

HNS Newsletter
Issue 52 - 26.02.2001
<http://net-security.org>
<http://security-db.com>

This is a newsletter delivered to you by Help Net Security. It covers weekly roundups of security events that were in the news the past week. Visit Help Net Security for the latest security news - <http://www.net-security.org>.

Subscribe to this weekly digest on:
<http://www.net-security.org/text/newsletter>

Archive of the newsletter in TXT and PDF format is available here:
<http://www.net-security.org/news/archive/newsletter>

Table of contents:

- 1) General security news
- 2) Security issues
- 3) Security world
- 4) Featured books
- 5) Security software
- 6) Defaced archives

General security news

THE TERRORISM ACT 2000

The Terrorism Act 2000 is designed to prevent dissident political groups from using the United Kingdom as a base for terrorism and recognises a new threat from cyberterrorists for the first time. But the Act also significantly widens the definition of terrorism to include those actions that "seriously interfere with or seriously disrupt an electronic system".

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2001/7/ns-21060.html>

BIOMETRICS: THE TIGHTROPE

At first look, biometrics is a mighty fortress. Or, does that initial impression overlook some subtle problems with the technology? If the prime directive of all security practice dictates that no security system is perfect, then biometrics definitely has shortcomings. To understand those problems, explaining two concepts becomes essential.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/biometrics20010220.html>

THE SMOKED CREW FAQ

"With all the recent media attention that the "smOked crew", an online group of web defacers, has been getting it was time to ask a couple of important questions. We've never done an interview of defacers before, but my curiosity gets the best of me quite often."

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cipherwar.com/news/01/smOked_crew.htm

EASY INTERNET SHARING NHF: VERSION 1.0

"This is a tutorial on sharing your Internet connection by configuring a Linux machine as your gateway/firewall. I've made this tutorial as easy as possible so that the average newbie can have a running and secure mini-home network. I'm sure you've probably been told that setting up firewall rules and IP masquerading can be difficult. Not so, as you will find out. In fact, we won't even be learning a single firewall rule."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://linuxnewbie.org/nhf/intel/network/eznetsshare.html>

PGP CREATOR ZIMMERMANN JOINS HUSH

One of the founding fathers of modern cryptography, Phil Zimmermann - who created PGP and thus introduced a generation of computer users to email encryption - has left the security firm Network Associates to join Irish-based encryption startup Hushmail. Zimmermann was at the forefront of the battle to give ordinary Internet users access to email encryption in the 1990s. When he released the first version of PGP in 1991, Zimmermann faced a three-year FBI investigation. Encryption was still viewed as a threat to the US government's intelligence operations and classified military munitions.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2001/7/ns-21079.html>

THE STATE OF MUSIC SECURITY

Recently, the digital rights management crowd got a sharp lesson from the entertainment industry. No more proprietary systems and hard-to-use digital rights management systems that consumers can't understand. Instead, they want clearinghouses where their content can be safely stored and streamed to end users who don't have to decipher which media player will work.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/business/0,1367,41874,00.html>

THEY REVEAL HIDDEN MESSAGES

U.S. government agencies, including the NSA and the Pentagon, are quietly funding research into steganalysis: the study of detecting hidden messages inserted into MP3 or JPEG files. What have they found? Current steganography programs don't work that well at all.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,41861,00.html>

CONFIGURING A QUICK-AND-DIRTY ROUTER AND PROXY

Setting up an unsecured router and proxy using IP Masquerading; plus, contrary to popular belief, Linux can play nice with PCI modems.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://linuxworld.com/linuxworld/lw-2001-02/lw-02-geek_2.html

ZIXMAIL SECURE DOCUMENT DELIVERY

ZixMail is a secure document delivery, private email and message tracking service that enables you to easily send encrypted and digitally signed

communications to any email address in the world. This means that only your intended email recipients will be able to open messages that you have sent.

