

Net-Sec newsletter  
Issue 32 - 02.10.2000  
<http://net-security.org>

Net-Sec 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>

Table of contents:

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

=====  
In association with Kaspersky Lab ([www.kaspersky.com](http://www.kaspersky.com)), HNS staff created a new section of the site, with about 400 descriptions of well known and not so know viruses. Specially interesting part of that section are screenshots of 50 virus infections. All viruses are well categorized and easy to browse.

Point your browser to this URL:  
<http://www.net-security.org/text/viruses>  
=====

#### General security news

-----

-----

#### RIJNDAEL CHOSEN BY US GOVERNMENT

It took 23 years, 15 different algorithms, and two conferences, but the U.S. government has finally chosen a new encryption standard. The winner: Rijndael, a cipher created by a pair of Belgian cryptographers. Btw Rijndael web site is in the time of writing this item inaccessible.  
Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wirednews.com/news/politics/0,1283,39194,00.html>

#### HK GOVERNMENT STRIVES TO ENSURE INTERNET SAFETY

Hong Kong government is making a lot of efforts to creating a trustworthy environment and provide a secure infrastructure for the conduct of electronic transactions, a senior information technology official said Thursday.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://english.peopledaily.com.cn/200009/30/eng20000930\\_51594.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://english.peopledaily.com.cn/200009/30/eng20000930_51594.html)

#### WHAT ARE DIGITAL SIGNATURES?

When President Clinton signed a law that gives digital signatures the same legal force as handwritten ones, he said Americans would marvel one day that this was considered a big deal. This short article describes what are digital signatures.

Link: [http://seattletimes.nwsourc.com/cgi-bin/WebObjects/SeattleTimes.woa/wa/gotoArticle?text\\_only=0&slug=esighow30&document\\_id=134236049&zsection\\_id=268448455](http://seattletimes.nwsourc.com/cgi-bin/WebObjects/SeattleTimes.woa/wa/gotoArticle?text_only=0&slug=esighow30&document_id=134236049&zsection_id=268448455)

#### HARDENING THE BIND DNS SERVER

This paper presents the risks posed by an insecure DNS server and walks through compiling, installing, configuring and optionally, chroot'ing BIND 8. The test environment is Solaris 2.5, 2.6, 7 and 8. Many configuration and troubleshooting tips are provided, along with up-to-date references on BIND and alternatives for NT, Linux and Solaris.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/cover/coverstory20001002.html>

#### SECURITY WITHOUT SERVICES

Cisco Systems Inc.'s new security blueprint, Safe, isn't an acronym, but it might as well stand for "Services Are Found Elsewhere." The Safe initiative, introduced here at NetWorld+Interop last week, is Cisco's overarching attempt to simplify its security architecture and message for network security users, many of whom have turned to companies such as Internet Security Systems Inc. and Check Point Software Technologies Ltd.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/eweek/stories/general/0,11011,2635351,00.html>

#### TWO VIEWS OF HACKING

For different perspectives on hacking, CNN Interactive posed a series of questions via e-mail to two experts in the field, one a computer security expert for IBM, the other, editor of 2600, the Hackers' Quarterly.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/TECH/specials/hackers/qandas/>

#### NEW TURN IN OLD WAR ON MACRO VIRUSES

Personal firewalls have become all the rage to protect home computer systems against the Internet's vandals. Now, the concept is being adapted to protect those same computers from macro viruses.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://dailynews.yahoo.com/h/zd/20000929/tc/new\\_turn\\_in\\_old\\_war\\_on\\_macro\\_viruses\\_1.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://dailynews.yahoo.com/h/zd/20000929/tc/new_turn_in_old_war_on_macro_viruses_1.html)

#### MULTI-ATTACK VIRUS DISCOVERED BY NORMAN DATA DEFENSE

Norman Data Defense said that it has discovered a new virus known as W32/MTX@mmin the wild that prevents virus patches from being

downloaded. The IT security firm said that the program will attach itself to a second e-mail sent from a computer to a recipient and also block access to several major anti-virus companies' Web sites, blocking reporting e-mails to these sites as well.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.telekomnet.com/news/9-29-00\\_multiattackvirus\\_norman.asp](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.telekomnet.com/news/9-29-00_multiattackvirus_norman.asp)

#### HACKING IN SOUTH AFRICA

During October, Ernst & Young aims to teach 60 people to break into Windows NT and Unix systems, and deface Web sites. A four-day Counterhack course, to be held in Cape Town and Johannesburg consecutively, will show corporate citizens with a responsibility for network security just how open their systems can be to attack.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://196.36.119.109/sections/computing/2000/0009290600.asp>

