director of the AMA study said: "Workplace privacy is a contradiction in terms. It's an oxymoron. I know the illusion of privacy is there, but you are not using your own stuff. The phone, the keyboard, the connections, the job itself – they don't belong to you; they belong to the company, legally." (San Jose Mercury News 9 June 2001) http://www.siliconvalley.com/docs/news/svfront/066891.htm

Category 31.1 Surveys, studies, audits

2001-07-15 Internet Web fraud statistics survey study report

NewsScan

INTERNET FRAUD KEEPS GOING AND GOING

The National Consumer League says that the average loss from Internet fraud rose from \$310 a person in 1999 to \$427 last year, when total losses from Internet fraud reached \$3.3 million. New York City's consumer affairs commissioner Jane Hoffman warns: "Internet fraud runs the gamut from work-at-home scams to bogus travel and vacation schemes, to securities fraud and investment scams... For many consumers the Internet can be a virtual nightmare when it comes to fraud." Hoffman says the five most common Internet scams are: Web auctions (mainly in the form of goods not delivered as promised, inflated prices, or fake bids to puff up prices); travel and vacation schemes with hidden costs; theft of ID numbers, bank data, or passwords; and investment schemes promising – but of course failing to deliver – huge profits. (AP/Washington Post 15 Jul 2001)

http://washingtonpost.com/wp-dyn/business/latestap/A492-2001Jul15.html

Category 31.1 Surveys, studies, audits

2001-08-03 security audit government passwords access confidentiality operations availability

NewsScan

NETWORK SECURITY PROBLEMS AT COMMERCE DEPARTMENT

The General Accounting Office has prepared a report critical of the U.S. Commerce Department's computer security measure: "Individuals, both within and outside Commerce, could gain unauthorized access to these systems and read, copy, modify and delete sensitive economic, financial, personnel and confidential business data. Moreover, intruders could disrupt the operations of systems that are critical to the mission of the department." Many users of Commerce systems were found to have easily-guessed passwords and to have greater network access than justified by their 'need-to-know' level. (AP/San Jose Mercury News 3 Aug 2001)

http://www.siliconvalley.com/docs/news/svfront/064118.htm

Category 31.1 Surveys, studies, audits

2001-08-28 survey study music intellectual property copyright sharing alternative

NewsScan

CONSUMERS NOT READY TO PAY FOR ONLINE MUSIC

Consumers are resistant to the idea of purchasing and downloading music from the Web and are likely to remain so, according to a poll of 4,000 Internet users by GartnerG2. Less than 50% of respondents listened to CDs on their computers, and only 25% had listened to music downloads on their PCs. Only 6% reported purchasing digital music downloads in the last three months. "The percentage of Internet music buyers is not likely to increase with new Internet services being developed by the big five music companies unless they make their copyright protection systems more flexible to entice consumers," says a Gartner analyst. "Digital distribution needs to be brain-dead simple for consumers, and any DRM solution deployed should work with all music software and hardware. In order for this to happen, the Big 5 need to work together, and that doesn't look hopeful before 2002." (Reuters 28 Aug 2001) http://news.cnet.com/news/0-1005-200-6997967.html?tag=nbs

Category 31.1 Surveys, studies, audits

2001-08-30 privacy online banking industry survey study report inadequate problems

NewsScan

PRIVACY INADEQUATE FOR ONLINE BANKING, SAYS REPORT

A report by the nonprofit advocacy group Center for Democracy and Technology says that the Center has filed a complaint with the Federal Trade Commission charging five regional bankers of failing to post any notice of their privacy rules. George Washington law professor Peter Swire said at the press conference held to announce the report's release: "The price of opening a checking account should not be that your personal information is traded, sold or swapped." The CDT found some banks much better than others with regard to privacy protection, and praised First Union Bank for providing multiple ways in which customers can protect their personal information from being shared with merchants and others. (Washington Post 30 Aug 2001)

http://washingtonpost.com/wp-dyn/articles/A16683-2001Aug29.html

Category 31.1 Surveys, studies, audits

2001-10-02 Web security audits studies vulnerabilities

NewsScan

NEW INTEREST IN NETWORK SECURITY

Security companies are being deluged with business opportunities, and CEO Peggy Weigle of the Internet security firm Sanctum explains, "Network security used to be a necessary evil, but now it's a core value of companies." Doing security audits commissioned by 300 organizations, Weigle found the results "scary" and said, "We could have stolen flight manifests, personnel files, sensitive data... We could have easily gotten onto a flight illegally." Research firms Gartner and IDC predict that the network security market in the U.S. will grow 20% to 24% a year between now and 2005. (USA Today 2 Oct 2001)

http://www.usatoday.com/life/cyber/tech/2001/10/2/network-security.htm

Category 31.1 Surveys, studies, audits

2001-11-16 security audit government departments agencies Congressional committee failing

grade GAO passwords encryption confidentiality

RISKS 21 76

Peter G. Neumann summarized another security evaluation of government departments and agencies:

"The latest quarterly computer-security report card put together by Congressman Steve Horn's House Reform Committee government efficiency subcommittee and the GAO and OMB gives the government an F grade (down from a D- a year ago), based on lax protection of federal computer networks against hackers, terrorists, and others. Two-thirds of the federal agencies flunked this time, including the departments of Defense, Commerce, Energy, Justice, Treasury, Agriculture, AID, Education, Health and Human Services, Interior, Labor, Transportation, Small Business, and Veterans Affairs. The B+ given to the National Science Foundation was tops, with Social Security getting a C+ and NASA C-. As expected, the GAO found systems with no passwords, with ``password'' as password, and with unencrypted accessible password files. [Source: AP Online via COMTEX, 9 Nov 2001, PGN-ed] "

Category 31.1 Surveys, studies, audits

2001-12-29 medical information security informatics implementation failures ignorance

RISKS 21 84

Laura S. Tinnel analyzed a medical-office's new online medical records system and wrote a good essay in RISKS about the perils of having amateurs deal with such systems. Some highlights (or maybe "lowlights" would be a better word) summarized from her interesting report:

- * Physically unprotected workstation allowed reboot and installation of Trojan software.
- * Live network connection allowed network access to anyone.
- * Responsible doctor had no idea how system was configured to avoid default wide-open state.
- * No thought about unauthorized write-access to patient data or consequences of such data diddling.

Category 31.1 Surveys, studies, audits

2002-01-10 copyright intellectual property music sales statistics survey study royalties fees

NewsScan

LET THERE BE MUSIC, LET THERE BE LOVE, LET THERE BE VULGAR ROYALTIES

Soundscan, a company that tabulates retail sales of recorded music, has reported that the number of albums sold last year dropped 2.8% from previous-year's sales, the first decline since the company began a decade ago. One record company executive warns, "We have to rethink our business, and it may not be the record business anymore." Concurring with that assessment, Michigan congressman John Conyers Jr., the senior Democrat on the House Judiciary Committee, says: "Technology is forcing the record labels and the artists and the writers and the composers to come together. The Internet says to the industry that you folks are yesterday's news, you're following outdated models, your business strategies don't work anymore, and your profit motive is showing rather vulgarly." And Eben Moglen, a Columbia University law professor and general counsel of the Free Software Foundation, pleads for a return to the spirit of "music before Edison" — a time when (he believes) music was not a commodity but a form of love. Alluding to the music-swapping experiments that take place on the Internet, Moglen argues that "everything that can be shared will be shared. But people make music because they love it, and they'll pay for it because they love it." (New York Times 10 Jan 2002)

http://partners.nytimes.com/2002/01/10/arts/music/10CONF.html

Category 31.1 Surveys, studies, audits

2002-01-30 non-profit organizations security practices survey audit results sensitive data

confidentiality intrusion vulnerability disaster recovery

RISKS 21 91

Audrie Kraus, Executive Director of NetAction, summarized the disturbing results of that organization's "survey of security practices in nonprofit organizations" which found among many other things that non-profits studied had "... substantial room for improvement, especially in maintaining the security of confidential and/or sensitive files, user work habits, and disaster planning."

http://netaction.org/security/.

Category 31.1 Surveys, studies, audits

2002-02-04 security industry survey study statistics revenue growth

NewsScan

SECURITY FIRMS PROSPERING UNDER NEW CONDITIONS

Computer security companies are surviving the technological recession quite nicely, and one of them, Symantec, expects to break the billion-dollar sales mark this year. Gartner says that Symantec is the No. 1 provider of security and antivirus software but that it has been trailing Internet Security Systems and Check Point Software Technologies in detection and firewall software. (San Jose Mercury News 4 Feb 2002) http://www.siliconvalley.com/docs/news/svfront/symant020402.htm

Category 31.1 Surveys, studies, audits

2002-02-25 online pornography addiction survey study statistics estimates

NewsScan

ADDICTED TO "ADULT" SITES

An online survey by the San Jose Marital and Sexuality Centre reports that 10% of the 7,037 individuals responding to the survey say they are addicted to cybersex. Other data: Neilsen/NetRatings figures indicate that there were 27.5 million U.S. visitors to adult-oriented sites last month; of that number, 72% were men and 28% women. (USA Today 25 Feb 2002)

http://www.usatoday.com/life/cyber/tech/2002/02/26/cybersex.htm

Category 31.1 Surveys, studies, audits

2002-02-25 music piracy copyright intellectual property theft survey study statistics losses

damage ethics

NewsScan

RIAA: PUT ANOTHER NICKEL IN THAT NICKELODEON FOR MUSIC, MUSIC, MUSIC

The music industry is desperate to find a way of downloading a solution to the problem of illegal downloading of copyrighted songs. The Recording Industry Association of America (RIAA) says that shipments by record companies to consumers have dropped by more than 10% in the past year, and RIAA president Hilary Rosen complains: "When 23% of surveyed music consumers say they are not buying more music because they are downloading or copying their music for free, we cannot ignore the impact on the marketplace. " (Reuters/New York Times 25 Feb 2002) http://partners.nytimes.com/reuters/technology/tech-leisure-music.html

31.2 Estimates, guesses, predictions, forecasts

Category 31.2 Estimates, guesses, predictions, forecasts

2001-01-29 spam junk unsolicited bulk e-mail costs fees

NewsScan

ONLINE MARKETERS WILL SOON HAVE TO PAY TO SPAM

Online marketers soon will have to pay for the privilege of sending promotional e-mail to consumers, says Jupiter Research, which predicts that 268 billion advertising messages will be sent in 2005 – 22 times the number sent in 2000. The trend will open up a substantial new revenue stream for portals, ISPs and Web-based e-mail services, but will raise the costs of e-mail marketing campaigns significantly. Jupiter says that sending solicitation messages to a user's "bulk" e-mail in-box likely will still be free, but that marketers will have to pay a premium for profiled delivery, based on individual usage behavior. The research firm suggests marketers should be working now to establish strategic partnerships with major e-mail service providers in the hope of securing reduced rates in the future. (NUA Internet Surveys 29 Jan 2001)

http://www.nua.ie/surveys/?f=VS&art_id=905356392&rel=true

Category 31.2 Estimates, guesses, predictions, forecasts

2001-03-27 junk unsolicited bulk e-mail spam international cooperation

NewsScan

EC STUDY TARGETS JUNK E-MAIL

A new report issued by the European Commission predicts that unsolicited e-mails could in the future cost about US\$10 billion a year to download, and calls on governments to coordinate efforts to stem the tide. Fueling the growth in unsolicited mail will be a sharp increase in legitimate, non-spam messages sent by companies with which the recipient might already have a business relationship. According to Jupiter Media Metrix, the number of commercial e-mails received each year by the average U.S. consumer will grow from 40 in 1999 to 1,600 in 2005. Meanwhile, Forrester Research is predicting that more than 200 billion e-mail messages will be sent by marketing companies in 2004, an average of nine per household every day. And while U.S. companies rely on consumers to "opt out" of receiving unwanted mail, European authorities are moving in the opposite direction. Five countries -- Austria, Denmark, Finland, Germany and Italy -- have legislated for an "opt in" system that prohibits sending e-mail to consumers unless they've indicated they wish to receive them. Marketing experts on both sides of the Atlantic say it will be difficult to resolve the differences between the two systems, and some have urged a differentiation between straight spam, mail sent by third parties, and mail sent to a company's existing customer database. (Financial Times 27 Mar 2001)

http://news.ft.com/news/industries/internet&e-commerce

Category 31.2 Estimates, guesses, predictions, forecasts

2001-04-19 music intellectual property copyright peer-to-peer networking violations

infringement intellectual property effects results sales

NewsScan

ONLINE MUSIC CUTS INTO MUSIC SALES IN U.S.

The U.S. record industry is blaming online music and the economic slowdown for a drop in music sales. Annual figures from the International Federation of the Phonographic Industry show sales of singles fell by 38% in the U.S., and cassettes by 46%. "The downturn in the USA brought down the overall sales figures," says a spokesman for the IFPI. "We also saw the first evidence of the impact of free online music, as well as damage done by unauthorized CD-R copying in some major markets." France, Italy and Germany also reported lower sales, which they attributed to illegal copying. Meanwhile, the bright spot was the UK, where a 6.2% increase in unit sales helped boost the European market overall. (Ananova 19 Apr 2001)

http://www.ananova.com/news/story/sm 263235.html?menu=news.technology

Category 31.2 Estimates, guesses, predictions, forecasts

2001-05-21 software piracy copyright intellectual property theft losses survey study

guesswork estimate

NewsScan

37% OF PROGRAMS USED IN BUSINESS ARE PIRATED

Software piracy grew in 2000 for the first time in more than five years, according to the Business Software Alliance, which estimates that 37% of all software programs used by businesses worldwide are illegal copies. The Asia-Pacific region -- where more than half of all software in use last year was stolen -- tops the list in terms of dollars (an estimated \$4 billion) lost to piracy. Meanwhile, Eastern Europe has the highest piracy rate, with 63% of its software illegally copied in 2000. In the U.S., 24% of programs are pirated copies. Although progress is being made in some regions, BSA director of enforcement Bob Kruger takes little comfort. "That's kind of like saying that I'm having fewer heart attacks than I used to. But the damage that's being caused by piracy is still devastating. It can be counted in the thousands of jobs and billions of dollars lost." (AP 21 May 2001) http://news.excite.com/news/ap/010521/07/software-piracy

Analyses in the RISKS Forum Digest 21.44 were highly critical of the methodology of this study. Critics pointed out, among other criticisms, that many assumptions were used in projecting piracy from the numbers of computers sold versus expected numbers of software licenses sold. Contributors also noted that the BSA has a vested interest in inflating such estimates and that members of the BSA were consulted during analysis of the results before publication.

Category 31.2 Estimates, guesses, predictions, forecasts

2001-05-28 Internet vulnerabilities weakness collapse virus

NewsScan

INTERNET "WAITING FOR ITS CHERNOBYL," SAYS SECURITY EXPERTS

Internet security experts such as Peter G. Neumann of SRI International and Bruce Schneier of Counterpane Internet Security believe that security on the Internet is very poor. Schneier characterizes the Internet as "just too complex to be secure," and Neumann predicts: "The Internet is waiting for its Chernobyl, and I don't think we will be waiting much longer; we are running too close to the edge." In the process of compiling material for a New Yorker magazine article on Internet security issues, journalist Michael Specter hung out with network "crackers" in Amsterdam and observed them take over the Los Angeles Police Department computer system, steal passwords from a university in Korea, and break into his own Web site. He also received a lesson in creating viruses and produced one that erased all the data on one of his computers. (New Yorker 28 May 2001) print only

Category 31.2 Estimates, guesses, predictions, forecasts

2001-08-01 software piracy copyright infringement intellectual property survey estimates

losses costs

NewsScan

SOFTWARE BANDITS "ARE EVERYWHERE" The software industry estimates that illegal copies of software robbed it of \$12 billion in revenue last year, an amount equivalent to 15% of the industry's total sales. A director of the corporate security firm Kroll Associates says: "Like drug trafficking, the counterfeit problem is so massive you don't know how to get a handle on it. The bandits are everywhere." And in recent years organized crime has taken over the software black market, according to Microsoft's head of investigations and a former FBI and Drug Enforcement Agency official. Criminal cases have confirmed involvement in the software black market by Chinese gangs, the Italian mafia, the Russian mob, the Irish Republican Army, and Middle Eastern terrorists. The Business Software Alliance, a trade association, estimates that 37% of the software sold worldwide is counterfeit. (USA Today 1 Aug 2001)

http://www.usatoday.com/life/cyber/tech/review/2001-08-01-software-piracy.ht m

Category 31.2 Estimates, guesses, predictions, forecasts

2001-08-30 security measures inadequate reliability industry problems widespread academic

research government regulation proposal

NewsScan

PETER NEUMANN SAYS ORGANIZATIONS LAGGING IN SECURITY MEASURES

The well-known security expert Peter Neumann, principal scientist at SRI International's computer science laboratory, told a congressional subcommittee yesterday that corporations are not making sufficient use of security and reliability measures developed by academic research. Neumann urged the government to find ways to encourage corporations to remedy that failing. (San Jose Mercury News 30 Aug 2001)

http://www.siliconvalley.com/docs/news/svfront/secur083001.htm

Category 31.2 Estimates, guesses, predictions, forecasts

2001-09-18 e-mail growth usage wireless survey prediction

NewsScan

MASSIVE E-MAIL GROWTH PREDICTED

E-mail use is set to grow 138% over the next four years, according to researchers at IDC, who are forecasting 1.2 billion e-mail mailboxes by 2005. By that time, the number of personal e-mail messages sent in an average day will exceed 36 billion. Growth will be fueled by increased use of free Web-based services, such as Hotmail, and the proliferation of Web-enabled devices, such as cell phones and PDAs. "Wireless access through e-mail devices will offer new ways for e-mail users to remain connected longer while on the move," says IDC researcher Mark Levitt. (Ananova 18 Sep 2001) http://www.ananova.com/news/story/sm 401552.html

Category 31.2 Estimates, guesses, predictions, forecasts

2001-10-01 critical infrastructure protection cyberterrorism

NewsScan

WARDING OFF CYBERTERRORIST ATTACKS

Internet experts believe that the threat of cyber-attacks are increasing, though not necessarily from Osama bin Laden's AlQaida network, which seems focused on destroying physical targets and killing civilians. Georgetown University computer science professor Dorothy Denning says, "It's my understanding that they're not teaching this in the terrorist-training camps," but rather that the danger comes from "these thousands of affiliates or sympathizers." Stephen Northutt, who runs an information warfare simulation for the SANS Institute, warns that terrorist could "potentially paralyze commerce" and might be able to "accomplish a cascading failure of the electronic grid." (San Jose Mercury News 1 Oct 2001)

http://www.siliconvalley.com/docs/news/depth/cyber100101.htm

Category 31.2 Estimates, guesses, predictions, forecasts

2001-10-30 steganography terrorism guess estimate Web content

NewsScan

THE DEVIL IS IN THE DETAILS (AND ON THE WEB) [6 Feb 2001]

Law enforcement officials in the U.S. and elsewhere are saying that international terrorists are increasingly used encrypted files on the Web to hide terrorist communications on sites supposedly devoted to pornography, sports, or other activities. Defense expert Ben Venzke says that encrypted terrorist information could be hidden in images that might "look no different than a photograph exchanged between two friends or family members," and notes: "There is a tendency out there to envision a stereotypical Muslim fighter standing with an AK-47 in barren Afghanistan. But Hamas, Hezbollah and bin Laden's groups have very sophisticated, well-educated people. Their technical equipment is good, and they have the bright, young minds to operate them." (USA Today 6 Feb 2001) http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm

TERRORISTS MAY BE HIDING MESSAGES IN DIGITAL PHOTOS [30 Oct 2001]

Terrorists may be hiding messages in digital photos sent over the Internet, using a process called "steganography" (from the Greek for "hidden writing") to embed secret messages in graphic or audio files to make them undetectable to the unaided human eye or ear. George Mason University professor and steganography expert Neil F. Johnson says that in the past two years, the number of steganography tools available over the Internet has doubled: "It's 140 and growing." He adds, "I have no reason to think that Al Qaeda is not using steganography." French law enforcement authorities who recently apprehended a man planning to blow up the U.S. embassy in Paris learned that the terrorist group of which he is a member had been instructed by a bin Laden associate to conduct all of its communications through pictures posted on the Internet. (New York Times 30 Oct 2001) http://partners.nytimes.com/2001/10/30/science/physical/30STEG.html

Category 31.2 Estimates, guesses, predictions, forecasts

2002-01-04 criminal hacker targets home PC wireless networking firewalls antivirus education awareness vulnerability warnings predictions

NewsScan

HOME PCs -- THE NEXT HACKER TARGET

Computer hackers are turning their sights to the humble home PC, which is now faster, more powerful and less secure than ever before. Fueling the onslaught are several factors, including the trend toward home-based DSL or cable connections that are "on" all the time, and the lackadaisical attitudes of most home PC owners who generally don't keep up to date with the latest antivirus and firewall software. In addition, many home users are naïve about the potential threat and willingly click on unsolicited e-mails that could be infected with malicious programs. "Home users have generally been the least prepared to defend against attacks," warns Carnegie Mellon's Computer Emergency Response Team Coordination Center. "In many cases, these machines are then used by intruders to launch attacks against other organizations." Antivirus firm Message Labs reported that it detected one virus per 370 e-mail messages in 2001, double the rate of the previous year. Meanwhile, Amit Yoran of computer security firm Riptech says the advent of wireless networking will increase the risk of attack significantly: "The standard itself is insecure What we're faced with is the widespread adoption [of wireless networks] throughout corporate America and throughout consumer markets and people haven't really thought through how to protect." (AP/Wall Street Journal 4 Jan 2002) http://interactive.wsj.com/articles/SB1010104082304162760.htm (sub req'd)

Category 31.2 Estimates, guesses, predictions, forecasts

2002-01-10 copyright intellectual property music sales prediction analysis royalties fees

NewsScan

2002: THE YEAR OF THE COPYRIGHT? "The recording industry has vowed to make 2002 the year of the copyright," says columnist Patti Waldmeir. To further that goal, record labels are experimenting with CDs that include technology that prevents them from being copied, even by owners for their own use, and several online music subscription services set to launch this year will be engineered to prevent unauthorized reproduction. If the technology is successful, it could be the year of ascendancy for copyright holders, who will find themselves wielding more power than was ever intended under U.S. copyright law or the constitution, says Stanford University law professor Lawrence Lessig. Lessig argues that by extending the term of copyrights 11 times in the last 40 years, Congress has exceeded its constitutional authority, granting copyright holders terms that extend long beyond a human lifetime. Lessig argues that these over-lengthy terms violate the constitution's command to "promote the Progress of Science and the useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." Under today's technology, the copyright on a locked CD may expire, but the CD would remain locked. In Lessig's recent book, "The Future of Ideas: The Fate of the Commons in a Connected World," he recommends a radical revision of copyright law: copyright protection should be cut to five years, renewable 15 times. If a copyright is not renewed, the work would enter the public domain. (Financial Times 10 Jan 2002)

Category 31.2 Estimates, guesses, predictions, forecasts

2002-01-11 copy protection music piracy countermeasures prediction public rejection

resistance

NewsScan

PHILIPS SAYS COPY-PROTECTED CDs WON'T LAST LONG

Philips Electronics, which invented the compact disc, says the controversial attempts by the recording industry to market "copy protected" CDs will fail because consumers just don't like it. As inventor of the CD standard and the industry's licensing body, Philips says it could refuse to license the new discs as genuine CDs or pursue some kind of legal action, but thinks the copy-protected CDs will disappear on their own as consumers reject them. "Any kind of legal action would take years and we don't expect these [discs] to last that long," says Gary Wirtz, general manager of the Philips Copyright Office. "At the moment we are trying to reason with people rather than sue them. [The technology is] not going to work, because any hacker can still make copies. It's only going to affect legitimate consumers and we know there have already been considerable complaints." Philips opposes the technology because it can make legitimate CDs unplayable in some older players and in-car audio systems. Critics maintain that the technique used to block copying can also impair the quality of a disc's audio content over time. (New Scientist 11 Jan 2002)

http://www.newscientist.com/news/news.jsp?id=ns99991783

Category 31.2 Estimates, guesses, predictions, forecasts

2002-02-06 survey study statistics prediction security budgets spending industry

NewsScan

CORPORATE SPENDING ON INFORMATION TECHNOLOGY

A Goldman Sachs survey of information technology executives at 100 large corporations suggests that tech spending will be flat in the year ahead. The only areas that would see increases are expected to be security software, data networking, database software, storage software, and disaster recovery. (Reuters/San Jose Mercury News 6 Feb 2002) http://www.siliconvalley.com/docs/news/svfront/057894.htm

32.1 USA

Category 32.1 USA

2001-01-26 legislation censorship video game violence children

NewsScan

SENATORS CRITICAL OF VIDEOGAME VIOLENCE

U.S. Senators Joseph Lieberman, Herb Kohl, and Sam Brownback plan to introduce legislation that will punish companies that market excessively violent video games to children. Kohl, a Wisconsin Democrat, said: "Practically everybody in the industry still markets inappropriate games to kids, practically every retailer regularly sells these games to kids, and practically all parents need to know more about the rating system." But Doug Lowenstein, president of the Interactive Digital Software Association, which represents video game makers, argues that such legislation could violate the First Amendment guarantees of freedom of speech and might simply make it more complicated for the video game industry to police itself. (AP/USA Today 25 Jan 2001) http://www.usatoday.com/life/cyber/tech/review/games/2001-01-25-violence.htm

Category 32.1 USA

2001-03-13 censorship censorware filtering library lawsuit CIPA

NewsScan

NEW EFFORT TO END INTERNET FILTERING PROGRAM IN LIBRARIES

The American Civil Liberties, the American Library Association, and other plaintiffs are filing federal lawsuits this [week] to overturn a new law called the Children's Internet Protection Act, which requires schools and libraries receiving federal money for technology to shield school children from pornography and violence transmitted over the Internet. The dispute splits political parties. One Republican, Ernest Istook of Oklahoma, says that civil libertarians falsely label the law censorship "if they're not permitted to expose our children to the very worst things on the Internet, using federal tax dollars to do so," whereas Republican Jeffrey Pollock (whose own political site was once blocked by filtering software) says: "To mandate the federal government to legislate morality, I find abhorrent." (New York Times 19 Mar 2001)

http://partners.nytimes.com/2001/03/19/technology/19FILT.html

Category 32.1 USA

2001-03-19 censorship library lawsuit law CIPA filtering

NewsScan

LIBRARIANS SUE OVER NET CENSORSHIP

The American Library Association says it plans to sue the U.S. over the legality of the Children's Internet Protection Act, which was signed into law December 21, 2000. The ALA says the law, which requires schools and libraries to install content filters on computers as a condition for U.S. government funding, infringes on First Amendment free-speech rights. Specifically, the ALA is alleging that the new filtering rules would serve to widen the so-called digital divide, which separates those with the means to access the Internet through their own household PCs from those who must rely on public-access machines. Even with the filter options turned on, says the ALA, there is no filtering software that "differentiates constitutionally protected speech from illegal speech on the Internet." That argument was successfully upheld in 1998 in a similar court case in Loudon County, Virginia. "The filters blocked so much constitutionally protected material that had absolutely nothing to do with pornography or anything like that," says Larry Ottinger, senior staff attorney at People for the American Way, the civil rights group that fought the Loudon restrictions. Among the sites blocked in that instance were the Yale University graduate school of biology, a Quaker Web site, Have an Affair Catering, and a beanie babies Web site. (NewsFactor Network 19 Jan 2001) http://www.newsfactor.com/perl/story/6838.html

NEW EFFORT TO END INTERNET FILTERING PROGRAM IN LIBRARIES

The American Civil Liberties, the American Library Association, and other plaintiffs are filing federal lawsuits this [week] to overturn a new law called the Children's Internet Protection Act, which requires schools and libraries receiving federal money for technology to shield school children from pornography and violence transmitted over the Internet. The dispute splits political parties. One Republican, Ernest Istook of Oklahoma, says that civil libertarians falsely label the law censorship "if they're not permitted to expose our children to the very worst things on the Internet, using federal tax dollars to do so," whereas Republican Jeffrey Pollock (whose own political site was once blocked by filtering software) says: "To mandate the federal government to legislate morality, I find abhorrent." (New York Times 19 Mar 2001)

http://partners.nytimes.com/2001/03/19/technology/19FILT.html

Category 32.1 USA

2001-05-21 pornography children censorship indecent constitution first amendment free

speech

NewsScan

CHALLENGE TO LAW RESTRICTING KIDS' ACCESS TO PORNOGRAPHY [21 May 2001]

The U.S. Supreme Court has agreed to hear a challenge to the constitutionality of a 1998 law passed by Congress imposing criminal penalties on operators of Web sites that expose children to commercially offered "indecent" material. The law does not cover e-mail or chat rooms. The issue is whether the attempt to shield children ends up abridging constitutional rights to freedom of speech. A supporter of the law says: "We're talking about material that would be harmful to minors. That is a test we have applied for years in the real world. If you walk into a bookstore, the pornography is wrapped, or behind a blinder or will be in a place where it is difficult for young people to reach it." An American Civil Liberties Union official who opposes the law counters that it "would send adults to prison for commercial speech that is unquestionably protected for them." (AP/USA Today 21 May 2001) http://www.usatoday.com/life/cyber/tech/2001-05-21-scotus-online-porn.htm

Category 32.1 USA

2001-11-29 code speech constitution first amendment lawsuit jurisprudence DVD decryption

software Web posting criminal hacker

NewsScan

APPEALS PANEL SEEKS ANSWERS ON COMPUTER CODE AS FREE SPEECH [11 May 2001]

A three-judge appeals panel has asked both sides in the case testing the constitutionality of the 1998 Digital Millennium Copyright Law to answer a list of 11 questions focusing on whether computer code can qualify as free speech. The case pits the major Hollywood studios against Eric Corley, the publisher of online magazine 2600. A federal judge previously issued an injunction blocking Corley from distributing a computer code that can break the security lock on a DVD. Corley's appeal argues that the injunction violates his right to free speech. "I've never seen this happen before," says one of Corley's attorneys. "What's clear is that neither Judge Kaplan's decision nor the briefs nor the oral arguments have given them the answer to the questions they think are most important." The questions suggest that the judges are looking beyond Corley's case to how the ruling might apply more generally. One question raised is whether software code is more like a list of instructions -- traditionally protected by free speech -- or a machine that simply happens to be built with speech, which would not fall under the scope of the First Amendment. (New York Times 11 May 2001)

http://www.nytimes.com/2001/05/11/technology/11CODE.html

COURT RULES AGAINST USE OF PROGRAM THAT UNLOCKS DVD ENCRYPTION [29 Nov 2001]