Link: <http://www.security-db.com/product.php?id=324&cid=65>

NSA CHIEF SAYS BIN LADEN HAS SUPERIOR TECHNOLOGY

Islamic terrorist Osama bin Laden has superior technology at his disposal than the National Security Agency, the head of the super-secretive spy agency has told an American documentary programme. Superior technological capabilities helped bin Laden to mastermind the simultaneous 1998 bombings of US embassies in Kenya and Tanzania that killed 224 people, said General Mike Hayden, head of the NSA, during an interview to be broadcast tonight on CBS' 60 Minutes II news show.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17072.html>

PANIC OVER VULNERABILITIES

The recent discovery of vulnerabilities in BIND quickly escalated from a reasonable security concern to widespread panic. In this week's Unix Security, Dev Zaborav looks at the increasing sensationalism that surrounds Internet security and worries that too many cries of emergency will leave administrators distrustful when critical situations actually arise.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sunworld.com/unixinsideronline/swol-02-2001/swol-0216-unixsecurity-dv.html>

NET ANONYMITY FIRMS SEEK THEIR MARKET

As an Internet user and online shopper, you may have more in common with your friendly neighborhood spook at the CIA than you think - both you and the agents who look out for your national security are concerned about remaining anonymous online. Unlike the CIA, you probably won't have to pay for it in the next few years - as long as the companies offering these tools can stay in business...

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computeruser.com/news/01/02/20/news15.html>

IS YOUR WEB SERVER RUNNING UNNECESSARY SOFTWARE?

This article quickly shares some ideas on how beginning webserver administrators can improve server efficiency, ease management and, hopefully, improve security as well. It gives a few examples of processes that don't need to be running, required programs and some ideas for BSD and System V-type systems for disabling startup scripts. This article doesn't go into great detail, but will give the newbie administrator some basic ideas.

Link: http://apachetoday.com/news_story.php?itsn=2001-02-20-003-06-PS-LF-AD

FBI AGENT SOLD SURVEILLANCE/NUKE DATA TO RUSSIA

FBI Special Agent Robert Philip Hanssen, aged 56, was placing a packet of classified information at a dead drop site near his residence in suburban Virginia Sunday night when the Feds collared him, much to his surprise. Hanssen gave his Russian handlers over 6,000 pages of secret and top secret documents, according to a detailed, 103-page FBI affidavit in support of a request for search and arrest warrants.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17078.html>

VENDOR KEY MANAGEMENT

Times sure do change. I remember when Linux was new, a "hacker's" OS. We had to walk 10 miles, uphill, to get install floppies for it. (Actually I was lucky, I only had to copy them my friend downloaded the Slackware images over a 9600 modem.) Back then security wasn't much of an issue for most Linux users. We used telnet, and we liked it. Software updates either consisted of downloading the source and compiling it, or using extremely simple package management such as Slackware provides (although calling tarballs package management does seem kind). GnuPG didn't exist, and PGP was still only used by a minority (an even smaller minority than today, if you can believe that).

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/closet/closet20010221.html>

BIOMETRIC SECURITY FOR E-BUSINESS

Computer Associates International and DataTreasury Corp. said they have formed an alliance to provide biometric security – which uses identifying traits like fingerprints, iris scans and voice patterns – to protect e-business transactions. The two companies said they hope to market the system to businesses that manage information worldwide, including healthcare organizations that hold sensitive data about patients. Computer Associates describes itself as an e-business management company, while DataTreasury said it is a data broker that operates a biometrics information clearinghouse.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/162257.html>

EARTHLINK SLOW TO ADMIT ATTACK

Crackers broke into Internet service provider Earthlink's network last week, but the company kept it quiet because it claims customer data was not compromised. A company spokesman said that it did not alert subscribers because the main security system remained intact, but a Wired News tipster said the crackers created a potentially dangerous backdoor to the system.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/business/0,1367,41934,00.html>

SECURING YOUR SOLARIS SERVER

Systems administrators are often too busy with their day-to-day work to concern themselves with system security. That means servers may end up without the latest security patches or fixes, offering easy ways for attackers to gain entry into their systems. In this Unix Insider feature, Jamie Wilson helps you secure your Solaris server by demonstrating how to disable inetd, secure su, find and secure setuid and setgid files, and install and configure ipfilter.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sunworld.com/unixinsideronline/swol-02-2001/swol-0216-hardening.html>

STUDYING FTP TRAFFIC

This is the second article in a three-part series devoted to studying normal traffic. Many intrusion detection analysts concentrate on identifying the characteristics of suspicious packets. However, it is also important to be

familiar with what normal traffic looks like. A great way to do this is to generate some normal traffic, capture the packets and examine them. The first article in this series explained how to capture packets using WinDump and reviewed some simple examples of normal TCP/IP traffic. In this article, we will be examining FTP traffic, which, from a traffic flow standpoint, is more complicated than many other protocols.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/ids/articles/normaltraf2.html>