#### BT INTERNET SECURITY BREACH

BBC reports that a serious internet security breach has been discovered at BT's free e-mail service Talk21. When following the link in the emails that users received, one person could easily see the refferer logs and enter their accounts.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://news.bbc.co.uk/hi/english/business/newsid\\_946000/946717.stm](http://www.net-security.org/cgi-bin/news.cgi?url=http://news.bbc.co.uk/hi/english/business/newsid_946000/946717.stm)

#### FBI CONSULTANT PLEADS GUILTY

Max Butler aka 'Max Vision' on Monday pleaded guilty to one felony count of unauthorized access to protected computers and recklessly causing damage. The former FBI consultant on computer crime had been indicted by a federal grand jury in March and charged with fifteen counts of breaking into scores of US government computers as well as possessing the passwords of 477 customers of California ISP Aimnet.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/1/13582.html>

#### MITNICK TALKS CORPORATE SECURITY

"Even though you've bought the best security products, some people will break through," he said, dressed in a dark suit, white shirt and tie.

"There's no sure-fire way to protect yourself. You have to manage the risk. There's no way you can eliminate it."

Link: <http://www.crn.com/Sections/BreakingNews/dailyarchives.asp?ArticleID=20257>

#### FREEBSD 4.1.1

Since 4.1-RELEASE was produced in August 2000, RSA released their code into the public domain and a number of other security enhancements were made possible through the FreeBSD project's permission to export cryptographic code from the United States. These changes are fully reflected in 4.1.1-RELEASE, making it one of the most secure "out of the box" releases of FreeBSD.

Contributed by Apocalypse Dow

Link: <http://docs.freebsd.org/cgi/getmsg.cgi?fetch=0+0+current/freebsd-announce>

#### HIPAA STANDARDS FOR SECURITY AND ELECTRONIC SIGNATURES

This issue of HIPAA's Impact on Health Care and Other Industries outlines HIPAA mandates for Security and Electronic Signature Standards. Since robust security is a critical component of any successful business, HIPAA standards provide sound security practices that will benefit any organization that conducts business electronically.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.gigaweb.com/Content/Adhoc/RAH-092000-00020.html>

#### HACKERS NOT WANTED FOR HACK JOB

A British IT company launched an anti-hacking unit Wednesday but said some of the best qualified candidates - the hackers - need not apply. The unit, which sees itself as capable as a hacker, is trying to tap the rapidly growing market for companies keen to protect themselves from cyber attacks.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/business/0,1367,39093,00.html>

#### ATTACKED WEBSITES COULD FACE LIBEL THREAT

Unsuspecting network managers could find themselves at the centre of libel action if their attacked websites publish slanderous statements. Despite not originating the offensive material, with software defences improving, ignorance may not be considered a defence in future.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1111742>

#### LINUX VIRUSES: SCANNER PLACEMENT

"A virus scanner doesn't do you any good if it's not somewhere along the path the virus takes to get into your network, onto your machine, and then executed. When deploying antivirus software, there are a number of factors to consider..."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/linuxvirus20000926.html>

#### CARNIVORE REVIEW TEAM EXPOSED!

An embarrassing oversight by the Justice Department has revealed confidential information about the team of researchers hired to conduct the review.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,39102,00.html>

#### TRULOCK SUES FBI, CIA, DOE, STATE DEPT. & WHITE HOUSE

Renowned former Energy Department Counter-Intelligence Director Notra Trulock filed two new lawsuits to protect his rights to speak freely about the gross negligence and coverup by the Clinton-Gore Administration over the historic breach of national security at the Los Alamos Nuclear Laboratory. Previously, when officials at the FBI illegally broke into his home and seized his computer, Mr. Trulock and his landlord, Linda Conrad, filed a civil rights lawsuit against FBI Director Louis Freeh, and others who were responsible.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://cipherwar.com/news/00/notra\\_trulock\\_3.htm](http://www.net-security.org/cgi-bin/news.cgi?url=http://cipherwar.com/news/00/notra_trulock_3.htm)

#### CISCOSECURE

Cisco Systems will launch CiscoSecure Encyclopedia, a free online source of news and information about network security issues, in Q4 this year. The Encyclopedia will include advice on issues like how to defend websites against denial of service attacks, and information about new security threats as they arise. Cisco Security Associates such as Baltimore, Verisign, F-Secure, RSA, Entrust and Microsoft are expected to make an active contribution.