The Motion Picture Association of American (MPAA) has prevailed in the U.S. Court of Appeals against a computer hacker publication's claim to have the right to publish a program that used reverse-engineering to unlock the copyright protection system of DVDs. At issue was the constitutionality of the Digital Millennium Copyright Act (DMCA) of 1998, which was challenged by programmer Eric Corley, who publishes the hacker magazine 2600. Corley and his supporters, which include the Washington-based civil liberties group called the Electronic Frontier Foundation, believe that the DMCA gives too much power to copyright-holders and violates First Amendment rights of researchers and consumers. (New York Times 29 Nov 2001)

http://www.nytimes.com/2001/11/29/technology/29DVD.html

32.2 Non-USA

Category 32.2 Non-USA

2001-06-07 censorship government vetting criminal prosecution Web content

NewsScan

TURKEY'S BATTLE FOR "TRUTH" ON THE WEB

Under a new law passed by the Turkish parliament, Web site operators publishing "untrue news, insults and similar material" are subject to fines of up to \$85,000. An earlier draft of the law would have required owners of Web sites to provide local prosecutors printed copies of the site every day. (AP/Salon 7 Jun 2001) http://www.salon.com/tech/wire/2001/06/07/turkey/index.html

Category 32.2 Non-USA

2001-07-23 censorship government policies Internet content access China

NewsScan

CHINA INTERNET USE GROWS WHILE GOV'T CRACKDOWN CONTINUES

China's crackdown on Internet cafes that allow its customers access to material the authorities consider "pornographic, anti-government, violent, unhealthy or superstitious" has led to the closing of more than 8,000 Internet cafes (Wang ba, or "Net bars") since April. At least 15 people have been detained by the police, and two were recently sentenced to up to four years in prison. But interest in the Internet remains strong, and there are now an estimated 26 million Internet users in China, compared to only 4 million two years ago. (San Jose Mercury News 23 Jul 2001) http://www.siliconvalley.com/docs/news/svfront/078240.htm

Category 32.2 Non-USA

2001-11-19 content filtering censorship control autocracy women's liberation female

autonomy culture conflict

NewsScan

SOFTWARE COMPANIES VIE TO PROVIDE SAUDIS WITH INTERNET FILTERS

When the Internet was introduced in Saudi Arabia in 1999, the Saudi royal family decreed that all public traffic into and out of the country would have to be funneled through a single control outside Riyadh. The contract for providing the filtering software to make that level of control possible will expire in 2003, and companies from the U.S., U.K., Germany and the Netherlands are engaged in spirited competition for the multimillion assignment. Yale law professor Jack Balkin says, "We have a really serious problem in terms of the American free speech idea. But it is very American to make money. Between anticensorship and the desire to make money, the desire to make money will win out." The sites blocked by the Saudis are pornographic or offer other challenges to Islamic political or cultural sensitivities. (New York Times 19 Nov 2001)

http://partners.nytimes.com/2001/11/19/technology/19SAUD.html

Category 32.2 Non-USA

2002-02-22 ISP Internet service providers hate speech censorship international regulation

agreement treaty harmonization cooperation law enforcement investigation

prosecution extradition

NewsScan

EUROPEAN "HATE SPEECH" LEGISLATION WORRIES CIVIL LIBERTARIANS [22 Feb 2002]

A proposal by the Council of Europe that would criminalize racist and other "hate speech" on the Internet is worrying both civil libertarian groups (which regard it as a blow against free speech) and Internet service providers (which are concerned about their legal liability for material posted without their consent). The principal administrator of the Council of Europe thinks that the various countries belonging to the organization must "harmonize" their laws "so that countries can cooperate in criminal investigations regarding the Internet," but the head of the Campaign Against Censorship on the Internet in Britain took a very different view: "This proposal could potentially outlaw free speech. That would be a great infringement of civil rights." (Reuters 22 Feb 2002)

 $http://www.reuters.com/news_article.jhtml?type=internetnews\&StoryID=623493$

33.1 Acceptable use

Category 33.1 Acceptable use

2001-03-19 availability saturation e-mail overuse acceptable use

NewsScan

WASHINGTON FLOODED WITH E-MAIL

U.S. lawmakers last year received 80 million e-mail messages from constituents and special-interest groups, most of which were routinely ignored, according to new study by the Congress Online Project. The number of e-mail messages to Congress has more than doubled in two years, says the group, with senators receiving as many as 55,000 messages per month. And while millions of the messages originate from constituents concerned about Medicare reform, tax cuts and other issues, the study attributed the e-mail explosion in large part to advocacy groups and corporations that increasingly use the Internet to lobby lawmakers day and night, overloading congressional computers and staff. "Rather than enhancing democracy--as so many hoped--e-mail has heightened tensions and public disgruntlement with Congress," says the report. "A growing number of citizens are increasingly frustrated by what they perceive to be Congress' lack of responsiveness to e-mail. At the same time, Congress is frustrated by what it perceives to be e-citizens' lack of understanding of how Congress works." The study urges grassroots lobbyists to adopt a "code of conduct" to curb mass e-mailings to lawmakers and also suggests the federal government to provide lawmakers with additional resources so they can buy new software and hire staff to answer electronic messages. According to the study, it could cost each office \$50,000 or more for hardware and software. (Reuters/CNet 18 Mar 2001)

http://news.cnet.com/news/0-1005-200-5173083.html?tag=lh

Category 33.1 Acceptable use

2001-04-06 e-mail posting publication confidentiality stock damage information warfare

sabotage appropriate use stupidity

RISKS 21 34

According to a report from the BBC <

http://news.bbc.co.uk/hi/english/world/americas/newsid_1263000/1263917.stm >, "A chief executive who used an e-mail to threaten his staff with the sack for being lazy has seen his company's share price collapse after the message appeared on the Internet. Neal Patterson, head of the Cerner Corporation in Kansas City, USA, had no idea his private directive to staff would end up being seen by millions of people on the world wide web. In the three days after the publication of the message, shares in the healthcare software development company plummeted 22% on the stock market."

RISKS correspondent Lord Wodehouse wrote, "It never ceases to amaze me that people armed with a computer and e-mail completely lose their common sense. However it seems to the the type of e-mail that should never have been written let alone sent and not by a senior person in the company. Gerald Ratner built up the family business, piling it high, selling it cheap and making a fortune out of cut-price jewelry. But a throw-away joke in a speech at the Royal Albert Hall in front of Chancellor Norman Lamont brought his empire crashing down around his ears. (he called a item he sold cr*p.) With the Internet the inept director can find that it is even easier to ensure that bad news travels faster and further."

Category 33.1 Acceptable use

2001-08-31 Internet chat room hate speech censorship lawsuit ISP Internet Service Provider

NewsScan

MUSLIM LAWSUIT AGAINST AOL CHARGES "HATE SPEECH" TOLERANCE [31 Aug 2001]

A class-action lawsuit has been filed in Alexandria, Virginia, charging America Online with violating the 1964 Civil Rights act by failing to curtail anti-Muslim "hate speech" in chat rooms for Muslims. An attorney for the Muslim plaintiffs says that the primary objective is to get AOL to enforce the terms of its own service agreement, which prohibits member s from using "offensive" speech in any of AOL's 14,000 chat rooms. An America Online executive calls the lawsuit "totally without merit" and says that the company has "zero tolerance for hate speech." (AP/USA Today 31 Aug 2001)

http://www.usatoday.com/life/cyber/tech/2001-08-31-aol-suit.htm

Category 33.1 Acceptable use

2001-09-20 monitoring logging confidentiality privacy Internet abuse appropriate use policy

NewsScan

JUDGES TOLD THEY CAN'T REFUSE TO HAVE THEIR COMPUTERS MONITORED [14 Aug 2001] In mid-September a policy-making group of 27 judges will decide whether to accept the recommendations of a report urging denial of one court's request to put an end to the monitoring of its computers for Internet misuse. One observer says: "When the courts find themselves as not the arbitrators but the victims of such a policy, all of a sudden you find judges saying 'this could very well be a violation of our rights.' Now the judges are beginning to understand how difficult this has been for the private sector so long." The judge who objects to the monitoring says it should be used to prevent vandal attacks by outside hackers, and not focused on internal computer uses. (AP/San Jose Mercury News 14 Aug 2001)

http://www.siliconvalley.com/docs/news/svfront/060305.htm

COURTS AFFIRM RIGHT TO PRIVACY FOR JUDGES AND STAFFS [20 Sep 2001]

In a move that is likely to set a precedent that could lead to stronger privacy protections for employees nationwide, the 27-judge Judicial Conference of the United States Courts agreed to a computer-use policy that drops language in an earlier draft saying that the nation's 30,000 court employees had no right to privacy when they used the Internet. The final version merely states that the court computers should be used largely for work, and not for viewing pornography, gambling, or exchanging media files for personal use. (Reuters/New York Times 20 Sep 2001) http://www.nytimes.com/2001/09/20/national/20JUDG.html

Category 33.1 Acceptable use

2001-10-15 acceptable use corporate policy bandwidth saturation throughput availability

denial of service streaming audio video employees survey study

NewsScan

RECORD NUMBER OF OFFICE WORKERS ACCESS STREAMING MEDIA

A record number of U.S. office workers took advantage of their corporate networks' high-speed Internet connections to access streaming audio or video media last month, including media from foreign countries. In most cases, people were trying to follow news related to last month's terrorist attacks. More than half (55.8%) of all employees who logged on from work last month watched or listened to streaming media, up from 50% in August, according to Nielsen/NetRatings. The previous record was set in November 2000, when 52.8% of office employees accessed streaming media while at work. Among the three formats available for streaming media, the most popular was RealNetworks' RealPlayer, followed by Microsoft's Windows Media and Apple's QuickTime. "What we saw starting with (Sept.) 11th was an unprecedented amount of ... live usage and an unprecedented amount of broadband-video usage" that continued through the month, said RealNetworks media manager Ben Rotholz. (Wall Street Journal 15 Oct 2001)

http://interactive.wsj.com/articles/SB1002819156270229840.htm

Category 33.1 Acceptable use

2001-11-18 content filtering edit selection private control censorship Web discussion board

chat room

NewsScan

MONITORING THE MESSAGE BOARDS [18 Nov 2001]

With the U.S. at war with terrorism, various Web services are choosing to decline submissions from people saying the country "deserved" to be attacked or making other comments along those lines. Stephen Killeen of Terra Lycos U.S. says that, in the past, "we would err on the side of 'If it's distasteful, let it stay.' Now, we err on the side of 'If you want to post this kind of information, you don't have to do it here.' The sentiment in the United States changed on Sept. 11 about what's acceptable and what's not in terms of what you can say." Of course, people are free to set up Web sites of their own and post whatever they want, just as private companies are free to accept or reject anything they want. UCLA law professor Stuart Biegel says, "In times of war, there has been a willingness among Americans to give up some rights – to honor curfews, martial law, and even restrictions on speech. The filtering of Internet message boards is part of all this." (San Jose Mercury News 18 Nov 2001) http://www.siliconvalley.com/docs/news/svfront/censor111801.htm

Category 33.1 Acceptable use

2002-01-20 Internet content filtering students schools portable games music piracy instant

messaging appropriate use policy

NewsScan

VIRGINIA COUNTY RECALLS STUDENT LAPTOPS [20 Jan 2002]

Henrico County, Va. school officials are recalling all 11,000 laptop computers that it distributed to its high school students in order to retrofit them with security software that will prevent students from using the devices for accessing pornography or changing their grades – abuses that reportedly have occurred since the machines were handed out last fall. Game and music downloading capabilities will also be eliminated or heavily restricted and instant messaging will be limited to home use. Teachers have complained that in-class use of entertainment file-sharing and messaging are disruptive. (AP/Wall Street Journal 20 Jan 2002)

http://interactive.wsj.com/articles/SB1011563803808773240.htm

33.2 Spam

Category 33.2 Spam

2001-01-10 spam personal preferences arrogance stupidity auction

NewsScan

E-BAY PONDERS THE MEANING OF THE WORD "NO"

Online auctioneer eBay has told its 6 million users that some sort of system glitch had misinterpreted the desire of many of them to receive its "valuable email communications with news, offers and special events." According to eBay, "many of your Notification Preference defaults were set to 'no' rather than to 'yes,' which means that unlike other eBay members, you're not receiving these types of communication." So it has changed those Notification Preferences from 'no' to 'yes," and that has angered many eBay uses, even though the company insists: "Our history tells us that the great majority of people leave it in the 'yes' position." (Washington Post 10 Jan 2001) http://washingtonpost.com/wp-dyn/articles/A39734-2001Jan9.html

Category 33.2 Spam

2001-02-12 spam instant messaging peer-to-peer networking

NewsScan

WILL INSTANT MESSAGING DRAW INSTANT SPAM?

Online marketers are salivating at the prospects for combining the power of instant messaging with peer-to-peer networks to create a new wave of Web advertising that some critics charge is more invasive than spam. When people sign onto file-swapping networks like Napster, many expose their instant messaging handles and entertainment tastes, opening up a new channel for targeted advertising. "It's a chilling thought," says Jason Catlett, president of Junkbusters. "The songs that make you visible to the world on Napster say a lot about you. Many people don't realize that when they're using these P2P services they are becoming publishers of their personal collections – it's like putting your CD collection in the window fronting the street." In a sign of things to come, online ad agency L90 last week inked a deal with peer-to-peer network Aimster in one of the first exclusive partnerships to promote goods to consumers via instant messaging. Aimster plans to start an IM advertising campaign, featuring clients such as Aerosmith, Microsoft and Columbia Tristar. "Essentially, it's the next wave of commercialization of the Net," says Aimster CEO Johnny Deep. "Instant messaging is the delivery vehicle for everything in the same way the Web used to be the delivery vehicle. Now we're using IM for everything, for MP3s, sending movie trailers, software, text." (CNet News.com 16 Feb 2001)

http://news.cnet.com/news/0-1005-202-4851077.html

Category 33.2 Spam

2001-05-02 spam volume growth news group

RISKS 21 39

Peter G. Neumann reported in May that for the first time ever, the number of spam messages exceeded the number of legitimate messages to RISKS. He commented, "I hate to recommend draconian anti-spam measures, but the problem is clearly out of control. We are of course opposed to short-sighted legislation and censorship – especially if it overzealously filters out desired e-mail. Perhaps it is time to implement some radical techniques such as that described in a 1992 paper by Cynthia Dwork and Moni Naor, Pricing Via Processing Or Combatting Junkmail, Proc. Crypto 1992, LNCS 740."

Category 33.2 Spam

spam unk unsolicited commercial e-mail cell phones short-messaging service SMS regulation fraud

RISKS 21 44

Simon Waters reported from Britain on a new variant of the old 809-pager-message scam (in which pagers were fed numbers in the Caribbean which racked up huge long-distance charges); seems some people have been sending "urgent" requests to call a high-cost "premium" number (equivalent to the US 900 numbers).

Category 33.2

Spam

2001-10-08

spam unk unsolicited commercial e-mail cell phones short-messaging service SMS

NewsScan

SPAM COMES IN SHORT MESSAGES, TOO [28 Mar 2001]

Millions of Americans who now have short-messaging service (SMS) capability on their cell phones are discovering the dark side of the service – they are being bombarded with unwanted commercial messages. Cell phone companies say they are powerless to stop the abuse. The problem stems partly from the fact that the account numbers for short-messaging phones are easily identifiable (usually they're just the user's cell phone number plus the name of the service provider). The practice is raising the ire of cell phone users because most get charged for receiving SMS messages, and the FCC says the legal status of cell phone spam is murky. Meanwhile, the number of phones capable of sending or receiving SMS messages is expected to increase to 110 million in 2002 from 37 million in 1999, according to the Yankee Group. (Wall Street Journal 28 Mar 2001)

http://interactive.wsj.com/articles/SB985735340294663006.htm (sub required)

WIRELESS SPAM [13 Apr 2001]

The text-messaging services now included as a standard feature by many wireless companies make it simple for senders of junk mail to target a specific audience by geographic location and pass the costs of their messages on to the people being spammed. Todd Bernier, a wireless technology analyst with Morningstar, predicts: "This will become a huge problem when text messages become more popular in the states. The industry is going to have to do something to control itself. People just won't tolerate it." (AP/USA Today 13 Apr 2001) http://www.usatoday.com/life/cyber/tech/2001-04-13-wireless-spam.htm

AD FIRMS TARGET ASIAN CONSUMERS WITH SMS [8 Oct 2001]

Ogilvy Interactive, part of the UK's WPP Group, has designed an outreach campaign for the Love Singapore coalition of more than 150 churches based on wireless short messaging (SMS). Consumers who've registered to receive them find messages like "Thank me it's Friday. Signed, God." on their mobile phone screens. Another SMS ad campaign touted a new Coca Cola fruit juice called Qoo so effectively that within nine weeks, Qoo became the No. 1 juice drink in Singapore. The company sent a picture message showing a blue-skinned animated Qoo character to 500 young people in the hope they would send it on to their friends. About half a million mobile users in Singapore have now received the character. "We knew we wanted to target teenagers with this brand," says a Coca Cola spokeswoman. "I think SMS speaks to this group of people especially when traditional methods like TV campaigns are less effective." About 5.6 billion text messages are sent a year in Asia, according to market research firm Mobile Streams. (Wall Street Journal 8 Oct 2001)

http://interactive.wsj.com/archive/retrieve.cgi?id=SB1002497419688848160.djm (sub req'd)

Category 33.2 Spam

2001-11-13 e-mail address harvesting interception eavesdropping confidentiality harvesting

sale contract violation insider crime danger spam unsolicited commercial bulk email forged IP headers SMTP bounce rejection messages

RISKS 21 76

In an interesting RISKS sequence of messages, Nickee Sanders reported that an e-mail bounce message appeared to indicate that someone had sent spam using her e-mail address as the source. Andrew Klossner responded to her puzzled account by explaining, "That 'original message' was never sent. The 'bounce notification message' was forged by the spammer. And it worked -- you paid close attention to it."

Allan Hurst then provided a detailed experimental analysis of what happened to e-mail addresses which were never made public (they were used only for test purposes). He wrote, "Within two months of opening the Yahoo! Mail account, it started receiving spam, none of it from Yahoo. Within three days of opening the HotMail account, it started receiving spam, in amounts far larger than the Yahoo account." Given that he explicitly opted out of any e-mail address sharing, then "Either Yahoo Mail and HotMail are lying about not publishing or selling addresses, or someone's harvesting e-mail addresses by sniffing packets. (Hence the subject of this message.) As much as I'd like to bash the vendors . . . I strongly suspect the answer is that someone's found a way to harvest e-mail addresses. (Keep reading.)"

His next test involved an e-mail address on MyRealBox.com, where he was very confident that the Internet service provider "do NOT sell the MyRealBox accounts, nor use them for marketing purposes of any kind." After about six months of completely spam-free existence of this new address, "Suddenly, I was flooded with everything from 'failed delivery' messages to angry missives threatening me with bodily harm for spamming them." Mr Hurst wondered exactly where the spammers picked up his e-mail address? And how could such abuse be stopped?

Several other contributors chimed in with evidence that unused e-mail addresses were nonetheless being addressed by spammers.

The next wave of responses suggested that the spammers were likely using a dictionary or brute-force attack on the ISPs: trying out every possible alphanumeric combination to find valid e-mail addresses (those that did not bounce). Although this might seem like a lot of work, Walter Dnes explained, "With today's fast computers and broadband, the above is feasible."

Category 33.2 Spam

2002-01-08 viral marketing e-mail chain letter consumer spam junk e-mail worm social

engineering

NewsScan

VIRAL MARKETING GOES MAINSTREAM

Viral marketing is set to invade your in-box, say advertisers who are looking to this upstart marketing method to boost their outreach efforts. "At the moment, say 'viral marketing' and you still think teens and fashion brands – cool things for cool people distributed via e-mail. But the principles that make viral marketing work should be taken on board by any brand-owner wanting to target any age group," says marketing consultant David Nichols. "Grown-up viral marketing is about involving people in things they love as a way of introducing a dialogue between brand and consumer." E-based marketing will become more prevalent, say many experts, but also will become increasingly permission-based. "I'm not convinced there is a future for viral marketing involving messages thrown out to hundreds of people in the hope someone will pass it on," says Tim Patten of marketing group HHCL Digital Solutions. "But I do believe there is value where people agree to receive messages, then – on the strength of the value of that message – decide to pass it on." Key to the success of these marketing efforts will be companies' willingness to participate in a true dialogue with their customers: "Too many marketers still believe when they speak consumers will listen. The enthusiasm amongst marketers for developing new ways of pushing information at consumers has not been matched by an enthusiasm to listen to what consumers say." says Mark Curtis, a partner at marketing consulting group Fjord. (Financial Times 8 Jan 2002)

http://news.ft.com/news/industries/internet&e-commerce

Category 33.2 Spam

2002-01-14 spam unsolicited commercial bulk e-mail countermeasures lawsuits statistics

growth

NewsScan

THE SPAM WARS

There has been a 16-fold increase in the number of unsolicited commercial e-mail messages in the past two years (according to the spam-filtering company Brightmail), and little progress has been made in fighting it, although sporadic lawsuits have sometimes yielded (very) small (and often uncollectable) cash judgments against the spammers. The president of the anti-spam Junkbusters Corporation has compared such lawsuits to "mopping up an oil spill with a toothbrush." Yet some anti-spammers feel the effort is worthwhile, and Bennett Haselton, who recently won four judgments of \$500 each in Washington state, plans to publish a how-to guide for the spam-perplexed, hoping that if [more] people "get in the habit of taking legal action if they get spammed, then it's going to become so expensive that spammers have to get out of business." (AP/San Jose Mercury News 14 Jan 2002) http://www.siliconvalley.com/docs/news/svfront/031444.htm

Category 33.2 Spam

spam unsolicited commercial e-mail chain letter Ponzi scheme pyramid fraud

settlement government regulators

NewsScan

FTC's FIGHT AGAINST SPAM

Saying that the Federal Trade Commission is "going after deceptive spam and the people who send it. We want it off the Net," FTC chairman Timothy Muris has announced that the agency has settled charges against seven people who ran an e-mail chain letter promising returns of up to \$46,000 on an investment of only \$5. The letter received responses from more than 2,000 people in nearly 60 countries. The research firm Jupiter Media Metrix says that Internet users received on the average 571 pieces of mail last year generated by unsolicited commercial mass-mailings of everything from pornography to fake diplomas; the firm predicts that number is likely to rise to 1,500 a year by 2006. (Reuters/USA Today 12 Feb 2002)

http://www.usatoday.com/life/cyber/tech/2002/02/12/ftc-spam.htm

33.3 Antispam

Category 33.3 Antispam

2001-01-18 antispam IP block e-mail diversion misleading messages lies collateral damage

unexpected consequences

RISKS 21 22

Bennett Haselton of Peacefire, an activist organization that fights censorware and spam, was blocked by Hotmail starting around August 2000 so that Hotmail users could not successfully send e-mail to Peacefire.org: "If you tried to send mail to a peacefire.org address from HotMail, you'd get a fake error message a day later saying that there was a problem on the recipient's end -- when it was really HotMail blocking the message from being delivered."

Apparently the problem arose because of HotMail's attempts to fight spam: "... HotMail didn't single us out for anything, we just happened to be in the same IP address block as other sites that were the original target of the boycott (e.g. ListSorcerer.com). When our ISP, Media3, didn't kick them off, the boycott organizers expanded the 'boycott list' to include hundreds of unrelated sites also hosted by Media3." Haselton noted that although Peacefire.org addresses were now unblocked, many other innocent users were still prevented from receiving e-mail from HotMail subscribers.

Category 33.3 Antispam

2001-02-02 privacy e-mail antispam corporate policy

NewsScan

EBAY TO CONCEAL CUSTOMER E-MAIL ADDRESSES

To protect its customers from receiving unsolicited mail from spammers, as well as to prevent the same customers from concluding their deals outside the system, online auctioneer eBay has decided to conceal the e-mail address of its customers. Under the new arrangement, buyers or sellers who wish to contact another other user will enter the user's name in a form and eBay will forward the messages, unread, to the person for whom they are intended. (AP/San Jose Mercury News 1 Feb 2001)

http://www.mercurycenter.com/svtech/news/breaking/ap/docs/810995l.htm

Category 33.3 Antispam

2001-02-12 anti-spam legislation

NewsScan

CONGRESS EYES ANTI-SPAM MEASURE

Legislation designed to block spam has been reintroduced in the U.S. House of Representatives by the same representatives who sponsored the legislation in the last Congress. Representatives Heather Wilson (R-NM) and Gene Green (D-Texas) resubmitted the Unsolicited Commercial E-Mail Act, which had passed the House last year by a vote of 427-1. The bill stalled in the Senate last year after being introduced late in the session, but "we are optimistic that we will have success this year," says a spokesman for Wilson. The legislation would give consumers the power to block unwanted e-mail and provide ISPs with the legal right to block those who dump unwanted messages onto their networks. It would require e-mail marketers to provide accurate return addresses on unsolicited commercial e-mail; make it illegal to continue sending e-mail after someone has requested to be removed from a distribution list; require unsolicited commercial e-mail to be labeled; and require ISPs to allow their customers to opt out of receiving junk e-mail if the ISP profits from allowing it on their system. ISPs would be allowed to sue spammers for \$500 per message if they violate their anti-spam policy. (InfoWorld.com 14 Feb 2001) http://www.infoworld.com/

Category 33.3 Antispam

2001-05-10 unsolicited bulk commercial e-mail spam junk anti-spam legislation

NewsScan

ANTI-SPAM LEGISLATION [BLOCKED] IN U.S. HOUSE [10 May 2001]

The House Judiciary Committee is blocking an anti-spam bill that previously passed the House Energy and Commerce Commission. The bill would impose a \$500 penalty for each piece of unsolicited e-mail a company distributes. Judiciary Committee member Bob Goodlatte (R., VA) said: "Legislation should be narrowly targeted to provide law enforcement with the tools they need to combat abuses without opening the floodgates to frivolous litigation or interfering with legitimate uses of e-mail for marketing purposes." The Committee favors an alternative bill, sponsored by Goodlatte, that penalize senders of unsolicited commercial messages only if the they used a bogus return address. (AP/USA Today 10 May 2001) http://www.usatoday.com/life/cyber/tech/2001-05-10-anti-spam-opposition.htm

Category 33.3 Antispam

spam unsolicited commercial bulk e-mail techniques countermeasures remote

control modem

RISKS 21 72

[Greg Searle provided RISKS readers with an excellent overview of the technical measures being used by spammers to get their material through to their victims. What follows is the complete text of Mr Searle's essay, which ends with a brief summary of the fundamentals of antispam origin-tracing.]

Here's the bag of tricks that many spammers are using to keep you from finding out who really sent you the spam:

- 1. The obvious find an open e-mail relay, and use it for "e-mail laundering". Forge the e-mail headers, and the e-mail becomes untraceable. All you see is the IP for the open relay, and whatever the spammer wants you to see afterward. The "From" header is always forged, and complaining to the ISP behind the "From" address is pointless. The most you can do is complain to the company that owns the open relay, and hopefully they will close it. Unfortunately, new mail servers appear on the net every day, and many IT "professionals" setting up these systems are just not aware of the open relay problem. There are many web pages which have the sole purpose of finding and listing these open relays.
- 2. Include a "relay" URL in the spam for potential customers. This URL is typically a "throwaway" account opened on one of the many free webpage services (tripod, geocities, angelfire, etc.) with false credentials. The spammer only expects this URL to exist for a day or two, as the provider will quickly terminate the page once complaints start coming in. The URL typically points to a file or page that will redirect the customer to the true page.
- 3. There are some businesses that are specifically set up to relay URLs for spammers. One of these is 1freesite.net (G Stubberfield Enterprises). Spammers hire the business to set up a relay page on their server, so they can include this page in their e-mails.
- 4. Obfuscate the URL in an attempt to make it untraceable. Do you know that IP addresses can be expressed as a single, decimal digit? Browsers will accept this digit and translate it into a valid IP address. Encoding the URL in hex is another trick. Browsers will convert two-digit hex digits that are preceded by a percent sign into a valid character. The URL specification also allows usernames and passwords in a URL. This can be used to mislead. For instance, the URL http://www.webservice.com:www.server.com@192.168.10.10/spampage.html seems to point to "webservice.com", but the piece of the URL before the second colon is really the "username", the piece before the at sign is the "password", and the real web server is the IP after the at sign! Most web servers simply ignore the user name and password if they don't need it. These techniques can be combined to make a URL really hard for a person to decode.
- 5. Compose the relay webpage in JavaScript. Encrypt the "real" web page and any URL's, and have a JavaScript function decode it.
- 6. Ask customers to respond to the message. Include a valid "Reply To" header that is different from the "From" header. The e-mail client will recognize this and send any responses to the "Reply To" address. The e-mail account set up to receive these messages is usually a "throwaway" address set up on a free mail service with false credentials.
- 7. Include an unlisted phone number, which is protected by the telephone company and is untraceable.
- 8. Included an executable at the URL enclosed in the message. This executable is typically compressed to obfuscate its contents from prying binary file editors. The executable then forwards the customer's computer to the business's true URL. Anybody who opens this executable file is too ignorant to know any better.

All of these methods, except for the telephone number and the reply-to address, are completely reversible to expose the company behind the e-mail. If the computer can get to the final page, then so can the person operating the computer, given enough knowledge of the technology involved. There is one particularly nasty spammer, hosted at sexmansion.com and web69.com, that includes a doubly-compressed executable in the page that they set up on a "throwaway" site. Their extremely explicit e-mailings point to this executable's URL. This executable is a dialer application that redirects the user's modem to an offshore telephone number and sends their browser to one of the above mentioned domains. This appears as a charge on their telephone bill. This business was rather clever with the obfuscating technology used to hide their presence, but the same technology can be used to unravel the obfuscation and find the business behind it.

Category 33.3 Antispam

2001-12-28 antispam filter software quality assurance

NewsScan

AOL TREATS HARVARD ACCEPTANCE LETTERS AS JUNK MAIL: WHY? [28 Dec 2001]

AOL's spam-filtering software thwarted Harvard College's attempt to use e-mail to give applicants the joyous news that they'd been accepted. An AOL spokesman was unable to explain why this happened. [Presumably the messages contained no objectionable words or graphics, but of course very few people can be certain of that, since very few people actually received them.] An AOL spokesman said: "We fight a daily battle against spam at the server level, where we filter it out. Spam is our No. 1 problem. But it's hard to say what would have caused the system to filter e-mail from Harvard." [Question to AOL: What about e-mail from NewsScan? We promise to be good, or at least better.] (Boston Globe/Atlanta Journal-Constitution 28 Dec 2001)

http://www.accessatlanta.com/ajc/epaper/editions/friday/news c3c211257171a1e100c2.html

Category 33.3 Antispam

2002-01-24 antispam excess algorithm wrong bad error false positive reject verification

RISKS 21 89

Jonathan Kamens reported his frustration at trying to reach another RISKS contributor whose Internet service provider blocked his e-mail for spurious reasons. It happened that Mr Kamens was unable to send his e-mail through his usual DSL line, so he sent his message via his ISP's SMTP server. The intended recipient's mail server rejected the message because, as Mr Kamens explained it, "... this site's system administrators have decided to block all E-mail for which the host name in the envelope address can't be matched up obviously (using a simple string comparison) with the host name of the mail server sending the message. In other words, if you have your own domain name, but you send E-mail through your ISP's mail server, you simply can't send E-mail to this site."

