

Net-Sec Newsletter  
Issue 44 - 01.01.2001  
<http://net-security.org>

[ -- Happy 2001 -- ]

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 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 articles
- 5) Featured books
- 6) Security software
- 7) Defaced archives

General security news

-----

-----

#### EGGHEAD.COM SYSTEM COMPROMIZED

"Egghead.com has discovered that a hacker has accessed our computer systems, potentially including our customer databases," the company said in a statement released yesterday.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.timesofindia.com/today/24info5.htm>

#### KASHMIR RELATED DEFACEMENTS

More than 40 Indian sites have been infiltrated this year by hackers like G Force Pakistan and Doctor Nuker, who have left poignant pro-Pakistan slogans and reasons why Kashmir belongs to that country. Wired has the report.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,40789,00.html>

#### PC GUARDIAN ENCRYPTION PLUS HARD DISK

Once Encryption Plus Hard Disk is installed on a user's computer, the system will not boot without the user's password. Even if an experienced user were to somehow work around the boot protection and access the hard disk, s/he would only be able to read file names. The data would remain encrypted. This feature alone should make encryption practically mandatory for notebook users.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.canadacomputes.com/v3/story/1,1017,5163,00.html>

#### INFORMATION SYSTEMS AND SURVEILLANCE

The miniaturization of electronic equipment and the advances in the production of armaments and computer science equipment, thanks to technological advances of knowledge and Information Systems (IS) have led some theoreticians to define war of the information era as digital war.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://cryptome.org/omni-is-spy.htm>

#### THE LINUX YEAR IN REVIEW

Linux Weekly News has put together a great summary of the major events surrounding Linux and open source over the past year. Continuing the popular tradition of our 1998 and 1999 Linux Timelines, here is our attempt to summarize what has happened in the Linux world over the last year. This is version 0.8.3 of the LWN 2000 Linux Timeline.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.lwn.net/2000/features/Timeline/>

#### SECURITY-ENHANCED LINUX

As part of its Information Assurance mission, the NSA has long been involved with the computer security research community in investigating a wide range of computer security topics including operating system security. The results of several previous research projects in this area have been incorporated in a security-enhanced Linux system. This version of Linux has a strong, flexible mandatory access control architecture incorporated into the major subsystems of the kernel. The system provides a mechanism to enforce the separation of information based on confidentiality and integrity requirements. This allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can be caused by malicious or flawed applications.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nsa.gov/selinux/>

#### ESTABLISHING EMAIL VALIDITY

Scenario: Christmas morning you get an angry phone call from one of your contractors. They claim to have received an email outlining why you have chosen to terminate their contract, that in no uncertain terms describes relations with their mother, family pet, or what have you. The caller can't believe how rampantly unprofessional this message is, and has already contacted their legal department about suing for damages and breach of contract. All of this information has taken you completely by surprise. As far as you know, no message has been sent by anyone at your company, especially given that you're the only employee currently employed by your company. How can you prove that no email was sent by you? How can you demonstrate in a court that no such email has originated from your system? What if it has? Can you prove that you were not the sender?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityportal.com/cover/coverstory20001225.html>

#### ONLINE SECURITY KEY TO EMBRACING SMART CARDS

Imagine a single card that lets you purchase and download an airline ticket using your PC. That same piece of plastic could also pay for a restaurant lunch,

open secure doors at the office, check out books at the library. It could even become your car keys. Sound like a script from the Jetsons? Not really. Thanks to the improving power and versatility of microprocessors embedded in the cards, consumers will not only be able to better protect themselves against online fraud as they bank or trade stocks. They will also be able to store digital cash, personal information, Web site passwords and addresses, and such things as loyalty coupons from merchants or frequent flyer points.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2000/TECH/computing/12/25/smart.cards.ap/index.html>

#### LINUX SECURITY WEEK

This week, advisories were released for ed, stunnel, bitchx, zope, nano, slocate, procps, oops, half lifeserver, ethereal, netscape, pam, jppilot, rp-pppoe, kerberised telnetd, ftpd, gnupg, mysql, and tcsh. The vendors include Conectiva, Debian, FreeBSD, Mandrake, NetBSD, OpenBSD, Red Hat, and Trustix.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxsecurity.com/articles/forums\\_article-2186.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxsecurity.com/articles/forums_article-2186.html)

#### STIFFER PENALTIES IN HONG KONG

Hong Kong police on Monday warned would-be computer hackers of the territory's stringent penalties against cybercrimes. The caution came as official figures showed a 300 percent increase in the number of people connected to the Internet across the territory in the last two years.