Link:

<http://www.netimperative.com/technology/newsarticle.asp?ArticleID=5394&ChannelID=3&ArticleType=1>

#### E\*TRADE FIXES ONE SECURITY PROBLEM, ADMITS ANOTHER

by LogError Wednesday 27 September 2000 on 12:26 AM

The vulnerability came to light after the company rushed to fix another security problem over the weekend. On Friday, San Francisco computer programmer Jeff Baker reported on the Bugtraq security mailing list that programming problems at E\*Trade had left individual customer accounts vulnerable to attacks. Baker identified at least two problems: vulnerability to cross-site scripting and an insecure cookie used to log into the popular online brokerage. E\*Trade fixed its cookie problem Sunday, changing the algorithm by which it scrambled the cookie data. But the cross-site scripting vulnerability remains.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1007-200-2870712.html>

#### QUANTUM CRYPTO SECRETS FROM JAPAN

Mitsubishi and Hokkaido University have completed a latest round of experiments in quantum cryptography over optical fibres. The two organisations say that their quantum cryptographic system is a success, and could have important implications for optical fibre networks already in use.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/5/13536.html>

#### NEW LINUX-CRYPTO MAILING LIST

Marc Mutz announced a new mailing list intended to be a forum for all sorts of crypto topics concerning Linux. "Since this list is new, it will be low-volume. If that volume grows, we may split the list into -devel and -users, but as for now, everyone is welcomed with open arms to join the list - be it newbie, be it developer."

Link: [http://linuxtoday.com/news\\_story.php?itsn=2000-09-26-009-04-NW-CY](http://linuxtoday.com/news_story.php?itsn=2000-09-26-009-04-NW-CY)

#### RUSSIAN CARNIVORE TO SHUT DOWN?

The Supreme Court of Russia nullified one of the articles of the Ministry of Communication Order No. 130, this year. The infamous Order would have forced telecom/datacom operators to install surveillance equipment on their networks. Being deployed such a system (the so called "SORM", Russian acronym for System of Research Operative Measures, much similar to the FBI's Carnivore) would have enabled the ex-KGB to exercise effective technological circumvention of current legislation on privacy.

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

-----

## Security issues

---

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

---

### CONECTIVA LINUX SECURITY - IMP UPDATE

There are several vulnerabilities in the horde and imp packages shipped with Conectiva Linux that allow an user to execute remote commands on the server as the user "nobody".

Link: <http://www.net-security.org/text/bugs/969921756,56833,.shtml>

### NMAP DOS AGAINST OPENBSD IPSEC

The protocol scanning option (-sO) in 2.54 Beta releases of nmap results in a remote denial of service against OpenBSD 2.7's IPSEC implementation due to its inability to handle tiny AH/ESP packets. Nmap protocol scans repeatedly cycle through IP protocol version numbers, attempting to elicit ICMP Protocol Unreachable messages in order to discover which IP protocols (ICMP,TCP,UDP, GRE,AH,ESP, etc.) are active on the target device.

Link: <http://www.net-security.org/text/bugs/969962574,40124,.shtml>

### CALDERA SECURITY ADVISORY - FORMAT BUG IN LPRNG

There is a format bug in the LPRng printer daemon that could possibly be exploited to obtain root privilege. This problem is particularly severe because it can be exercised remotely.

Link: <http://www.net-security.org/text/bugs/969962727,59437,.shtml>

### NEW VARIANTS OF TRINITY AND STACHELDRAHT

New versions of Stacheldraht and Trinity distributed denial of service attack tools have been found in the wild. The new versions of Stacheldraht include "Stacheldraht 1.666+antigl+yps" and "Stacheldraht 1.666+smurf+yps". A variant of the Trinity tool called "entitee" has also been reported.

Link: <http://www.net-security.org/text/bugs/969963115,73435,.shtml>

### MEDIA PLAYER 7 "OCX ATTACHMENT" VULNERABILITY

The USSR Team has found a problem in the Windows Media Player 7 ActiveX control, which could be used in a denial of service attack against RTF-enabled e-mail clients such as Outlook 2000 and Outlook Express. If the affected control were programmatically embedded into an RTF mail and then sent to another user, the user's mail client would fail when he closed/moved the mail.

Link: <http://www.net-security.org/text/bugs/970053513,31576,.shtml>

The vulnerability has been patched.