When he tried again, this time via his restored DSL service, his mail was rejected because his mail server was incorrectly labeled as a spam relay.

Although the site claimed that they would correct mistaken assignments to the rejection list, Mr Kamens found it particularly irritating that the administrators of this picky site did not provide any way to reach them online. [MK adds that presumably, even if they had, the explanation or complaint would never make it to their e-mail inbox if it came from the affected mail server.]

34.1 Net filters

Category 34.1 Net filters

2001-06-06 censorware content filtering algorithms heuristics errors false positives QA

quality assurance design flaw e-mail blocking

RISKS 21 47

Dan Birchall found that his e-mail newsletter was rejected by some censorware products, apparently because the phrase "sizzling summer" was determined to be indicative of pornography. Birchall suggested, "A better method might combine heuristics with the scoring capability in some mail server software (I'm personally familiar with Exim), incrementing or decrementing a counter based on the occurrence of given words or phrases, with actions depending on the final value of the counter. Thus, if "sizzling" is a +1 word, "video" a +2 word, and "sex" a +3 word, a threshold of 3, 4 or 5 might be used for blocking."

Category 34.1 Net filters

2001-06-10 censorware content filtering algorithms heuristics errors false positives QA

quality assurance design flaw e-mail blocking

RISKS 21 47

Lauren Weinstein, moderator of the PRIVACY Forum, tracked down the reason a censorware content filter blocked his respected publication on a particular site: his quotation of the day included a reference to the movie, "I Love You, Alice B. Toklas!" Unfortunately, the ScanMail filter spotted the "I Love You" and apparently classified the message as a worm or virus. A disgusted Weinstein added, "With such a level of "stone club" analysis at work, one can only imagine what other innocent e-mail is being injected, inspected, detected, infected, neglected, and selected by the "sophisticated" algorithms of filtering programs to be flagged, reviewed, dropped, banned, burned, or trashed."

Category 34.1 Net filters

2001-06-27 censorware e-mail filter algorithm false positive crude gross heuristics pattern

matching

RISKS 21 50

Jurjen N.E. Bos contributed yet another e-mail filter failure to RISKS:

"The IACR (International organisation of Cryptology Research) has someone on its Board of Directors named Don Beaver. The direct result of this is that the recent IACR newsletter (a 34K document full of relevant news on the cryptologic community) was rejected by our company firewall, because his name was in there too many times. It also contained other "dirty" words, such as LaTeX, hardcore, and so on. Our IT department told me that the message would *not* have been rejected if it was split in two, since the number of dirty words would have been halved."

Category 34.1 Net filters

2001-07-25 censorship content filtering parental control technology V-chip television

NewsScan

FIVE YEARS AFTER INTRODUCTION, V-CHIP GETS VERY LITTLE USE

The so-called V-chip devices, which have been installed in new TV sets since 1996 (when President Clinton urged Congress to make them mandatory so that parents could "assume more personal responsibility for their children's upbringing"), are used by only 7% of all parents. The Kaiser Family Foundation said the reason the V-chip is used so little is that the TV networks have little interest in promoting it (since programs from those same networks be blocked by the device). (New York Times 25 Jul 2001)

http://partners.nytimes.com/2001/07/25/arts/television/25CHIP.htm

Category 34.1 Net filters

2001-10-23 content filtering censorship labeling voluntary children parental guidance

NewsScan

AOL, YAHOO, MSN BACK NET FILTERING SYSTEM

The Internet Content Rating Association, supported by AOL, Yahoo, and MSN, will use a rating system in which Web operators would label their sites if they have potentially objectionable material (such as nudity or gambling), so that parents can approve or disapprove each category for access by the children. An executive of the Association says that the value of a voluntary self-labeling system is that it's "about choice--not censorship--on the Internet. We believe that good corporate citizenship and tools that help parents made good decisions is a much better alternative than government regulation." (AP/Washington Post 23 Oct 2001)

http://www.washingtonpost.com/wp-dyn/articles/A37920-2001Oct23.html

Category 34.1 Net filters

2002-01-23 censorware content filtering antispam algorithm simplistic false positive

availability

RISKS 21

MS-Outlook's "adult content filter" assumes that the phrase "over 18" automatically and inevitably means that an e-mail message is pornographic spam. Outlook therefore rejected an issue of Microsoft's own e-mail MSDN Flash newsletter because it contained the phrase "provides over[space]180 hours of content in three technical conferences."

Usage monitoring, audit trails (employees, children)

Category 34.2 Usage monitoring, audit trails (employees, children)

2001-02-23 privacy children censorware

NewsScan

FILTERING FIRM ABANDONS PLANS TO SELL DATA ON KIDS

Under heavy pressure from privacy groups, the company N2H2, a maker of the "Bess" Internet filtering software, has decided to stop selling marketing research companies its "Class Clicks" list that reports the Web usage patterns of school children. The Bess software is used by 14 million students in the U.S. Company executive Allen Goldblatt says that no personally identifiable data on children were ever collected or sold and that "we never would, never have, and never will jeopardize anyone's privacy." Although characterizing the controversy as "a distraction for us," Goldblatt added: "I think any time you have a great public debate about privacy issues, ... this is a good thing." (AP/USA Today 23 Feb 2001)

http://www.usatoday.com/life/cyber/tech/2001-02-23-kids-privacy.htm

Category 34.2 Usage monitoring, audit trails (employees, children)

2001-04-01 privacy Web cookies usage monitoring lawsuit judgement

NewsScan

FEDERAL COURT RULES IN FAVOR OF COOKIES

U.S. District Court Judge Naomi Reice Buchwald has dismissed a class-action suit against online advertiser DoubleClick accusing that company of privacy-related violations of three federal laws. The judge concluded that DoubleClick had not violated those laws through its use of "cookies" (techniques for automatically tracking the movements of Web surfers), and ruled that Web sites could be considered DoubleClick's real "users" and could therefore give consent to monitoring of the transactions with individual customers who visited those cites. Privacy expert Paul Schwartz of Brooklyn Law School offers a different view: "The court said the Web site is the 'user' of the electronic service and can give consent to DoubleClick. So what are the individual consumers, chopped liver?" (New York Times 6 Apr 2001) http://www.nytimes.com/2001/04/06/technology/06CYBERLAW.html

Category 34.2 Usage monitoring, audit trails (employees, children)

2001-06-12 information gathering data mining investigation audit scanning workplace privacy forensics investigation police law enforcement management policy

NewsScan

NEW CORPORATE SOFTWARE SEARCHES EVERYWHERE -- EVEN PERSONAL HARD DRIVES

New productivity software from AltaVista will allow companies to collect data from anywhere in the organization: including not only corporate networks but also individual e-mail accounts and employee PCs. The software is able to search through more than 200 different computer applications and recognize 30 different languages. Privacy advocates are worried. Attorney Gregg Williams says: "This could open a real Pandora's Box. There are some private things on office computers that you really don't want to know about." And Richard Smith of the Privacy Foundation says the software is "really dangerous" and warns that it "would hurt both companies and their employees by damaging morale." But Dana Gardner of the Aberdeen Group has little use for such concerns: "For every person that gets a little embarrassed because some personal information gets passed around the office, there are going to be more people who are able to find important information that helps them close a sale with an important customer or build a better mousetrap." (AP/Washington Post 12 Jun 2001)

http://washingtonpost.com/wp-dyn/business/latestap/A54075-2001Jun12.html

Usage monitoring, audit trails (employees, children) Category 34.2

2001-12-11 Internet instand-messaging chat monitoring logging audit trail parental

supervision children

NewsScan

NEW SOFTWARE SPIES ON INSTANT MESSAGING

New software from Ascentive Inc. enables parents to record their children's instant-messaging chats just like a VCR records a television program, allowing the PC owner to view frequent screen shots of actual conversations and to search and view IM logs for certain words. ChatWatch, a feature included in Ascentive's BeAware PC monitoring software, is more effective than filtering, says Ascentive CEO Adam Schram: "Filters give you too many false positives and negatives -- they block breast-cancer sites but not all porn sites." Instant messaging has soared in popularity over the past few years, with IM use up 34% at work and 28% at home this year. (Wall Street Journal 11 Dec 2001) http://interactive.wsj.com/articles/SB1008016926590752280.htm (sub req'd)

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2002-02-17 surveillance technology spyware logging audit trail employee privacy keystroke

logging pornography appropriate use policy

NewsScan

THE CASE OF THE HORRIFIED SPY

The man who conceived and wrote the software thinks of himself as a privacy lover and says that what his program does is "horrifying": "Every time I add a feature into it, usually it's something that I've fought for a long time." But he's sold more than 200,000 copies of his \$99 downloadable Investigator software, which can read every e-mail message, instant message and document someone sends and receives, and will take pictures from a Web cam, save screen shots, and read keystrokes in numerous languages. The program is hidden on the target's computer, as are the files containing the information it gathers. Ari Schwartz of the Center for Democracy and Technology concedes that the surveillance technology is a valuable tool in fighting fraud or child pornography, but thinks that companies need to resist using it too readily because "we think morally there are some very large issues" raised when employers track the personal habits of their workers. (AP/San Jose Mercury News 17 Feb 2002) http://www.siliconvalley.com/mld/siliconvalley/2693278.htm

35.1 Cybersquatting

Category 35.1 Cybersquatting

2001-04-04 cybersquatting lawsuit decision judgement penalty fine pornography

NewsScan

SEX.COM THIEF MUST PAY \$65 MILLION In a record verdict against a cyber-squatter, a federal judge in San Francisco awarded the original owner of the sex.com domain name \$65 million for the five years' loss of use he suffered after the address was hijacked by fugitive Stephen Cohen, who now lives in Tijuana. "The number is big, but it is unlikely that I will ever see more than a small fraction," said plaintiff Gary Kremen. Meanwhile, Kremen's site has dropped the hard-core images placed by high-paying porn advertisers, and now uses a text-based dictionary that links to other sex sites by topic. "We have done what we said we were going to do – reduce the amount of pornography on the site as we transition to more mainstream content," said Kremen. (Los Angeles Times 4 Apr 2001) http://www.latimes.com/business/20010404/t000028664.html

Category 35.1 Cybersquatting

2001-06-04 cybersquatting DNS domain name system entrepreneurs competition registration

NewsScan

WHAT'S IN A NAME

When an Internet domain name is not renewed (whether intentionally or by accident), it goes back on the market, and some companies specialize in buying them up and reselling them for other purposes. Ray King of SnapNames says: "The bigger the company, the easier it is. They just lose track of it... Any good name that expires you, can be certain there will be at least a couple hundred people trying to get it." A short, clever name with a good search position at Yahoo is vulnerable to being recaptured for use as an "adult" site. (USA Today 4 Jun 2001) http://www.usatoday.com/life/cyber/tech/2001-06-04-domain-name-woes.htm

Category 35.1 Cybersquatting

2001-10-26 DNS domain name system registration maintenance pornographers

cybersquatting

NewsScan

HOW A KIDS SITE WAS TAKEN OVER BY PORNOGRAPHERS

A Web site offering a math-and-money game for children was turned into a porn site after an employee's departure left VeriSign unable to get paid for the renewal of the site's registration. With the fee unpaid, the domain name was sold to a pornographer, because "they felt we weren't paying our invoices. But we weren't getting any because of confusion over the contact information." The game is now offered at Moneyopolis.com. (New York Times 26 Oct 2001) http://partners.nytimes.com/2001/10/26/technology/26NET.html

Category 35.1 Cybersquatting

2001-11-13 DNS domain name system cybersquatting extortion pornography

RISKS 21 76

Malcolm Pack, writing in RISKS, gave a startling explanation of why so many sites have been converted to pornographic content. He suggests, "...[The] presence of pr0n on the 'hijacked' site is a blackmail tool, which would explain why so many domain names obviously targeted at children become (apparently inexplicably) pr0n sites. I'd never thought of pr0n as a weapon...."

[Mr Pack uses "pr0n" as a substitute for "porn" presumably to avoid triggering e-mail content filters.]

Dan Fandrich confirmed that extortionists are indeed buying expired domain names and installing porn in order to embarrass former domain owners and extort high repurchase prices. He wrote, "...[P]ornographers bought up close to 2000 expired domains ..., including domains owned by respectable organizations with hundreds of inbound links, such as the TCL Consortium, XIII International AIDS Conference, Evian, Universal ADSL Working Group, and Craig's List. I tracked down the original owners of about 60 of these sites with the most inbound links and warned them of the problem Five months later, only three of those 60 sites have done anything about their former domains, either buying them back from the extortioners or getting links changed to their new sites."

Mr Fandrich offers some thoughtful advice to anyone thinking about letting a domain name registration lapse: "Some of the former owners I talked to seem to have trouble seeing that their web sites did not stand in isolation, that people outside their organization had links to their web site and others had bookmarks and those links attached to their names were now serving up porn. I got responses to the effect of «We have a new domain name now, so we don't care what happens to the old one.» One certainly takes a RISK in letting one's domain name expire, but when the gamble fails and what must be about the worst case scenario occurs, the indifference I've seen surprised me. I find it hard to believe that so many people have so little respect for their viewers and customers."

Category 35.1 Cybersquatting

2002-02-15 cybersquatting dishonesty Web hijacking political propaganda trickery

NewsScan

LYING FOR TRUTH

Some unknown person or group has created a Web site called www.reedcollegis.com intended to fool people looking for Reed College (www.reed.edu) and send them an anti-abortion site called www.abortionismurder.com. Reed College chief technology officer Martin H. Ringle says, "We've paid for 'reed.com' and 'reed.org,' and so on, in an effort to pre-empt cybersquatting. But it's impossible to imagine every variation of the name and how it could be used -- although in hindsight, reedcollegis.com was an obvious one." The site abortionismurder.com is maintained by a Florida man, Thomas P.A. Fitch, who denies involvement with or knowledge of the creation of reedcollegis.com, but does admit to owning an address similar to that of the College Board. His aim is to attract college applicants to his anti-abortion site to expose "to the truth" students who are "going to run this country in fifteen years... I'd say our tactics are not dishonest. They're creative, they're on the edge, they're bold. Thank you for the publicity because it's only helping our cause." Sheldon E. Steinbach of the American Council on Education says of use of the name reedcollegis.com to divert unsuspecting surfers from their intended goal: "This is the first instance, to my knowledge, that a university or college name has been hijacked for seemingly a political purpose." (Chronicle of Higher Education 15 Feb 2002)

http://chronicle.com/free/2002/02/2002021501t.htm

35.2 Trademarks vs DNS

Category 35.2 Trademarks vs DNS

2001-05-24 DNS domain name system trademark infringement lawsuit

NewsScan

UNIVERSITY SUES ADULT SITE FOR USING ITS TRADEMARK [24 May 2001]

The University of North Carolina has filed a \$100,000 lawsuit against the adult Web site uncgirls.com, which is registered to Universal Nude College Girls Sites. The suit charges the owners of the site with misappropriating the university's trademark "UNC." A university official said, "We don't want our trademarks diluted, and we don't want the good name of the university to be smirched." In addition monetary damages, the suit demands that the domain name uncgirls.com be transferred to the university. (AP/USA Today 24 May 2001) http://www.usatoday.com/life/cyber/tech/2001-05-24-unc-adult-site-suit.htm

Category 35.2 Trademarks vs DNS

2001-08-15 DNS domain name system registrar name conflict trademarks challenge

arbitration

NewsScan

INTERNET REGISTRAR TO CHALLENGE NAME CLAIMS [15 Aug 2001]

In response to widespread criticism, Afilias -- the company that runs the new ".info" domain -- says it will challenge some of the more shaky claims made on the most desirable names. The situation arose when Afilias allowed businesses to claim their trademarks before registration was opened up to the general public. Many of those claims were made on common dictionary words, with registrants providing little or no trademark documentation. Afilias rules allowed would-be challengers to register their complaints, but charged them \$295 to begin the process. Even if they were successful, challengers were refunded only \$220 of that fee. More than 25,000 .info names have been claimed since preliminary registration opened July 25, and Afilias exec Roland LaPlante says his company expects to file hundreds of challenges with arbiters at the World Intellectual Property Organization. Some of the names already claimed include books.info, consumers.info and business.info. (AP 15 Aug 2001)

http://news.excite.com/news/ap/010815/00/internet-names-for-grabs

Category 35.2 Trademarks vs DNS

2002-01-16 DNS domain name system registrar trademark conflict investigation

NewsScan

INTERNET REGISTRAR CHALLENGES '.INFO' TRADEMARK CLAIMS [16 Jan 2002]

Afilias, the company responsible for registering ".info" names, is challenging 741 registrations made by people who claimed they owned the trademark on the name. Afilias says it didn't have the time to verify that applicants actually held the trademarks that they claimed. "It would have been too complicated and slow, since there is no unified worldwide database for trademarks," says Phillipp Grabensee, an Afilias board member. "We would have had to check every single brand." Afilias is now attempting to sort through its database and weed out fraudulent applications, referring them directly to an international mediator for resolution. During the two-month period set aside for trademark holders to preregister for their names, 52,245 names were registered, and it's estimated about 20% of those names were fraudulently acquired. "Some people seem to have registered a whole dictionary," says Grabensee. (Handelsblatt/Wall Street Journal 16 Jan 2002)

http://interactive.wsj.com/articles/SB10112144497968880.htm (sub req'd)

35.3 Politics of the DNS

Category 35.3 Politics of the DNS

2001-02-05 DNS domain name system new politics

NewsScan

ICANN DEFENDS NAME CHOICES

ICANN chairman Vinton Cerf acknowledges that the group may have rejected qualified proposals when it approved seven new domain names last year, but says that the goal "was not to have a contest and pick winners." ICANN purposely kept the pool of new names small, so that it could test whether the additions caused any problems with the overall system. Domain names, he says, have never been added "in the context of the Internet as it exists today. We want to do so without endangering the utility of what has become a global medium for communications and commerce." (AP/Washington Post 8 Feb 2001)

http://washingtonpost.com/wp-dyn/articles/A44287-2001Feb8.html

Category 35.3 Politics of the DNS

2001-07-26 DNS domain name system ICANN lawsuit lottery

NewsScan

LAWSUIT CHALLENGES .BIZ 'LOTTERY' [26 Jul 2001]

A class-action lawsuit filed in Los Angeles Superior Court this week alleges that NeuLevel, the operator of the new ".biz" domain, is running an illegal lottery by charging customers just for a chance to register a .biz name. There is no guarantee that a customer will be awarded a desired name, as more than one customer may pay for a chance on the same name. The suit names as co-defendant the Internet Corporation for Assigned Names and Numbers (ICANN) and several registrars, including VeriSign and Register.com, which have been licensed to sell .biz and other Internet domain names to the public. The plaintiffs argue that NeuLevel's "lottery enterprise" is not only illegal, but unfair because it allows those with larger financial resources to increase their odds of getting a name by buying multiple chances. (InteractiveWeek 26 Jul 2001)

http://dailynews.yahoo.com/h/zd/20010726/tc/lawsuit challenges dot biz lottery 1.html

Category 35.3 Politics of the DNS

2001-11-06 ICANN DNS domain name service politics election candidates

NewsScan

ICANN CONSIDERS REDUCING PUBLIC ROLE IN INTERNET MANAGEMENT [6 Nov 2001]

The At-Large Membership Study Committee of ICANN, the nonprofit international organization responsible for developing policies for Internet address assignment and management, is recommending that special fees be charged to members of the public who want to participate as at-large directors in ICANN's decision-making processes. Former Swedish Prime Minister Carl Bildt, who heads the Committee, says that existing and other proposed methods for picking at-large directors are unworkable: "You can have all sorts of visionary schemes but we living in the reality of today. ICANN needs stability. This is not the time for experiment." Last year's at-large elections allowed voting by e-mail, and suffered from technical and administrative difficulties. (AP/San Jose Mercury News 6 Nov 2001) http://www.siliconvalley.com/docs/news/svfront/043415.htm

Category 35.3 Politics of the DNS

2001-11-13 ICANN security DNS domain name service registrars security attacks

vulnerability Internet

NewsScan

ICANN REVIEWS NETWORK SECURITY ISSUES [13 Nov 2001]

Speaking at the annual meeting of the Internet Corporation for Assigned Names and Numbers (ICANN), network security expert Paul Vixie warned: "The Internet is very fragile. It would be very easy for an angry teenager with a \$300 computer to create almost unlimited pain for anyone on the Internet and not get caught. We've got to have attention focused on this." Some ICANN critics charge the organization with having ignored security concerns until forced to address them, and Paul-Jean Jouve, president of the network security company Brinx Corp, wrote in a letter: "I am deeply troubled by the complacency of the ICANN leadership on the subject of security. It took worldwide fears to stimulate the dialogue on this issue." (Reuters/New York Times 13 Nov 2001) http://partners.nytimes.com/reuters/technology/tech-tech-icann-security.html

Category 35.3 Politics of the DNS

2001-11-14 DNS domain name system international conflict dispute control

NewsScan

DOMAIN NAME FIGHTS IN NONWESTERN COUNTRIES

Many of the world's Internet users have address suffixes indicating the countries in which they are located (such as ".fr" for France), but often "location" is not really the right word. For example, the ".tj" domain for Tajikistan is actually run out of Fresno, California, and 800 of the 1,000 Web sites are pornographic in nature. Tajik activist Asomiddin Atovev, who works with the Global Internet Project Initiative, sees both the problem and the solution: "The first step is getting control out of the U.S." (Reuters/San Jose Mercury News 14 Nov 2001) http://www.siliconvallev.com/docs/news/svfront/029080.htm

Category 35.3 Politics of the DNS

2002-01-14 domain name system DNS regulations limits trademarks

NewsScan

ICANN HEAD FAVORS MEMBERS-ONLY DOMAINS [10 Jan 2002]

ICANN president M. Stuart Lynn says he favors creating new members-only suffixes, such as .edu and .museum, over unrestricted domains such as .biz and .info. "A lot of the problems surrounding the new (top-level domains) are less (common) in a sponsored environment," he said, echoing sentiments expressed by ICANN chairman Vint Cerf at a meeting in December. Problems such as cybersquatting disputes would be greatly diminished in a more tightly regulated domain, said Lynn. "It may be that a number of these cybersquatting or trademark disputes are going to be less because there's a lot of careful evaluation to make sure that someone really is using them for their announced" purpose. Lynn and Cerf have both emphasized that their opinions are their own and not those of ICANN, but that they've talked with many people who agree with them. "More people I talk to think it's the more likely direction," said Lynn. (Reuters/CNet 10 Jan 2002)

http://news.cnet.com/news/0-1005-200-8436749.html?tag=mn hd

THE INTERNET NAME GAME [14 Jan 2002]

The London-based Global Name Registry has begun offering registration of Internet names for individual persons. Name registration will cost about \$30 a year (not including Internet access), and the registry plans to expand ".name" designations to mobile phones and other personal devices by the end of the year. (AP/San Jose Mercury News 14 Jan 2002)

http://www.siliconvalley.com/docs/news/svfront/002411.htm

Category 35.3 Politics of the DNS

2002-01-21 DNS domain name system lottery

NewsScan

REGISTRARS REJECT VERISIGN'S 'PAY-TO-WAIT' PROPOSAL [21 Jan 2002]

Internet domain name registrars overwhelmingly oppose VeriSign's proposal to create a pricey waiting list for registered domain names, calling it too expensive and anti-competitive. VeriSign has suggested charging registrars \$40 for first dibs on a registered domain name. A subscriber would be guaranteed first-refusal rights to the name if it becomes available, but would still have to pay even if the current owner decided to renew its subscription. VeriSign said the waiting list would provide a new source of revenue and discourage speculation in domain names by raising the cost. Other registrars complained that instead of solving the cybersquatting problem, the proposal would just shift the action to the waiting list. In addition, some expressed suspicions that VeriSign would use the waiting list to hoard all the best names for itself, but Chuck Gomes, VP of policy and compliance for VeriSign's Global Registry Services, said his company maintained a strict "firewall" between the two sides of the business: "I ensure that day by day we're not advantaging any registrar I understand the mistrust, but it's unwarranted." (Wired.com 21 Jan 2002) http://www.wired.com/news/business/0,1367,49756,00.html

Category 35.3 Politics of the DNS

2002-02-25 DNS domain name system government involvement politics policy model

NewsScan

ICANN PRESIDENT WANTS MORE GOVERNMENTAL PARTICIPATION

Stuart Lynn, president of the nonprofit Internet Corporation for Assigned Names and Numbers, says the organization he heads needs to be restructured to obtain more governmental participation: "I am now convinced that the original desire to avoid a totally governmental takeover ... led to an overreaction – the choice of a totally private model." Such a model is unworkable, Lynn says, because it leaves ICANN "isolated from the real-world institutions – governments – whose backing and support are essential.'' His recommendation calls for the next ICANN board to have 15 members – one-third nominated by governments, one-third selected through a committee process, and the remaining consisting of the group's president and appointments by four policy and technical groups. (AP/San Jose Mercury News 25 Feb 2002)

http://www.siliconvalley.com/mld/siliconvalley/2741326.htm

NEW PROPOSAL DISPARAGED BY ICANN CRITICS [25 Feb 2002]

The proposal made by ICANN president Stuart Lynn to expand the participation of the world's governments in making policy decisions over Internet domain names and other issues is being widely criticized for "closing the door to the public" (Karl Auerbach) and for giving "totalitarian governments power to influence rules that would go into direct effect in the United States" (Michael Froomkin). Lynn maintains that the national governments are "the most evolved form of representation of the public interest," even if not all are democratic. The acronym ICANN stands for Internet Corporation for Assigned Names and Numbers. (AP/San Jose Mercury News 25 Feb 2002) http://www.siliconvalley.com/mld/siliconvalley/2745051.htm

Education in security & ethics

Category 37 Education in security & ethics

plagiarism penetration teenagers adolescent criminal hackers education ethics

awareness parental guidance ignorance

RISKS 21 18

Winn Schwartau wrote in RISKS, "Two 8th-grade honor students in Tampa, Hillsborough County, Florida, hacked into the school computer and copied the final exam for one of their courses. They have been suspended. [PGN-ed]

We've wired up the country's schools, put the kids on the Internet, and only a small handful of teachers have any clue as to what goes on behind the mouse button. The teachers are not technically trained, they are underpaid and underappreciated. Is it any wonder? And I doubt the kids have been taught the first thing about CyberEthics by their schools or their parents."

Category 37 Education in security & ethics

2001-05-23 information assurance education university government scholarships

NewsScan

U.S. GOVERNMENT PLANS SCHOLARSHIPS FOR CYBER-SECURITY CORPS

The National Science Foundation has selected six universities to participate in a \$8.6-million scholarship program designed to fund a "cyber corps" of 200 computer-security students who would earn graduate or undergraduate degrees in information security or a related field and agree to take government jobs upon graduating. The program would pay two years' tuition and participants would work at least one year for each year of assistance they received. Afterward they would be free to take jobs in the private sector. Participating schools include Carnegie Mellon, Iowa State, Purdue, the University of Idaho, the University of Tulsa and the Naval Postgraduate School. (Wall Street Journal 23 May 2001)

http://interactive.wsj.com/articles/SB990572871992181459.htm (sub req'd)

Category 37 Education in security & ethics

2001-10-08 information security education failure weakness inadequate

NewsScan

WULF AND SPAFFORD SAY U.S. DEFICIENT IN SECURITY RESEARCH

William Wulf, president of the National Academy of Engineering, and Eugene Spafford, director of Purdue University's Center for Education and Research in Information Assurance and Security, have a told a Congressional science committee that the nation must take serious steps to increase support for academic research on computer security techniques. Wulf said he was "appalled" at the state of security research in academia, while Spafford noted that he found that only 23 students involved in cybersecurity research have earned doctorates in the last three years. (Federal Computer Week 8 Oct 2001)

http://www.fcw.com/fcw/articles/2001/1008/web-cip-10-11-01.asp

Category 37 Education in security & ethics

2002-02-07 anti-fraud online safety security privacy education awareness Web alliance

consumer protection

NewsScan

NEW SUPPORT GROUP TARGETS PC SECURITY

A government-and-business alliance called the Stay Safe Online Campaign has established a site at http://www.staysafeonline.info to provide home and small business computer users with information about security techniques to protect themselves against network vandals. A spokesman for the group explains that individuals and small businesses "don't have the infrastructure support that people who work in large companies have at the office," and a recent study by Digital Marketing Services found that 97% of such users are vulnerable to attacks on the Internet because they fail to update antivirus software on a regular basis. (San Jose Mercury News 7 Feb 2002) http://www.siliconvalley.com/mld/siliconvalley/2627667.htm

Category 37 Education in security & ethics

2002-02-14 Internet fraud scam teenagers adolescents children ethics training education law

enforcement police prevention prediction

NewsScan

INTERNET KIDS: I WAS A TEENAGE SCAMMER

FBI agent Frank Harrill of the Los Angeles cybercrime squad says, "We have seen a rise in the crimes [Internet scams], with an increasing degree of sophistication by a younger demographic. I think it's safe to say we are going to see more of it." The use of the Internet to make fraudulent credit card purchases with stolen account numbers has become a fairly common practice. One knowledgeable observer says, "It's easy for them to pull off. A lot of teens don't take it seriously. They think it's a game." Chris Painter of the U.S. Department of Justice thinks he sees an answer to the problem: "We have to teach these kids some kind of cyberethics." (AP/USA 14 Feb 2002) http://www.usatoday.com/life/cyber/tech/2002/02/14/net-scammers.htm

38.1 Consumer profiling

Category 38.1 Consumer profiling

privacy ISP Internet service provider cable DSL Web access logging monitoring

recording data collection privacy consumer profiling

NewsScan

COMCAST RECORDS SURFING MOVEMENTS OF ITS SUBSCRIBERS [12 Feb 2001]

Comcast, the nation's third-largest cable company and a provider of high-speed Internet access to a million computer users, says it has begun recording the Web surfing movements of its subscribers in order to improve its technology and services. Admitting that it began the monitoring without notifying its customers, the company said it believes its actions are permitted by the language in their service agreements with subscribers, and insists that "Comcast absolutely does not share personal information about customers, and we have the utmost respect for our customers' privacy." Privacy advocates are upset about the Comcast action, and Internet security expert (and Comcast customer) George Imburgia says: "I'm furious." (AP/San Jose Mercury News 12 Feb 2001) http://www.siliconvalley.com/mld/siliconvalley/2661735.htm

COMCAST STOPS STORING INDIVIDUAL WEB-SURFING PATTERNS [14 Feb 2002]

In response to criticism from privacy advocates, Comcast has decided to cease collecting data that would allow it to track the Web surfing habits of individual subscribers. The company says it had never contemplated using the information for anything other than to determine aggregate usage patterns so it could improve the performance of its computers and networks. Comcast executive Dave Watson says, "We don't want anyone to be concerned we'd take that next step forward. We just want to take this issue off the table." David Sobel of the Electronic Privacy Information Center says his group's concern was not necessarily that Comcast itself would track individual usage, but that law enforcement agencies might get the information by subpoena. (New York Times 14 Feb 2002) http://partners.nytimes.com/2002/02/14/technology/14PRIV.html

Category 38.1 Consumer profiling

2001-06-07 consumer profiling GPS geographical positioning system law enforcement surveillance personal information privacy accident emergency vehicle

RISKS 21 46

Chris Norloff contributed an interesting essay to RISKS about the implications of having GPS on automobiles:

"You just can't outrun a satellite. A Merced, California, man took his fully equipped 2001 SUV out onto some nearby country roads, navigating swiftly and confidently with the optional OnStar Global Positioning System. When he got into an accident, he decided to run for it. But the guidance system had already notified OnStar headquarters of the accident, specifying where it had happened and giving a complete description of his vehicle to the California Highway Patrol. The officers followed a trail of coolant about a mile into an orchard, where they found and arrested the driver. [Source: *Road & Track* magazine, July 2001; PGN-ed]"

Norloff continued, "What constitutes an "accident"? (Air bags seem to go off quite easily, taking out the windshield and dashboard [\$\$\$] in a fender-bender). Will GPS-reported accidents become like household burglar alarms - sending out mostly false alarms? Who will hack into the OnStar system to falsely report accidents? Who will use the OnStar system to efficiently dispatch lawyers to accident sites? How soon until OnStar sells accident records so used-car purchasers can learn the vehicle's history?"