Link:

<http://www.dotcomdirectory.newsalert.com/bin/story?StoryId=CoKBuueibntaWmJKZndi2>

#### "ANTITRUST" - HOLLYWOOD FILM ON TECH INDUSTRY DUE

"AntiTrust," a new motion picture from MGM scheduled to hit theaters Jan. 12, 2001. Tim Robbins plays Gary Winston, the brilliant and driven mastermind behind N.U.R.V., which stands for "Never Underestimate Radical Vision," a software company dedicated to monopolizing digital convergence. Winston dazzles promising young computer science student Milo, played by Ryan Phillippe, into abandoning his plans to launch a start-up company with his college buddy and come work for N.U.R.V. Winston's mantra is, "In this business, you are either a one or a zero." At the heart of N.U.R.V. is the Synapse project, which is described as the world's first satellite-delivered global communications system. "AntiTrust" explores the issues of surveillance, corporate espionage and intellectual property theft.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computeruser.com/news/00/12/26/news20.html>

#### ETISALAT HACKING

The lawyer representing a young Briton accused of hacking into Emirates Telecommunications Corp's (Etisalat) Internet system says he plans to ask the Public Prosecutor to produce its evidence or drop the case.

Link: <http://www.gulf-news.com/Articles/news.asp?ArticleID=5629>

We covered the story closely, so you can find more information here:

<http://net-security.org/cgi-bin/pr0n/viewnews.cgi?searchetisalat>

#### HACKER ATTACKS ON SHARP RISE

Safeguards against hacker attacks are urgently needed, the Korea Information

Security Agency (KISA) said. The Ministry of Information and Communication-affiliated institute said there were a total of 1,858 cases of hacking detected in the nation as of November, more than triple the 572 cases found last year. There were a mere 147 hacker attacks in 1996, and the figure dropped to 64 in 1997. However, cyber crime began rising sharply again, with the figure climbing to 158 in 1998, and 572 last year. KISA noted that corporations appear to be the main target for hacker attacks. Ninety-two, or 40.5 percent of 227 hacker attacks that occurred in November were targeted against corporations, for example. "This is an indication that security systems at Korean corporations are frail and that companies lack mindset for security," a KISA official said.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.koreaherald.co.kr/SITE/data/html\\_dir/2000/12/27/200012270081.asp](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.koreaherald.co.kr/SITE/data/html_dir/2000/12/27/200012270081.asp)

#### BAD DAYS FOR NETWORK ASSOCIATES

Network Associates Inc.'s top three executives, including Chairman and Chief Executive William Larson, resigned suddenly Tuesday, shocking investors, who sliced the company's stock price in half in after-hours trading. As we could see from various news outlets their shares fell for 65% (according to ZDNet), 68% (according to InfoWorld) and 72% (according to Reuters). Below you can read a few articles that are covering the story.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/51/ns-19913.html>

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www0.mercurycenter.com/svtech/news/indepth/docs/networ122700.htm>

Link: <http://www.crn.com/Sections/BreakingNews/dailyarchives.asp?ArticleID=22548>

#### NATIONAL SECURITY RISK

In a report released this month titled "Cyber Threats and Information Security: Meeting the 21st Century Challenge," the Center for Strategic and International Studies (CSIS) concluded that the government and the private sector should be concerned about the "trustworthiness" of future Microsoft products in the aftermath of the hack into the company's network.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idg.net/ic\\_335424\\_1794\\_9-10000.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idg.net/ic_335424_1794_9-10000.html)

#### DEMAND FOR NET-BASED SECURITY PRODUCTS

Demand for Internet-based security products is exploding, as sales reached \$243 million last quarter and are expected to more than double next year, a new study shows.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1004-200-4290053.html>

#### HONG KONG POLICE OFFER CHRISTMAS WARNING TO HACKERS

Computer whizzes in Hong Kong who like to test their skills on the Web sites of others will receive little sympathy from the Hong Kong Police who issued a warning about the consequences of such actions.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computeruser.com/news/00/12/28/news16.html>

#### CRYPTOGRAPHY IN YOUR POCKET

Recently, some announcements have been made of commercial encryption programs for the PalmPilot personal organizer. Some of these were for subroutines that might be used in programs whose primary purpose is not encryption, for purposes such as software registration. Also, Network Associates, the company that owns PGP, has a commercial product, PGPwireless, specifically aimed at those who use their Palm Pilots (and, shortly, other similar devices) to connect to the Internet.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityportal.com/articles/pocket20001228.html>

#### NO MONEY IN HACKERDOM, VERSION 1.0

"ESR has an article that explains some ways for you to become a Hacker. I'm not going to repeat all the points he has in that article, as you can look at that article for the specifics. I am going to make the argument that Hackers do not generally Hack because they have to for work. Instead, it is their passion, their life, in a dramatic way. Also, I'm going to make the argument that, and this is not how ESR feels, Hackers can be non-contributing authors to the code base of the world. That code base is better known as Open Source or Free Software today."