PRACTICE SAFE INTERNET SHOPPING

If there is one thing to blame for the slow adoption of Internet commerce, it's the age-old credit card. Many consumers are simply afraid to use it online. And they have reason. A report released Monday by the European Commission revealed that credit card fraud ballooned last year by approximately 50 percent in Europe amid an increase in Internet commerce transactions. The study follows repeated news reports of attacked credit card databases and failed security at a number of high-profile Internet sites.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.upside.com/Ebiz/3a9454365.html>

NET FILTERING LAW DRAWS FINAL COMMENTS

Regulators accepted final public comments on a new law requiring libraries and schools that accept federal funds to install computer filters aimed at blocking access to adult material online. Librarians and educators criticized the law, saying it may be impossible to enforce. But conservative groups praised the plan, saying it will save children from finding pornography on the Internet.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/newsbursts/0,7407,2689132,00.html>

ELIMINATING IP ADDRESS FORGERY

"It seems that eliminating IP address forgery is now all the rage because it is now affecting enough people who are important enough to get the whole Internet to take action. And it is indeed gratifying to see this - despite the frustration I suffer over the lack of citation to my original paper on the subject and my firewalls course that has covered this subject in detail for the last five years."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.all.net/journal/netsec/0005.html>

NETMAX FIREWALL WORTH THE FICKLE INSTALLATION

NetMAX FireWall from Cybernet Systems is a smooth-running, easily configurable firewall, if you can get past its annoying setup and installation. I'd like to mention some useful-looking features that I was unable to test. NetMAX FireWall includes a traffic monitor that logs and graphically displays all traffic over the network. That kind of monitoring could be very useful -- not only for ISPs, but in almost any corporate setting. If the quarterly report is due in an hour, but bandwidth seems a little slow, pop up the bandwidth report and find out that Johnny is on Napster again.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxworld.com/linuxworld/lw-2001-02/lw-02-netmax.html>

DECSS UPDATE

In a filing submitted to the 2nd U.S. Circuit Court of Appeals in New York, the Justice Department lashed out at hackers and praised a lower court ruling that bans hacker magazine 2600 from publishing a code known as DeCSS.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2689144,00.html)

[bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2689144,00.html](http://www.zdnet.com/zdnn/stories/news/0,4586,2689144,00.html)

ENGINEER PLEADS SELF DEFENCE IN HACKING CASE

The Criminal Investigation Bureau referred to prosecutors a computer engineer who allegedly hacked into a computer server in what he called "self-defense."

The Hsinchu computer engineer, surnamed Fan (S), said he thought that the other side attacked his computer first, while the truth was that the other side was an innocent party which had been attacked by a Trojan horse. A man last year reported to the police that a Web site which teaches magic and is run by him, had been hacked. He said some Web pages had been altered and some registered users' access to the Web site blocked.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.taipetimes.com/news/2001/02/21/story/0000074560)

[bin/news.cgi?url=http://www.taipetimes.com/news/2001/02/21/story/0000074560](http://www.taipetimes.com/news/2001/02/21/story/0000074560)

TIME TO UN-BIND YOUR NETWORK!

This post by D. J. Bernstein, author of djbdns, a "secure" DNS server, wrote this message prompted by the recent problems experienced with BIND 9 and its "300000 lines of bad code." "BIND 9 is good code, you say? The BIND programmers learned their lesson from these security disasters and rewrote everything from scratch?" Professor Bernstein's opinion differs...

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxsecurity.com/articles/server_security_article-2566.html)

[bin/news.cgi?url=http://www.linuxsecurity.com/articles/server_security_article-2566.html](http://www.linuxsecurity.com/articles/server_security_article-2566.html)

WEF HACKER ARRESTED

Swiss police arrested a man today on suspicion of hacking into the computer systems of the World Economic Forum and stealing private information about participants.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://abcnews.go.com/sections/scitech/DailyNews/hacker010223.html)

[bin/news.cgi?url=http://abcnews.go.com/sections/scitech/DailyNews/hacker010223.html](http://abcnews.go.com/sections/scitech/DailyNews/hacker010223.html)

STORY OF MICROSOFT 'HACK'

A top Microsoft executive revealed how a hacker was able to view some of the company's top-secret source code last October. The attacker gained broad access because an employee forgot to create a password when configuring a server, leaving the password blank.