Category 38.1 Consumer profiling

2001-10-22 cookies persistent state targeted advertising consumer profile privacy

NewsScan

AOL TO USE "COOKIES" FOR TARGETED ADVERTISING

Privacy advocates seem to have no objections to AOL's new decision to begin using "cookies" (tiny files left on user computers to track their Web travels), which AOL says it's doing to help prevent customers from receiving advertisements irrelevant to their interests. AOL maintains that the company and its advertisers will use cookies "to determine, on an anonymous basis, which advertisements members have seen and how members respond to them," but will not let the cookies to be used "to compile profiles about the different Web sites that a particular member visits." (Gannett/USA Today 22 Oct 2001)

http://www.usatoday.com/life/cyber/2001/10/22/aol-cookies.htm

Category 38.1 Consumer profiling

2002-02-21 consumer privacy contract tracking surveillance vehicle automobile rental GPS

Geographical Positioning System

NewsScan

RENT-A-CAR COMPANY WILL CONTINUE SPYING ON SPEEDERS [9 Jul 2001]

Acme Rent-a-Car in New Haven has rebuffed the Connecticut Department of Consumer Protection and plans to continue using Global Positioning System (GPS) technology to track individuals who speed in rented vehicles, and levy fines on them of \$150 if the speeding continues for more than two minutes. The consumer agency's complaint against Acme is based not on privacy issues but on the charge that Acme's rental contract didn't give adequate information about what it was doing. (USA Today 9 Jul 2001)

http://www.usatoday.com/life/cyber/tech/2001-07-09-rental-car-tracking.htm

CAR RENTAL AGENCY CITED FOR SPYING ON SPEEDERS [21 Feb 2002]

Acme Rent-a-Car, based in Connecticut, has been cited by the state's Consumer Protection Commission for its practice of tracking customers' driving habits via GPS devices and assessing customers \$150 each time they exceeded 79 miles per hour. The commission said the company violated Connecticut's unfair trade practices act by not notifying customers of the monitoring, and ordered Acme to pay back "every single customer who they took money from illegally." Many car rental agencies use GPS to locate their vehicles in case they are stolen or taken out of the country. (Reuters/CNet 21 Feb 2002)

http://news.com.com/2100-1040-842821.html

38.2 Trade in personal information

Category 38.2 Trade in personal information

2001-01-10 data subject personal information database privacy

NewsScan

DEFUNCT TOYSMART AGREES TO DESTROY CUSTOMER DATABASE

Online etailer Toysmart, which was sued by the Federal Trade Commission and other plaintiffs to prevent it from selling its customer database when it went out of business, has agreed to destroy the database in exchange for \$50,000 from a subsidiary of its majority stockholder, the Walt Disney company. A spokesman for the privacy group TRUSTe said, "This is a landmark case because it tells other companies that the privacy promises you make while you're in business must be kept when you go out of business. If you don't keep them, there are third parties that will stop you." (AP/USA Today 10 Jan 2001)

http://www.usatoday.com/life/cyber/tech/cti977.htm

Category 38.2 Trade in personal information

2001-04-03 privacy consumer information resale mergers acquisitions

NewsScan

EBAY MODIFIES PRIVACY POLICY TO ALLOW POSSIBLE USER INFO SALE

EBay has refined its privacy policy to clarify its right to sell users' information if the company is acquired or merges with another business. In a notice on its Web site, eBay said it is "possible that eBay, its subsidiaries, its joint ventures, or any combination of such, could merge with or be acquired by another business entity. Should such a combination occur, you should expect that eBay would share some or all of your information in order to continue to provide the service." EBay said it was making the change in response to government efforts to block the sale of customer information by ToySmart.com, a bankrupt toy e-tailer, to other companies. (Wall Street Journal 3 Apr 2001) http://interactive.wsj.com/articles/SB986241729530570517.htm

Category 38.2 Trade in personal information

2001-08-20 privacy protection technology Internet consumer information traffic

NewsScan

HP CHIEF CALLS FOR WEB PRIVACY LEGISLATION

Carly Fiorina, the chief executive of Hewlett-Packard, told a technology conference this week that federal legislation is needed to protect the privacy of Internet users, and suggested that the problem is caused technologists more than it is by technology itself: "I think we in the technology industry have fallen in love with technology. And in the end it is not about the technology. Privacy and security, or trust, are vital to consumers, and that is what we should focus on. There is a role for legislation." (Reuters/New York Times 20 Aug 2001)

http://partners.nytimes.com/reuters/technology/tech-tech-privacy.html

Category 38.2 Trade in personal information

2001-12-07 trade commerce sell personal information privacy identity theft government

authentication opt-out

NewsScan

CALIFORNIA SELLS BIRTH DATA TO PRIVATE WEB SITE, 'RAISES RED FLAG' [29 Nov 2001]

The State of California has sold the birth data of California residents to a privately operated genealogy Web site that can now be used to retrieve such personal data as someone's place of birth or mother's maiden name — information frequently used as identifying information for purposes of accessing bank accounts and making various kinds of financial transactions. State Senator Jackie Spier (D, San Mateo) warns: "The time has come for us to recognize that identity theft has become a big problem. The fact that this information is public should raise a red flag." (San Jose Mercury News 29 Nov 2001)

http://www.siliconvalley.com/docs/news/svfront/037140.htm

ASK AND YOU SHALL BE REMOVED ... BUT YOU'VE GOT TO ASK [30 Nov 2001]

Responding to complaints by consumers and privacy advocates who protested California's legal sale to the Web genealogy company RootsWeb.com of public information containing such personal data as people's birth dates and their mothers' maiden names, the company now says it will remove from its Web site the names of anyone who makes a specific request. A spokesman for the company said: "The mission of our company is to create places to help people reconnect with their families. We're not in any way doing anything except helping our customers and if a customer is concerned about it, it doesn't do any good to leave them up on the site." A legal council for the Electronic Privacy Information Center says that California's sale of data to the genealogy Web site "a situation where all the residents of California have now been exposed to a new risk of identity theft." (San Jose Mercury News 30 Nov 2001) http://www.siliconvalley.com/docs/news/svfront/priv113001.htm

CALIFORNIA GOVERNOR HALTS SALES OF BIRTH & DEATH RECORDS [7 Dec 2001]

California Gov. Gray Davis has issued an order placing a 45-day freeze on the state's sale to Web sites of records containing such personal data as mothers' maiden names of state residents. Critics of the sale of this kind of information are afraid it could be used for identity theft and other fraudulent purposes, while defenders of the practice say there's no evidence that the sites are actually being used like that. The general counsel for the California Newspaper Publishers Association says: "I'm an eighth-generation Californian and the fact that my ancestors were born here and died here is pretty much basic historical information. That has always been accessible in California and I'm not sure what new emergency there is that would warrant this executive order." (San Jose Mercury News 7 Dec 2001)

http://www.siliconvalley.com/docs/news/svfront/trade120701.htm

According to several reports to RISKS (see for examle issue 21.81), as of at least 1 December 2001, the entire CA and TX birth records databases were removed from the MyFamily.com, Ancestry.com and RootsWeb.com Web sites.

Category 38.2 Trade in personal information

2001-12-18 children online privacy data information traffic trade government regulation

proposed legislation Congress

NewsScan

GOVERNMENT PLANS TO RESTRICT SALE OF KIDS' PERSONAL DATA [18 Dec 2001]

Congress and the Bush administration seem united in a broad effort to require public schools to give parents the right to deny businesses the ability to gather personal information about their children. Senator Richard C. Shelby (R., AL.) complains, "They're basically selling access to kids without parents knowing about it," and Senator Christopher J. Dodd (D., CN) agrees, saying: "These companies were using the classroom market research." Some of the opposition to the proposed restrictions on sharing student data has come from the National School Boards Association, which says the law could become an "administrative nightmare" that would deprive schools of "productive relationships with businesses." (Washington Post 18 Dec 2001)

http://www.washingtonpost.com/wp-dyn/articles/A57156-2001Dec17.html

38.3 Industry efforts for privacy protection

Category 38.3 Industry efforts for privacy protection

2001-12-10 corporate privacy policy P3P Platform for Privacy Preferences legal liability

Microsoft MS browser IE6 Internet Explorer

RISKS 21 82

Attorney Ben Wright noted in RISKS that the new defaults in MS Internet Explorer version 6 may pose a problem for corporations:

"The filters force administrators to post new privacy policies for their Web sites, coded in a technical language called P3P. The filters punish administrators who fail to publish properly coded P3P privacy policies by blocking or impeding their cookies.

The P3P coding language raises, for any corporation, government agency or other institution that uses it, a lawsuit danger. A privacy policy written in it exposes the organization to liability, with little or no escape.

A privacy policy, even one written in computer codes, can be legally enforceable like a contract. In lawsuits filed in 1999, plaintiffs forced US Bancorp to pay \$7.5 million for misstatements in a privacy policy posted on its Web site.

Web administrators face a dilemma. They want to satisfy IE 6's technical requirement for P3P codes, but they also want to sidestep liability. See Webserver Online Magazine article: http://webserver.cpg.com/news/6.12/n5.shtml

One solution is to deploy dummy P3P codes, with an extra legal code that disavows any liability for the codes, as explained at < http://www.disavowp3p.com>."

41 Cryptanalysis techniques

Category 41 Cryptanalysis techniques

decryption cracking law enforcement police investigation forensics swap file data

remanence rubber-hose cryptanalysis

RISKS 21 58

A report om the cryptography mailing list republished in RISKS included the following information about a police investigation that used cryptanalysis against a disk encryption program:

The German encryption program Safeguard Easy has been broken by the Danish police. Today the police from the city Holstebro in Jutland presented evidence in court, that was provided after breaking the encryption on five out of sixteen computers that where seized april 25 this year.

All 16 computers were protected with Safeguard Easy from the german encryption provider Utimaco. It is not known whether DES, 128-bit IDEA, Blowfish or Stealth was used as algorithm on the computers. All four algorithms are built in Safeguard Easy. Details are sparse. It is not known how the encryption was broken, whether it was brute forced or flaws in the program was exploited.

In followup correspondence, commentators suggested that since only some of the encrypted systems were cracked, perhaps the forensic analysis was able to locate passwords in the Windows swap file.

However, it turned out that actually the cryptanalysis was based on password guessing.

42.1 Weaknesses

Category 42.1 Weaknesses

2001-03-20 cryptanalysis public key cryptosystem weakness private key cracking

RISKS 21 28

David Kennedy, CISSP summarized a report about a major problem with OpenPGP: with access to a PGP user's private keyring, it is possible to obtain the private key and then use it to forge PGP signatures. Kennedy pointed to research by Czech cryptologists published at < http://www.i.cz/en/onas/tisk4.html >. The quoted material included this description of the cryptanalysis: "A slight modification of the private key file followed by capturing a signed message is enough to break the private key. These tasks can be performed without knowledge of the user's passphrase. After that, a special program can be run on any office PC. Based on the captured message, the program is able to calculate the user's private key in half a second. The attacker can then sign any messages instead of the attacked user. Despite of very quick calculation, the program is based on a special cryptographic know-how."

In a later posting to RISKS, Kennedy wrote, "Hal Finney has a succinct analysis posted to the Open-PGP list archived at: http://www.imc.org/ietf-openpgp/mail-archive/msg04767.html

My [DK's] summary of Hal's analysis:

- 1. Attackers have to diddle the secret key.
- 2. Does *not* work with commercial PGP 7.0.3 w/RSA keys (unknown about earlier).
- 3. Does work with all DSA keys and RSA keys in GPG."

Category 42.1 Weaknesses

2001-07-26 cryptography weakness wireless protocol WEP 802.11 eavedropping cracking

known-ciphertext attack

RISKS 21 55

Famed cryptographer Adi Shamir (the "A" in "RSA") announced a new paper on weaknesses in WEP (Wired Equivalent Privacy):

"WEP is the security protocol used in the widely deployed IEEE 802.11 wireless LAN's. This protocol received a lot of attention this year, and several groups of researchers have described a number of ways to bypass its security.

Attached you will find a new paper which describes a truly practical direct attack on WEP's cryptography. It is an extremely powerful attack which can be applied even when WEP's RC4 stream cipher uses a 2048 bit secret key (its maximal size) and 128 bit IV modifiers (as proposed in WEP2). The attacker can be a completely passive eavesdropper (i.e., he does not have to inject packets, monitor responses, or use accomplices) and thus his existence is essentially undetectable. It is a pure known-ciphertext attack (i.e., the attacker need not know or choose their corresponding plaintexts). After scanning several hundred thousand packets, the attacker can completely recover the secret key and thus decrypt all the ciphertexts. The running time of the attack grows linearly instead of exponentially with the key size, and thus it is negligible even for 2048 bit keys."

Peter G. Neumann wrote, "Matt Blaze . . . put Adi's paper at < http://www.crypto.com/papers/others/rc4_ksaproc.ps >"

Rubin and colleagues published another relevant paper a week later; in RISKS, Rubin wrote the following:

Using the Fluhrer, Mantin, and Shamir Attack to Break WEP by Adam Stubblefield, John Ioannidis, and Aviel D. Rubin

We implemented an attack against WEP, the link-layer security protocol for 802.11 networks. The attack was described in a recent paper by Fluhrer, Mantin, and Shamir. With our implementation, and permission of the network administrator, we were able to recover the 128-bit secret key used in a production network, with a passive attack. The WEP standard uses RC4 IVs improperly, and the attack exploits this design failure. This paper describes the attack, how we implemented it, and some optimizations to make the attack more efficient. We conclude that 802.11 WEP is totally insecure, and we provide some recommendations.

http://www.cs.rice.edu/~astubble/wep/

Category 42.1 Weaknesses

2001-08-06 cryptographic algorithm weakness e-commerce Passport single signon

RISKS 21 58

David P. Kormann and Aviel D. Rubin, Risks of the Passport Single Signon Protocol, IEEE Computer Networks, volume 33, pages 51-58, 2000.

. . .

Abstract:

Passport is a protocol that enables users to sign onto many different merchants' web pages by authenticating themselves only once to a common server. This is important because users tend to pick poor (guessable) user names and passwords and to repeat them at different sites. Passport is notable as it is being very widely deployed by Microsoft. At the time of this writing, Passport boasts 40 million consumers and more than 400 authentications per second on average. We examine the Passport single signon protocol, and identify several risks and attacks. We discuss a flaw that we discovered in the interaction of Passport and Netscape browsers that leaves a user logged in while informing him that he has successfully logged out. Finally, we suggest several areas of improvement. http://avirubin.com/passport.html

Category 42.1 Weaknesses

2001-08-15 encryption algorithm cracked weakness decryption video chilling effect lawsuits

DMCA HDCP

RISKS 21 60

Monty Solomon wrote in RISKS that a video crypto standard was reported cracked:

"Noted cryptographer Niels Ferguson says he's broken Intel's vaunted High-bandwidth Digital Content Protection (HDCP) Digital Video Encryption System, but fear of U.S. law is keeping him silent on the details. HDCP connects digital cameras, high-definition televisions, cable boxes, and video disks players. [Source: Article by Ann Harrison, 13 Aug 2001, PGN-ed;

http://www.securityfocus.com/news/236]"

Peter G. Neumann added: [Intel has not threatened him, but he can still be sued by the U.S. Govt under DMCA, or by the motion-picture industry. His comments are at < http://www.macfergus.com/niels/dmca/index.html >. Knowledge that it is (or might be) breakable is likely to result in other folks doing it, and perhaps posting it anonymously in some non-US Web site. The globalization of the Internet is clearly going to be an increasingly difficult problem for industries trying to defend information supposedly protected under flawed standards. . . .]

Niels Ferguson wrote an essay in RISKS 21.60 entitled, "Censorship in action: why I don't publish my HDCP results ." Some excerpts:

I have written a paper detailing security weaknesses in the HDCP content protection system. I have decided to censor myself and not publish this paper for fear of prosecution and/or liability under the US DMCA law.

Introduction

My name is Niels Ferguson. I'm a professional cryptographer. My job is to design, analyse, and attack cryptographic security systems, a bit like a digital locksmith. I work to make computer systems and the Internet more secure. You would think that people would be in favour of that, right?

Computer security and cryptography are hard. It is easy to make mistakes, and one mistake is all it takes to create a weakness. You learn from your mistakes, but there are too many mistakes to make them all yourself. That's why we publish. We share our knowledge with others, so that they don't have to repeat the same mistake. Take a look at http://www.macfergus.com/niels/dmca/index.html./pubs/publist.html > my publications. You will see a mixture of new designs, analyses, and attacks. This is how we learn and how we improve the state of the art in computer security.

HDCP

Recently I found the documentation of the < http://www.digital-cp.com > High-bandwidth Digital Content Protection (HDCP) system on the Internet. HDCP is a cryptographic system developed by Intel that encrypts video on the DVI bus. The DVI bus is used to connect digital video cameras and DVD players with digital TVs, etc. The aim of HDCP is to prevent illegal copying of video contents by encrypting the signal.

HDCP is fatally flawed. My results show that an experienced IT person can recover the HDCP master key in about 2 weeks using four computers and 50 HDCP displays. Once you know the master key, you can decrypt any movie, impersonate any HDCP device, and even create new HDCP devices that will work with the 'official' ones. This is really, really bad news for a security system. If this master key is ever published, HDCP will provide no protection whatsoever. The flaws in HDCP are not hard to find. As I like to say: "I was just reading it and it broke."

[Later in the paper, Ferguson pens a cogent attack on the very premise of the DMCA (Digital Millennium Copyright Act):]

The DMCA imposes a serious restriction on the freedom of speech. The DMCA makes it illegal to talk about certain security systems. The equivalent law for non-digital protection systems would make it illegal to warn people about a cheap and very weak door lock being installed on their houses because criminals could also use that same information.

In western society we restrict the freedom of speech only for very serious reasons, and after careful consideration. For example, it is illegal to shout "fire" in a crowded theatre, or to ask someone to commit a murder. The DMCA restricts the freedom of speech because the movie industry is afraid of losing money. Below I will argue that the DMCA does not achieve that goal, but that aside: do we really want to sell our freedom of speech for money?

The DMCA is a scary development. Next time that commercial interests clash with the freedom of speech, the industry will point to the DMCA and claim they need equivalent protection. They might outlaw the publication of a report detailing bad safety features in a car, or of flaws found in a particular brand of tires. After all, those publications harm industry too. Where will it stop?

[I encourage everyone interested in the DCMA to read the entire text of this essay, which is available at < http://www.macfergus.com/niels/dmca/index.html > . - MK]

Category 42.1 Weaknesses

2002-03-10 weak encryption vulnerabilities ICAT CVE

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported 10 vulnerabilities involving weak encryption out of a total of 1241 for the period from 1 Jan 2001 to 10 Mar 2002. This represents about 1% of all vulnerabilities logged for that period. Overall, for the entire period since the CVE began recording vulnerabilities in 1995, weak encrytion is named in 51 of the 3677 vulnerabilities or about 1% of the total. The vulnerabilities listed for 2001 and up to 10 Mar 2002 are as follows:

CAN-2001-1005: Starfish Truesync Desktop 2.0b as used on the REX 5000 PDA uses weak encryption to store the user password in a registry key, which allows attackers who have access to the registry key to decrypt the password and gain privileges. Published Before: 8/31/2001 Severity: Medium

CAN-2001-1003: Respondus 1.1.2 for WebCT uses weak encryption to remember usernames and passwords, which allows local users who can read the WEBCT.SVR file to decrypt the passwords and gain additional privileges. Published Before: 8/31/2001 Severity: Medium

CAN-2001-0983: UltraEdit uses weak encryption to record FTP passwords in the uedit32.ini file, which allows local users who can read the file to decrypt the passwords and gain privileges. Published Before: 8/31/2001 Severity: High

CAN-2001-0618: Orinoco RG-1000 wireless Residential Gateway uses the last 5 digits of the 'Network Name' or SSID as the default Wired Equivalent Privacy (WEP) encryption key. Since the SSID occurs in the clear during communications, a remote attacker could determine the WEP key and decrypt RG-1000 traffic. Published Before: 8/2/2001 Severity: High

CAN-2001-0352: SNMP agents in 3Com AirConnect AP-4111 and Symbol 41X1 Access Point allow remote attackers to obtain the WEP encryption key by reading it from a MIB when the value should be write-only, via (1) dot11WEPDefaultKeyValue in the dot11WEPDefaultKeySTable of the IEEE 802.11b MIB, or (2) ap128bWepKeyValue in the ap128bWEPKeyTable in the Symbol MIB. Published Before: 7/21/2001 Severity: Medium

CAN-2001-0382: Computer Associates CCC\Harvest 5.0 for Windows NT/2000 uses weak encryption for passwords, which allows a remote attacker to gain privileges on the application. Published Before: 6/18/2001 Severity: High

CAN-2001-0133: The web administration interface for Interscan VirusWall 3.6.x and earlier does not use encryption, which could allow remote attackers to obtain the administrator password to sniff the administrator password via the setpasswd.cgi program or other HTTP GET requests that contain base64 encoded usernames and passwords. Published Before: 3/12/2001 Severity: High

CAN-1999-0757: The ColdFusion CFCRYPT program for encrypting CFML templates has weak encryption, allowing attackers to decrypt the templates. Published Before: 3/12/2001 Severity: Medium

CAN-2001-0103: CoffeeCup Direct and Free FTP clients use a weak encryption to store passwords in the FTPServers.ini file, which could allow attackers to easily decrypt the passwords. Published Before: 2/12/2001 Severity: Medium

CAN-2000-1173: Microsys CyberPatrol uses weak encryption (trivial encoding) for credit card numbers and uses no encryption for the remainder of the information during registration, which could allow attackers to sniff network traffic and obtain this sensitive information. Published Before: 1/9/2001 Severity: Medium

42.3 Implementation flaws

Category 42.3

Implementation flaws

2001-11-09

cryptography hardware software weakness vulnerability cracking penetration decryption abuse insider crime confidentiality passwords bank automated teller machines

RISKS 21 74

Andrew Brydon, writing in RISKS, summarized the findings of research on automated banking machine security in Britain: "A serious weakness has been discovered in the methods used by banks to protect the number that lets you get money from a cash machine. Researchers from the University of Cambridge have found that the computer systems which check that these numbers are valid are easy to defeat. They warn that unscrupulous insiders could exploit these weaknesses to raid customer accounts. The researchers have called on banks to revise their security arrangements and use more open procedures to protect customers' cash. . . . The physical construction of the cryptoprocessors is certified to a high standard to ensure that the boxes cannot be forced to give up the keys they use to scramble data. Any physical tampering with the box makes them destroy the keys they use. [However,] security researchers Michael Bond and Richard Clayton have found serious weaknesses in the software cryptoprocessors use to handle the encryption keys as they talk to different programs. ... using the clues provided by the leaky software, the cracking time can be reduced to just 24 hours."

http://news.bbc.co.uk/hi/english/sci/tech/newsid_1645000/1645552.stm

43.1 Tokens

Category 43.1 Tokens

2001-10-29 token-based identification authentication I&A military smart cards

NewsScan

NEW "SMART CARDS" FOR THE TROOPS

Four million U.S. troops and civilian Defense Department employees will be receiving new credit-size "smart cards" that will enable them to unlock doors, get cash, make purchases, check out weapons, and obtain computer and network access. There will be no medical data on the cards. A Pentagon spokesman says that "there's a very limited amount of intrusion into anyone's privacy." (AP/Washington Post 29 Oct 2001)

http://www.washingtonpost.com/wp-srv/aponline/20011029/aponline173744_000.htm

Category 43.1 Tokens

2002-01-08 token identification authentication I&A drivers' license registration national

identity card

NewsScan

'SMART' DRIVERS' LICENSES UP AHEAD

The U.S. Transportation Department is working with the states to develop a new generation of drivers' licenses that contain electronically stored information such as fingerprints or retinal scans. Privacy advocates say the move toward "smart" licenses is really a backdoor way to establish federal ID cards -- an idea that has gained popularity among government officials following the Sept. 11 terrorist attacks. "The debate after Sept. 11 showed that Americans are instinctively suspicious of a single federally issued card, but they might be more sympathetic to identifications issued by businesses or perhaps states," says Jeffrey Rosen, a law professor at George Washington University. "What you're seeing here is a sort of a hardening of the driver's license that could lead to development of a national ID system without creating a national ID card," says Marc Rotenberg, who heads up the Electronic Privacy Information Center. (AP 8 Jan 2002)

http://apnews.excite.com/article/20020108/D7GTF1H01.html

Category 43.1 Tokens

2002-02-06 smart card token consumer profiling data storage identification authentication

I&A e-commerce

NewsScan

NEW SMART CARD COULD KNOW EVERYTHING

A San Francisco company called PrivaSys has developed a battery-powered smart card that could be used to replace all the individual credit and debit cards a consumer might carry. The internal chip on the card will be able to store "loyalty" accounts (such as Frequent Flyer data) for a number of different vendors. The company has struck a deal with First Data, but will have to form additional alliances with other credit-processing companies to achieve its plan to make its card the only one you'll need in your purse or wallet. (USAToday 6 Feb 2002)

http://www.usatoday.com/life/cyber/tech/review/2002/2/06/smartcard.htm

Category 43.1 Tokens

2002-02-27 personal identification implanted token microchip skin transponder privacy

nonymity

NewsScan

CHIP ID IS ONLY SKIN-DEEP [19 Dec 2001]

Applied Digital Solutions, based in Palm Beach, Florida, is making headlines with plans to become the first company to sell microchips designed to be implanted into humans. One initial target market is likely to be people with artificial limbs and organs -- a user could have up to 60 words of relevant medical information embedded in the chips, which could then be read by medical personnel if the patient were brought unconscious into an emergency room. With rollout in South America scheduled in about 90 days, another potential market is potential kidnap targets who could use the chips in combination with GPS devices to alert security personnel to their whereabouts. Future plans call for ordinary people to use the chips as the ultimate ID, supplanting the functions now performed by passwords and keys. "I'd be shocked if within 10 years you couldn't get a chip implanted that would unlock your house, start your car and give you money," says Chris Hables Gray, author of "The Cyborg Citizen." And lest you think it unlikely that you'd want to try something like this out, futurist Paul Saffo reminds us, "As some people wring their hands about the invasion of privacy and civil liberty, a whole other generation is going to go, 'Cool! I've always wanted to embed technology in my body.' It's going to be fashion. One sure sign that teenagers will love it is if it terrifies their parents." (Los Angeles Times 19 Dec 2001)

http://www.latimes.com/technology/la-000100545dec19.story?coll=la%2Dheadlines%2Dtechnology

CHIP IMPLANT COMPANY SEEKS FDA APPROVAL [27 Feb 2002]

A Florida company that has developed a computer ID chip suitable for implanting in the human body has applied to the Food and Drug Administration for approval of its product. The VeriChip, as it's called, can be used to store information, such as medical records, which could be accessed by emergency medical personnel in the event of an accident. Applied Digital Solutions says it plans to limit its marketing of the VeriChip to companies that ensure its human use voluntary. A person or intermediary company would buy the chip for about \$200 and have it encoded with the desired information. The person seeking the implant would then take the chip — about the size of a grain of rice — to a doctor, who would insert it under the skin with a large needle device. Meanwhile, privacy advocates have expressed doubts about the VeriChip: "The problem is that you always have to think about what the device will be used for tomorrow. It's what we call function creep. At first a device is used for applications we all agree are good but then it slowly is used for more than it was intended," says Lee Tien, an attorney for the Electronic Frontier Foundation. (AP Feb 27 2002)

http://apnews.excite.com/article/20020227/D7HUDV3O0.html

43.2 Biometrics

Category 43.2 Biometrics

2001-07-31 voice synthesis recognition biometric authentication I&A vulnerability

NewsScan

VOICE CLONING

AT&T Labs has created new text-to-voice software that makes it possible for a company to use recordings of a person's voice (for example, John F. Kennedy's) to utter life-like statements that they never made. Priced in the thousands of dollars and called "Natural Voices," the software could be used by telephone call centers and other such activities. An AT&T executive said: "If ABC wanted to use Regis Philbin's voice for all of its automated customer-service calls, it could." Issues sure to arise include disputes over voice-licensing rights and measures to prevent fraudulent uses. One potential client for the software noted: "Just like you can't trust a photography anymore, you won't be able to trust a voice either." (New York Times 31 Jul 2001)

http://www.nytimes.com/2001/07/31/technology/31VOIC.html

Category 43.2 Biometrics

2001-10-01 biometric identification authentication I&A e-commerce fingerprint recognition

NewsScan

PUTTING A FINGER ON E-PAYMENTS

Indivos, an Oakland, Calif. firm, has developed software that uses fingerprint scanners to process electronic payments of all kinds. "We're putting this in front of the mainstream consumer," says a company spokesman. "You won't need cash or cards to pay for anything. All you need is your finger and you never leave home without it." Indivos has partnered with fingerprint sensor manufacturer Digital Persona to test the service at a "major fast food chain" in California and supermarkets throughout the country. Fingerscans, which are the leading biometric application, will represent 33% or \$300 million of the market by 2006, according to Frost & Sullivan. (Wired.com 1 Oct 2001) http://www.wired.com/news/business/0,1367,47127,00.html

Category 43.2 Biometrics

2001-10-26 biometric face recognition surveillance terrorism airport security privacy

NewsScan

BOSTON'S LOGAN AIRPORT TO USE FACE-RECOGNITION SYSTEM

Boston's Logan Airport, where the September 11th terrorists boarded planes they hijacked for their attacks on New York and Washington, has decided to install face-recognition technology to scan the faces of travelers and compare them against a computerized database of suspected terrorists. The American Civil Liberties Union has opposed the technology, calling it intrusive and ineffective. (AP/USA Today 26 Oct 2001)

Category 43.2 Biometrics

2001-11-01 face recognition biometric identification authentication

NewsScan

THE FACE-RECOGNITION SOFTWARE MARKET

Since the September 11th terrorist attacks, face-recognition technology has been given a much friendlier reception than it did when it was introduced at the last Super Bowl game or at Tampa early this year. Now, Visionics and Viisage, the two major companies in that industry, are engaged in fierce competition for dominance in a market expected to grow from \$200 million in revenue this year to \$2 billion in 2004. Face-recognition systems compare digital translations of a person's facial characteristics to images in a database of suspected terrorists and criminals. Critics of the technology insist that its use is likely to be expanded into uses beyond the apprehension of evil-doers, and argue that it is not always accurate. In response, advocates for the technology admit that it is "not as precise as fingerprints" but insist that occasional "false positives" can easily be resolved by local authorities. (Washington Post 1 Nov 2001) http://www.washingtonpost.com/wp-dyn/articles/A20852-2001Oct31.html

Category 43.2 Biometrics

2001-11-08 fingerprint recognition biometric identification authentication I&A

NewsScan

REPLACING PASSWORDS WITH FINGERPRINTS

A new fingerprint-recognition device called U.are.U could soon eliminate the need to remember passwords for accessing restricted Web sites, making it as easy as the touch of a finger. The \$69 system, from Silicon Valley-based DigitalPersona, is aimed at consumers and small businesses, and designed to work with systems running Windows XP. Once the device has been "trained" to recognize a fingerprint, all the user has to do is type his or her user ID and password for each secure Web page into the software that controls the fingerprint module. From then on, access will be granted just by tapping the device. U.are.U can also encrypt certain files or folders on the PC so that they can be read only by designated people. (Wall Street Journal 8 Nov 2001) http://interactive.wsj.com/articles/SB1005172330856003280.htm

Category 43.2 Biometrics

2002-01-03 biometric face recognition identification authentication surveillance screening

NewsScan

DIGITAL PHOTO DATABASE TO CONFIRM IDENTITY OF FOREIGN TRAVELERS

The U.S. State Department will soon begin comparing foreign travelers' faces with digitized photographs to confirm that individuals shown in their travel papers are the same persons who actually applied and were approved for admission to this country. And new legislation being considered in Congress would require biometric identifiers on passports issued by a number of countries, including Japan and most of Western Europe, that are in the visa-waiver program. (San Jose Mercury News 3 Jan 2002)

http://www.siliconvalley.com/docs/news/svfront/026914.htm

Category 43.2 Biometrics

2002-01-25 biometric face recognition I&A identification authentication airport security

RISKS 21 89

Iceland's main airport will have face recognition systems installed. Chris Leeson notes in RISKS that this can work only for known faces and he hopes that the security staff will not come to rely mainly on the system.