Link: <http://www.net-security.org/text/bugs/970053598,21505,.shtml>

### IE 5.5/OUTLOOK EXPRESS SECURITY VULNERABILITY

Internet Explorer 5.5/Outlook Express/(probably Outlook if Active Scripting is enabled) under Windows 98/2000 (suppose all other versions are also vulnerable)

allow reading local and UNC files.

Link: <http://www.net-security.org/text/bugs/970053772,30044,.shtml>

#### CISCO SECURE PIX FIREWALL MAILGUARD VULNERABILITY

The behavior is a failure of the command "fixup protocol smtp [portnum]", which is enabled by default on the Cisco Secure PIX Firewall. If you do not have protected Mail hosts with the accompanying configuration you are not affected by this vulnerability. To exploit this vulnerability, attackers must be able to make connections to an SMTP mail server protected by the PIX Firewall.

Link: <http://www.net-security.org/text/bugs/970095462,66863,.shtml>

#### PALMOS PASSWORD RETRIEVAL AND DECODING

PalmOS offers a built-in Security application which is used for the legitimate user to protect and hide records from unauthorized users by means of a password. In all basic built-in applications (Address, Date Book, Memo Pad, and To Do List), individual records can be marked as "Private" and will only be accessible if the correct password is entered. It is possible to obtain an encoded form of the password, determine the actual password due to a weak, reversable encoding scheme, and access a users private data. In order for this attack to be successful, the attacker must have physical access to the target Palm device.

Link: <http://www.net-security.org/text/bugs/970146391,76361,.shtml>

#### E\*TRADE SECURITY CONCERNS - FORWARD #1 AND #2

"I wrote E-Trade expressing my concern about the security vulnerabilities that people are discussing on Bugtraq. Here's their response."

Link: <http://www.net-security.org/text/bugs/970162272,16928,.shtml>

Link: <http://www.net-security.org/text/bugs/970165300,30855,.shtml>

#### NETSCAPE NAVIGATOR BUFFER OVERFLOW

Netscape Navigator is vulnerable to trivial, remote buffer overflow attack when viewing prepared html:

```
< form action=something method=something >
< input type=password value=reallylongstring... >
....other form tags...
< /form >
```

Link: <http://www.net-security.org/text/bugs/970185574,9095,.shtml>

#### SCP FILE TRANSFER HOLE

This issue appears quite often - tar suffers from problem of this kind as well (using cute symlink tricks, you can create an archive, which, when unpacked, can overwrite or create specific files anywhere in your filesystem). This time, similar scp vulnerability has been found and acknowledged in sshd 1.2.xx releases (no information on 2.0.xx). When you are scp'ing files from remote machine to your local computer, modified scp service on the second endpoint can spoof legitimate scp data, overwriting arbitrary files.

Link: <http://www.net-security.org/text/bugs/970403620,35951,.shtml>

#### CONNECTIVA LINUX - PROBLEM WITH TRACEROUTE

Previous releases of traceroute contained some problems that could be exploited to gain local root access. All users should upgrade the traceroute package.

Link: <http://www.net-security.org/text/bugs/970406453,49781,.shtml>

#### CALDERA LINUX - PROBLEMS WITH TRACEROUTE

There is a bug in the traceroute command that can possibly be used by local users to obtain super user privilege. There are no exploits available so far, but we encourage our customers to upgrade nevertheless.

Link: <http://www.net-security.org/text/bugs/970406605,5363,.shtml>

#### HOW SLASHDOT GOT PENTRATED INTO

In prior versions of slash there are several issues that one must be aware of that are covered in the INSTALL. One must change the default admin user/passwd from God/Pete to something else. Proper setup of Slashcode depends on people reading the INSTALL. Because of the slash install and code not having something that forces the admin user to change the password, one may inadvertently be leaving themselves open to access from the outside by unauthorized users.

Link: <http://www.net-security.org/text/bugs/970407017,97688,.shtml>

---

#### Security world

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

---

#### INCORRECT AND MISLEADING NEWSPAPER CLAIMS - [25.09.2000]

Fiserv, Inc. announced that a story in Sunday's Observer and Guardian newspapers in London alleging Internet banking security breaches involving Fiserv clients was incorrect and misleading. A British Internet banking customer quoted in the stories accessed only demonstration accounts at sites maintained for clients of a Fiserv servicing unit. The demonstration accounts contain only fictitious data used for training and sales purposes.

