

HNS Newsletter  
Issue 31 - 25.09.2000  
<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

=====  
Sponsored by Dialego - Online Market Research  
=====  
We conduct the first world-wide online survey for IT-security specialists. Please click [http://www.dialego.de/1033\\_it/\\_e/sman.php3?co=e](http://www.dialego.de/1033_it/_e/sman.php3?co=e) , fill in the online questionnaire and you may be one of the lucky people to win prizes in the amount of altogether € [EURO] 1500:  
1st prize: Casio Digital Camera  
2nd prize: 3Com Palm Personal Digital Assistant  
3rd prize: Tandem parachute jump  
plus 50 personal firewalls as individual protection for your computer plus 50 programs for boot protection and hard disk encryption  
=====

General security news  
-----

-----  
**GUIDE - BUILDING A DHCP SERVER**

A DHCP server is incredibly easy to set up in Linux. This guide at FrankenLinux.com will help you do it in 12 minutes. Also, we have an article dealing with DHCP in our Articles section.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.frankenlinux.com/guides/dhcpserver.html)

[bin/news.cgi?url=http://www.frankenlinux.com/guides/dhcpserver.html](http://www.frankenlinux.com/guides/dhcpserver.html)

Link: [http://www.net-security.org/text/articles/lg\\_3.shtml](http://www.net-security.org/text/articles/lg_3.shtml)

**NEW BLOW TO INTERNET BANKING SECURITY**

The future of internet banking was thrown into chaos last night after a British computer expert accessed bank account details of

millions of Americans from his home in the Isle of Man during a routine check on his US bank account. Ralph Dressel, a 28-year-old software analyst at Royal Skandia Investment bank, contacted The Observer having obtained bank security details that allowed him to "walk" straight into internet bank accounts at institutions across the US.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.guardian.co.uk/internetnews/story/0,7369,372676,00.html>

#### E-MAIL TAMPERING

A Singaporean man was sentenced to five months in jail for illegally accessing the e-mail account of his former girlfriend, making him the first to be convicted of such a crime in the city-state, the Straits Times reported several days ago.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://web.lexis-nexis.com/more/cahners-chicago/11407/6341404/2>

#### THE :CUECAT PRIVACY ADVISORY

The Privacy Foundation has released an advisory this morning calling for changes in the way the :CueCat bar code scanner is tracking users. The full text of the advisory is available on the following link

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.privacyfoundation.org/advisories/advCueCat.html>

#### CARNIVORE FAQ

Our affiliates at LinuxSecurity.com host a rather large Carnivore FAQ (Frequently Asked Questions). Document provides some answers to common questions posted about Carnivore.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxsecurity.com/resource\\_files/documentation/carnivore-faq.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxsecurity.com/resource_files/documentation/carnivore-faq.html)

#### PRIVACY CONCERNS OVER AUSTRALIAN E-HEALTH NETWORK RISE

There have been a number of calls for a slow-down in the implementation of an Australia-wide electronic health network as consumer groups and privacy advocates become concerned over the security and uses made of patients' medical information.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computeruser.com/news/00/09/23/news8.html>

#### ATTACKERS

Two attackers, who allegedly entered the National Aeronautics and Space Agency (NASA) and other government and university computers, are feeling the real-time pinch of the long arm of the law.

Link: <http://www.32bitsonline.com/article.php3?file=news/200009/nb200009221&page=1>

#### PHONE.COM TAKES AIM AT WAP SECURITY HOLE

In current WAP transmissions, data must use two security protocols - WTLS during the wireless part of the journey and SSL once the data hits the wires. There is a split second when the data must decrypt and

re-encrypt to switch from one protocol to the other. A security flaw could occur if someone was able to crash the machine in the split second between decryption and re-encryption, causing a memory dump to the disk.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/38/ns-18063.html>

#### WAP VERSION OF HELP NET SECURITY

Help Net Security is available for viewing via WAP enabled GSM appliances. With a script created by Gordan Gledec you can read latest security news on your GSM phone or any other device that uses WAP. If you are interested how it looks like visit the following link (powered by Gelon Wapalizer).

Link: <http://wap.net-security.org/wap/>

#### "COMRADE" SENTENCED TO 6 MONTHS

A 16-year-old Miami male pleaded guilty to two acts of juvenile delinquency for computer hacking and was sentenced to six months in a detention facility, said attorney general Janet Reno Thursday.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.techweb.com/wire/story/TWB20000921S0023>

#### HERBLESS INTERVIEWED

PhantasmP of HWA-Security yesterday interviewed one of the names that were in the news for the past few days - Herbless. He is connected to some defacements where he put his opinions on DeCSS and fuel situation and if you saw the item below, he announced he quits defacing.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://hwa-security.net/herbless.txt>

#### HERBLESS QUILTS

Herbless, who defaced the websites of HSBC, Legoland and 450 others as part of the fuel protest in the last month, has announced his sudden exit from the scene. Speaking exclusively to vnunet.com, Herbless said: "For various reasons that may or may not become apparent, I have left the hacking scene for good. You won't hear of any more defacements by Herbless. Let's just say that it is the price of freedom, and is worth paying."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1111333>