Category 43.2 Biometrics

2002-02-18 token smart card identification authentication I&A immigration government

identity thumbprint fingerprint recognition biometrics

NewsScan

HONG KONG TO USE DIGITAL ID CARDS

Hong Kong is planning to introduce an identity card with an embedded digital chip containing a replica of the cardholder's thumbprint, for matching against an optical reader at border crossings into China. "You don't have to have an immigration officer there to look at the card," says an immigration official in Hong Kong. "It's just a self-service kiosk." Besides verification of identity, the chip could be made to include medical, financial, and other data on an individual, but at least for now the card will contain only basic information. Sin Chung-kai, a pro-democracy member of the Hong Kong legislature, says: "We're not opposed to people having to carry ID cards. The crux of the controversy is how much information should be stored on the card... If I were a film star and I had some kind of disease, I wouldn't want it to be on my ID card. I also wouldn't want the ID to be my cash card. I don't want my spending traced." (New York Times 18 Feb 2002)

http://www.nytimes.com/2002/02/18/technology/18KONG.html

43.3 Passwords

Category 43.3 Passwords

palm computer password back door failure bug weakness vulnerability

confidentiality encryption decryption

RISKS 21 26

According to Robert Lemos, writing for CNET News, the security company @Stake reported that any devices using the Palm operating system (PalmOS) have no effective security despite the password function. Apparently developer tools supplied by Palm allow a back door conduit into the supposedly locked data. The firm warned that "If someone finds or steals a Palm, the owner's data is basically an open book. And the theft of mobile devices for their data is becoming more common." In addition, wrote Lemos, "Last September, @Stake discovered that the encrypted password used by Palm OS to protect so-called private records from prying eyes could easily be broken. With the discovery of the latest back door, it would seem that no data is safe."

Category 43.3 Passwords

2001-05-11 canonical passwords voicemail confidentiality

RISKS 21 40

Vodafone Australia's mobile phone voicemail uses a canonical password if a user has not set one. As RISKS contributor Andrew Goodman-Jones noted, "Need to check on your friends', your ex's, your boss', your children's voicemail?"

Category 43.3 Passwords

2001-07-23 password cracker MS Microsoft IE Internet Explorer freeware

RISKS 21 56

A freeware application to crack the S Internet Explorer file that stores passwords was released on the Web with the following notice in the Earthlink Weekly Email Newsletter on 07/23/2001: "If you tell your browser to save Web site passwords so that you don't have to reenter them, you might forget those passwords over time. This program can reveal the passwords hidden behind those asterisks in Web site login screens."

Category 43.3 Passwords

2001-09-05 password management modification data corruption user interface design flaw

stupidity error bug

RISKS 21 65

Bill Bumgarner discovered that entering a password with an exclamation mark in the new-password fields for Consumer Reports' Web site results in _silent_ exclusion of the character. Thus when the user tries to enter the accepted password with the "!", the system naturally rejects the password. However, one can always get a plaintext copy of the "corrected" password via unsecured e-mail. . . .

[MORAL: designers must not modify a password without notifying the user of the change.]

Category 43.3 Passwords

2001-12-03 credit card identification authentication I&A password fraud

NewsScan

CREDIT CARD COMPANIES DEVELOP NEW PASSWORD SYSTEMS

To give customers an added feeling of security when they provide their credit card numbers to make purchases over the Internet, Visa and Mastercard will offer new password systems. The Visa system is being launched today as a optional feature, and will invite cardholders to link their cards to an additional password, beyond the information on the card itself; the Mastercard system, still in development, will require the user to download a small program. Amazon is one of the merchants that has declined to participate in the system, because "it would turn one-click ordering into four-point, three-click ordering." Dell, on the other hand, has already signed up for the system, not so much because of its own concerns about fraudulent purchases but because "we want to give customers more confidence in buying online," even though cardholders are not actually liable for fraudulent purchases made on their accounts. Credit card fraud is not a major problem for most companies, and Visa says that just 7 cents out of every \$100 is lost to fraud. (New York Times 3 Dec 2001)

http://partners.nytimes.com/2001/12/03/technology/ebusiness/03CARD.html

Category 43.3 Passwords

2002-08-03 password policy reset e-mail canonical password stupidity awareness

RISKS 21 57

[No point in abstracting this one: here's Jim Horning's contribution to the demonstration of the state of security awareness (or even just of common sense) in corporate America:]

Subject: Password changes -- SIGH!

- > From: <HR Department>
- > Sent: Friday, August 03, 2001 10:12 AM
- > To: <US Employees>
- > Subject: IMPORTANT <HR Database> INFORMATION PLEASE READ
- >
- > We want to make you aware that <HR Database> will be unavailable from 6pm
- > (PT) on Friday, August 3 to 11:59pm (PT) on Sunday, August 5 due to server
- > upgrades. During this time, you will not be able to access the website.
- > In < Outsourced supplier > 's ongoing effort to improve site performance,
- > these upgrades are occurring to load balance and increase site stability.
- > Part of this site upgrade includes a password change. ALL USERS WILL HAVE
- > A PASSWORD OF "change123" as of 12:01am PT Monday, August 6th, 2001. Once
- > you enter the system for the first time on or after August 6th, you will
- > be required to change your password and answer a secret question. In the
- > future, you will be able to use the answer to the question to reset your
- > own password.
- > If you experience problems, please contact the whereiwork help desk at
- > support@<Outsourced supplier>.

44.1 Algorithms

Category 44.1 Algorithms

2001-02-12 encryption stream cipher

NewsScan

VANISHING ENCRYPTION

Harvard computer science professor Michael Rabin and his doctoral student. Yan Zong Bing have developed a way of sending messages using an encryption scheme that can not be broken, because the code is created from a stream of random numbers that are never stored in the computer's memory and in effect vanish at the same time a message is coded or decoded. Dr. Richard Lipton of Princeton and Georgia Tech says: "It's like in the old 'Mission Impossible,' where the message blows up and disappears." But some computer scientists, such as Professor Dorothy Denning at Georgetown, say that the technique is impractical for large messages, while Dr. Peter G. Neumann at SRI International suggests that cryptography's role in protecting privacy is more cosmetic than real: "If you think cryptography is the answer to your problem, then you don't know what your problem is." (New York Times 20 Feb 2001)

http://partners.nytimes.com/2001/02/20/science/20CODE.html

Category 44.1 Algorithms

2001-11-26 encryption algorithm intellectual property movies audio distribution

NewsScan

DOROTHY DENNING AND THE DEVELOPMENT OF GEO-ENCRYPTION

Among the "next wave of innovators" identified by Time magazine, Georgetown computer science professor Dorothy Denning was chosen for her previous accomplishments in computer security as well for current work in pioneering a new field she calls geo-encryption, which provides a way to keep information undecipherable until it reaches its location. With geo-encryption, movie studios could be assured that when they used the Internet to distribute films they films would end up at movie theaters rather than in the hands of pirates, and the State Department could be assured that classified messages could only be decoded at embassies, and not by terrorists. (Time 26 Nov 2001) http://www.time.com/time/magazine/article/0,9171,1101011126-184999,00.html

45.1 Digital signatures / certificates

Category 45.1 Digital signatures / certificates

digital certificates software authenticity fraud bogus impersonation quality assurance revocation list risk management security model

RISKS 21 29

Many correspondents reported the issuance of bogus digital certificates assigned to Microsoft by Verisign. Jeff Savit's summary was as follows:

"Spoofing hazard: Verisign gave digital certificates under Microsoft name to an individual not from Microsoft. Microsoft issued a bulletin at < http://www.microsoft.com/technet/security/bulletin/MS01-017.asp > that describes the risk of running code that erroneously appears to be signed by Microsoft (eg: ActiveX controls), and discusses the risks due to not having a proper revocation mechanism.

Note that the certs were made available January 30th, so who knows what code has been accepted and executed since then. Microsoft is a victim in this particular instance."

Later contributions to RISKS and BUGTRAQ provided more details of the security breach. Roy Sinclair pointed to a paragraph from the Frequently Asked Questions at http://www.microsoft.com/technet/security/bulletin/MS01-017.asp >:

"The update is needed because of a characteristic of VeriSign code-signing certificates. Every certificate issuer periodically generates a Certificate Revocation List (CRL), which lists all the certificates that should be considered invalid. A field in every certificate should indicate the CRL Distribution Point (CDP) - the location from which the CRL can be obtained. The problem is that VeriSign code-signing certificates leave the CDP information blank. As a result, even though VeriSign has added these two certificates to its current CRL, it's not possible for systems to automatically download and check it."

Sinclair continued, "The first question I have after seeing that is how many of the rest of the 500,000 certificates that Verisign says they have issued also do not have this CRL Distribution Point field properly filled in. In the lack of any information to the contrary I would hazard to guess that it's probably that none of the 500,000 certificates issued by Verisign have supplied the information that should be in this field. If this is truly the case then we have yet another problem of much wider scope than the improper issuance of two certificates, there are a great number of valid certificates which could be stolen or misused and even if Verisign were to add them to their CRL the certificates themselves don't point to the CRL so they won't be properly rejected. Two things need to be done, one is that software which checks certificates must be changed to warn users that certificates lacking a CRL are much more suspect and Verisign needs to re-place all certificates that currently lack this critical information with new certificates that have this field properly filled in. Additional questions that come to mind is how many other certifying agencies have also failed to fill in the information in this field and what percentage of the certificates being used today are unverifiable?"

Michael Sinz pointed to the well-known fallacy of confusing authentication with quality or trustworthiness.: "So, lets see - Microsoft says that ActiveX is secure as long as the software (ActiveX thing) is not from an 'evil' source. To prevent bad software from being used, they use digital signatures to identify the person or company who made the software such that you could either trust them or know who to go after when it does something bad. The OS and system infrastructure does not try to enforce anything other than to check these certificates and warn you based on your settings as to if you want to run unsigned software or any software signed by company 'X' or a number of other possible combinations of warnings. There is no built in security beyond that point. Once you say 'Yes, run it' you are opening up your system to complete control by the ActiveX control. Ok, in a perfect world, with no one wishing to do harm or rob you blind, such a mechanism would work just fine. The Internet is not such a world."

Category 45.1 Digital signatures / certificates

2001-07-11 digital certificate authority CA signature trust password single point of failure

identification and authentication I&A

NewsScan

MICROSOFT TO USE VERISIGN TO PROVIDE SECURITY FOR ".NET"

Microsoft's ".NET" and "Hailstorm" paid subscription services -- which will rely on customer willingness to store personal and credit information on a Microsoft system called Passport -- will be protected by the Internet security company VeriSign. VeriSign will provide "digital certificates" over the Passport system when extra security is needed for financial and other transactions requiring strict security protection. Customers will need to remember just a single password, but VeriSign's chief executive insists that simplicity won't take away from security: "The issue you deal with is that customers want ease-of-use but they also want higher levels of trust. Before, those two things were mutually exclusive, but now they can be as simple as one password." (AP/San Jose Mercury News 11 Jul 2001) http://www.siliconvalley.com/docs/news/syfront/079055.htm

Category 45.1 Digital signatures / certificates

2001-07-26 bad PGP digital signature Microsoft security bulletins alerts

RISKS 21 56

A report published in RISKS pointed to a serious problem with Microsoft security bulletins:

> For at least four months, Microsoft has been sending out security bulletins which fail a popular e-mail authentication system. As a result, the company could be opening the door to counterfeit bulletins from malicious hackers.

To protect against forgery, Microsoft's security response center digitally signs its bulletins with PGP before e-mailing them to subscribers of its security notification service. But since at least March, if recipients attempt to verify the messages' authenticity, PGP will issue a warning that the bulletins contain an invalid signature.

"The problem is that Microsoft's bulletins effectively look as if they're forged. And telling a Microsoft forgery from someone else's is virtually impossible," said Paul Murphy, head of information technology at Gemini Genomics, a genetic research firm in Cambridge, England. [...] <

[MORAL: check the digital signature after you publish a signed document.]

45.4 E-payments / e-wallets

Category 45.4 E-payments / e-wallets

2001-07-27 electronic commerce e-commerce payment digital identity wallet payment privacy

NewsScan

AOL CONSIDERS OFFERING 'IDENTITY SERVICE' [27 Jul 2001]

AOL Time Warner is said to be considering creation of "Magic Carpet," a so-called "identity service" to compete against Microsoft's Passport as an Internet gatekeeper that would allow consumers to store all their personal identifying data (including credit information) in one place. Passport now has more than 160 million accounts, and is being challenged in the courts by consumer and privacy groups concerned with how the service would work in conjunction with Microsoft XP, that company's new Internet-oriented operating system. Sun Microsystems chief executive Scott NcNealy welcomes AOL into the fray: "It's a nice alternative choice to Microsoft, and maybe having two companies go at each other will neutralize each other." (Washington Post 27 Jul 2001 http://washingtonpost.com/wp-dyn/articles/A56191-2001Jul26.html

Category 45.4 E-payments / e-wallets

2001-08-15 e-commerce digital signature certificate electronic wallet cash privacy consumer

complaints objections

NewsScan

PRIVACY GROUPS STILL UNHAPPY WITH MICROSOFT

A coalition of consumer and privacy groups, including Junkbusters and the Electronic Privacy Information Center, is making a new assault on Microsoft, objecting to the Microsoft Passport service that will be included in the forthcoming Windows XP: "We charge Microsoft with specific unfair, deceptive and illegal behavior in collecting information [about Passport users], and their [Microsoft's] response is to make merchants use this pseudo-privacy technology. It's just insultingly nonresponsive." Microsoft denies the group's claims, and says that Passport will give people more convenience and control over what information they reveal about themselves. (USA Today 15 Aug 2001) http://www.usatoday.com/life/cyber/tech/2001-08-15-xp-privacy-complaint.htm

Category 45.4 E-payments / e-wallets

2001-09-20 e-commerce digital cash electronic wallet e-payments

NewsScan

MICROSOFT PASSPORT SYSTEM OPENS UP TO RIVAL SITES

Microsoft, which has been criticized by privacy groups and others for using its Passport online identification technology to establish a dominant role in e-commerce, says it will make the system compatible with competing offerings by competing companies. A Microsoft executive said: "We do not want to be the one authentication scheme across the Internet. We see ourselves as one of many producers." (New York Times 20 Sep 2001) http://www.nytimes.com/2001/09/20/technology/20SOFT.html

Category 45.4 E-payments / e-wallets

2002-02-28 token identification authentication I&A e-commerce wireless interception man-in-

the-middle attacks penetration confidentiality wristwatch

NewsScan

WRISTWATCHES TO TELL TIME, ORDER HAMBURGERS, PAY FOR GAS

The Timex watch company has developed some wristwatches with Speedpass technology that uses a radio frequency transponder to communicate credit or debit card information allowing customers to pay instantly in places like Exxon and Mobil gas stations and McDonald's restaurants. The watch is currently being test-marketed in Illinois. (AP/USA Today 28 Feb 2002)

http://www.usatoday.com/life/cyber/tech/review/2002/2/28/timex-speedpass.htm

45.5 Watermarks

Category 45.5 Watermarks

2001-01-23 intellectual property protection watermark audit trail privacy contract law

NewsScan

IBM UNVEILS NEW COPYRIGHT TECHNOLOGY

IBM has added new features to its Electronic Media Management System, which is used by copyright holders to control under what circumstances their music is distributed. "We announced two fundamental enhancements," says IBM VP Steve Canepa. "One is superdistribution, which allows for peer-to-peer file distribution. Once the file gets to the consumer, whether it's on a PC or a PDA or whatever, it can now be passed along. A track has a set of usage criteria that can follow it wherever it goes." Translated, that means that fans who buy a music track encoded with EMMS can pass it along to a friend, but the friend may then have to buy the track. The second enhancement provides more choices for rules set by the content owner. For instance, downloadable tracks could expire on the album's release date in one country, but never expire in another country. Music files can also be tracked so that the content owner knows where each copy is, who acquired it and how, and whether it was passed along to others. (Hollywood Reporter 23 Jan 2001)

http://www.hollywoodreporter.com/convergence/index.asp?ee

Category 45.5 Watermarks

2001-07-17 copyright content protection video movies standard 5C DTLA Digital

Transmission Licensing Administrator

NewsScan

SONY & WARNER AGREE ON CONTENT-PROTECTION STANDARD [17 Jul 2001]

Sony Pictures and Warner Bros. Studio have agreed to accept the content-protection standard developed by the so-called "5C Group" of manufacturers (Intel, Matsushita, Toshiba, Sony, and Hitachi) who are joined in an alliance called the Digital Transmission Licensing Administrator. The standard specifies a technology for protecting digitized movies and as they are exchanged among set-top boxes, computers, and televisions when the exchange is made over cables. Disney and Vivendi, which have not signed on to this standard, are holding out for the development of a way to protect transmissions even when they are broadcast over the air and received via antennas. (Wall Street Journal 17 Jul 2001) http://wsj.com (sub. req'd)

Category 45.5 Watermarks

2001-11-08 digital watermark legal dispute DVD copy protection patent

NewsScan

DIGITAL WATERMARKING DISPUTE DELAYS DVD STANDARD [8 Nov 2001]

The adoption of a technical standard for DVD copy-protection will suffer delays as Verance and Digimarc, two of the lead digital watermarking companies, head to court over their long-standing intellectual property dispute. Digital watermarking places a unique bit of code into a sound or image file that makes it difficult to play without permission from copyright holders. Verance has now filed a lawsuit charging Digimarc with violating antitrust and unfair competition laws, alleging that Digimarc illegally submitted Verance's digital watermarking technology to a standards group. The suit "is going to delay an adoption of a standard for DVD copy-protection," says a Raymond James Financial analyst. "The longer they hash it out in the Portland courts, the longer it's going to take for the industry to (accept a) solution and get some compliant software out there." Digimarc is a member of the Video Watermarking group, a coalition of consumer electronics companies that includes Hitachi, Macrovision, NEC, Philips Electronics, Pioneer and Sony. The group hopes to set a digital watermarking standard that will allow film studios to distribute content online securely. (CNet News.com 8 Nov 2001)

http://news.cnet.com/news/0-1005-200-7820458.html?tag=lh

45.6 Other e-commerce security measures

Category 45.6 Other e-commerce security measures

2001-01-04 e-commerce dispute resolution alternative arbitration

NewsScan

E-COMMERCE PROTOCOL AIMS AT QUICK DISPUTE RESOLUTION

In an effort to speed up e-commerce dispute resolution, a number of major companies, including AT&T, DaimlerChrysler and Microsoft, are signing on to an "e-commerce protocol" drafted by the American Arbitration Association. The document, being released today, lists only vague principles, such as "fairness," "continuity of business" and "commitment to technology," but arbitration association president William K. Slate II says his organization will be rolling out over the next several months "proprietary" technologies that will make it possible to resolve disputes quickly. (Wall Street Journal 4 Jan 2001) http://interactive.wsj.com/articles/SB978566423262962375.htm

2001-04-21 copyright intellectual property digital rights management DRM patent

infringement lawsuit

NewsScan

Category 45.6

INTERTRUST SUES MICROSOFT FOR PATENT INFRINGEMENT [27 Apr 2001]

Other e-commerce security measures

InterTrust Technologies, which makes copyright-protection technology, has sued Microsoft for patent infringement, alleging that the software giant's Windows Media product violates a patent issued to InterTrust in February. The case focuses on digital rights management (DRM) technology, which typically is used in conjunction with downloadable music and other intellectual property to limit access to paying customers. DRM can also be used to enforce any rules set by copyright holders, for instance, allowing a customer to listen to a song three times for free and then cutting off access until a credit card number is submitted. InterTrust has tried unsuccessfully to get Microsoft to license its technology, but Microsoft has continued to ship its own DRM software as part of Windows Media. "InterTrust has invested quite heavily in its patent portfolio," says an InterTrust division president. "We believe we've made seminal investments that relate to the digital-rights management space." A Microsoft spokesman said the company is reviewing the complaint, but that it had been developing its own content-protection technology for years. (Wall Street Journal 27 Apr 2001) http://interactive.wsj.com/articles/SB988324594170991932.htm

Category 45.6 Other e-commerce security measures

2001-08-20 encryption movie Internet distribution copyright intellectual property

NewsScan

HOLLYWOOD TO OFFER VIDEO-ON-THE-NET [17 Aug 2001]

Hoping to ward off movie piracy over the Internet, Hollywood studios Warner Bros., MGM, Paramount, Sony Pictures, and Universal Studios are entering into a joint venture that will be used to distribute their products over the Internet to personal computers. The transmissions, which will take 20 to 40 minutes for downloading of a feature-length film, will be encrypted to prevent them from being intercepted. One executive involved in the joint venture calls the plan "an offensive move by the studios," intended both to create "a new distribution platform through the PC," and also to offer "a high-quality, legal, convenient, user-friendly service for movies over the Internet." (New York Times 17 Aug 2001) http://washingtonpost.com/wp-dyn/articles/A23001-2001Aug16.html

[And a few days later, a report on a way to transfer the download to a normal DVD player:]

HP UNVEILS FIRST DVD+RW DRIVE [20 Aug 2001]

Hewlett-Packard next month will debut the first commercially available DVD drive for PCs that allows users record a movie, watch it on a typical home DVD player, and then erase and record again on the same disc. The DVD-writer dvd100i will carry a price tag of \$599, and PC and electronics makers are hoping the new product will jumpstart holiday sales as consumers seek out the latest gadgetry to complement their home entertainment centers. Dataquest estimates that 2.1 million DVD rewritable drives will ship by the end of next year, and that by 2005, that number will reach 14.3 million drives. In addition to HP's backing, the DVD+RW format has the support of Dell, Sony, Philips Electronics, Mitsubishi, Ricoh, Thomson Multimedia and Yamaha. (ZDNet News 20 Aug 2001) http://news.excite.com/news/zd/010820/07/hp-plays-first

Category 45.6 Other e-commerce security measures

2001-12-17 copy protection incompatibility uncopiable

NewsScan

MORE MUSIC, LESS RIPPING AND BURNING [17 Dec 2001]

To protect itself against people who try to make illegal copies of music, the recording company Universal Music is issuing its newest release ("Fast & Furious: More Music") in a copy-protected form intended to prevent consumers from "ripping" tracks in digital MP3 format. The disk will also be unplayable on Mac computers, DVD players, and game consoles. Hilary Rosen of the Recording Industry Association of America says, "Unfortunately, phenomena like Napster and the ease of 'ripping and burning' are causing artists and record companies real harm... Most movies and video games sold today have some form of protection – musicians are an exception to the case and do not enjoy the same protection. It is not surprising, therefore, that the recording industry is taking steps to get in tune with the rest of the entertainment field." (San Jose Mercury News 17 Dec 2001) http://www.siliconvalley.com/docs/news/svfront/cd121701.htm

46 Cryptography exports from US

Category 46 Cryptography exports from US

2001-01-11 EAR Export Administration Regulations loosening restrictions high technology

supercomputers

NewsScan

FURTHER RELAXATION OF TECHNOLOGY EXPORT REGULATIONS

The Clinton Administration has relaxed restrictions on the export of high-speed commercial computers, and will now add to the list of so-called "Tier 1" countries that U.S. manufacturers can sell computers without obtaining individual export licenses the countries of Central and South America; South Korea and many other Southeast Asia countries; Slovenia; most countries in Africa; and Lithuania. The new guidelines will be reviewed by the Bush Administration after it takes office. (New York Times 11 Jan 2001)

http://partners.nytimes.com/2001/01/11/technology/11EXPO.html

Category 46 Cryptography exports from US

2001-06-08 export administration regulations EAR study

NewsScan

COMPUTER EXPORT CONTROLS? GIVE THEM UP, SAYS REPORT

A new study by the Center for Strategic and International Studies concludes that this country's 1990s-vintage computer export controls are irrelevant to U.S. security and urges that they be discarded. "Computing power is considerably less important for building modern weapons than is the ability to integrate materials, manufacturing equipment and technology... The problem is that the supercomputer of 1990 – a computer then manufactured only in the dozens of units – had by the year 2000 become the laptop manufactured in the hundreds of thousands." (Reuters/San Jose Mercury News 8 Jun 2001)

http://www.siliconvalley.com/docs/news/svfront/001404.htm

Category 46 Cryptography exports from US

2002-01-02 EAR Export Administration Regulations loosening restrictions high technology

supercomputers

NewsScan

BUSH RELAXES COMPUTER EXPORT CONTROLS [2 Jan 2002]

The Bush administration has rolled back restrictions on sales of high-speed computers to Russia, China, India and some countries in the Middle East, more than doubling the allowable processor speed to 195,000 MTOPS (millions of theoretical operations per second). A typical U.S. home PC now sold in retail stores tops out at about 2,100 MTOPS. The change means that those countries will now have access to U.S. computers capable of complex 3D modeling, calculating fluid dynamics, and other advanced applications. The U.S. will maintain its high-tech embargo on exports to North Korea, Iran, Iraq, Libya, Cuba, Sudan and Syria. (Reuters 2 Jan 2002)

http://www1.excite.com/home/technology/tech_article/0,2109,199172|technology_|01-02-2002::19:33|reuters,00.html

49.1 International agreements on security, privacy, Net law

Category 49.1 International agreements on security, privacy, Net law

2001-08-16 international privacy guidelines Web standards audit failure study

NewsScan

U.S. WEB SITES FALL SHORT OF GLOBAL PRIVACY STANDARDS

A survey of 75 U.S. corporate Web sites found that none were in compliance with a set of international privacy guidelines developed by the U.S. and the European Union last year. The guidelines require companies to: notify consumers how their personal data is used; use the information only for its stated purpose; allow consumers to examine and correct data collected about them; give consumers an option to forbid sharing that data for marketing purposes; store the data in a secure manner; and provide recourse for consumers whose privacy has been violated. The survey, conducted by Andersen, found that travel and leisure companies scored the best on notice and security provisions, while financial services firms were most likely to offer adequate choice. U.S. companies must make progress on revamping their Web privacy standards or "Disruption to the conduct of business is a real risk," says Andersen principal Kerry Shackelford. (Reuters 16 Aug 2001)

http://news.excite.com/news/r/010816/11/net-tech-privacy-dc

49.2 EC legislation & regulation

Category 49.2 EC legislation & regulation

2001-04-10 music copyright intellectual property legislation law proposal

NewsScan

EU PROPOSES NEW DIGITAL COPYRIGHT LAWS

Ministers from the 15 European Union member nations adopted a copyright directive yesterday aimed at updating copyright laws for the digital age. Member nations now have 18 months to ratify and implement the new regulations, which, according to the EC, will provide a "secure environment for cross-border trade in copyright protected goods and services, and will facilitate the development of electronic commerce in the field of new and multimedia products and services." Under the proposed law, online swapping of copyrighted music files for free would be outlawed, but consumers would be allowed to make a limited number of copies for private use. The EU directive is comparable to the 1998 U.S. Digital Millennium Copyright Act, but differs in that it does not provide for "fair use" of copyrighted material for the purposes of scholarship and research. In contrast, the EU doctrine includes a laundry list of optional exceptions that allow copying for technical reasons, personal use and archival purposes. Member states may make their own decisions as to which exceptions to adopt. (E-Commerce Times 10 Apr 2001) http://www.ecommercetimes.com/perl/story/8826.html

Category 49.2 EC legislation & regulation

2001-11-30 Internet service providers ISPs logging user traffic data monitoring privacy law

enforcement police investigation evidence

NewsScan

EUROPEANS DEBATE PRIVACY RIGHTS ON THE INTERNET [30 Nov 2001]

Two different institutions, the European Parliament and the Council of Ministries, are in disagreement over a proposed Europe-wide law requiring Internet service providers to extend the length of the time customer "traffic data" be kept available for use in investigations by law enforcement officials. The Council's pro-law-enforcement position has hardened since the terrorist attacks of September 11, but the European Parliament is resisting changes that would make it easier for authorities to gain access to personal data. Erkki Liikanen, the Finnish commissioner who has the job of revising Europe's data-protection laws for the digital age, says: "We must look at the world differently after September 11. We must be careful to ensure that law enforcement officials do have the powers they need, but I believe it is possible to reach a balance between this and citizens' rights to privacy." (New York Times 30 Nov 2001) http://partners.nytimes.com/2001/11/30/technology/30DATA.html