Link: [http://seattletimes.nwsourc.com/cgi-](http://seattletimes.nwsourc.com/cgi-bin/WebObjects/SeattleTimes.woa/wa/gotoArticle?zsection_id=268448455&text_only=0&slug=hack23&document_id=134269414)

[bin/WebObjects/SeattleTimes.woa/wa/gotoArticle?zsection_id=268448455&text_only=0&slug=hack23&document_id=134269414](http://seattletimes.nwsourc.com/cgi-bin/WebObjects/SeattleTimes.woa/wa/gotoArticle?zsection_id=268448455&text_only=0&slug=hack23&document_id=134269414)

FIGHTING CHILD PORN

Tony Blair and George Bush are to lead a global crusade against the internet perverts who peddle child porn. The Prime Minister and the President sealed the deal during late night talks at Camp David at the end of their two-day summit. Mr Blair's government will immediately reinforce the deal with new tough laws on Internet paedophiles, to be announced in the House of Commons on Monday.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsoftheworld.co.uk/news/4165837)

[bin/news.cgi?url=http://www.newsoftheworld.co.uk/news/4165837](http://www.newsoftheworld.co.uk/news/4165837)

INSURANCE AGAINST CYBER ATTACKS

An internet user or ISP in India, so far, has no option if threatened by an attacker except to lodge a police complaint and change the profile of the internet service. Soon, Net users and ISPs can have insurance cover against cyber attacks. For the first time in India, insurance is being offered against all kinds of cyber crime, including loss of airtime, to the extent of \$25 million. The insurance package, which was introduced in the US, UK and Japan last year, will be brought to India by Tata-AIG, a joint venture by the Tatas and American Insurance Group Incorporate.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.indian-express.com/ie/daily/20010226/ina26039.html>

SURFINGATE AGAINST MALICIOUS WEB CONTENT

SurfinGate provides proactive gateway security for malicious Web content including ActiveX, Java, Visual Basic Script and JavaScript. Using a sophisticated real-time content-inspection process, SurfinGate identifies and blocks malicious code without relying on database updates. Centrally managed, SurfinGate allows companies to tailor policies for departments and users and enables secure e-business.

Link: <http://www.security-db.com/product.php?id=606&cid=132>

IDS REVIEW: INTRODUCTION

IDSes as we know them today are a relatively new phenomenon in the computer security field, but they have been improving rapidly and quickly becoming more complex, making them difficult for non-specialists in security to understand, and similarly difficult to judge when you are entertaining the thought of purchasing one. This article is intended to help you understand what these boxes are and give you some hopefully :-) informed opinions about the leading products on the market and what applications make sense for each.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/idsintroduction20010226.html>

Security issues

All vulnerabilities are located at:
<http://net-security.org/text/bugs>

RED HAT LINUX - NEW VIXIE-CRON PACKAGES

New vixie-cron packages are available that fix a buffer overflow in the 'crontab' command; this could allow certain users to gain elevated privileges.

Link: <http://www.net-security.org/text/bugs/982685081,35659,.shtml>

IMMUNIX OS - VIXIE-CRON UPDATE

Immunix has tested the versions of the vixie-cron packages that are shipped with Immunix OS 6.2, 7.0-beta, and 7.0 and they are not vulnerable to the buffer overflow (due to the use of the StackGuard compiler). However, we are making updated packages available for those users who want to upgrade.
Link: <http://www.net-security.org/text/bugs/982754741,49344,.shtml>

SECURITY FLAW IN TELOCITY'S "GATEWAY MODEM"

Telocity provides DSL to their customers through what they call the Telocity "Gateway Modem". In the modems, you can connect to them through your web browser to view usage statistics, your assigned IP, the DHCP server IP (Modems IP), Management's IP (Modem's IP, different than the previous), DNS IP, and the hardware software version information. In the older model modem, it is possible to remotely view the "Details" section of the modem, thus revealing all the above mentioned information to a possible intruder. Telocity has numbered their gateways in sequential order, so it would be possible to write a script that would search for <http://123.123.123.1/stats> in a range of addresses.

Link: <http://www.net-security.org/text/bugs/982781361,33018,.shtml>

LINUX MANDRAKE - VIXIE-CRON UPDATE

A buffer overflow exists in the 'crontab' command if it was called by a user with a username longer than 20 characters. If the system administrator has created usernames of that length, it would be possible for those users to gain elevated privileges.

Link: <http://www.net-security.org/text/bugs/982858260,74013,.shtml>

NT DRIVERS AND FORMAT STRING BUG

Many NT drivers are potentially vulnerable to "format string bug". The problem is concerned with DbgPrint function that is used for debug messages. Some drivers instead of directly call of this function use additional intermediate functions. Those functions add a prefix to an outputted string, resolve a string format and pass the final string to DbgPrint. Note the DbgPrint also additionally resolves format specifications.