Link: <http://www.linuxpower.org/display.php?id=200>

#### AN INTRODUCTION TO VIRUSES AND MALICIOUS CODE PART TWO

In Part One of this series SecurityFocus.com writer Brad Griffin introduced readers to viruses and other forms of malicious code. He discussed the various ways in which viruses can infect a user's computer and how they can affect a user's important data. This article, the second in a three-part series, will discuss ways of protecting computers against virus infection, including: anti-virus software, proper handling of e-mail and external media such as floppy disks, the dangers of non-essential software, and the necessity of user education.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/basics/articles/malintro2.html>

#### ANTI-DEFAMATION LEAGUE WEB SITE ATTACKED

The ADL Web site was taken over for about 20 minutes by attackers who identified themselves as the "World's Fantabulous Defacers." In lieu of the ADL home page, the attackers posted threats to Israelis as well as pro Palestinian sentiment. The attackers did not gain access to any sensitive information. The group closed the site a few minutes after the attack was discovered, according to an ADL representative. Four hours later, the site was restored.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1007-200-4292972.html>

#### THE STORY OF JEFF: PART VI

This story is the ongoing saga of Jeff, a tragic tale full of hardship, heartbreak and triumph over impossible odds. Jeff is your average network administrator, responsible for Acme, Inc.'s Microsoft-based corporate network. A brightly lit server room. Fans humming quietly, a glass wall at one end; on the other side we see a table with several people sitting around it. Scattered on the table are several pads of paper, pencils, pagers and a laptop. We see Jeff, eyes a healthy shade of bloodshot pink accented by dark bags underneath. Lifting a

cup of cold coffee to his lips, he grimaces and takes a deep gulp, swallowing it hurriedly.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/jeff20001229.html>

#### THE 101 USES OF OPENSSSH: PART I

This month we'll cover ssh's background and architecture, how to build and/or install OpenSSH, how to use ssh as an encrypted replacement for Telnet, how to set some basic ssh configuration options and how to use scp for encrypted file transfers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www2.linuxjournal.com/lj-issues/issue81/4412.html>

#### UPDATE ON EGGHEAD.COM PENETRATION

Egghead.com, the Internet firm that had 3.6 million credit cards compromised before Christmas when security on its e-commerce site was cracked, said it will know by the end of the week whether the hacker managed to steal the financial information of its customers.

Link: <http://www.nationalpost.com/tech/story.html?f=/stories/20001228/418915.html>

#### DAILY NEWS THAILAND DEFACED

The Web site of the Daily News newspaper ([www.dailynews.co.th](http://www.dailynews.co.th)) was defaced late on Tuesday night, the third such break-in in recent years, its webmaster said today. No information was destroyed or altered.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/00/159816.html>

#### BEWARE OF HAPPY NEW YEAR VIRUS

A new e-mail virus is on the loose, according to Computer Associates International. The "Tqll-A" worm is typically found in electronic messages bearing a Happy New Year greeting in the subject field, said Ian Hameroff, business manager for antivirus solutions for Computer Associates. The latest threat, which CA detected at its global research centers, conveys itself via Microsoft Outlook. When people open the "happynewyear.txt.vbs" attachment, the virus then installs itself on the user's hard drive.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.techweb.com/wire/story/TWB20001229S0006>

#### FEDS WARN OF CONCERTED ATTACKS ON NEW YEAR' EVE

Federal computer security experts are urging system administrators to take added precautions in securing Web servers and network firewalls in advance of the New Year's holiday weekend, citing FBI reports indicating an increase in activity that often precedes widespread cyber attacks. Authorities at the National Infrastructure Protection Center - the FBI's cyber crime division - said data gleaned from FBI investigations and other sources indicate that many computer systems may already have been turned into "zombies" waiting for commands from hackers to cripple the Internet.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/00/159873.html>