Press release:

< <http://www.net-security.org/text/press/969896092,84365,.shtml> >

---

#### 24/7 MEDIA SUPPORTS E-MAIL PRIVACY PROTECTION - [25.09.2000]

24/7 Media, one of the largest global Internet marketing and technology solutions companies, announced it intends to vigorously support the guidelines set forth this morning by the Responsible Electronic Communications Alliance (RECA), which call for industry-wide standards to protect consumer privacy. A draft of the new guidelines was announced at the DMA Net.Marketing event in Boston.

Press release:

< <http://www.net-security.org/text/press/969896167,16298,.shtml> >

---

INTRUSION.COM ANNOUNCES INVESTMENT BY SAIC - [25.09.2000]

Intrusion.com, Inc. announced that SAIC Venture Capital Corporation exercised its second and final warrant to purchase 750,000 shares of Intrusion.com common stock for \$10.50 per share. As a result of the exercise of this warrant, Intrusion.com received approximately \$7.9 million.

Press release:

< <http://www.net-security.org/text/press/969896225,42751,.shtml> >

-----

ESECURITY INNOVATION CENTRE - [26.09.2000]

JAWS Technologies Inc., a leading provider of end-to-end information security solutions, announced TELUS Corporation has signed on as a founding sponsor of the eSecurity Innovation Centre. Launched jointly by the University of Calgary and JAWS, the eSecurity Innovation Centre is a facility that brings together the latest technology and the most skilled computer security professionals from around the globe to generate information security solutions. The first-of-its-kind facility will serve as a focal point for computer security training, certification, demonstrations, research and development, as well as cybercrime investigations.

Press release:

< <http://www.net-security.org/text/press/969922167,45152,.shtml> >

-----

IKEY ENABLES LAPTOP AND WEB-SERVER SECURITY - [26.09.2000]

Recent high-profile Web site hacks, headline-making system abuse and corporate laptop thefts have highlighted a growing need for the type of strong, two-factor authentication enabled by Rainbow Technologies' iKey workstation security solution. This small, lightweight token fits on a key ring and can be used to secure any USB-enabled computer, from the CEO's notebook to a company's Web server.

Press release:

< <http://www.net-security.org/text/press/969922231,40909,.shtml> >

-----

VPN CONSORTIUM CERTIFIES CYLINK'S NETHAWK VPN - [26.09.2000]

E-business security pioneer Cylink Corporation announced that its NetHawk VPN has received IPSec-standard conformance certification from the Virtual Private Network Consortium, the international trade association for manufacturers of appliances that create private networks to run over the public Internet to ensure user privacy.

Press release:

< <http://www.net-security.org/text/press/969922458,83423,.shtml> >

-----

SECURECOM NET AND RAINBOW TECHNOLOGIES PARTNER - [27.09.2000]

SecureCom Networks, Inc., a leading provider of Internet communications security appliances, and Rainbow Technologies Inc., a leading provider of high-performance security solutions for the Internet and eCommerce, announced an agreement to integrate Rainbow's CryptoSwift technology into SecureCom Networks' Secure Mail Router appliance family, the S/MX series.

Press release:

< <http://www.net-security.org/text/press/970089462,96618,.shtml> >

-----

#### THE INDUSTRY FIGHTS BACK AGAINST DDOS - [27.09.2000]

Top computer security executives discussed the latest requirements and technologies to provide early warnings of, mitigate the impact of, reduce production outages and system breakdowns from, and promote industry-wide communications regarding Denial of Service attacks through the Internet. The event, which included a public panel discussion and reception, was held at the Ritz Carlton Hotel in conjunction with NetWorld+Interop 2000 in Atlanta.

Press release:

< <http://www.net-security.org/text/press/970089541,90808,.shtml> >

-----

#### E-SECURITY CONFERENCE & EXPOSITION - [27.09.2000]

Intermedia Group and META Group announced that the E-Security Conference & Exposition has exceeded all expectations and garnered record industry support, establishing the event as the industry's leading forum for e-security education and solutions. The event is targeted at business and information technology managers that have direct or indirect responsibility for their organization's overall e-business security. The event will be held in Washington, DC November 30 - December 1, 2000.

Press release:

< <http://www.net-security.org/text/press/970089662,64034,.shtml> >

-----

#### SEATTLE LAB ANNOUNCES REMOTENT-2000 V3.1 - [28.09.2000]

RemoteNT-2000 version 3.1, offering comprehensive network administration and monitoring with Web-based access, was released by Seattle Lab. RemoteNT-2000 v3.1 enables system administrators to easily monitor their systems for security and NT events, download the event log and schedule tasks. One of the key features in the latest release of RemoteNT-2000 gives administrators the ability to monitor security audits and logon attempts based on an NT event from the event log and performance counters.