Link: <http://www.net-security.org/text/bugs/982858351,64712,.shtml>

WIN2K DIRECTORY SERVICES WEAKNESS

"We came across one security issue; which may be critical for large organizations planning to deploy Windows 2000 and Active Directory in one forest. Imagine that there is a forest with more than one domain. (Tree hierarchy does not matter in this situation.) Every domain has its own set of administrators. In Active directory there is one Configuration Container for the whole forest. So every domain controller has its own copy of Configuration Container and is able to change it and replicate changes to other domain controllers. The only obstruction for changing configuration are ACLs. But ACLs are checked on local system and if you somehow modify it to avoid this checking, you can modify this Container."

Link: <http://www.net-security.org/text/bugs/982858422,97626,.shtml>

TURBOLINUX - BIND UPDATE

Two vulnerabilities have been discovered in ISC BIND 8. Please update the packages in your installation as soon as possible.

Link: <http://www.net-security.org/text/bugs/982910525,58182,.shtml>

LINUX MANDRAKE - CUPS UPDATE

A number of problems were found by the SuSE security team recently during an internal audit of the CUPS printing package. These problems have been resolved with the latest CUPS release which include temp file creation vulnerabilities, potential buffer overflows, and other security enhancements. It is highly recommended that all Linux-Mandrake users upgrade to this new version of CUPS.

Link: <http://www.net-security.org/text/bugs/982910560,1837,.shtml>

SEDUM V2.1 HTTPD - DENIAL OF SERVICE

SEDUM v2.1 is vulnerable to a nasty Denial of Service attack where it can be flooded with useless junk until the server crashes promptly. Once it has been crashed it needs to be restarted again for it to work properly. All windows versions appear to be affected.

Link: <http://www.net-security.org/text/bugs/983031499,96065,.shtml>

MERCUR MAILSERVER 3.3 BUFFER OVERFLOW

By default SMTP server is installed to be run from LocalSystem account. This makes it easy to make any action on the target system if an attacker could gain control over the code execution flow of the product.

Link: <http://www.net-security.org/text/bugs/983031584,54993,.shtml>

Security world

All press releases are located at:
<http://net-security.org/text/press>

ITALIAN PETROLEUM GIANT CHOSSES SECURE COMPUTING - [21.02.2001]

Secure Computing announced that its SafeWord Plus authentication and authorization solution will be used by the Italian petroleum company, AgipPetroli Spa, to add strong security to all of its present and future intranet applications. AgipPetroli, an ENI Group company, operates in the oil, natural gas, petrochemicals, oilfield services and engineering industries, and is one of the largest natural gas companies in the world with operations in many countries.

Press release:
< <http://www.net-security.org/text/press/982725334,11543,.shtml> >

BALTIMORE TECHNOLOGIES CHOSEN BY EORIGINAL - [21.02.2001]

Baltimore Technologies, a global leader in e-security, announced it has

been chosen by eOriginal, the leading provider of Electronic Negotiable Instrument Software Solutions, to be included in the development of a trusted security infrastructure for the real estate financing, equipment and vehicle leasing, and the trade and transportation industries. Baltimore's award winning technology will enable eOriginal to deliver a secure and trusted environment for eOriginal's business partners to execute critical transactions, and trade or transfer legally enforceable electronic negotiable instruments and securities such as electronic mortgages, leases, bills of lading, letters of credit, regulatory filings and stock certificates.

Press release:

< <http://www.net-security.org/text/press/982755394,25511,.shtml> >

ZERO-KNOWLEDGE SYSTEMS INTRODUCES PRIVACY EYE - [21.02.2001]

Study after study indicates that consumers value their privacy, but they are often unaware of personal privacy intrusions and unsure of how to protect themselves. To empower individuals with valuable privacy information, Zero-Knowledge Systems today introduced Privacy Eye, a digital source of privacy news and commentary edited by author, journalist and privacy expert Tom Maddox. Whether they are average citizens with questions and concerns or informed privacy advocates, readers of Privacy Eye will find valuable privacy resources from the Web site (<http://privacy.zeroknowledge.com/privacyeye/>), including:

- * Expert commentary on privacy issues from Editor-in-Chief Tom Maddox
- * The most recent privacy headlines
- * Information about how consumers can protect their privacy online

Press release:

< <http://www.net-security.org/text/press/982848200,50350,.shtml> >

CISCO TEAMS UP WITH VIGILANTE - [22.02.2001]

The E-Business Security Forum 2001 is organized by Cisco and associated companies involved in the European data security market (VIGILANTE, RSA, MIMESweeper, Arthur Andersen, Websense, Netforensics, Tripwire). The goal of the roadshow is to bring together speakers from a variety of technology, consulting and related backgrounds to provide customers with a clear set of perspectives on how to secure their data networks in the E-Business world. The roadshow is FREE for all attendees and will be visiting a total of 12 European cities over the course of 3 weeks during Feb-Mar 2001. Be one of the expected 2,500 people to experience this exciting and informative event!

Press release:

< <http://www.net-security.org/text/press/982851597,49360,.shtml> >

ODYSSEY - DEPLOYING CA'S UNICENTER TNG - [22.02.2001]

Computer Associates International, Inc. announced that Odyssey Technology, Inc. (Odyssey), an innovative developer of IT-focused business solutions for

the retail industry, is deploying CA's Unicenter TNG to manage a revolutionary turnkey Web-based marketing solution. By providing a fully integrated solution for controlling Odyssey's highly dynamic eBusiness infrastructure, Unicenter TNG will ensure a highly available and secure environment in which consumers, retailers, manufacturers and national brands can conveniently exchange information and efficiently conduct transactions.

Press release:

< <http://www.net-security.org/text/press/982852099,26710,.shtml> >

SAFENET - SECURE 3 REMOTE ACCESS PROGRAM - [22.02.2001]

SafeNet, Inc., a leading provider of Internet security technology that is the de facto standard in the VPN industry, today announced the introduction of the SafeNet Secure 3 Program. Through this program, preferred customers can be assured that they have continued access to SafeNet's industry-leading remote access client software. Program participants will get SafeNet's new product, SoftRemote, which includes several important new features like support of industry-standard Smart Cards, full-featured personal firewall capabilities, centralized management, and enhanced interoperability. In addition, preferred customers will have the ability to input into the future direction of SoftRemote.

Press release:

< <http://www.net-security.org/text/press/982875227,80539,.shtml> >

TUMBLEWEED GRANTED PATENT FOR PRIVATE URLS - [23.02.2001]

Tumbleweed Communications Corp., a leading provider of mission critical messaging solutions, today announced that the U.S. Patent and Trademark Office granted the company patent no. 6,192,407, which protects private, trackable URLs for directed document delivery. The private URL technology is included in Tumbleweed Integrated Messaging Exchange™ (IMETM), a platform and set of applications for creating secure communications channels between a business and its customers, partners, and suppliers. Tumbleweed IME generates a private URL for each secure delivery. The private URL that IME creates is unique, tied to the sender of the package or transaction, to the content being sent, and to the intended recipient. In practice, the private URL binds the recipient's e-mail identity to the content being sent, assuring that the information being sent is delivered only to the intended recipient. The private URL also binds a recipient's e-mail identity to an on-line transaction, facilitating authentication for both business-to-consumer and business-to-business online commerce.

Press release:

< <http://www.net-security.org/text/press/982910862,83436,.shtml> >

CAMELOT'S NETWORK INTELLIGENCE TECHNOLOGY - [24.02.2001]

Camelot today announced the launch of Hark! automated access control solution into the marketplace. Based on groundbreaking Network Intelligence technology, Hark! solves the problem of defining, managing and enforcing access control in

today's interconnected e-business world. Developed by Israel-based Camelot, the Network Intelligence technology utilizes proprietary, advanced discovery algorithms to analyze network events and deduce the functional structure of an organization, extracting and mapping the relationship between users and various network resources.

Press release:

< <http://www.net-security.org/text/press/983031879,1997,.shtml> >

Featured books

The HNS bookstore is located at:
<http://net-security.org/various/bookstore>

Suggestions for books to be included into our bookstore can be sent to staff@net-security.org

INFORMATION SECURITY RISK ANALYSIS

Risk is a cost of doing business. The question is, "What are the risks, and what are their costs?" Knowing the vulnerabilities and threats that face your organization's information and systems is the first essential step in risk management. This book shows you how to use cost-effective risk analysis techniques to identify and quantify the threats - both accidental and purposeful - that your organization faces. You can find books that cover risk analysis for financial, environmental, and even software projects, but you will find none that apply risk analysis to information technology and business continuity planning or deal with issues of loss of systems configuration, passwords, information loss, system integrity, CPU cycles, bandwidth, and more. Information Security Risk Analysis shows you how to determine cost effective solutions for your organization's information technology.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0849308801/netsecurity> >

SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS

The first quick reference guide to the do's and don'ts of creating high quality security software. Ross Anderson, one of the world's foremost authorities on security design for such companies as Microsoft, Intel, and VISA, presents a comprehensive security design tutorial that covers the complete suite of security applications referred to as "end2end" security. Designed to meet a growing, critical need among today's programmers, most of whom have no security training but need to build better "mousetraps", this book illustrates basic concepts of security engineering through real-world examples, including system design successes and failures. It provides security designs tips, tricks, and, sometimes, even secrets from military and medical records to Internet

intrusion detection and burglar alarms. The author explains how to use a wide range of security tools, including cryptography, DES, AES, Skipjack, Unix passwords, hash functions, stream ciphers, and public keys to build secure, crime-fighting, virus-proof security systems for industry.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0471389226/netsecurity> >

CRYPTOGRAPHY AND E-COMMERCE: A WILEY TECH BRIEF

Cryptography basics for non-technical managers working with e-business products and services. With more and more companies vying for e-commerce market share, the competitive edge belongs to those who can offer the best and most secure services over the Internet. This book offers a handy, quick reference guide to cryptography--the enabling technology for secure Internet based transactions. The author takes the mystery out of the math, injects humor, and provides clear, easy-to-understand explanations and case studies. Graff responds to the growing need among managerial and sales and marketing staff for a brief, non-technical version of Bruce Schneier's Applied Cryptography. The author draws on a successful presentations given at Cylink, Amdahl, Wells Fargo, KPMG Peat Marwick, Deloitte & Touche, and NetReliance. Topics covered include keys & management, Kerberos, Window 2000 security, PKI, cryptography protocols, certificates, digital signatures, and government policy.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0471405744/netsecurity> >

THE INTERNET SECURITY GUIDEBOOK: FROM PLANNING TO DEPLOYMENT

This book provides a complete analysis of an enterprise's Internet security. Strategies, steps, and procedures for conducting business securely on the Internet are discussed and reviewed. Very few organizations take the needed precautions to protect their Internet enterprise. Protection is not simply a firewall or technology; it is a strategy that encompasses risk, trust, business goals, security processes, and technology. The holistic approach offered in this book evaluates security needs in relation to business goals and the current attacks on the global Internet. The goal of The Internet Security Guidebook is to protect the business-computing environment by keeping our online enterprises functioning correctly and securely. Unlike other books available, this book contains a complete guide to Internet security that is accessible to both novices and computer professionals. The specific steps discussed and illustrated show the reader how to implement security from the individual process to the complete corporate enterprise. The reader will also learn about resources that can help such as the CERT, the FBI, and even their own software vendors.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0122374711/netsecurity> >

INFORMATION HIDING: STEGANOGRAPHY AND WATERMARKING - ATTACKS AND COUNTERMEASURES (ADVANCES IN INFORMATION SECURITY, VOLUME 1)

This book deals with information hiding. With the proliferation of multimedia on the Internet, information hiding addresses two areas of concern: privacy of information from surveillance (steganography) and protection of intellectual property (digital watermarking). Steganography (literally, covered writing) explores methods to hide the existence of hidden messages. These methods include invisible ink, microdot, digital signature, covert channel, and spread spectrum communication. Digital watermarks represent a commercial application of steganography. Watermarks can be used to track the copyright and ownership of electronic media. In this volume, the authors focus on techniques for hiding information in digital media. They analyze the hiding techniques to uncover their limitations. These limitations are employed to devise attacks against hidden information. The goal of these attacks is to expose the existence of a secret message or render a digital watermark unusable. In assessing these attacks, countermeasures are developed to assist in protecting digital watermarking systems.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0792372042/netsecurity> >

Security Software

All programs are located at:

<http://net-security.org/various/software>

AVX FOR ICQ

AVX for ICQ is a FREE utility which uses new technology to intercept; filter, and virus scan all files sent during an ICQ chat session. The new proprietary technology incorporates features found on enterprise-class corporate firewalls. AVX for ICQ uses the same powerful virus protection scan engine incorporated into the AntiVirus eXpert Professional (AVX), a full-featured virus protection application for desktops.