#### REPORT: MICROSOFT HACK A U.S. SECURITY RISK

Although Microsoft Corp. has denied that the hacker who penetrated its network in October gained access to any of the company's source code, a recent report by a Washington-based think tank is warning that the compromise may hold grave national security implications.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2000/TECH/computing/12/29/csis.microsoft.report.idg/index.html>

#### NEW ATTACK ON DIGITAL PIRACY

Hollywood has teamed up with some of the biggest players in computer storage technology to build a copy-prevention scheme into every hard drive and memory card - opening a new front in the war against online piracy. If widely adopted, the technology would make it more difficult for consumers to duplicate copyrighted files such as music and movies without the permission of the companies that own the rights. Hard drives and memory cards are used to store information on everything from personal computers and MP3 music players to digital cameras and palm-size organizers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www0.mercurycenter.com/svtech/news/indepth/docs/copy122900.htm>

#### LINUXPPC SECURITY PRIMER, PART I

"So you've bought that new G4 you've been eyeing for lo these many months. Or perhaps you've blown the dust off of some aging Performa you've kept in your basement. Either way, you've decided to install Linux on your PowerPC box, but you're worried about some '31337 haxOr d00dz' gaining control of your machine through some security hole. It turns out there's both good news and bad news for you."

Link: [http://linuxppc.org/security/articles/lppc\\_security\\_primer\\_1.php3](http://linuxppc.org/security/articles/lppc_security_primer_1.php3)

#### 'THE ANALYZER' ADMITS SABOTAGE

'The Analyzer' was convicted yesterday by the Kfar Sava Magistrates Court after striking a plea bargain deal with prosecutors. Tannenbaum, a 21 year old Hod Hasharon resident, confessed to offenses of conspiracy, wrongful infiltration of computerized material, disruption of computer use, and destroying evidence.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www3.haaretz.co.il/eng/htmls/kat18\\_2.htm](http://www.net-security.org/cgi-bin/news.cgi?url=http://www3.haaretz.co.il/eng/htmls/kat18_2.htm)

#### SO MANY PREDICT SO MUCH

The three most important tech issues of 2001 will be free speech, privacy and e-money. ISPs will continue to be the targets of governments such as France who want to control what their citizens see and read. Privacy in all instances will be contentious, especially when it comes to genetics. E-money will appear back on the scene as countries other than the United States (for example, Japan), begin to experiment and succeed with viable e-money systems.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,40906,00.html>

-----

## Security issues

---

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

---

### THE END OF SSL AND SSH? FOLLOW-UP

"Well, I certainly managed to kick over a hornet's nest with my article "The End of SSL and SSH?". There were quite a few points I did not cover in the article, many I did not think of, and some I trimmed. This article will cover the reaction to SSL and SSH being "dead", as well as numerous implementation issues I did not cover. The real issue is that technology cannot solve problems completely."  
Link: <http://www.net-security.org/text/bugs/977746823,69115,.shtml>

### 1ST UP MAIL SERVER V4.1 VULNERABILITY

The Ussr Team has recently discovered a Buffer Overflow in 1st Up Mail Server v4.1 where they do not use proper bounds checking. The overflow is in the field "mail from: < ", a large number of aaaaaa's "> (over 300). It then displays this message: "Application popup: smtp server: smtp server.exe - Application Error : The instruction at "0x00402f23" referenced memory at "0x61616161". The memory could not be "read". This results in a Denial of Service against the service in question.  
Link: <http://www.net-security.org/text/bugs/977788101,95356,.shtml>

### DEBIAN LINUX - DIALOG SYMLINK ATTACK

Matt Kraai reported that he found a problem in the way dialog creates lock-files: it did not create them safely which made it susceptible to a symlink attack. This has been fixed in version 0.9a-20000118-3bis.  
Link: <http://www.net-security.org/text/bugs/977886772,81869,.shtml>

### DEBIAN LINUX - MULTIPLE STUNNEL VULNERABILITIES

Lez discovered a format string problem in stunnel (a tool to create Universal SSL tunnel for other network daemons). Brian Hatch responded by stating he was already preparing a new release with multiple security fixes:

1. The PRNG (pseudo-random generated) was not seeded correctly. This only affects operation on operating systems without a secure random generator.
2. Pid files were not created securely, making stunnel vulnerable to a symlink attack
3. There was an insecure syslog() call which could be exploited if the user could manage to insert text into the logged text. At least one way to exploit this using faked identd responses was demonstrated by Lez.