US legislation & regulation 49.3

Category 49.3 US legislation & regulation

HIPAA privacy illness health records solicitation marketing 2001-01-15

NewsScan

LOOPHOLES IN NEW HEALTH RECORD PRIVACY REGULATIONS

The Clinton administration's new federal privacy regulations explicitly allow doctors, hospitals, health services, and their business associates to use patient records for marketing and fundraising. People with a certain disease could receive unsolicited telephone calls touting relevant health products or asking for donations for research to find a cure for that disease. Consumer and privacy advocates are charging that these provisions of the privacy law violate its basic intent, and medical ethicist Thomas Murray says: "Your medical record was meant for your medical care. Now your medical record becomes a marketing tool." But Health and Human Services official Gary Claxton defended the law: "It's the best we could do and we think we did a good job. There's going to be a lot of discussion as this is implemented. If changes need to be made, they should be made." (Washington Post 16 Jan 2001) http://washingtonpost.com/wp-dyn/articles/A63303-2001Jan15.html

Category 49.3 US legislation & regulation

2001-01-24 privacy Web data collection regulation investigation advertising

NewsScan

FTC CLEARS DOUBLECLICK

The Federal Trade Commission has ended its investigation into the data collection practices of Internet advertising firm DoubleClick, concluding that "DoubleClick never used or disclosed" consumers' personal information "for purposes other than those disclosed in its privacy policy." The inquiry was initiated in response to complaints that DoubleClick's \$1.7-billion purchase of direct marketer Abacus would enable it to cross-reference its records of consumers' online habits with Abacus's database including names and other identifying information. DoubleClick eventually scrapped those plans and has now promised the FTC that it will provide consumers an "opt out" option and will clarify its privacy policy. (AP/USAToday 24 Jan 2001)

http://www.usatoday.com/life/cyber/tech/2001-01-23-doubleclick.htm#more

US legislation & regulation Category 49.3

2001-01-24 Web privacy personal information opt out legislation

NewsScan

CONGRESS TACKLES INTERNET PRIVACY LEGISLATION

Two U.S. Representatives -- Chris Cannon (R-Utah) and Anna Eshoo (D-Calif.) -- have introduced legislation that would require Web sites to notify visitors how personal data such as telephone numbers and ZIP codes are used, and allow visitors to "opt out" of that use. "Consumers shouldn't have to reveal their life story every time they surf the Web," said Eshoo. The bill mirrors legislation introduced in the Senate last year by Sen. John McCain (R-Ariz.) and Sen. John Kerry (D-Mass.), and lawmakers agree that Congress will probably pass some type of Internet privacy bill this year. (Reuters/San Jose Mercury News 24 Jan 2001)

http://www0.mercurycenter.com/svtech/news/breaking/internet/docs/792207l.htm

US legislation & regulation Category 49.3

2001-02-12 privacy policy government organization coalition

NewsScan

GROUP ASKS FEDERAL OFFICIALS TO MAKE PRIVACY PLEDGE"

The Privacy Coalition, a group of national organizations that include the liberal ACLU, conservative Eagle Forum, the Electronic Privacy Information Center, the American Library Association, the United Auto Workers union, and nine other member organizations, is asking federal officials to make a "privacy pledge" to set "strong, basic privacy standards" to ensure that companies will inform consumers how their personal data is used, protect that data from hackers, and give them power over that data. (AP/USA Today 12 Feb 2001) http://www.usatoday.com/life/cyber/tech/2001-02-12-privacy-challenge.htm

Category 49.3 US legislation & regulation

2001-03-14 privacy government regulation activists

NewsScan

FTC HEARS FROM PRIVACY GROUPS

In a Federal Trade Commission workshop held yesterday focused on how companies exchange information about their customers, privacy groups told the agency that companies should do a better job explaining how they share such information with other firms and should let consumers decide whether or not they want their names and addresses shared like that. However, House Majority Leader Dick Armey says he's just as worried about how the government itself treats information about its citizens: "If the government is going to monitor the information sharing practices of the private sector, I'd like to know who's going to monitor the government." A number of companies gather information about the purchasing preferences of their customers. (USA Today 14 Mar 2001) http://www.usatoday.com/life/cyber/tech/2001-03-13-privacy.htm

Category 49.3 US legislation & regulation

2001-04-23 privacy laws legislators legislation proposals lawmakers amateurs

NewsScan

PLEA FOR CAUTION WHEN WRITING NEW PRIVACY LAWS [9 Apr 2001]

House Majority Leader Dick Armey (R-Texas) has written a letter to his fellow lawmakers urging them not to let the current prominence of privacy issues stampede them into writing careless laws. "I don't want strangers poking around in my business any more than they want me poking around in theirs," the letter said, but emphasized the need for proceeding cautiously before writing laws for a new and unpredictable technology-based economy: "Congress is an inexperienced and amateur mechanic trying to tinker with the supercharged, high-tech engine of our economy. We need to be careful not to let our good intentions get in the way of common sense." An official of the United States Public Interest Research Group criticized Armey's letter as an attempt to promote an "anti-privacy agenda." (New York Times 9 Apr 2001)

http://www.nytimes.com/2001/04/09/technology/09PRIV.html

WHAT PRICE PRIVACY? [23 Apr 2001]

A new study by the Progressive Policy Institute, a moderate Democrat research group, is warning that any proposed privacy legislation that would significantly restrict Web sites from collecting personal information about their visitors will endanger the viability of sites whose advertising support allows them to disseminate information for free. Progressive Policy Institute president Robert Atkinson says, "If we pass draconian privacy legislation we're going to seriously damage the economics of the Internet." (San Jose Mercury News 23 Apr 2001) http://www.siliconvalley.com/docs/news/svfront/priv042301.htm

Category 49.3 US legislation & regulation

2002-02-19 sex offender public list privacy anonymity constitutionality judicial review lawsuit

NewsScan

ONLINE SEX-OFFENDER LISTS TO BE GIVEN CONSTITUTIONAL SCRUTINY [19 Feb 2002]

The U.S. Supreme Court will decide the question of whether the Constitution allows states to pass legislation enabling the use of Internet registries of convicted sex offenders who have served their time in jail and been released back into society. All states have some version of a sex-offender law, which typically allows publication of a convicted offender's name, address, and other personal information. Such laws are deemed to conform to the Constitution if they are narrowly focused on public safety and not used to extend the punishment of someone beyond what was prescribed by the sentence given to him by the courts, because it is unconstitutional to punish someone twice for the same crime. (AP/USA Today 19 Feb 2002)

http://www.usatoday.com/life/cyber/tech/2002/02/19/scotus-sex-offender-registries.htm

49.5 Law enforcement

Category 49.5 Law enforcement

2001-09-17 wiretap constitution fourth amendment search seizure warrant changes proposals

terrorists

NewsScan

DISCUSSIONS OF PLANS TO CHANGE WIRETAP RULES [17 Sep 2001]

U.S. Attorney General John Ashcroft met with Congressional leaders Sunday to begin a review of possible changes in the laws governing use of wiretapping techniques to fight terrorism. House Minority Leader Richard Gephardt (D-Mo.) called the meeting constructive and Sen. Patrick Leahy (D-Vt.) said he would be open to revising the wiretapping laws to keep pace with technology change. At a press conference, Ashcroft said: "It's easier to investigate someone involved in illegal gambling schemes than it is to investigate someone involved in terrorism. Telephone surveillance has been limited historically to specific telephones, rather than to people." Pointing out that we have entered an era of disposable phones and Internet cafes, Ashcroft added, "it simply doesn't make sense to have the surveillance authority associated with the hardware or with the phone instead of with the person or the terrorist." Privacy advocates are urging lawmakers to proceed with caution. (San Jose Mercury News 17 Sep 2001) http://www.siliconvalley.com/docs/hottopics/attack/005143.htm

Category 49.5 Law enforcement

2001-09-24 biometric face recognition identification authentication terrorism airports

scanning privacy surveillance

NewsScan

FACE-RECOGNITION SYSTEM RECOMMENDED FOR AIRPORT SECURITY [24 Sep 2001]

A government committee appointed to review airport security procedures will recommend to Transportation Secretary Norman Y. Mineta the employment of face-recognition systems that create a digital map of a person's face and translate it into mathematical formulas claimed to be as uniquely distinguishing as a fingerprint. Privacy advocates like David Sobel regard this as a "potentially invasive technology" whose use will eventually expand to other purposes and endanger the civil liberties of ordinary people. The president of FaceIt Systems, one of the best-known manufacturers of face-recognition systems, says he shares privacy concerns and asserts that the answer is to have rules governing whose photos can be included in a database of suspects or criminals for comparison with mere passers-by. (Washington Post 24 Sep 2001)

http://www.washingtonpost.com/wp-dyn/articles/A14273-2001Sep23.html

Category 49.5 Law enforcement

2002-02-13 surveillance cameras law enforcement police crime prevention anonymity public

expectation privacy

NewsScan

WASHINGTON POLICE EXPAND USE OF SURVEILLANCE TECHNOLOGY [13 Feb 2002]

Noting that people in the United Kingdom have "easily adapted" to pervasive public surveillance and that "there has not been an outcry about privacy there," Washington, D.C. police officials are busy expanding the public use of surveillance cameras. A police department spokesman says, "In the context of September 11, we have no choice but to accept the greater use of this technology." MIT emeritus sociology professor Gary T. Marx concedes that "almost all of the surveillance innovations are easily justifiable" but worries that "the major concern is: where is it leading?" (Wall Street Journal 13 Feb 2002)

http://online.wsj.com/ (sub req'd)

49.6 Surveillance & anonymity

Category 49.6 Surveillance & anonymity

2001-07-12 surveillance biometric face recognition privacy public anonymity

NewsScan

ACLU UPSET ABOUT HIGH-TECH SURVEILLANCE AT SUPER BOWL [2 Feb 2001]

The American Civil Liberties Union has written to Tampa, Florida's mayor protesting the surveillance procedures used by Tampa's police department at last week's Super Bowl football game. In attempt to identify any well-known criminals or terrorists in the stadium, the police set up hidden video cameras that took pictures of thousands of fans and transmitted the images to computers at a central command post for comparison with file photographs. In the letter, ACLU executive Howard Simon wrote: "The ACLU believes this activity raises serious concerns about the Fourth Amendment right of all citizens to be free of unreasonable searches and seizures," Simon wrote to Tampa Mayor Dick Greco. "Aside from the constitutional issues raised by the developing use of surveillance technology, we believe the public should be given an opportunity to ask -- and have answered -- the many questions raised by this practice." (USA Today 2 Feb 2001)

http://www.usatoday.com/life/cyber/tech/2001-02-02-super-bowl-surveillance.htm

CONSERVATIVE AND LIBERAL AGREEMENT: NO HIGH-TECH SURVEILLANCE [12 Jul 2001]

Dick Armey, the conservative House Majority Leader, and the left-leaning American Civil Liberties Union (ACLU) have issued a joint statement deploring the growing use by law enforcement agencies of high-tech surveillance tools to monitor ordinary people in public places. Recent news stories have revealed attempts in Tampa and Virginia Beach to use face-recognition software to identify passers-by on city streets. An Armey spokesman calls that trend disturbing, and says that "the American public doesn't want Big Brother looking over its shoulder." (Newsbytes/USA Today 12 Jul 2001)

FACE-OFF: SURVEILLANCE SYSTEMS VS. PRIVACY ADVOCATES [1 Aug 2001]

U.S. federal agencies have committed millions of dollars to the improvement of facial-identification systems that lets cameras scan faces in a crowd and automatically compare them to stored images. An example of this technology is the FaceIt system (developed by Visionics), which has been used in Israel to manage the flow of individuals entering and exiting the Gaza strip and in Tampa, Florida to taking photos of individuals walking in an entertainment district and matching the photos with digital mug shots of known criminals. The Visionics system and systems developed by its competitors have been funded by such agencies as DARPA, NSA, and the U.S. Justice Department. George Washington University law professor Jeffrey Rosen, a privacy advocate who is critical of these developments, warns: "America now faces a choice about how far we want to go down the road to being a surveillance society." (San Jose Mercury News 1 Aug 2001)

http://www.siliconvalley.com/docs/news/svfront/016044.htm

Category 49.6 Surveillance & anonymity

2001-09-23 national identification systems ID card terrorism surveillance

NewsScan

ELLISON PROPOSES NATIONAL IDENTIFICATION SYSTEM [23 Sep 2001]

Oracle chief executive Larry Ellison says that America needs to create a national identification card system, and is offering to donate Oracle's database software to make such a system possible: "We need a national ID card with our photograph and thumbprint digitized and embedded in the ID card. We need a database behind that, so when you're walking into an airport and you say that you are Larry Ellison, you take that card and put it in a reader and you put your thumb down and that system confirms that this is Larry Ellison." Asked about privacy concerns, he responded: "Well, this privacy you're concerned about is largely an illusion. All you have to give up is your illusions, not any of your privacy. Right now, you can go onto the Internet and get a credit report about your neighbor and find out where your neighbor works, how much they earn and if they had a late mortgage payment and tons of other information.'' Ellison argues that shoppers now have to disclose more information to make a purchase at a shopping mail than they do to get on an airplane, and poses the following question: "Let me ask you. There are two different airlines. Airline A says before you board that airplane you prove you are who you say you are. Airline B, no problem. Anyone who wants the price of a ticket, they can go on that airline. Which airplane do you get on?" (San Jose Mercury News 23 Sep 2001)

http://www.siliconvalley.com/docs/news/svfront/ellsn092301.htm

Category 49.6 Surveillance & anonymity

2001-12-19 identification paper tracing audit trail stamps fibers forgery impersonation

privacy anonymity

NewsScan

'SMART' TECHNOLOGY EYED FOR POSTAL SECURITY [19 Dec 2001]

Rep. Henry Waxman (D-Calif.) has proposed a "smart" suggestion for improving the security of the U.S. Postal Service. He's pushing a two-dimensional barcode "stamp" that would contain the sender's ID as well as the date, time and place the postage was paid. Meanwhile, Maynard H. Benjamin, president of the Envelope Manufacturers Association, has suggested that the agency consider "fiber fingerprinting," which identifies correspondence by the unique characteristics possessed by each piece of paper. Privacy experts say that traceable mail would stifle whistle-blowers and government critics, and that the security measures might not be effective anyway. "You'll have the same fraudulent problems that you have with IDs and credit cards now," says Lauren Weinstein, moderator of the Privacy Forum. "The bottom line is that the bad guys are going to find a way around it. What if they steal your stamps, and you get framed for something you didn't send?" (Wired 19 Dec 2001) http://www.wired.com/news/conflict/0,2100,49186,00.html

4A2 Pointing, linking, metatext

Category 4A2 Pointing, linking, metatext

2001-01-12 trespass linking bots spiders Web lawsuit jurisprudence precedent

NewsScan

WHAT DOES "TRESPASS" MEAN IN CYBERSPACE?

Recent court cases have used the ancient law of "trespass" to rule against companies that used software robots to search the public Web sites of other companies to capture sales leads for mass marketing purposes. However, the original idea of trespass is that trespasser causes some kind of harm (such as crashing the site being trespassed upon). But what if there is no harm - crash or traffic gridlock or anything else? The recent decisions do not seem to require that a plaintiff allege real harm, and some legal observers are concerned that the decisions will have bad unintended consequences. Dan L. Burk, a University of Minnesota law professor, warns: "If I don't like your linking to my site, or searching my site, even though it is open to the public, and I say, 'Stop,' you have to stop... whether you are actually hurting me or not." (New York Times 12 Jan 2001)

http://partners.nytimes.com/2001/01/12/technology/12CYBERLAW.html

Category 4A2 Pointing, linking, metatext

2001-01-18 linking URL advertising intellectual property law jurisprudence

NewsScan

'DEEP LINKING' COMES UNDER FIRE

StepStone, a UK online recruitment company, has obtained an injunction in Germany preventing Danish rival OFiR – a media firm that owns online recruitment portals in the UK, Germany, Denmark and France – from linking to StepStone Web pages. The move is one of the few cases to test the law on "deep linking" – links between sites that bypass home pages and therefore miss the advertising on them. "It is not, of course, every case of hypertext linking which is unlawful – the Internet would grind to a halt," said Adrian Lifely, an attorney for Osborne Clark, the law firm advising StepStone. "But the courts in Europe do have power to intervene where linking is extensive and prejudicial to the site involved." The law firm said OFiR was using the link to StepStone's database to boost the number of job offerings it claimed to provide. The ruling in favor of the injunction was based on new European laws regulations on database and copyright protection, said Lifely. (Financial Times 18 Jan 2001) http://news.ft.com/news/industries/internet&e-commerce

Category 4A2 Pointing, linking, metatext

2001-06-29 copyright intellectual property Web search engines metatext

NewsScan

LAWSUIT OVER INVISIBLE REPRODUCTION OF COPYRIGHTED MATERIAL [29 Jun 2001]

The Belgian company Euregio.net is suing the astrology site EasyScopes owned by Women.com (recently acquired by iVillage) for copyright infringement, even though the disputed material was not placed on the EasyScopes to be read (it was in white letters on a white background, and therefore essentially undecipherable). Euregio says the misappropriated material was used by EasyScopes to trick Internet search engines and "try to get the people who would normally be interested in the information on our site, to try to get them on their site." (New York Times 29 Jun 2001)

http://partners.nytimes.com/2001/06/29/technology/29CYBERLAW.html

4A3 Jurisdiction

Category 4A3

Iurisdiction

2001-01-11

taxation Web jurisdiction international agreement OECD

NewsScan

OECD REACHES CONSENSUS ON WEB TAXES

The Organization for Economic Cooperation and Development, which represents 30 leading industrialized nations, says its members have reached a landmark agreement that defines how countries should tax business conducted over the Internet. Tax experts say the deal marks an important milestone, but that wealthy nations need to hold further talks to develop a comprehensive approach to e-commerce taxation. The OECD's committee on fiscal affairs ruled that doing business through a Web site would not leave a company liable to taxation in the country from which the Web site had been accessed. The exemption from liability applies even if the company's Web site is hosted by a third party, such as an ISP. But the committee ruled that a company should generally pay tax in countries hosting servers through which the business was conducted. A company would be liable for paying tax if the server were performing functions that formed a core part of the business activity, such as downloading software. Jacques Sasseville, head of the OECD's tax treaty unit, said the consensus marked an interim solution and that more clarification would be necessary. (Financial Times 11 Jan 2000)

http://news.ft.com/news/industries/internet&e-commerce

Category 4A3

Iurisdiction

2001-06-27

international jurisdiction Web content national law regulations international agreement

NewsScan

EUROPEAN E-COMMERCE: WHOSE LAW IS IT ANYWAY? [27 Jun 2001]

The European Commission is rethinking a policy that currently applies the law of the country in which the consumer resides to trans-border e-commerce disputes. The reason for the reconsideration is that publishers and others have been complaining that it is impossible to do business internationally if a single country can force its rules on the whole world. Case in point: the dispute between a French court and the U.S. portal Yahoo.com, where the court is insisting that Yahoo must abide by French laws that prohibit displays or sales of Nazi memorabilia on Web sites. If the French prevail, they will have made their laws apply to citizens of all other countries that have no such laws. (New York Times 27 Jun 2001) http://partners.nytimes.com/2001/06/27/technology/27CROS.html

Category 4A3 Jurisdiction

2001-09-03 cy

cybersquatting DNS domain name system trademark extortion international regulation agreement policy proposal intellectual property

NewsScan

U.N. WANTS STRONGER PROTECTIONS AGAINST CYBERSQUATTING

The World Intellectual Property Organization (WIPO), an agency of the United Nations, wants to protect high-profile individuals and organizations from having their names misappropriated by "cybersquatters" who register domain names of well-known people or companies without their permission. Recent examples have included celebrities such as Julia Roberts and Mick Jagger and soccer clubs like Real Madrid. A WIPO official said: "There is evidence of widespread registration of Internet domains by people who have no connection whatsoever with the names they give their sites. We are recommending that governments look at how the legal basis for dealing with this can be extended." (Reuters/New York Times 3 Sep 2001)

http://partners.nytimes.com/reuters/technology/tech-tech-internet.html

Category 4A3 Jurisdiction

2002-02-27 hate speech auction censorship filtering court ruling judgement appeal

international conflict jurisdiction

NewsScan

NAZI MEMORABILIA CASE GETS SECOND LOOK IN U.S. COURTS [11 Feb 2002]

About a year ago a French court decided that Yahoo had violated French law by allowing French citizens to view auction sites displaying Nazi memorabilia and ruled that Yahoo pay \$13,000 a day in fines; however, in the U.S. (where the auction sites are located), a federal judge ruled that the French judgment can not be enforced in this country. That ruling is now being appealed by the two original plaintiff groups, The International League Against Racism and Anti-Semitism and the Union of French Jewish students. Alan Davidson, an attorney for the Washington, D.C.-based Internet civil liberties group Center for Democracy and Technology, warns that the French ruling "really puts free expression and communication in jeopardy on the Net," by reducing online speech to the lowest-common denominator of what is permissible as dictated by the most repressive nations. Taking a contrary point of view, University of Chicago law school professor Jack Goldsmith says that countries have the right to choose for themselves what is lawful within their own borders: "That is the essence of territorial sovereignty." (New York Times 11 Feb 2002)

http://partners.nytimes.com/2002/02/11/technology/11NECO.html?pagewanted=print

YAHOO FACES CRIMINAL CHARGES IN FRANCE[27 Feb 2002]

A French criminal court says it plans to prosecute Yahoo and its former president Timothy Koogle for allegedly condoning war crimes by selling Nazi memorabilia. Koogle faces a maximum sentence of five years and an approximately \$40,000 fine if found guilty – a verdict that could have profound implications for free speech on the Net. France had ordered Yahoo in November 2000 to block French citizens from access the sites, but a U.S. federal judge ruled last fall that Yahoo, as a U.S.-based site, was not bound by French laws governing content. (Financial Times 27 Feb 2002)

http://news.ft.com/news/industries/internet&e-commerce

4A4 Blocking

Category 4A4 Blocking

2001-12-12 e-mail property rights free speech criticism lawsuit ruling court judgement

NewsScan

FLOODING A COMPANY'S MAIL SYSTEM: FREE SPEECH ISSUE OR PROPERTY ISSUE? [12 Dec 2001] An appellate court in California has ruled that an ex-Intel employee had no right to send e-mail messages criticizing the company to 30,000 Intel employees. The ex-employee argued that the company's e-mail system is entitled to the First Amendment protections of a public forum; a divided court disagreed, with the majority saying that "Intel is as much entitled to control its e-mail system as it is to guard its factories and hallways." An appeal is expected. (San Jose Mercury News 12 Dec 2001)

http://www.siliconvalley.com/docs/news/svfront/email121201.htm

Archives 4A5

Category 4A5 Archives

2001-05-07 copyright intellectual property privacy archives USENET persistence

NewsScan

NET CONVERSATION: OPEN, CASUAL... AND ETERNAL

Privacy advocates haven't been expressing much concern about the creation by the Internet search Google of its "archive of human conversation," which allows the searching of archived postings of the Usenet bulletin boards (http://groups.google.com). Devorah Pierce, a lawyer for the Electronic Frontier Foundation, a noted advocacy group for privacy on the Internet, says that contributors to Usenet discussions shouldn't expect too much privacy because "if that's not a public forum I don't know what is." But she and others worry that people don't expect their casual conversations to follow them forever. Another privacy advocate, Bruce Koball, says: "People can be rightfully mortified when the come back five years from now and see a post that they made. And now it's enshrined in magnetic media for time immemorial." (New York Times 7 May 2001)

http://www.nytimes.com/2001/05/07/technology/07NECO.html

Category 4A5 Archives

2001-08-15 copyright intellectual property archive Web broadcast permission

NewsScan

THIRD-PARTY ARCHIVING COMES UNDER FIRE [15 Aug 2001]

Public companies have embraced Internet technology to offer investors access to live webcasts of once-private meetings, where company officials discuss quarterly results and business outlooks. But in some cases, creating a historical record can become a headache when that record is archived on other companies' Web sites. In one of the highest-profile disputes, R.J. Reynolds has demanded that financial news provider Bloomberg stop archiving the tobacco firm's conference calls, saying that the information exchanged in those calls belongs to the company. Bloomberg has responded that it's not violating any copyright restrictions because it records the calls itself, rather than using recordings produced by another company. Reynolds' policy is to make each call available on its Web site for just seven days, saying that investors could be confused if information exchanged in the call is taken out of context, but Bloomberg has refused to take the calls off its own site, saying it is valuable for shareholders to be able to go back and listen to officials' reasoning for making a business decision. One copyright expert says it would be difficult for a company to sue for unauthorized use of a conference call unless it is registered with the copyright office, especially when the call includes outside analysts as interviewers. Bloomberg records and archives between 500 and 1,000 conference calls each quarter, and customers pay \$1,285 a month for the company's flagship Bloomberg Professional service. (Wall Street Journal 15 Aug 2001)

http://interactive.wsj.com/archive/retrieve.cgi?id=SB997196102924013249.djm

Category 4A5 Archives

2001-11-28 Web sensitive data archiving duplication control copyright intellectual property

distribution removal impossible change

RISKS 21 80

David Colker of the Los Angeles Times wrote, "Government agencies have tried to remove sensitive information, only to discover that copies have proliferated and they're virtually impossible to eradicate. Within days of the 11 Sep attacks, the federal Agency for Toxic Substances and Disease Registry rushed to pull a suddenly sensitive report from its Web site titled "Industrial Chemicals and Terrorism." The agency eliminated all traces of the document and its description of sources for home-brew nerve gases and improvised explosives. But on the World Wide Web, almost nothing truly dies. . . . "

http://www.latimes.com/news/printedition/la-000094419nov27.story

Category 4A5 Archives

2001-12-20 Web copyright intellectual property archives long-term retention

NewsScan

LONG-TERM RETENTION OF DIGITAL RESEARCH MATERIALS [5 Sep 2001]

RLG has released the second report developed in collaboration with OCLC Online Computer Library Center to advance long-term retention of digital research materials. In a joint announcement of the report, RLG president James Michalko said he hopes the study will spark a debate that ultimately will result in "some small number of trusted, reliable service providers, whether they are research institutions themselves or third parties." OCLC president and chief executive officer Jay Gordon explained that OCLC's digital archiving initiatives "are guided by active participation in this working group and other key projects." The paper is freely available as a PDF document from the RLG web site at www.rlg.org/longterm/attributes01.pdf and is linked to from www.oclc.org/digitalpreservation and www.oclc.org/presres.

PRIVACY, SECRECY AND RESPONSIBILITY [20 Dec 2001]

[Another in a series]. . . of two reports collaboratively prepared by RLG and OCLC Online Computer Library Center to advance long-term retention of research materials held in digital form is now available from RLG and OCLC. Dialogue on the standards, criteria, and mechanisms for certifying digital information repositories will encourage an international consensus. "Ultimately," says RLG president James Michalko, "I'd like to see the debate result in some small number of trusted, reliable service providers, whether they are research institutions themselves or third parties." (RLG News Issue 53)

http://www.rlg.org/longterm/attributes01.pdf

Category 4A5 Archives

2002-01-22 Internet Web archives legal implications lawsuit trial judgement ruling

RISKS 21 88

Roger Needham wrote in RISKS that a judge thinks that archiving news stories may violate the integrity of a criminal prosecution. "It is a principle in many jurisdictions that a jury should not know about prior charges or convictions of the accused. In a Scottish court a man was accused of a particularly revolting crime, he having been acquitted of a similar offence on a technicality a number of years ago. The judge ruled that the editor of a newspaper was in contempt of court by leaving reports of the earlier trial on line in his archive, because he had made it too easy for jurors to find out what they were not meant to know. The judge apparently believed that the greater ease of access of the on line archive as compared to a paper archive was a difference not of degree but of kind."

Category 4A5 Archives

2002-03-04 archive data loss compatibilitie media retention archives readability accessibility

expiration degradation

RISKS 21 91

Chris Leeson summarized another case of technological obsolescence and data loss in archives: "The BBC's 1986 Domesday Project (a time capsule containing sound, images, video and data defining life in Britain) is now unreadable. The data was stored on 12-inch video discs that were only readable by the BBC Micro, of which only a handful still exist. The time capsule contains "250,000 place names, 25,000 maps, 50,000 pictures, 3,000 data sets and 60 minutes of moving pictures.". The article notes that the original Domesday Book (compiled in 1086 for tax purposes) is still in "mint condition."