Info/Download:

< <http://www.net-security.org/various/software/983140894,72643,windows.shtml> >

SAFEMAIL V.2.1

SafeMail allows you to communicate and exchange information securely with other people. Based on well known standards, SafeMail will allow you to easily "digitally sign" all messages and files. SafeMail protects your data against any prying eyes while your messages travel through the Internet. In addition, SafeMail automatically compresses messages and files thus saving valuable transmission time.

Info/Download:

< <http://www.net-security.org/various/software/982874633,89644,mac.shtml> >

OPENSSSH 2.5.1P1

This is a Linux/portable port of OpenBSD's excellent OpenSSH. OpenSSH is based on the last free version of Tatu Ylonen's SSH with all patent-encumbered algorithms removed, all known security bugs fixed, new features reintroduced, and many other clean-ups. Changes: Added support for RSA pubkeys, Agent forwarding, remote forwarding, and SFTP. Also includes many bug fixes.

Info/Download:

< <http://www.net-security.org/various/software/983140424,48189,linux.shtml> >

PASSVAULT 3.1

PassVault is a database that will enable you to keep your all your Passwords, Account Numbers, PIN Numbers, Locker Combinations, Credit Card Numbers and more in a consolidated place.

Info/Download:

< <http://www.net-security.org/various/software/983140266,5770,windows.shtml> >

NMAP 2.54 BETA 19

Nmap is a utility for port scanning large networks, although it works fine for single hosts. Sometimes you need speed, other times you may need stealth. In some cases, bypassing firewalls may be required. Not to mention the fact that you may want to scan different protocols (UDP, TCP, ICMP, etc.). Nmap supports Vanilla TCP connect() scanning, TCP SYN (half open) scanning, TCP FIN, Xmas, or NULL (stealth) scanning, TCP ftp proxy (bounce attack) scanning, SYN/FIN scanning using IP fragments (bypasses some packet filters), TCP ACK and Window scanning, UDP raw ICMP port unreachable scanning, ICMP scanning (ping-sweep), TCP Ping scanning, Direct (non portmapper) RPC scanning, Remote OS Identification by TCP/IP Fingerprinting, and Reverse-ident scanning. Nmap also supports a number of performance and reliability features such as dynamic delay time calculations, packet timeout and retransmission, parallel port scanning, detection of down hosts via parallel pings.

Info/Download:

< <http://www.net-security.org/various/software/983140545,60712,linux.shtml> >

Defaced archives

[20.02.2001] - Iraki Satellite Television
Original: <http://www.irakitv.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/20/www.irakitv.com/>

[20.02.2001] - Kolinska

Original: <http://www.kolinska.si/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/20/www.kolinska.si/>

[20.02.2001] - Pension Fund of America

Original: <http://www.pensionfundofamerica.com/>

Defaced:

<http://www.attrition.org/mirror/attrition/2001/02/20/www.pensionfundofamerica.com/>

[20.02.2001] - Laser Technology

Original: <http://www.laser-printer-tech.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/20/www.laser-printer-tech.com/>

[20.02.2001] - Tatung Netherlands

Original: <http://www.tatung.nl/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/20/www.tatung.nl/>

[20.02.2001] - ICQ Groups

Original: <http://groups.icq.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/20/groups.icq.com/>

[21.02.2001] - Adidas de Mexico

Original: <http://www.adidas.com.mx/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/21/www.adidas.com.mx/>

[21.02.2001] - Best Buy Internet

Original: <http://www.bestbuyinternet.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/21/www.bestbuyinternet.com/>

[21.02.2001] - Internet Communication Network

Original: <http://klaatu.fusive.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/21/klaatu.fusive.com/>

[21.02.2001] - Toshiba International Corporation

Original: <http://www.toshiba.com.au/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/21/www.toshiba.com.au/>

[21.02.2001] - Hacker (HK)

Original: <http://www.hacker.com.hk/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/21/www.hacker.com.hk/>

[21.02.2001] - Kentucky State Government

Original: <http://kydisweb1.state.ky.us/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/21/kydisweb1.state.ky.us/>

[22.02.2001] - Governo do Estado de Sao Paulo

Original: <http://www.procon.sp.gov.br/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/22/www.procon.sp.gov.br/>

[22.02.2001] - Le Ministre de l'Agriculture

Original: <http://www.agr.gouv.qc.ca/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/22/www.agr.gouv.qc.ca/>

[22.02.2001] - Hewlett-Packard Company

Original: <http://www.netserver.hp.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/02/22/www.netserver.hp.com/>

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org

<http://net-security.org>

<http://security-db.com>