These problems have been fixed in version 3.10-0potato1.  
Link: <http://www.net-security.org/text/bugs/977886802,94324,.shtml>

### DEBIAN LINUX - TWO GPG PROBLEMS

There is a problem in the way gpg checks detached signatures which can lead to false positives. Detached signature can be verified with a command like this:  
gpg --verify detached.sig < mydata  
If someone replaced detached.sig with a signed text (ie not a detached signature) and then modified mydata gpg would still report a successfully

verified signature.

Link: <http://www.net-security.org/text/bugs/977886820,3938,.shtml>

#### ORACLE INTERNET APPLICATION SERVER BUGS

The first possible vulnerability is essentially a configuration issue associated with the Portal Listener and modplsql. When these are installed, the default configuration allows all users access to the Listener and modplsql administration pages. A second potential vulnerability may occur if customers grant public access to PL/SQL procedures, in particular those which access an Oracle database such as OWA, SYS and DBMS. Since publicly accessible procedures may be accessed through a URL, it may be possible to to invoke these procedures through a URL and cause SQL statements to be executed on a back-end Oracle database.

Link: <http://www.net-security.org/text/bugs/977886859,308,.shtml>

#### NSA SECURITY-ENHANCED LINUX PROBLEM

The most recent version that appears to be available is dated last week, slinux-200012181053-release.tgz. In this distribution, the find\_default\_type function in libsecure/get\_default\_type.c attempts to extract a type field from the file /etc/security/default\_type and copy it to a result buffer (specifically, to the argument "char \*\*type"). Memory for this result buffer is allocated using malloc, but the argument to malloc is always one character too small. For example, the role argument might typically be "sysadm\_r" and the len argument would then be 8. With the initial installation, the first value of buf would be "sysadm\_r:sysadm\_t\n". There are no leading spaces, so i is 0. In the statement

```
(*type) = (char*) malloc (sizeof(char) * (strlen(buf)-i-len-1));
```

the argument to malloc is 18 - 0 - 8 - 1, which is 9. Then,

```
strcpy ((*type), &buf[i]+len+1);
```

attempts to copy the 10 characters "sysadm\_t\n\0" into the 9-character buffer.

Link: <http://www.net-security.org/text/bugs/977971173,27822,.shtml>

#### MORE PROBLEMS FOR TECHNOTE

in main.cgi ,failed properly validate user input which arguments a call to open().

FREE\_BOARD is a default db

<http://localhost/technote/main.cgi/oops?>

board=FREE\_BOARD&command=

down\_load&filename=../.././main.cgi

Link: <http://www.net-security.org/text/bugs/977971189,41142,.shtml>

#### REMOTE VULNERABILITY IN IKONBOARD

Ikonboard is a free forum system. Similar to UBB and UB. Versions up to and including 2.1.7b contain a vulnerability that allows commands to be executed as the script user. Therefore compromising security of the system running the board and allowing an attacker to get passwords of the board users, because they are in no way encrypted/hashed.

Link: <http://www.net-security.org/text/bugs/978186540,73624,.shtml>

-----

Security world  
-----

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

-----

EGGHEAD.COM INVESTIGATES PENETRATION - [24.12.2000]

Egghead.com, Inc., released the following statement: "Egghead.com has discovered that a hacker has accessed our computer systems, potentially including our customer databases. As a precautionary measure, we have taken immediate steps to protect our customers by contacting the credit card companies we work with. They are in the process of alerting card issuers and banks so that they can take the necessary steps to ensure the security of cardholders who may be affected.

Press release:

< <http://www.net-security.org/text/press/977664283,29904,.shtml> >

-----

RSA CONFERENCE 2001 ASIA RFP - [27.12.2000]

RSA Security Inc. announced a call for papers and demonstrations for the first annual RSA Conference in Asia. RSA Conference 2001, Asia, is scheduled to be held July 9 - 12, 2001, at the Singapore International Convention and Exhibition Center in Suntec City, Singapore. The event is expected to bring together decision-makers and influencers from financial services, government, education, information technology, telecommunications and the media. Security professionals, cryptographers, analysts, developers and strategic partners are encouraged to submit presentations on their security implementations, applications or research.

Press release:

< <http://www.net-security.org/text/press/977887231,94789,.shtml> >

-----

RSA KEON CERTIFICATE SERVER 5.5 CLOSE TO EAL4 - [27.12.2000]

Reinforcing its commitment to product security, quality and reliability, RSA Security Inc., the most trusted name in e-Security, announced that the RSA Keon Certificate Server 5.5, RSA Security's digital certificate management system designed to add trust to e-government, has been accepted into evaluation against the Common Criteria (CC) for Information Technology Security Evaluations. The Common Criteria for Information Technology Security Evaluation (CC) V2.1/IS 15408 is an international standard for evaluating the security of IT products. This important achievement indicates that the RSA Keon Certificate Server is on its way to achieving CC evaluated status recognized by governments and businesses around the world, including Australia, Canada, France, Germany, the Netherlands, the United States, the United Kingdom, Italy, Spain, Greece, Norway, Finland, and New Zealand.