4A6 Libel

Category 4A6 Libel

2001-08-09 libel Internet republishing culpability liability ISP news group

NewsScan

LIBEL IN CYBERSPACE [9 Aug 2001]

A trial court judge in California has interpreted federal law to mean that a person who re-posts libelous information on the Internet is protected against libel suits. The ruling stands a dramatic contrast to traditional libel law, which holds that someone who carelessly or recklessly circulates a defamation may be just as guilty as the originator of the libel. The judge in this case gave a broad interpretation to a federal law passed to protect Internet service providers and news group operators from being held responsible for postings made by third-party individuals. The plaintiffs, who will appeal the judge's decision, charge that "what this ruling does is open the door for any number of wrongdoers to just basically take something that's libelous, republish it and claim immunity." (New York Times 9 Aug 2001) http://partners.nytimes.com/2001/08/09/technology/10CYBERLAW.html

Category 4A6 Libel

2001-12-11 online journalists print libel protection lawsuit court ruling judgement

NewsScan

ONLINE JOURNALISTS HAVE SAME PROTECTIONS AS PRINT [11 Dec 2001]

Online journalists enjoy the same free-press protections against libel charges as those accorded to print, radio and TV reporters, according to a recent ruling in the New York State Supreme Court. The case, National Bank of Mexico v. Narconews.com, was initiated when the Bank of Mexico -- now part of Citigroup -- sued the drug-war investigative reporting Web site, charging that reports linking the Bank's then-president with narcotics trafficking were false and libelous. A 1964 U.S. Supreme Court decision -- New York Times v. Sullivan -- had established that defamation cases brought against journalists must meet a "higher standard," and that journalists can only be found guilty of libel if their actions are deemed malicious. "This court finds that Narconews is a media defendant and is entitled to a heightened protection under the First Amendment," wrote New York Supreme Court Justice Paula Omansky, citing the NYT v. Sullivan precedent. Al Giordano, editor and publisher of Narconews, said the decision should encourage online journalists to take on more hard-hitting news assignments. "The case law that comes out of Judge Omansky's decision is a miracle for online news sites like my own and online journalists like myself. It establishes that an online news provider now has the same rights as The New York Times or any other newspaper or magazine in the eyes of the law." (Wired.com 11 Dec 2001)

http://www.wired.com/news/politics/0,1283,48996,00.html

4B1 Copyright

Category 4B1 Copyright

2001-02-05 intellectual property rights copyright copying duplication private use Europe

regulation

NewsScan

EUROPEAN PARLIAMENT OKAYS PRIVATE COPYING OF DIGITAL WORKS

The European Parliament has issued a preliminary decision to extend, with some limitations, the private copying permissible in the analog world to digital media. New-media companies, consumer-electronics makers and citizens' rights groups applauded the decision to reject all but 16 of a record 197 proposed amendments to the EU's Copyright Directive, which faces a full vote next week. Among the amendments approved was a provision allowing copyright owners to employ technical protection measures, such as encryption, to prevent their works from being pirated. Copies could, however, be made "by a natural person for private use and for ends that are neither directly nor indirectly commercial." Fair practice lobbyists said the final version represented a reasonable compromise: "Everybody gained something and everybody lost something," said the head of the European Digital Media Association. The music industry, however, was more critical of the decision: "Private copying really has to be fore the private circle," said the European regional director of the Federation of Phonographic Industries. (Wall Street Journal 6 Feb 2001) http://interactive.wsj.com/articles/SB981401558502841316.htm [subscription req'd]

Category 4B1 Copyright

2001-02-15 intellectual property music legislation peer-to-peer networking privacy

NewsScan

EUROPEAN PARLIAMENT BLOCKS SONG SWAPS

The European Parliament has okayed rules that will block companies such as Napster from operating in the 15-member bloc without authorization from recording artists. Wednesday's ruling compromised between extreme measures suggested by both sides on the issue, and seeks to ease record companies' concerns over piracy while at the same time allowing individuals to continue making a limited number of copies for personal use. Publishers and music and film producers will, for the first time, be allowed to use "technical protection measures," including encryption, to prevent unauthorized copying. Enrico Boselli, who guided the legislation through the parliament, noted that the Copyright Directive was badly needed "to set clear rules for consumers, consumer-electronics manufacturers, Internet service providers and others. Copyright owners now have wider protection here than in the U.S." (Wall Street Journal 15 Feb 2001)

http://interactive.wsj.com/articles/SB982159222697782071.htm

Category 4B1 Copyright

2001-03-02 copyright intellectual property law lawmakers amateurs

NewsScan

E-MAIL SHARING BANNED BY LAW IN AUSTRALIA

Forwarding e-mail to friends, family or colleagues without permission from the sender is now illegal in Australia, thanks to a new law that took effect yesterday. Penalties for violation could be as much as five years' jail time or fines of AU\$60,000 (US\$31,400). The motivation behind the law is copyright protection for the sender of the original e-mail. But in addition to material that already has copyright protection, such as excerpts from books or song lyrics, the new measure also affects personal messages. "It's quite possible that the forwarding of an e-mail could be a technical infringement of copyright," says a legal advisor for Australia's attorney general. "E-mailing something is a 'communication' under the Digital Agenda Act and so is putting something up on a Web site." This new interpretation means a simple e-mail about office gossip or holiday plans also carries personal copyright protection. It is estimated that 5 million or more e-mail messages are forwarded around Australia every day. (The Sunday Telegraph 4 Mar 2001)

http://www.news.com.au/common/story_page/0,4057,1768268%5E421,00.html

Category 4B1 Copyright

2001-06-28 copyright intellectual property CD-RW fees

NewsScan

GERMAN COURT IMPOSES FEES ON HP TO COMPENSATE MUSICIANS

Upholding a law passed by Germany's copyright society (GEMA) that targets manufacturers of equipment used to violate piracy laws, a court in that country is assessing fees on CD burners sold by Hewlett-Packard to compensate musicians whose copyrighted works are being downloaded from the Internet without their permission. HP plans to appeal and says that the best way to oppose piracy is not by inflating the price of equipment but by offering individual licensing and user fees. (AP/Washington Post 28 Jun 2001)

http://washingtonpost.com/wp-dyn/articles/A56397-2001Jun28.html

Category 4B1 Copyright

2001-07-12 copyright intellectual property moral rights authors distributors lawsuit

NewsScan

COPYRIGHT BATTLE ERUPTS OVER E-BOOKS [6 May 2001]

Bertelsmann's Random House and startup Rosetta Books will square off this week in a court battle that could have as much influence on the future of publishing as Napster had on the music industry. Random House is pursuing its claim that authors who sign over the rights to publish their works in "book form" before the existence of the Internet also granted the rights for e-publications. Rosetta Books had contracted directly with a group of authors, including William Styron and Kurt Vonnegut, for the electronic publishing rights to some of their Random House titles, which it says are not included in the print contracts. E-books are poised to become the third branch of online copyright disputes, which are already causing upheaval in the music and film industries. The music industry has pressured Napster to add filters to its popular file-sharing service, and the film industry last week announced plans to go after Gnutella users who traffic in pirated movies. (CNet News.com 6 May 2001) http://news.cnet.com/news/0-1005-200-5826755.html?tag=lh

WHEN IS A BOOK NOT A BOOK? WHEN IT'S AN E-BOOK! [12 Jul 2001]

Federal District Judge Sidney H. Stein has ruled that the term "book" in a book contract does not automatically include the right to offer digital versions of that same book. Judge Stein therefore denied a request by Random House to enjoin RosettaBooks from publishing new digital editions of such Random House authors as Robert B. Parker, Kurt Vonnegut, and William Styron. The case will now go to full trial, although the judge said that "Random House is not likely to succeed on the merits of its copyright infringement claim." [(NY Times, 12 Jul 2001)] http://partners.nytimes.com/2001/07/12/technology/ebusiness/12BOOK.html

Category 4B1 Copyright

2001-08-02 intellectual property moral rights actors streaming radio rebroadcast

NewsScan

RADIO STATIONS HALT STREAMING OVER ACTOR DISPUTE [21 Apr 2001]

Hundreds of commercial radio stations have put a stop to Internet broadcasts, prompted by a dispute with the actors on commercials who want to be paid extra to have their voices streamed online. The American Federation of Television and Radio Artists (AFTRA) says the stations have known for months that they were responsible for paying the actors, and are shutting down to avoid paying record labels and artists, who also want extra payments for streamed broadcasts. Four of the largest U.S. commercial radio companies -- Clear Channel, Citadel Broadcasting, Emmis Communications and Jefferson Pilot Communications -- ended their real-time audio feeds last week. "We are working hard to resolve outstanding issues with all concerned parties," says Clear Channel CEO Kevin Mayer. "It is our intention to put the streams back up when it makes legal and financial sense." Mayer says his company is looking into technology that could strip the commercials out of the streams. (AP 21 Apr 2001) http://news.excite.com/news/ap/010421/18/internet-radio

COURT BACKS ONLINE RADIO RULING [2 Aug 2001]

The broadcasting industry suffered a setback Wednesday when a U.S. district judge threw out a challenge to the U.S. Copyright Office, which ruled last year that radio stations must pay additional royalties to stream music over the Internet. The National Association of Broadcasters responded that the ruling would upset a long-standing, mutually beneficial relationship between the broadcasting and recording industries. "Broadcasters currently pay in excess of \$300 million annually in music licensing fees to compensate songwriters and music publishers. Any additional fee to compensate record companies would be unfair and unreasonable," said NAB president and CEO Edward O. Fritts. The ruling was hailed as a victory by the Recording Industry Association of America. "Any licensing fees that these companies would be paying would pale in comparison... to the cost to stream their signal over the Internet," said RIAA senior VP Steven M. Marks. (AP 2 Aug 2001) http://news.excite.com/news/ap/010802/22/online-radio

Category 4B1 Copyright

2001-08-30 music royalties copyright intellectual property distribution proposal legislation

NewsScan

US REGULATORS FOCUS ON ONLINE MUSIC COPYRIGHT LAW [30 Aug 2001]

Questions on copyright laws for online music have been raised by Web companies, which contend that vague rules have enabled music publishers to seek multiple royalty payments that could stymie their fledgling industry. Currently, music publishers get paid in two ways: once when songs are performed and once when they are recorded. Some publishers have argued that they should be paid in both ways whenever Web users choose to hear a song online. The U.S. Copyright Office has therefore asked Congress to pass legislation that stipulates payment rules. The Copyright Office says online music services shouldn't have to pay royalties on "buffer" copies of songs that enable smoother audio streaming, and contends that when Web companies sell music downloads, they shouldn't have to pay a performance fee. The Digital Media Association characterized the Copyright Office's stand as a "home run," but music publishers were concerned that the recommended rules "may not adequately protect creators or copyright owners." (Wall Street Journal 30 Aug 2001)

http://interactive.wsj.com/articles/SB999125016154381702.htm (sub req'd)

Category 4B1 Copyright

2001-12-07 international intellectual property WIPO law treaty agreement moral rights

related residual copyright protection

NewsScan

WORLD COPYRIGHT LAW TO PROTECT DIGITAL WORKS [7 Dec 2001]

A World Intellectual Property Organization treaty protecting copyrighted digital works will go into effect in March, and a second WIPO treaty will protect the so-called "related rights" of performers, producers and broadcasters whose work is transmitted on the Internet. WIPO director-general Kamal Idris says the treaties "will let composers, artists, writer and others to use the Internet with confidence to create, distribute and control the use of their works within the digital environment." (AP/Washington Post 7 Dec 2001)

http://www.washingtonpost.com/wp-dyn/articles/A8037-2001Dec7.html

Category 4B1 Copyright

2001-12-17 copyright intellectual property journalists freelance writers Web CD-ROM Web

republication derivative works moral rights residuals database CD-ROM Web

publishing Webcast lawsuits court rulings judgements agreements

NewsScan

ONLINE USE OF FREELANCE WORK TO BE DECIDED BY COURT [28 Mar 2001]

The U.S. Supreme Court is hearing a case about whether freelance authors are entitled to receive additional compensation when their articles are incorporated into electronic databases and commercial CD ROMs. On the side of the writers: organizations such as the American Library Association and the Association of Research Libraries. On the publisher side: the New York Times, Newsday, Time, AOL Time Warner, the Washington Post, Gannett, Lexis/Nexis, and UMI. The central issue is whether a published article entered into an archival database is a mere "revision" of the original work (in which case the publisher wins, since it has already paid for the work once), or whether the article must be considered an entirely new product (in which case the author wins). The writers argue that the search capabilities of databases give publications completely new and separate lives, for which the authors should get completely separate compensation. (Washington Post 28 Mar 2001) http://washingtonpost.com/wp-dyn/articles/A1815-2001Mar27.html

FREELANCE WRITERS VS. PUBLISHERS [28 Mar 2001]

The U.S. Supreme Court heard oral arguments yesterday in a case that will decide what rights freelance writers have when their work is incorporated into electronic databases. Representing the publishers, Laurence H. Tribe insisted that an article is not made into something new just by being incorporated into a database, it is a mere "revision" of the original article that the publisher has already paid for and shouldn't have to pay for again. Representing the freelance writers, Laurence Gold argued that when publishers put articles into the "undifferentiated mass" of an electronic database they "are creating a quite different work." (New York Times 29 Mar 2001) http://partners.nytimes.com/2001/03/29/technology/29WRIT.html

COURT SIDES WITH WRITERS OVER COPYRIGHT DISPUTE [26 Jun 2001]

In a blow to big media firms, the U.S. Supreme Court ruled Monday that freelance writers may control whether articles they write for print publication can then be reproduced in electronic form. Large publishers have argued that if they have to renegotiate over electronic publication rights, they probably will remove a substantial amount of material from their electronic databases. "Historians, scholars and the public lose because of the holes in history created by the removal of these articles from electronic issues of newspapers such as the Times," said New York Times chairman Arthur Sulzberger Jr. The ruling will affect primarily content written before the mid 1990s, which most publishers updated their contracts to include electronic as well as print publishing rights. The National Writers Union, however, estimates a range of potential liabilities between \$2.5 billion and \$600 billion. The decision in this case could have broad ramifications in similar disputes in the book and music publishing businesses. (Wall Street Journal 26 Jun 2001)

http://interactive.wsj.com/archive/retrieve.cgi?id=SB993473705172238884.djm (sub req'd)

LIBRARIANS LEFT TO CLEAN UP ELECTRONIC DATABASES [29 Jun 2001]

In the wake of the recent Supreme Court ruling over freelancers' right to control distribution of electronic versions of their work (Tasini et al. vs. the New York Times et al.), publishers are deleting tens of thousands of freelance articles spanning decades. And who gets stuck with the job? "The librarians, of course," says Tim Rozgonyi, assistant technology systems editor for the Pittsburgh Post-Gazette. "The librarians will save the publishers' bacon by cleaning up the data... [The] Tasini [decision] is the closest thing to a lifetime employment guarantee for news librarians that you will ever see." Meanwhile, some newspapers are turning back to microfilm, which is exempt from the ruling, to digitize a complete archive of their collections. But microfilm could prove another source of legal contention in the future. "The royalty potential [of digitizing over 100 years of microfilm] is massive," says Tampa Tribune archive and research manager Jody Habayeb. Some archivists have suggested that publishers could post citations only, rather than the full text of articles that don't comply with the Tasini ruling, but others argue that most users don't want to have to go through a third party to find an article online. "I hate to see it go that way, but it's an option," says Habayeb. "The beauty of the Internet is the immediacy of it." (Wired.com 29 Jun 2001) http://www.wired.com/news/culture/0,1284,44905,00.html

NY TIMES "SOLUTION" NOT WHAT FREELANCE WRITERS HAD IN MIND [6 Jul 2001]

A Pyrrhic victory for freelance writers? Maybe. After the U.S. Supreme Court ruled last week that the New York Times (and two other publishers) had violated the rights of freelancers by not paying them new compensation for old material made accessible in electronic databases, the Times decided simply to remove the disputed material entirely. Characterizing the newspaper's action as a "complete violation of the spirit of the Supreme Court decision," the writers are insisting that "there is no need to delete articles" and are filing a new lawsuit. They say they want their works to

remain in the databases, and merely want to be receive what they consider appropriate compensation. (New York Times 6 Jul 2001)

http://partners.nytimes.com/2001/07/06/technology/06WRIT.html

JOURNALISTS WIN ANOTHER CONTEST OVER DIGITAL RIGHTS [10 Oct 2001]

The U.S. Supreme Court has refused to hear an appeal by National Geographic after an appellate court sided with a photo journalist who sued the publication for including his work in CD-ROM form without his permission and without offering him additional payment. The freelancer's photographs had appeared in the National Geographic over three decades. (San Jose Mercury News 10 Oct 2001)

http://www.siliconvalley.com/docs/news/svfront/072212.htm

GROUPS REACH TENTATIVE DEAL ON WEBCAST ROYALTIES [17 Dec 2001]

Attorneys representing radio broadcasters, record labels and music artists have signed a tentative settlement in an ongoing dispute over whether radio broadcasters owe additional royalty payments when they put their stations' programming online. If the deal is finalized, it could be an important step toward resolving the tangle of legal issues surrounding online music. Radio companies currently do not pay recording firms royalties on songs they broadcast over the airwaves and have argued that the exemption should apply to online "Webcasts" as well. That issue is now on appeal. The current agreement depends on the U.S. Copyright Office to support arbitration to resolve the question of a royalty rate to be paid by Internet-only Webcasters who offer music online but don't own any radio stations. (Wall Street Journal 17 Dec 2001)

http://interactive.wsj.com/articles/SB1008547645508673600.htm

Category 4B1 Copyright

2002-01-08 copyright fair use intellectual property CD music DMCA amendment proposal

legislation

NewsScan

BILL AIMS AT PROTECTING RIGHT TO COPY DIGITAL FILES [8 Jan 2002]

Rep. Rick Boucher (D-Va.) says he will introduce legislation that would amend the Digital Millennium Copyright Act to protect consumers' right to make copies of digital files, such as songs on a CD. Boucher also has written a letter to the Recording Industry Association of America, suggesting that copy-protected CDs may violate the 1992 Audio Home Recording Act. Under that law, consumers pay a few cents extra each time they buy a blank CD, with the money going toward the recording industry to compensate them for potential losses caused by unauthorized copying. Boucher says, "I am particularly concerned that some of these technologies may prevent or inhibit consumer home recording." (Los Angeles Times 8 Jan 2002)

http://www.latimes.com/technology/la-000001793jan08.story?coll=la%2Dheadlines%2Dtechnology

Category 4B1 Copyright

2002-02-20 copyright extension judicial review lawsuit legislation constitutionality

NewsScan

COURT TO REVIEW COPYRIGHT EXTENSION LAW [20 Feb 2002]

The U.S. Supreme Court announced it will review a challenge to a 1998 law that extends by 20 years the lifetime of all existing copyrights and increases the lifetime of future copyrights from 50 to 70 years after the death of the creator. The legislation, called the Sonny Bono Copyright Term Extension Act, was named after the late Sonny Bono, congressman and former entertainer. Stanford University law professor Lawrence Lessig, an attorney for one of the groups seeking to declare the legislation unconstitutional, says the case is important "so that the next Walt Disney can do to Disney what Disney did to Grimm's fairy tales" — entirely transform material taken from the public domain. But the court likely will focus not on the substance of the law but on the issue of whether the law extends a copyright's duration far longer than what was envisioned by the framers of the Constitution. Wayne State University law professor Jessica Litman argues: "It's important for the Supreme Court to reassert that there's no copyright exception in the Constitution that Congress can do whatever it pleases. Congress has limited powers." Lawyers for the government insist that there are no legal precedents barring Congress from enacting the legislation. (Washington Post 20 Feb 2002)

http://washingtonpost.com/wp-dyn/articles/A35750-2002Feb19.html

4B2 **Patents**

Category 4B2 **Patents**

2001-01-25 Web index patent infringement claim lawsuit intellectual property

NewsScan

ALTAVISTA SAYS IT OWNS WEB INDEXING TECHNOLOGY

AltaVista has claimed a patent on a method of indexing Web sites used by most search engines and company intranets, and is threatening to sue companies using these search techniques for patent infringement. "We believe that virtually everyone out there who indexes the Web is in violation of at least several of [AltaVista's] key patents," says David Wetherell, CEO of CMGI, AltaVista's parent company. AltaVista owns 38 patents, "many of which we think are fundamental to the search area," and has applications pending for another 30, says Wetherell. "If you index a distributed set of databases -- that's what the Internet is. And even within intranets, that's one of the patents." AltaVista's move will intensify the debate over to what extent companies should be allowed to claim monopolies over methods that have become building blocks of the Internet. "If nothing is done, the Web will become fenced in by competing patents, turning an open, free and transparent playing field into a proprietary wasteland littered with nonsensical and stifling legislation," says one critic, CEO of a Web design and development company. (Financial Times 25 Jan 2001)

http://news.ft.com/news/industries/infotechnology

Category 4B2 **Patents**

2001-05-10 patent infringement lawsuit judgement fraud

NewsScan

RAMBUS FOUND GUILTY OF FRAUD

In a back-and-forth legal battle with Infineon Technologies, memory chip maker Rambus has been found guilty of fraud and slapped with punitive damages of \$3.5 million. The fine was later reduced to \$350,000 because of limitations in the local Virginia law. The verdict was a shocking turnaround for Rambus, which had sued Infineon on 57 charges of patent infringement. The jury agreed with Infineon's claim that Rambus had committed fraud because it participated in a broad chip industry project to develop fast memory chips, but did not reveal it had patents on similar technology. The goal of the cooperative project was to develop chips that would be royalty-free. (Financial Times 10 May 2001)

Category 4B2 **Patents**

2001-08-07 patent Internet software update delivery subscription

NewsScan

MCAFEE PATENT COVERS SUBSCRIPTION-BASED SOFTWARE

A new patent awarded to security software maker McAfee.com covers its system for delivering software and services over the Internet, giving it a potential advantage in the emerging trend of subscription-based software. "This doesn't close the door for competitors, it simply sets some boundaries for them," says market research executive Harry Fenik. Microsoft and other software vendors are already testing the concept of selling ongoing Web-based subscriptions to their products rather than collecting one-time fees for packaged goods, and now these companies "will have to tread carefully" to avoid infringing on McAfee's patent, or agree to pay licensing fees, says Fenik. Meanwhile, McAfee CEO Srivats Sampath says it's too early to say whether his company will sue potential violators, but "we will be sensitive to someone willfully flaunting the technology," he warns. (AP 7 Aug 2001)

http://news.excite.com/news/ap/010806/23/mcafee-patent

Category 4B2

Patents

2001-08-28

patent infringement lawsuit digital television TV

NewsScan

MIT SUES SONY OVER DIGITAL TV [28 Aug 2001]

The Massachusetts Institute of Technology is suing Sony Electronics, alleging that Sony's digital television business is infringing on four patents owned by MIT. The lawsuit says the technology was contributed by MIT scientists to the so-called "Grand Alliance" set up by the FCC in 1993, in which corporations and researchers collaborated to set a uniform U.S. standard for digital TV. Earlier, MIT won concessions by taking similar action against Sharp and Toshiba America, which also sell digital TVs. The digital sets cost anywhere from \$800 to \$12,000 or more, and MIT says it is entitled to a share of the profits. (AP 28 Aug 2001) http://news.excite.com/news/ap/010828/11/mit-sony

Category 4B2

Patents

2001-12-21

patent infringement handwriting recognition lawsuit judgement court ruling

NewsScan

PALM JUDGED GUILTY OF INFRINGING ON XEROX PATENT [21 Dec 2001]

A federal judge in Rochester, NY, has found handheld computer maker Palm Inc. and 3Com (Palm's former parent company) guilty of violating a Xerox's patent on handwriting recognition software called Unistrokes, which takes a simplified version of the alphabet that can be entered on a tablet with pen strokes. Palm will apparently have to decide whether to pay royalties to Xerox or discontinue using the software; in any event, it will have to pay Xerox damages for past infringement. Palm's sales were down 44% this quarter compared to the same quarter a year ago, and industry analyst Dylan Brooks of Jupiter Media Metrix comments: "With Palm reporting enormous losses and with some of the problems they've had in the market lately, this is the last thing they need." (Washington Post 21 Dec 2001) http://www.washingtonpost.com/wp-dyn/articles/A9556-2001Dec20.html

Category 4B2

Patents

2002-02-13

patent litigation lawsuit royalties hyperlinking Web

NewsScan

CLICK-AND-PAY: BT ASSERTS PATENT CLAIM FOR HYPERLINKS [7 Feb 2002]

The BT Group in the U.K. is targeting Prodigy in the first of a series of planned lawsuits aimed at enforcing its claim to have a copyright covering hypertext links. The claim, which is supported by a U.S. patent obtained in 1984 (before the creation of the World Wide Web), would allow BT to demand royalty payments from Internet service providers who offered their users the ability to surf the Web by using hyperlinks. A company spokesman argues: "We believe we have a duty to protect our intellectual property and we would expect companies to pay a reasonable royalty based on the revenues that they have enjoyed through the use of that intellectual property." Various critics of the BT lawsuit maintain that hyperlinking was conceived all the way back in the 1960s, and promoted by such well-known Internet luminaries as Ted Nelson and Doug Engelbart. (Retuers/USA Today 7 Feb 2002) http://www.usatoday.com/life/cyber/tech/2002/02/07/patent-suit.htm

DOUBTS ARISE OVER BT'S CASE FOR HYPERLINK PATENT [13 Feb 2002]

Judge Colleen McMahon, the judge assigned to British Telecom's case defending its right to collect royalties from a 26-year-old patent covering hyperlinking, has raised doubts over the validity of the case. She noted that it would be difficult to prove that a patent first filed in 1976 — long before the Web was created — would apply to today's technology, and that comparing a 1976 computer to a 2002 computer was like comparing a mastodon with a jet. If BT prevails, its first likely target for royalty collection is Prodigy Communications, and if that attempt is successful, BT will notify other ISPs in the U.S. that they must pay up. (The U.S. is the only country where the patent has not yet expired.) Some analysts say the royalties could total tens of millions of dollars if the patent is upheld. (Financial Times 13 Feb 2002)

http://news.ft.com/news/industries/internet&e-commerce

Reverse engineering 4B3

Category 4B3 Reverse engineering

2001-01-24 standards corruption sabotage lawsuit settlement ntellectual property reverse

engineering license contract

NewsScan

SUN CLAIMS VICTORY OVER MICROSOFT IN JAVA DISPUTE

Microsoft yesterday agreed to settle a long-running legal dispute with Sun Microsystems over Sun's Java programming language and related software development tools. Under the terms of the settlement, Microsoft will pay Sun \$20 million and accept Sun's termination of its prior Java licensing agreement. In addition, Microsoft will relinquish use of the Java trademark. The lawsuit, originally filed in 1997, alleged that Microsoft had modified Java in order to optimize its performance with the Windows operating system. Microsoft said it decided to settle in order to avoid "costly litigation" and left open the possibility that it might now proceed to develop its own, independent version of Java. Meanwhile, Sun CEO Scott McNealy called the settlement "a victory for our licensees and consumers. The software development] community wants one Java technology. This agreement further protects the authenticity and value of Sun's Java technology." (Financial Times 24 Jan 2001)

http://news.ft.com/news/industries/infotechnology

Category 4B3 Reverse engineering

2001-06-07 reverse engineering intellectual property contract copyright research

vulnerability weakness encryption watermarking steganography

NewsScan

RECORDING INDUSTRY THREATENS RESEARCHER WITH LAWSUIT [24 Apr 2001]

The litigation department of the Recording Industry Association of America (RIAA) has threatened legal action against a Princeton University computer scientist if he and his colleagues give a conference presentation this week explaining how to get around a system developed by the industry to protect copyrighted music. The researcher, Dr. Edward W. Felton, works in the field of steganography, which develops techniques such as digital watermarking. The head of RIAA's litigation department insists: "There is a line that can get crossed, and if you go further than academic pursuit needs to go, you've crossed the line and it's bad for our entire community, not just for artists and content holders, it's everyone who loves art, and it's also bad for the scientific community." (New York Times 24 Apr 2001) http://www.nytimes.com/2001/04/24/technology/24MUSI.html

COMPUTER RESEARCHERS YIELD TO THREAT OF LITIGATION [27 Apr 2001]

A group of computer scientists at Princeton and Rice universities has decided to withdraw an academic paper that was to be presented at a conference this week, because the Recording Industry Association of America said that public presentation of the work would violate the Digital Millennium Copyright Act of 1998, because it would describe how to evade the systems used to protect copyrighted music. Princeton computer scientist Edward W. Felton explained the group's decision by saying: "Litigation is costly, time-consuming, and uncertain, regardless of the merits of the other side's case. We remain committed to free speech and to the value of scientific debate to our country and the world." John McHugh of Software Engineering Institute at Carnegie Mellon University commented: "This was an excellent technical paper. This was pure and simple intimidation. This paper didn't do anything that a bright technical person couldn't easily reproduce." (New York Times 27 Apr 2001) http://www.nytimes.com/2001/04/27/technology/27MUSI.html

COURT CASE TESTS ACADEMIC FREEDOM AND COPYRIGHT LAW [7 Jun 2001]

Princeton University computer scientist Edward W. Felton and colleagues at Princeton, Rice and Xerox, have asked a federal court for a declaratory judgment that would overturn a part of the 1998 Digital Millennium Copyright Act. The scientists say that the DMCA has constrained them from presenting their research results because the recording industry said the research, if made public, would undermine the industry's antipiracy technology, used to protect content on compact disks. Dr. Felton says that what is needed is "a broad principle that scientific investigation and publication is okay, that discussion of these technologies is okay. Publication is how scientists communicate with each other." (New York Times 7 Jun 2001) http://www.nytimes.com/2001/06/07/technology/07CODE.html

Category 4B3 Reverse engineering

2001-11-05 music piracy peer-to-peer encryption DMCA Digital Millennium Copyright Act

awsuits

NewsScan

AIMSTER VS. RECORDING INDUSTRY [21 May 2001]

The recording industry may be hoist on its own petard if the Napster-like music swapping service called Aimster is successful in its legal strategy against the Recording Industry Association of America (RIAA). Unlike Napster, Aimster (which has no central servers to maintain and leaves users individually responsible for their actions) encrypts transmissions, and so there is no way for the RIAA or any other outside party to distinguish between files which are in compliance with copyright law and those that infringe on it. Of course, RIAA could simply decrypt the files – but then it would be in violation of the Digital Millennium Copyright Act (DMCA), a law that it strongly supports, and that makes it a criminal offense to circumvent encryption protection of copyrighted material. (The New Republic 21 May 2001)

http://www.tnr.com/cyberlaw/babbitt051101.html

NOW IT'S AIMSTER'S TURN [25 May 2001]

"This is Napster all over again": Five major record companies, of which four are represented by the Recording Industry Association of America (RIAA), have filed a lawsuit against the Internet service Aimster, charging it with allowing users to illegally exchange copyrighted music. But Aimster insists that, unlike Napster, it's "not a music sharing service" but a service that delivers private messages and files (music or any other kinds of files) and is not authorized to examine the content of those communications. (New York Times 25 May 2001) http://www.nytimes.com/2001/05/25/technology/25MUSI.html

AIMSTER TARGETED BY NEW LAWSUIT [5 Jul 2001]

Aimster, already being sued for copyright infringement by a long list of recording companies, is now being sued by the National Music Publishers Association (NMPA), whose chief executive says: "We are extremely disappointed that before the ink was even dry on Ninth Circuit Court of Appeals' opinion concluding that Napster was engaging in massive copyright infringement, another Internet music service would seek with impunity to supplant Napster and expect to get away with it." But the Aimster's chief executive charges that the publishers are in collision with the recording industry, and says that Aimster is quite different from Aimster. He insists that Aimster is not a music-swapping service like Napster, but rather an instant messaging system that, coincidentally, allows files of all kinds to be swapped confidentially through member "buddy lists." (Reuters/USA Today 5 Jul 2001) http://www.usatoday.com/life/cyber/tech/2001-07-05-aimster.htm

NAPSTER ALTERNATIVE USE UP 20% [5 Nov 2001]

The use of Napster-like peer-to-peer music file-sharing sites like Kazaa, MusicCity and Grokster rose 20% during the month of October, signaling U.S. Internet users' insatiable demand for digital music and video downloads. All three sites use software licensed from FastTrack, an Amsterdam-based technology company, and share the same network. "The growth of the FastTrack network continues to be astounding," says a Webnoize analyst. "During the last four months the number of users typically logged on has risen by 480%, and in November will likely surpass the 1.57 million simultaneous users that Napster... enjoyed at its peak... As higher awareness translates into higher usage, the FastTrack network may ultimately become many times larger than Napster ever was." Meanwhile, a recent Jupiter Media Metrix survey shows that song-swapping has declined in Europe over the same period. According to the report, music downloads are down by 50% in Europe since February, the point at which Napster usage hit its zenith. (Reuters 5 Nov 2001)

http://news.excite.com/news/r/011105/14/net-tech-webnoize-dc

Category 4B3 Reverse engineering

2001-11-07 copyright reverse engineering remote control lawsuit robot dog

NewsScan

SONY TELLS AIBO HACKER "NO NEW TRICKS" [7 Nov 2001]