Press release:

< <http://www.net-security.org/text/press/970161760,3573,.shtml> >

-----

ZTANGO CHOSSES RSA FOR ITS WAP GATEWAY SOLUTION - [28.09.2000]

Ztango, a Wireless Application Service Provider providing wireless extension and wireless application solutions to network operators, e-companies, and corporations, announced that it has licensed RSA BSAFE Crypto-C software from RSA Security Inc. for its WAP gateway product. By including RSA Security's software in its gateway solution, Ztango is able to deliver end-to-end secure communications for a wide variety of applications, commerce and financial services.

Press release:

< <http://www.net-security.org/text/press/970161861,71920,.shtml> >

---

SECURE COMPUTING HELPS 3COM IN EXTRANET SECURITY - [28.09.2000]

Secure Computing announced that it is helping 3Com Corporation develop the next-generation of information technology security. The two companies are combining their expertise to address a segment of corporate information technology assets that is largely un-addressed today and where, according to recent US Federal Bureau of Investigation studies, the majority of security breaches occur - inside the perimeter of the firewalls.

Press release:

< <http://www.net-security.org/text/press/970161964,54863,.shtml> >

---

SAFEGUARD PERSONAL FIREWALL BY UTIMACO - [29.09.2000]

SafeGuard Personal FireWall complements Utimaco Safeware AG's range of Internet security products. The company now offers a seamless security concept for professional Internet workstations from smartcard-based authentication to encryption, digital signature and VPN to firewall systems. SafeGuard Personal FireWall protects Internet-connected PCs against attacks which firewalls and virus scanners are powerless to stop. Designed to enhance a company's central firewall system, the new product can also provide genuine firewall protection to mobile and remote workstations (notebooks, telecommuter workstations).

Press release:

< <http://www.net-security.org/text/press/970227951,73648,.shtml> >

---

E&Y LAUNCHES ANTI-HACKING COURSE IN SOUTH AFRICA - [29.09.2000]

True to the organisation's commitment to generating ideas and solutions that positively transform clients' businesses, Ernst & Young South Africa - part of the global network of Ernst & Young International - has announced the launch of the first definitive anti-hacking course in South Africa. Titled counterhack TM, the course is designed to familiarise approved participants with network based attack and penetration techniques that hackers may use against corporate networks. Being completely solutions driven and determined to deliver and share a superior knowledge base with clients, Ernst & Young will demonstrate to participants - in a detailed, methodical manner - how to compromise and ultimately how to protect a system and network from attack.

Press release:

< <http://www.net-security.org/text/press/970256875,11930,.shtml> >

---

ISS FORMS STRATEGIC BUSINESS UNITS - [29.09.2000]

To accelerate the delivery of its market-leading security management solutions and continue to meet customers' information protection needs in a growing market, Internet Security Systems announced its new corporate organizational structure. The company will form two strategic business units - Enterprise Solutions and Managed Security Services – each chartered to address unique customer needs and delivery requirements of ISS' leading SAFEsuite enterprise security management products and outsourced security, consulting and education services.

Press release:

< <http://www.net-security.org/text/press/970258423,96440,.shtml> >

---

SECURE INTERNET MESSAGING SOLUTIONS FROM SENDMAIL - [02.10.2000]

Sendmail, Inc., a leading provider of Internet messaging solutions, announced that several of its content management partners are ready to deliver their mail filter plug-ins for use with its product lines. Sendmail, Inc.'s partnerships with ActiveState, Brightmail and Trend Micro were developed to deliver secure Internet messaging solutions to enterprises and service providers who rank security and control of their Internet messaging systems as critical requirements.

Press release:

< <http://www.net-security.org/text/press/970509916,41460,.shtml> >

---

LINUXSOLVE INC. LAUNCHES THE LINUXSOLVE CACHE - [02.10.2000]

LinuxSolve, the leading developer of secure server appliances for Internet infrastructure, announced that it is shipping the Cache secure server appliance, the industry's first secure internet caching appliance. The LinuxSolve Cache is the latest in a strong line of secure server appliance products introduced by LinuxSolve. The Cache product enables content consumer-side or content delivery-side companies to speed up the loading of frequently accessed Web pages, cache DNS information, IP and Web address filtering for content, and reduce overall latency times, freeing up network traffic.

Press release:

< <http://www.net-security.org/text/press/970510011,37533,.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)

Listed below are some of the recently added articles.