Press release:

< <http://www.net-security.org/text/press/977887369,30178,.shtml> >

---

BINDVIEW'S BV-CONTROL FINALISTS IN INFOSEC MAG - [2.12.2000]

BindView Corporation, a leading provider of IT security management solutions, announced that its bv-Control product family has been selected as a finalist in the Security Management & Auditing Category for the Information Security Excellence Award given by Information Security Magazine. The winners will be announced at an awards luncheon in February at the MIS Training Institute's InfoSec World Conference in Orlando.

Press release:

< <http://www.net-security.org/text/press/977948954,9040,.shtml> >

---

TRIPWIRE GETS "NSS APPROVED" STATUS - [28.12.2000]

Tripwire Inc., the leading provider of data and network integrity software, announced that Tripwire HQ Manager and Tripwire HQ Connector for NT were awarded the internationally recognized "NSS Approved" status for their exceptional performance. Tripwire's products were thoroughly tested in the Intrusion Detection Software (IDS)/Vulnerability Assessment Group Test 2000 by The NSS Group, Europe's foremost independent test organization focusing on security issues.

Press release:

< <http://www.net-security.org/text/press/978020664,85700,.shtml> >

---

SYMANTEC CEO COMMENTS SECURITY MARKET - [28.12.2000]

On the heels of a recent Network Associates announcement, Symantec Corp. issued the following statement to its investors and customers: "We have never been more confident in our future," said John W. Thompson, chairman, president and CEO of Symantec. "Symantec continues to gain momentum in the enterprise security business. Industry leaders such as Oracle, Cobalt, Yahoo and Earthlink have recently chosen Symantec's security technology. Global leaders in industries ranging from automotive, telecommunications and financial services are showing increasing confidence in our products and our company. In addition, our recently completed merger with AXENT Technologies makes Symantec the largest Internet security company in the world."

Press release:

< <http://www.net-security.org/text/press/978020871,73838,.shtml> >

---

475,000 DOWNLOADS OF AVX VIRUS PROTECTION - [29.12.2000]

At a time when other anti-virus software providers are posting losses, Central Command Inc., a leader in the anti-virus industry, announced that within the last 45 days more than 475,000 people have downloaded AVX virus protection to protect their computers from viruses. AVX Professional software, with its new virus prevention technology designed around an open plug-in architecture, is quickly becoming a standard among Internet users.

Press release:

< <http://www.net-security.org/text/press/978091342,18550,.shtml> >

---

#### FLORIDA SUPREME COURT SELECTS IDENTIX - [29.12.2000]

Identix Incorporated, the worldwide leader in providing user authentication, security and identification solutions, announced that the Florida State Supreme Court has selected Identix's fingerprint biometric security solutions to secure its 650 seat Wide Area Network (WAN) enterprise-wide, which encompasses five District Courts of Appeal and the State Supreme Court.

Press release:

< <http://www.net-security.org/text/press/978091572,661,.shtml> >

---

#### NEW CUSTOMERS USING CERTICOM'S SSL - [29.12.2000]

Continuing to strengthen its position as a leading provider of e-business security, Certicom, announced that it has signed license agreements with five new companies. Additional licensees are Alteon WebSystems, i-drive, Five Nine Solutions, Inc., Pono Corp. and Tempest Software. These companies have licensed Certicom's leading SSL Plus software to enhance the security and trust of their respective internal applications and e-business offerings.

Press release:

< <http://www.net-security.org/text/press/978091709,67478,.shtml> >

---

#### Featured articles

---

All articles are located at:

<http://www.net-security.org/text/articles>

Articles can be contributed to [staff@net-security.org](mailto:staff@net-security.org)

Below is the list of the recently added articles.

---

#### YOUR OPINION: "WHAT ARE THE CURRENT PRIVACY THREATS?"

Recently we held a survey on HNS regarding the current privacy threats. Many visitors decided to share their opinions with us. In this article you can read some of the most interesting opinions.