Sony has demanded that the owner of a Web site that distributes free software for enhancing the smarts of the cuddly robot pets, remove the software from its site on pain of prosecution for copyright infringement and altering its product without a license. The software could be used to teach Aibo new tricks, such as disco dance steps and additional vocabulary. "This is a legal issue," said a Sony Entertainment spokesman. "We don't support the development of software by manipulating the existing Aibo software code -- hacking it." The company's action has irked Aibo owners, who usually spend hundreds of dollars on software from Sony, and were thrilled to get the free enhancements. (AP 7 Nov 2001)

http://news.excite.com/news/ap/011107/14/sony-robot-hack

Category 4B3 Reverse engineering

2001-12-14 Digital Millennium Copyright Act DMCA reverse engineering decryption

electronic book copyright protection intellectual property lawsuit prosecution

arrest

NewsScan

CRYPTOGRAPHER ARRESTED FOR VIOLATING DIGITAL COPYRIGHT LAW [18 Jul 2001]

Law enforcement officials have arrested Dmitri Sklyarov, a 27-year-old Russian graduate student at Moscow State Technical University, on charges of unauthorized copying of digitized material that he obtained breaking the electronic book encryption code developed by Adobe Systems. Accused of violating the Digital Millennium Copyright Act of 1998, he will face up to five years in jail and a \$500,000 fine if he is found guilty. (New York Times 18 Jul 2001) http://partners.nytimes.com/2001/07/18/technology/18CRYP.html

IN DIGITAL AGE, SECURITY ISSUES PLAY LARGE ROLE [23 Jul 2001]

The Electronic Frontier Foundation, a civil liberties group, is helping to underwrite challenges against the Digital Millennium Copyright Act (DMCA) of 1998, which was used last week as grounds for arresting an encryption expert accused of violating its restrictions on circumventing security schemes for protecting electronic books. One critic of the law says, "It's distressing that if someone writes software they say is secure and you prove them wrong, you can go to jail." Those opposed to the DMCA argue that by allowing copyright-holders to protect their work by encryption and making it a crime to break that encryption, the law is taking away the "Fair Use" exceptions that have always allowed people to copy portions of copyrighted works for purposes such as scholarship, criticism, or parody. (New York Times 23 Jul 2001)

http://www.nytimes.com/2001/07/23/technology/23DIGI.html

ADOBE CHIMES IN, ASKS GOVERNMENT TO FREE DMITRY [24 Jul 2001]

Adobe Systems is asking the government to release Russian programmer Dmitry Skylarov, who was arrested last week in Las Vegas for violating the Digital Millennium Copyright Act (DMCA) by trafficking in code used to break the encryption used to protect Adobe's eBook Reader software. An international "Free Dmitry" movement has protested the government's action, which was taken at Adobe's urging. Adobe now says that although it strongly supports the DMCA and the enforcement of copyright protection of digital content, it believes that "the prosecution of this individual in this particular case is not conducive to the best interests of any of the parties involved or the industry.' A lawyer for the Electronic Frontier Foundation, a civil liberties advocacy group, said: "We explained to Adobe, imagine how you would feel if one of your programmers was visiting in Russia and was arrested for making software that was considered illegal there? It sort of hit home with them that what they are doing here isn't right.' However, a government attorney prosecuting the case says: "This is a criminal case brought by the United States against the defendant, and to that extent no one else is a party.' (San Jose Mercury News 24 Jul 2001) http://www.siliconvalley.com/docs/news/svfront/adobe072401.htm

"FREE DMITRY" PROTESTS CONTINUE [31 Jul 2001]

About a hundred protesters showed up yesterday in San Francisco to denounce the arrest of Russian programmer Dmitry Sklyarov, who the government has accused of violating the U.S. Digital Millennium Copyright Act (DMCA). The charge was based on Sklyarov's role in the development of software used to evade copyright protections used on Adobe eBook software. An attorney for the Electronic Freedom Foundation told the gathering of Sklyarov supporters that the long-standing "Fair Use" principle of copyright law "allows people to make use of things freely without the permission of the copyright holder." One protester said: "I'm interested in freedom of speech and trying to redress the balance between copyright holders to control information and the lack of the individual's right to challenge that." (Reuters/San Jose Mercury News 31 Jul 2001)

http://www.siliconvalley.com

BAIL FOR DMITRI [7 Aug 2001]

A federal district court in San Jose has released the 26-year-old Russian programmer and graduate student Dmitri Sklyarov on \$50,000 bail. Arrested at a software conference in Las Vegas, he is charged with criminal violation of the Digital Millennium Copyright Act (DMCA) of 1998, and faces up to five years in prison and a half-million dollar fine for promoting a software product that evades the encryption algorithms used by Adobe Systems to protect e-books. Sklyarov is viewed by many as a martyr for the cause of freedom of information, and his lawyer says: "If there are constitutional questions out there, we're certainly going to be raising them. I see this as being an intellectual fight to the death. Either the criminal provisions of the DMCA are going to be killed, or we're in a position where some civil liberties are going to be killed." (New York Times 7 Aug 2001)

http://partners.nytimes.com/2001/08/07/technology/07HACK.html

The Russian official responsible for fighting high-tech crimes in that country says that programmer Dmitri Sklyarov, arrested in Las Vegas for violating U.S. digital copyright laws, broke no Russian laws. "If this case was being reviewed in Russia, we would have nothing against Dmitri Sklyarov. No crime falling under current Russian law has been committed." Sklyarov, now out on \$50,000 bail, is charged with having violated the 1998 Digital Millennium Copyright Act (DMCA) by promoting software capable of evading the encryption used by Adobe's eBook Reader. Adobe has dropped its support of the case. (AP/San Jose Mercury News 9 Aug 2001) http://www.siliconvalley.com/docs/news/svfront/075617.htm

WHAT IS DMITRI THINKING? [3 Aug 2001]

Here's what Dmitri Skyarov -- the 26-year-old Russian cryptographer arrested in Las Vegas for violating the Digital Millennium Copyright Act -- has this to say about what has happened to him: "If someone will allow me to choose not to be famous in this case, I would prefer not to be famous. I'm not company chief. I'm just a programmer." The programs he developed are written in Russia and violate no Russian laws. He's anxious to return to his wife and two children in Moscow, where his hope is "to be as independent as possible. It's very hard to have real dreams in Russia. All things change very fast, and you never know what will happen tomorrow." (San Jose Mercury News 13 Aug 2001) http://www.siliconvalley.com/docs/news/svfront/sklyar081101.htm

RELEASE OF RUSSIAN PROGRAMMER [14 Dec 2001]

Dmitry Sklyarov, the 27-year-old Russian programmer arrested in the U.S. for violating the Digital Millennium Copyright Act (DMCA) by writing and promoting code that could be used to evade the copy-protection features of the Adobe Acrobat eBook Reader, is being released, but the U.S. government will continue its prosecution of his employer, ElcomSoft of Moscow. Skylarov's cause was embraced by a worldwide collection of programmers, scientists, free-speech advocates and civil libertarians who organized "Free Dmitry" rallies. (San Jose Mercury News 14 Dec 2001)

http://www.siliconvalley.com/docs/news/svfront/hacker121401.htm

4B4 EULA (End-user license agreements)

Category 4B4 EULA (End-user license agreements)

2001-03-30 copyright e-mail Web office software .NET intellectual property appropriation

theft contract

RISKS 21 32

RISKS correspondent Michael Sinz reported on astounding claims in the end-user license agreement (EULA) for .NET and HailStorm PassPort services. He summarized the situation as follows: "If you send source code or business plans or a chapter of your first novel or anything else of any value (or of no value), Microsoft has the right to use, exploit, and sublicense any and or all of it without any payment to the copyright holder. It also has the right to any trademark, service mark, or patent that you might use in such communications or documents that are used/stored/transmitted via their service!" Mr Sinz bolstered his reaction with quotations from the LICENSE TO MICROSOFT section of the EULA for the Passport site, which included the following text:

"By posting messages, uploading files, inputting data, submitting any feedback or suggestions, or engaging in any other form of communication with or through the Passport Web Site, you warrant and represent that you own or otherwise control the rights necessary to do so and you are granting Microsoft and its affiliated companies permission to:

- 1. Use, modify, copy, distribute, transmit, publicly display, publicly perform, reproduce, publish, sublicense, create derivative works from, transfer, or sell any such communication.
- 2. Sublicense to third parties the unrestricted right to exercise any of the foregoing rights granted with respect to the communication.
- 3. Publish your name in connection with any such communication.

The foregoing grants shall include the right to exploit any proprietary rights in such communication, including but not limited to rights under copyright, trademark, service mark or patent laws under any relevant jurisdiction. No compensation will be paid with respect to Microsoft's use of the materials contained within such communication. Microsoft is under no obligation to post or use any materials you may provide and may remove such materials at any time in Microsoft's sole discretion."

Category 4B4 EULA (End-user license agreements)

2001-07-13 contract law end-user license agreement EULA

NewsScan

USER AGREEMENTS REQUIRE USER CONSENT

A federal judge in New York has ruled that individuals who downloaded free software from Netscape's Web site are not bound by a "conditions of use" statement they hadn't read. The reason? The site had not required them to take positive action -- prior to the download -- to show they agreed to Netscape's conditions. A lawyer who represented the plaintiffs against Netscape praised the court's decision: "It applies an ancient and fundamental principle in a novel context. That is, you can't be bound to that which you don't agree to." (New York Times 13 Jul 2001) http://www.nytimes.com/2001/07/13/technology/13CYBERLAW.html

Category 4B4 EULA (End-user license agreements)

2001-09-21 UCITA EULA end-user license agreement

RISKS 21 68

Alistair McDonald noted in RISKS that "the latest MS Front Page licence agreement prevents you from any antimicrosoft Web content with it." The quoted text from the EULA is "You may not use the Software in connection with any site that disparages Microsoft, MSN, MSNBC, Expedia, or their products or services "

http://slashdot.org/article.pl?sid=01/09/20/1443226 reports that

Category 4B4 EULA (End-user license agreements)

2002-02-08 end-user license agreement EULA lawsuit antivirus censorship contract

NewsScan

SOFTWARE REVIEW PROHIBITION CHALLENGED BY LAWSUIT [8 Feb 2002]

The State of New York is suing Network Associates, a company that makes McAfee Virus Scan and other software products, over a Network Associates prohibition which specifies: "The customer will not publish reviews of this product without prior consent from Network Associates Inc." New York says that the company is guilty of censoring consumers in order to shield itself "from criticism and commentary that is the essence of the free market." Network Associates argues that its use of the restriction is nothing more than an attempt by the firm to exercise its right "to set the terms of its license," which is a matter between the consumer and the company. In its response to the lawsuit, the company has also explained that its only motivation for the restriction was to make sure that customers did not publish reviews of outdated versions of products. (New York Times 8 Feb 2002) http://partners.nytimes.com/2002/02/08/technology/08VIRU.html

4B5 Trademarks

Category 4B5 Trademarks

2001-12-20 trademark infringement lawsuit emulator monopoly

NewsScan

MICROSOFT SUES LINDOWS FOR TRADEMARK INFRINGEMENT [20 Dec 2001]

Microsoft has sued a small startup called Lindows, charging that the name infringes on its Windows trademark. Lindows software is based on the Linux operating system and is capable of running programs made for Windows. "The similarity between the Lindows and Windows marks is likely to lead consumers to mistakenly conclude that the Lindows product was exclusively or jointly developed by, licensed or certified by, or otherwise sponsored or approved by Microsoft," said the software giant in its complaint. Microsoft is hoping to settle the dispute out of court, says a company spokesman. (Reuters 20 Dec 2001)

http://www1.excite.com/home/technology/tech_article/0,2109,196677 | technology!12-20-2001::19:45 | reuters,00.html

4C1 Paradigms, security standards

Category 4C1 Paradigms, security standards

2001-07-22 privacy risk management false positives power of a test suspicion reporting law enforcement police notification postal service

RISKS 21 54

Alan Wexelblat noted in RISKS a report by "Insight Magazine . . . [1] that since 1997, the US Postal Service has been reporting innocent activity it deems 'suspicious' to federal law enforcement officials. Evidence includes a training video with this chilling instruction: 'It's better to report 10 legal transactions than to let one illegal transaction get by.'

The risks of a system that presumes guilt until innocence is proven are too numerous to list here. Not least of them is the impossibility of proving a negative (I did not intend this cash to be used for illegal purposes). A similar reporting system in the banking arena is known to generate ratio of 99,999 false positives for every true positive. Yes, I do mean a ratio of 10^5:1 errors to correct results. I can't imagine any other system in which that error rate would be acceptable.

The information on suspicious activities is, of course, kept in a database controlled in secret and used for purposes no one is willing to discuss. The Post Office will not discuss the parameters used to flag 'suspicious' activity, though the video states that unwillingness to give out personal information such as date of birth and/or produce identification papers is automatically suspicious.

Someone help me verify that I'm still living in America, please?

[1] http://www.moreprivacy.com/editorials/postaleye.htm"

Category 4C1 Paradigms, security standards

hardware software integration identification authentication I&A BIOS firmware

biometric fingerprint recognition digital certificate root key

NewsScan

THE MARRIAGE OF HARDWARE AND SOFTWARE SECURITY

A number of technology companies are introducing new products that embed security features inside computer hardware, to add to the protections offered by software alone. IBM and Targus Systems have developed a new biometric fingerprint reader that's built into a PC card inserted into the new IBM ThinkPad laptops, and another example of the trend is the announcement that VeriSign's "root key" software will be put into the next version of Phoenix Technology's BIOS (i.e., its basic input-output software), so that no one but an authorized user can be authenticated on the computer. (Reuters/San Jose Mercury News 23 Feb 2002) http://www.siliconvalley.com/mld/siliconvalley/2734756.htm

4C2 Risk management methodology & tools

Category 4C2 Risk management methodology & tools

2001-07-01 Digital Millennium Copyright Act DMCA video bootleg copyright infringement

intellectual property ISP Internet Service Provider liability lawsuit judgement

NewsScan

EBAY GRANTED VICTORY IN COPYRIGHT LAWSUIT

EBay won what it called a precedent-setting lawsuit Thursday when a federal judge ruled that the online auction company was not liable for copyright infringement under the Digital Millennium Copyright Act in the case of bootlegged copies of a Charles Manson documentary that were sold on the site. The case was touted as the first to test whether a Web site has a "safe harbor" if people who use the site sell items that infringe on copyrights. In his ruling the judge agreed with eBay's position that it is not like a real-world auctioneer that vouches for the items on sale, but rather is more like a provider of stalls at a flea market. (AP/Silicon Valley Sep 7 2001) http://www.siliconvalley.com/docs/news/svfront/000051.htm(-20-)

Category 4C2 Risk management methodology & tools

2001-08-24 downstream liability negligence standard due care Web vandalism denial of

service DoS

NewsScan

BLAME THE VICTIM: VANDALIZED WEB SITES MAY BE LIABLE FOR DAMAGES

Some legal scholars are suggesting that a Web site vandalized by hacker attacks may itself be legally liable if its customers suffer damages and if the site was negligent in maintaining security. Law professor Margaret Jane Radin of Stanford University predicts: "A court is going to say it is negligent of you not to implement preventative measures if they are reasonably effective and affordable." No reported court decisions have dealt with the issue, but Radin says that lawsuits in the near future are highly likely to be lodged against companies and network providers targeted by "denial of service" attacks. (New York Times 24 Aug 2001)

http://partners.nytimes.com/2001/08/24/technology/24CYBERLAW.html

Category 4C2 Risk management methodology & tools

2001-10-19 criminal hacker attack Web Internet disclosure reporting announcement

proposed legislation confidentiality law enforcement investigation statistics

NewsScan

WHITE HOUSE SUPPORTS LIMITED DISCLOSURE ON HACK ATTACKS

The Bush administration is backing bipartisan legislation aimed at limiting government disclosures about hack attacks. Congressional supporters of the proposed law include Senators Robert Bennett (R-UT) and John Kyl (R-AZ) and Representatives Tom Davis (R-VA) and James Moran (D-VA). Bennett told his Senate colleagues that if they didn't pass the bill — which is designed to protect the confidentiality of information disclosed by companies about attempts to hack into their computers — then companies will simply not provide all the details of such attacks to government security investigators. (AP/San Jose Mercury News 19 Oct 2001)

http://www.siliconvalley.com/docs/news/svfront/054790.htm

Category 4C2 Risk management methodology & tools

2001-10-31 availability bugs repair artificial intelligence AI quality assurance

NewsScan

IBM INTRODUCES SELF-HEALING BUSINESS SOFTWARE SYSTEMS

Adapting the same kind of "brute force" computing strategy of its chess-playing Deep Blue supercomputer, IBM's ebusiness Management Services is introducing "self-healing" business software that will allow machines to detect and work around failing parts and work overloads without requiring the intervention of onsite technicians. Irving Wladawsky-Berger, the company's vice president for technology and strategy, says: "This is really the essence of making systems behave in an intelligent manner... God knows if this means they are intelligent. But what we really like about this, and we learned a lot about this in Deep Blue, is the brute force techniques of having a lot of information and a lot of computer power is the most effective way of making systems behave in what we humans would call intelligence." (Reuters/San Jose Mercury News 31 Oct 2001)

http://www.siliconvalley.com/docs/news/svfront/076589.htm

Category 4C2 Risk management methodology & tools

2001-11-12 national identity card terrorists reliance incorrect assumption risk management

RISKS 21 75

Frequent RISKS contributor Adam Shostack pointed out a significant risk of national ID cards: mistaken reliance on identification as a substitute for trustworthiness. His cogent analysis follows:

"I believe that there is an important risk, that of reliance, that will accompany a high-tech national ID card. Every terrorist commits their first act of terrorism at some time in their life, and before that time, they cannot be any database of known terrorists.

Once you start issuing cards, people will start relying on 'identity verification' rather than threat management. We'll see people relying on background checks [1] rather than xrays. We'll see special lines for frequent fliers, who are 'known trustworthy.' They differ from pilots and flight crew in that they don't run into co-workers who can notice and react to strange behavior before the flight. If you want to keep knives and guns off of planes, the answer lies in xrays, magnetometers, and other searching technology, not in believing that you know who's who. Many of the national id card risks come from a layer of indirection from the real problem, which is not "Is Alice trusted," but, "Is the person in front of me trusted?" National ID cards not only do nothing to solve this problem, they distract us from attempting to solve it."

[1] See the last para of http://www.spectrum.ieee.org/WEBONLY/special/sept01/idcards.html

4C3 Certification of site security, privacy protection

Category 4C3 Certification of site security, privacy protection

2001-12-14 Web site health information privacy security accreditation certification

NewsScan

HEALTH SITES GET ACCREDITATION FROM STANDARDS GROUP

The American Accreditation Health Care Commission has put the stamp of its approval on 13 online health-care sites, the first such sites to earn AAHCC accreditation. AAHCC sets quality standards for managed-care and other health-care programs. The move is aimed at helping people sort out good information from bad in the health care field, which has become a popular area of online research among consumers. "There is so much bad information on the Internet, especially about health-care content," said Kevin Noland, COO of A.D.A.M., one of the sites to earn accreditation this week. "Someone needs to set a standard so people feel they are getting information from a trusted source." Standards for approval include full disclosure about funding and advertising, quality of editorial content, linking to other sites, and privacy and security. Other accredited sites include WellMed, WebMD and Health Insurance Association of America. (Wall Street Journal 14 Dec 2001)

http://interactive.wsj.com/articles/SB1008284518346277800.htm

Category 4C3 Certification of site security, privacy protection
2002-02-04 Web security certification consumer guidance

NewsScan

BETTER BUSINESS BUREAU TARGETS ONLINE PRIVACY WITH NEW SITE

The Better Business Bureau has launched a new Safe Shopping Web site that enables consumers to locate online companies that have met BBB standards for privacy in e-commerce. Visitors to

http://www.bbbonline.org/consumer/ will find nearly 11,000 Web sites that have earned one or both of the BBBOnline Privacy and Reliability seals. A recent survey showed that almost 90% of consumers would feel safer making a purchase from an online company that displays one of the seals than from a company that does not, according to Greenfield Online. "The BBB system will encourage the business community to step up to the plate and meet consumer expectations regarding online privacy," says Ken Hunter, president and CEO of the Council of Better Business Bureaus and BBBOnline. (E-Commerce Times 4 Feb 2002)

http://www.ecommercetimes.com/perl/story/16149.html

4D Funny / miscellaneous

Category 4D Funny / miscellaneous

2001-01-03 virus propagation e-mail joke satire funny amusing

SatireWire; http://www.satirewire.com/news/0103/outlook.shtml

FOOT-AND-MOUTH BELIEVED TO BE FIRST VIRUS UNABLE TO SPREAD THROUGH MICROSOFT OUTLOOK Researchers Shocked to Finally Find Virus That Email App Doesn't Like

Atlanta, Ga. (SatireWire.com) — Scientists at the Centers for Disease Control and Symantec's AntiVirus Research Center today confirmed that foot-and-mouth disease cannot be spread by Microsoft's Outlook email application, believed to be the first time the program has ever failed to propagate a major virus.

"Frankly, we've never heard of a virus that couldn't spread through Microsoft Outlook, so our findings were, to say the least, unexpected," said Clive Sarnow, director of the CDC's infectious disease unit.

The study was immediately hailed by British officials, who said it will save millions of pounds and thousands of man hours. "Up until now we have, quite naturally, assumed that both foot-and-mouth and mad cow were spread by Microsoft Outlook," said Nick Brown, Britain's Agriculture Minister. "By eliminating it, we can focus our resources elsewhere."

However, researchers in the Netherlands, where foot-and-mouth has recently appeared, said they are not yet prepared to disqualify Outlook, which has been the progenitor of viruses such as "I Love You," "Bubbleboy," "Anna Kournikova," and "Naked Wife," to name but a few.

Said Nils Overmars, director of the Molecular Virology Lab at Leiden University: "It's not that we don't trust the research, it's just that as scientists, we are trained to be skeptical of any finding that flies in the face of established truth. And this one flies in the face like a blind drunk sparrow."

Executives at Microsoft, meanwhile, were equally skeptical, insisting that Outlook's patented Virus Transfer Protocol (VTP) has proven virtually pervious to any virus. The company, however, will issue a free VTP patch if it turns out the application is not vulnerable to foot-and-mouth.

Such an admission would be embarrassing for the software giant, but Symantec virologist Ariel Kologne insisted that no one is more humiliated by the study than she is. "Only last week, I had a reporter ask if the foot-and-mouth virus spreads through Microsoft Outlook, and I told him, 'Doesn't everything?'" she recalled. "Who would've thought?"

RECOMMEND THIS PAGE Copyright [©] 2001, SatireWire.

Category 4D Funny / miscellaneous 2001-03-13 bugs history folklore

NewsScan

WORTH THINKING ABOUT: THE HISTORY OF BUGS

Princeton University's Edward Tenner wants us to know that bugs, those notorious enemies of technology, have been around long before computers: "The bug, that perverse and elusive malfunctioning of hardware and later of software, was born in the nineteenth century. It was already accepted shop slang as early as 1878, when Thomas Edison described his style of invention in a letter to a European representative: 'The first step is an intuition and it comes with a burst, then difficulties arise — this thing gives out and then that — "Bugs" — as such little faults and difficulties are called — show themselves, and months of intense watching, study and labor are requisite before commercial success — or failure — is certainly reached.' "Edison implies that this use of 'bug' had not begun in his laboratory but was already standard jargon. The expression seems to have originated as telegrapher's slang. Western Union and other telegraph companies, with their associated branch offices, formed America's first high-technology system. About the time of Edison's letter, Western Union had over twelve thousand stations, and it was their condition that probably helped inspire the metaphor. City offices were filthy, and clerks exchanged verse about the gymnastics of insects cavorting in the cloakrooms. When, in 1945, a moth in a relay crashed the Mark II electromechanical calculator that the Navy was running at Harvard — it can still be seen taped in the original logbook — the bug metaphor had already been around for at least seventy-five years."

See http://www.amazon.com/exec/obidos/ASIN/0679747567/newsscancom/ for Edward Tenner's "Why Things Bite Back." (We donate all revenue from our book recommendations to Literacy Action's adult literacy programs.)

Category 4D Funny / miscellaneous
2001-04-30 error message funny amusing QA quality assurance
RISKS 21 37

Jean-Jacques Quisquater reported this gem to RISKS:

"Q276304 - Error Message: Your Password Must Be at Least 18770 Characters and Cannot Repeat Any of Your Previous 30689 Passwords"

Commented the correspondent drily, "New level of security at Microsoft."

Category 4D Funny / miscellaneous

2001-05-05 cryptography geek humor funny

RISKS 21 42

Date: [not included]

From: "Keith F. Lynch" < kfl@KeithLynch.net >

Subject: Converting Pi to binary: DON'T DO IT! (via Russ Perry Jr.)

Newsgroup: alt.math.recreational

WARNING: Do NOT calculate Pi in binary. It is conjectured that this number is normal, meaning that it contains ALL finite bit strings.

If you compute it, you will be guilty of:

- * Copyright infringement (of all books, all short stories, all newspapers, all magazines, all web sites, all music, all movies, and all software, including the complete Windows source code)
- * Trademark infringement
- * Possession of child pornography
- * Espionage (unauthorized possession of top secret information)
- * Possession of DVD-cracking software
- * Possession of threats to the President
- * Possession of everyone's SSN, everyone's credit card numbers, everyone's PIN numbers, everyone's unlisted phone numbers, and everyone's passwords
- * Defaming Islam. Not technically illegal, but you'll have to go into hiding along with Salman Rushdie.
- * Defaming Scientology. Which IS illegal -- just ask Keith Henson.

Also, your computer will contain all of the nastiest known computer viruses. In fact, all of the nastiest POSSIBLE computer viruses.

Some of the files on my PC are intensely personal, and I for one don't want you snooping through a copy of them.

You might get away with computing just a few digits, but why risk it? There's no telling how far into Pi you can go without finding the secret documents about the JFK assassination, a photograph of your neighbor's six year old daughter doing the nasty with the family dog, or a complete copy of the not-yet-released Pearl Harbor movie. So just don't do it.

The same warning applies to e, the square root of 2, Euler's constant, Phi, the cosine of any non-zero algebraic number, and the vast majority of all other real numbers.

There's a reason why these numbers are always computed and shown in decimal, after all.

Category 4D Funny / miscellaneous
2001-05-29 spam humor etymology

NewsScan

SPAM THE LUNCHEON MEAT

Look, we don't want to waste your time -- or ours. So here's the story: Hormel Foods, the maker of Spam luncheon meat, no longer minds if you use the lower-case word "spam" to refer to unsolicited commercial mail that invites you to make \$\$\$, lose weight, or find new friendships. But if you want to say something about SPAM, the luncheon meat, use capital letters and show a little respect. It's not Hormel's fault that the name of its product was appropriated as a synonym for junk mail. So how did that happen? In an old Monty Python comedy routine, a group of Vikings bellowed a chorus of "spam spam spam spam" to drown out all other conversation, in the same way spam in your inbox makes it harder and harder to find real and important mail -- like NewsScan Daily. (San Jose Mercury News 29 May 2001)

http://www.siliconvalley.com/docs/news/svfront/026425.htm

Category 4D Funny / miscellaneous

2001-07-12 default design flaw error QA quality assurance power failure charge charging rechargable batteries brake on switch

RISKS 21 50

Ray Todd Stevens was in a store where wheelchairs with rechargeable batteries were lined up against a wall being recharged. Mr Stevens wrote in RISKS, "When the power failed, all of these units took off and most ran into things before the staff could stop them, trailing their cords behind them. . . . It seems that there are several . . . glaring design flaws in these units.

- 1. The stopped position on the handle is not the default position. Instead, the control is all the way down for forward, all the way up for reverse and half way in between for neither. Meaning that the nature position is forward.
- 2. There is also a foot brake, but it must be pushed to stop.
- 3. [The] power switch.... must be turned on to charge the unit.
- They seem to assume that no electricity means that they are now to take off and do so driverless."

Mr Stevens added that we ought to be thinking about the default mode for computers and network equipment when planning for power failures.

Category 4D Funny / miscellaneous
2001-07-19 automated alertness monitor automobile squirtgun water distraction startle emergency

RISKS 21 53

[The following item from John Arundel in RISKS leaves this editor speechless:]

Annova notes an IBM system to stop drivers falling asleep at the wheel. It asks you questions and if you fail to respond promptly, it shoots a jet of cold water over you. http://www.ananova.com/news/story/sm 355015.html

In the time-honoured phrase, "the RISKS are obvious". I wouldn't like to imagine the consequences if a driver was unexpectedly soaked with ice water during a high-speed overtaking manoeuvure on a motorway...

[FORDing the flood? CHEVY to the levee? NOVAcaine mutiny? PGN]

Category 4D Funny / miscellaneous
2002-01-29 search engine play game bandwidth denial-of-service attack resource exploitation
saturation

NewsScan

GOOGLEWHACKING GAINS POPULARITY

Googlewhacking -- an offbeat pursuit of bored Web surfers -- is increasing in popularity and spawning its own legion of enthusiasts. The game starts by typing two unrelated words, such as colonoscopy and cockatiel, into Google's search bar, with the goal of obtaining a single result. The challenge is to find two words so disparate that only one match will occur among Google's 3 billion indexed Web pages. The idea originated with Gary Stock, who tracks the trend on his Web site (http://www.unblinking.com/heh/googlewhack.htm). "It used to be people wandered around the Web, but today people find themselves a space and stay there too much," says Stock. "To me, this is a good way to get people to learn." (CNet News.com 29 Jan 2002)

http://news.com.com/2100-1023-825602.html

Category 4D Funny / miscellaneous

2002-02-08 geek humor music rock 'n' roll logic gates circuit design

NewsScan

COMPUTERS AND ROCK 'N' ROLL: THAT'S WHAT IT'S ALL ABOUT

In the current issue of Computer magazine, former Intel computer architect Bob Colwell has an amusing piece on the relation between computers and rock 'n' roll, and here's a sample: "I particularly like spotting the correspondences between the arts and sciences. For example, you might not think a rock musician would understand what an inverter logic gate does, but apparently Eric Clapton does in his song 'Opposites': "Night after day, day after night./White after black, black after white./Fight after peace, peace after fight./Life after death, death after life." Colwell comments that "Clapton clearly understands that there is a time delay involved in propagating through the gate – hence the word 'after.' When he figures out AND and OR gates, Clapton will be able to devise entire computers in his lyrics. Wait – maybe that's what 'I Shot the Sheriff' is all about. Never could figure out why it was okay to shoot the sheriff but not the deputy. But that construction is very clearly a conjunctive logical expression (S AND NOT D – hey, maybe that's why he needed the inverter)." To explain functional languages, Colwell analyzes the lyrics of "The Locomotion": "Ev'rybody's doin' a brand new dance now./ C'mon baby, do the locomotion./ I know you'll get to like it if you give it a chance now./ C'mon baby, do the locomotion." And vector processing? Well, what better example than "The Hokey Pokey": "You put your right foot in,/ You put your right foot in,/ And you shake it all about./You do the Hokey-Pokey,/ And you turn yourself around./That's what it's all about!" (IEEE Computer Feb 2002)

http://www.computer.org/computer/homepage/0202/ar/index.htm