---

#### SURFING BETWEEN THE FLAGS: SECURITY ON THE WEB by Catherine Allen

This paper discusses security with respect to the World Wide Web. This paper is aimed to promote an awareness of security issues in general WWW users without resorting to scare tactics. Practical solutions and precautions for security problems are discussed. The concepts and issues described in this paper apply to all operating systems, servers and clients, although implementation differences may cause different specific vulnerabilities. Examples used throughout this paper assume a UNIX host.

Article:

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

---

#### THE SIX HEADED SPAM MONSTER by Berislav Kucan aka BHZ

Several days ago I visited an on-line forum of one of the Internet Presence Providers (IPP) in my country and found a topic dealing with spam. One user of the IPP in this topic, posted that by accessing his web site he receives the standard 403 forbidden message. He thought that it was some kind of a problem on the server, but the reality is that his account was shut down (and all files deleted?)...

Article:

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

---

#### SURVEY 2000 - SECURITY FOCUSED

New research confirms that corporations are spending more and more money on securing their digital information, but cybersecurity breaches continue to climb anyway. According to a survey published this month in Information Security magazine, the number of companies spending more than \$1 million annually on computer security nearly doubled in the past year, and is up by 188 percent over the last two years. Nevertheless, security breaches originating from both inside and outside the corporation continue to grow as the threat of outside hackers and deviant/careless employees increases.

Survey:

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

---

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)

-----  
**NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS**

Provides an integrated, comprehensive, up-to-date coverage of internet-based security tools and applications vital to any treatment of data communications or networking.

Book:  
< <http://www.amazon.com/exec/obidos/ASIN/0130160938/netsecurity> >

-----  
**SECURE ELECTRONIC COMMERCE: BUILDING THE INFRASTRUCTURE FOR DIGITAL SIGNATURES AND ENCRYPTION**

This book describes the technologies used to make electronic commerce secure, together with their business and legal implications. The book begins with an introduction to the underlying technologies and inherent risks of electronic commerce. It considers the role of computer networks, the Internet, EDI and electronic mail, as well as the problem of ensuring that electronic transactions are resistant to fraud, may be traced, and are legally binding in all jurisdictions.

Book:  
< <http://www.amazon.com/exec/obidos/ASIN/0134763424/netsecurity> >

-----  
**TANGLED WEB: TALES OF DIGITAL CRIME FROM THE SHADOWS OF CYBERSPACE**

With the intense growth of e-business, we hear about an increase in hacking and technology-based criminal incidents. Institutions such as Citibank and Ebay have faced intrusions that have cost them millions of dollars in damages. With the onset of these criminal attacks, there is an increase in demand for products and services that provide more information for people. Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace portrays the shadow side of cyberspace by taking you into the lairs of hackers, crackers, researchers, private investigators, law enforcement agents and intelligence officers. The book covers what kinds of cyber-crimes are going to affect business on the Internet, their cost, how they are investigated, and the motivation of hackers and virus writers. Also covered are the problems faced by law enforcement, corporate cyber security professionals, and real-world examples of cyber crimes and lessons learned.

Book:  
< <http://www.amazon.com/exec/obidos/ASIN/078972443X/netsecurity> >

-----

## HIGH TECHNOLOGY CRIME INVESTIGATOR'S HANDBOOK

This book is coming at a time when high technology crime is growing at a rapid pace, and private and public law enforcement are struggling to keep up. The book will inform readers about the potential of high tech crimes, in addition to the resources that are available to combat them. This book is unique in that it fully covers the management of a high tech investigation unit. Criminals today are often better equipped than the agencies responsible for stopping them. Federal, state, county, and local law enforcement agencies and civilian investigative organizations lag far behind in their procurement and use of high technology equipment, and methods of conducting technology-related investigations.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/075067086X/netsecurity> >

---

## SMART CARD SECURITY AND APPLICATIONS

Smart cards are all around us, and their security features can be utilized to protect data in almost any computer system. In clear, comprehensible language, this book provides a solid overview of the benefits and limitations of smart cards for secure applications, and shows how to implement the procedures needed to make smart cards effective in protecting information.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0890069530/netsecurity> >

---

## Security Software

---

All programs are located at:

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

---

## SYSCRON 0.6.0 (LINUX)

Syscron is a cron system which allows jobs to be run on many hosts using a central set of scripts. It uses a variety of methods to ensure the security of the system and authenticity of the scripts before executing them.