Read more:

< <http://www.net-security.org/text/articles/opinion.shtml> >

---

## ICMP USAGE IN SCANNING VERSION 2.5 by Ofir Arkin

"The Internet Control Message Protocol may seem harmless at first glance. Its goals and features were outlined in RFC 792 (and than later cleared in RFCs 1122, 1256, 1349, 1812), as a way to provide a means to send error messages, troubleshoot networking problems, and more. There is no consent between the experts in charge for securing Internet networks (Firewall Administrators, Network Administrators, System Administrators, Security Officers, etc.) regarding the actions that should be taken to secure their network infrastructure in order to prevent those risks. The risks involved in implementing the ICMP protocol in a network, regarding scanning, are the subject of this research paper".

PDF Version:

< <http://www.net-security.org/text/articles/index-download.shtml#ICMP> >

---

## THE ABC OF COMPUTER SECURITY by Paul Ducklin

This White Paper gives an introduction to computer security and its significance for businesses, followed by an alphabetical guide to common security measures and threats.

PDF Version:

< <http://www.net-security.org/text/articles/index-download.shtml#ABC> >

---

## RESULTS OF THE SECURITY IN ACTIVEX WORKSHOP

On August 22-23, 2000, the CERT Coordination Center hosted a workshop in Pittsburgh, Pennsylvania, for twenty invited experts to address security issues related to ActiveX controls. The primary goal of the workshop was to identify the situations under which ActiveX and related technologies may be used safely and to produce a paper describing security concerns and configuration guidance. That goal was achieved and the result of the workshop, this paper, serves not only to dispel unwarranted myths about the safety of using ActiveX but also to furnish guidance to network administrators and others faced with security issues involving mobile code in general and ActiveX in particular.

Read more:

< <http://www.net-security.org/text/articles/index-download.shtml#active> >

---

## 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](mailto:staff@net-security.org)

---

#### CIM IP ROUTING DVP SIMULATOR (CISCO CAREER CERTIFICATIONS)

With CIM IP Routing: Distance-Vector Protocols, you can master protocols that are the backbone of the Internet and enable traffic to move across business networks. Offering self-paced instruction and practice, this robust learning tool gives you a quick and cost-effective way to acquire Cisco knowledge and expertise. From an overview of IP routing concepts to the development of IP access lists, you'll learn the difference between routing functions and strategies, routing traffic using multiple paths, and how to implement routing protocols for quick convergence times with minimal network traffic through Cisco internetworking devices. Mastering techniques developed by Cisco Technical Assistance Center engineers, you'll practice configuring and troubleshooting RIP, IGRP, and EIGRP over IP networks. CIM IP Routing: Distance-Vector Protocols is an excellent preparation tool for the Cisco Certified Network Associate (CCNA) exam.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1587200120/netsecurity> >

---

#### IN THE TRENCHES: CUSTOMIZING AND UPGRADING LINUX

A reference for the busy professional to installing and administering Linux, detailing the difference between Linux and other Unix systems. The CD-ROM contains Red Hat Linux 6.2, to enable the reader to follow along with the text and see how Linux works.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1930713010/netsecurity> >

---

#### GNU AUTOCONF, AUTOMAKE, AND LIBTOOL

This is a technically adept and expert guide to using these utilities effectively. Any C/C++ or script programmer who writes software under Unix/Linux will want to have a copy of this book to make better use of these powerful and sometimes obscurely documented tools. This text is filled with the nuts-and-bolts details of running these three utilities, including command-line switches and the actual, generated files that automate the build process and help programmers port code between different environments. As such, this title will be appreciated by those at their workstations who want a hands-on guide to using the autotools. There's a danger of missing the forest for the trees here, with all of this necessary detail, but the middle sections of this book pull back a little with several useful chapters on the bigger picture of code "portability." Chapters on both C and C++ portability explore language features that likely will cause trouble when code is moved between different versions of Unix (or even between Unix and Windows). A similar section also discusses the issues when developing portable shell scripts.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1578701902/netsecurity> >

---

## LINUX IP STACKS COMMENTARY

The book is an in-depth look at the TCP/IP protocol implementation as implemented in Linux. Using the style of John Lion's original much-photocopied A Commentary on the Unix Operating System, Linux IP Stacks Commentary guides you through the ins and outs of TCP, UDP, ICMP, routing, IPCHAIN firewall code, and the Linux TCP/IP applications interface. The source for the network code is included in the book and on the CD-ROM.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1576104702/netsecurity> >

---

## APACHE SERVER COMMENTARY

A guide for programmers and developers who need to understand and master the source code that runs the world's most popular Web server. Holden (author and president of Stylus Media), Nicholas Wells (technical writer and consultant), and Matthew Keller (programmer/analyst for Distributed Computing and Telemedia department at the State U. of New York College) conduct a line-by-line examination of the core code, as well as the standard Apache modules that control logging, directory indexing, access control, CGI, and other essential aspects of running a full-featured Web site. Flow charts illustrate how individual modules work. The included CD-ROM contains the complete source code for version 1.3.6 of the Apache Web server package, a precompiled binary version of Apache for Windows 32-bit platforms, ApacheWrapper version 1.3.29, Comanche, IPTraf version 1.4.3, and Chili!Soft ASP 3.0.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1576104680/netsecurity> >

---

## Security Software

---

All programs are located at:  
<http://net-security.org/various/software>

---

## W32.KRIZ PREVENTION TOOL

This tool is a preventive measure against the W32.Kriz virus. It will not repair damage done after the virus has been launched.

Info/Download:

< <http://net-security.org/various/software/977614917,63951,.shtml> >

---

## KILL\_CIH REMOVAL TOOL

The KILL\_CIH tool is designed to safely detect and remove all known strains of the W95.CIH (Chernobyl) virus (known strains as of August 3rd, 1998) from memory under Windows 95 and Windows 98 (the W95.CIH virus cannot infect Windows NT systems). If the tool is run before the virus has infected the system, it will also "inoculate" the computer's memory to prevent the W95.CIH virus from infecting the system until the next system reboot.

Info/Download:

< <http://net-security.org/various/software/977615146,72255,.shtml> >

---

## W32.NAVIDAD REMOVAL TOOL

This tool will only work for W32.Navidad and it will not work for the W32.Navidad.16896 variant.

Info/Download:

< <http://net-security.org/various/software/977615252,711,.shtml> >

---

## CHKROOTKIT-0.19

chkrootkit locally checks for signs of a rootkit. Includes detection of LKM rootkits, ifpromisc.c to check and see if the interface is in promisc mode, chklastlog.c to check lastlog for deletions, and chkwtmp.c to check wttmp for deletions. Tested on Linux, FreeBSD, Solaris, and OpenBSD.

Info/Download:

< <http://net-security.org/various/software/978188214,78469,.shtml> >

---

## SECURE DISK EXPLORER 1.1.3

Secure Explorer is a full-featured file manager similar to Windows Explorer. However, the biggest difference is that this program provides a completely secure environment for data and documents on your system. It's capable of encrypting files and locking folders, thus making them inaccessible to other users. Like Explorer, Secure Explorer supplies its very own shell context menu. As you browse your hard drive, simply right-click an item and select the appropriate protection option from the menu. The program gives you the option of preventing Explorer from displaying these items. Meanwhile, files and folders are stored inside tabs on the interface, which require passwords for entry. Like Explorer, Secure Explorer supplies its very own shell context menu.

Info/Download:

< <http://net-security.org/various/software/978188372,43683,.shtml> >

---

Defaced archives

-----  
[25.12.2000] - ChangChun Science&Technology, China

Original: <http://www.ccst.gov.cn/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/12/25/www.ccst.gov.cn/>

[25.12.2000] - Slackware

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/12/25/www.slackware.com/>

[25.12.2000] - Nasdaq Japan

Original: <http://www.nasdaq.co.jp/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/12/24/www.nasdaq.co.jp/>

[25.12.2000] - Administrative Office of the U.S. Courts

Original: <http://www.nywd.uscourts.gov/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/12/25/www.nywd.uscourts.gov/>

[26.12.2000] - Hizbollah

Original: <http://www.hizbollah.org/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/12/26/www.hizbollah.org/>

[27.12.2000] - Government Republic Of Moldova Site

Original: <http://ministry.moldova.md/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/12/27/ministry.moldova.md/>

[27.12.2000] - National Oceanic and Atmospheric Administration

Original: <http://www.fob.noaa.gov/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/12/27/www.fob.noaa.gov/>

[28.12.2000] - US DOI, Bureau of Land Management

Original: <http://www5.ca.blm.gov/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/12/28/www5.ca.blm.gov/>

[29.12.2000] - Embassy of Israel, Wellington, New Zealand

Original: <http://www.israel.org.nz/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/12/29/www.israel.org.nz/>

[29.12.2000] - Human Right Education Programme, Pakistan

Original: <http://www.hrep.com.pk/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/12/29/www.hrep.com.pk/>

-----  
Questions, contributions, comments or ideas go to:

Help Net Security staff

[staff@net-security.org](mailto:staff@net-security.org)

<http://net-security.org>