Link:

< <http://net-security.org/various/software/970438463,76833,.shtml> >

---

## LIDS-0.9.9-2.2.17 (LINUX)

The Linux Intrusion Detection System is a patch which enhances the kernel's security. When it's in effect, many system administration operations can be

made impossible even for root. You can turn the security protection on or off on the fly and you can hide sensitive processes and prevent anyone from using ptrace or any other capability on your system. LIDS can also provide raw device and I/O access protection.

Link:

< <http://net-security.org/various/software/970438717,65085,.shtml> >

---

#### SNORT INTRUSION DETECTION SYSTEM (LINUX)

SnortSnarf is a Perl program that takes files of alerts from the free Snort Intrusion Detection System, and produces HTML output intended for diagnostic inspection and tracking down problems. The model is that one is using a cron job or similar to produce a daily/hourly/whatever file of snort alerts. This script can be run on each such file to produce a convenient HTML breakout of all the alerts.

Link:

< <http://net-security.org/various/software/970438840,60948,.shtml> >

---

#### PASSWORD PROTECTION 2.1

"Enable a login screen on your computer whenever you wish! Allows you the freedom to calmly leave big downloads running overnight, or keep co-workers out of your files. Comes with both picture and texture options; fully customizable."

Link:

< <http://net-security.org/various/software/970439089,22181,.shtml> >

---

#### DON'T PANIC V.1.2

Immediately clear cache, cookies, browser history, recently viewed documents, and other personal history lists without closing your browser or restarting your computer. Stop Internet Explorer pop-up windows without adjusting proxy settings, or adding sites to a list. Instantly hide or close any or all application/s with a mouse click or keystroke. Free up disk space and leave no telltale footprints behind. A network mode is included to alert and communicate between other Don't Panic users on a local network.

Link:

< <http://net-security.org/various/software/970439170,83102,.shtml> >

---

#### 4T PERSONAL V.1.4 (PALMOS)

4T Personal is a free, full-featured personal information storage application that is used to store valuable, yet varied information such as bank account information, credit card numbers, email, phone cards, and so on. 4T Personal is password protected and utilizes a 448-bit encryption scheme (Blowfish) for secure data. Pull-down menus are utilized throughout to make data entry simple. Other features include user-customizable categories, a customizable password generator, a quick

lock icon, and login screen password protection.

Link:

< <http://net-security.org/various/software/970439247,52341,.shtml> >

-----  
Defaced archives  
-----

[24.09.2000] - Washington Red Cross

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/24/www.washingtonredcross.org/>

[24.09.2000] - Metropolitan Washington Airports Authority

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/24/www.metwashairports.com/>

[24.09.2000] - Bureau of Medicine and Surgery, Naval Computer and Telecommunications Station

Original: <http://med01.nctsw.navy.mil/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/24/med01.nctsw.navy.mil/>

[24.09.2000] - Hackers Haven

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/24/www.hackers.com/>

[24.09.2000] - PalmComputing.com

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/24/www.palmcomputing.com/>

[25.09.2000] - DISA Information Systems Center

Original: <http://maestro.den.disa.mil/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/25/maestro.den.disa.mil/>

[26.09.2000] - Sourceforge.Net

Original: <http://linuxplace.sourceforge.net/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/27/linuxplace.sourceforge.net/>

[27.09.2000] - Committee for the National Institute for the Environment

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/27/www.cnie.org/>

[28.09.2000] - Census 2000, New York State Government

Original: <http://www.census2000.state.ny.us/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/28/www.census2000.state.ny.us/>

[28.09.2000] - Computer Networking Associates

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/28/www.cnanet.com/>

[28.09.2000] - #2 Slashdot

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/28/www.slashdot.org/>

[29.09.2000] - Mail Server for Vtay Technology

Original: <http://mail.vtay.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/29/mail.vtay.com/>

[29.09.2000] - Aviation Systems Division, NASA Ames Research Center

Original: <http://www.aviationsystemsdivision.arc.nasa.gov/>

Defaced:

<http://www.attrition.org/mirror/attrition/2000/09/29/www.aviationsystemsdivision.arc.nasa.gov/>

[29.09.2000] - Linux Ink

Original: <http://www.linux-ink.ru/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/29/www.linux-ink.ru/>

[30.09.2000] - r00tz

Original: <http://www.r00tz.net/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/30/www.r00tz.net/>

[30.09.2000] - National Oceanic and Atmospheric Admin

Original: <http://storms-dev.nos.noaa.gov/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/30/storms-dev.nos.noaa.gov/>

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

Help Net Security staff

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

<http://net-security.org>