#### AOL'S LOOSE CANNON: JUSTIN FRANKEL

The programmer's an employee of America Online, but the creator of Gnutella's has a funny way of saying thank you. Frankel has, in fact, devised some software, but not the kind AOL was expecting. The latest creation of the 21-year-old programmer enables users of AOL's wildly popular Instant Messenger to delete the ads from the online chat program. What's more, a Web site owned by Nullsoft, and ultimately AOL, has been giving away the software.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2630789,00.html>

#### VIDEO INTERVIEW

Mudge, @stake's Vice President of Research & Development, gives us his thoughts on the state of computer security today and why, as time has gone by, we still have a long way to go.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/media/64>

#### WHITE HAT HACKERS BREAK INTO VA BENEFITS COMPUTERS

At a House oversight subcommittee hearing today, the VA's inspector general's office said it had contracted with a private security company to conduct penetration tests of the department's computer systems, tests that led hired hackers to gain "high level" access to VA records.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.telekomnet.com/news/9-21-00\\_hackers\\_vacomputers.asp](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.telekomnet.com/news/9-21-00_hackers_vacomputers.asp)

#### MP3.COM OFFERS SECURE PAYMENTS SERVICE

Online music service provider MP3.com is offering a secure and convenient payment system with eCharge Corp. MP3.com customers can now purchase CDs and MP3.com merchandise online with an eCharge Net Account, which uses proprietary encryption technology and digital certificates.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.techweb.com/wire/story/TWB20000921S0012>

#### COMPANIES CAPITALISE ON WEB FRAUD FEARS

US credit card companies portray themselves as watchdogs guarding customers against Internet fraud, but some of their security measures are just clever marketing tools to win new customers. Credit card theft occurs three to ten times more online than it does in stores, and such card companies as American Express are rushing to devise online security measures to protect people.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/37/ns-18024.html>

#### THIS EMAIL WILL SELF-DESTRUCT

"SafeMessage is the electronic answer to the shredding machine. It is the first industrial-strength, secure messaging product of its kind for not only large corporations, but also individuals," said Graham Andrews, chief executive officer of AbsoluteFuture, which developed the product.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,38936,00.html>

#### TARGETING US-RUSSIAN EXERCISE

Hackers in the US attempted to disrupt a combined US-Russian exercise aimed at dealing with major natural disasters, reported AFP quoting the ITAR-TASS news agency. Looks fishy...

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/6/13420.html>

VBS.DISABLED.WORM

VBS.Disabled.Worm is a script worm that is similar in function to VBS.NewLove.Worm. It uses Microsoft Outlook to send itself. Upon execution, it deletes all files from your hard drive except for files in the root directory. The body of the email message is in French.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.symantec.com/avcenter/venc/data/vbs.disabled.worm.html>

COPA READIES ITS REPORT

A federally created commission studying online child protection will recommend to Congress that an independent research bureau be created to review filtering software and may also push for a special kid-friendly Internet zone, its chairman says.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.mercurycenter.com/svtech/news/breaking/ap/docs/4205291.htm>

ONLINE PRIVACY

Industry watchers say growing consumer concerns over the use of personal online data is a huge obstacle for e-commerce. So far, lawmakers have refrained from regulating general online privacy.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.techweb.com/wire/story/TWB20000920S0013>

GERMAN HACKER BIDS TO JOIN INTERNET BOARD

Andy Mueller-Maguhn, spokesman of the Chaos Computing Club, is one of seven candidates from Europe hoping to be elected to the board of the Internet Corporation for Assigned Names and Numbers (Icann). He is emerging as the surprise favourite with 2866 endorsements - more than any other candidate worldwide.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1111267>

NTBUGTRAQ ACQUIRED BY ICSA.NET

One of the places where NT hackers and security experts post their opinions and vulnerabilities has been acquired. Russ Cooper, moderator of the popular e-mail list NTBugTraq, sold the list to ICSA.net. He will stay aboard as the moderator of the list.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.msnbc.com/news/459092.asp>

-----

=====  
==

Sponsored by Dialego - Online Market Research

=====  
==

We conduct the first world-wide online survey for IT-security specialists. Please click [http://www.dialego.de/1033\\_it/\\_e/sman.php3?co=e](http://www.dialego.de/1033_it/_e/sman.php3?co=e) , fill in the online questionnaire and you may be one of the lucky people to win prizes in the amount of altogether € [EURO] 1500:

1st prize: Casio Digital Camera  
2nd prize: 3Com Palm Personal Digital Assistant  
3rd prize: Tandem parachute jump  
plus 50 personal firewalls as individual protection for your computer plus  
50 programs for boot protection and hard disk encryption

=====  
==

## Security issues

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

### ----- MAJOR VULNERABILITY IN ALABANZA CONTROL PANEL

This is serious enough since you can delete all resold domains for a particular webhosting company. You can also change the default MX and CNAME records of all associated domains.

Link: <http://www.net-security.org/text/bugs/969896875,69779,.shtml>

### E\*TRADE LOGINS/PASSWORDS REMOTELY RECOVERABLE

Due to flaws in E\*TRADE's software, a remote third party can recover the usernames and plain-text passwords of any E\*TRADE user. The vector of attack can be a malicious (but innocent looking) web site, an email, or a variety of more obscure methods. A local compromise of the user's machine is not required. The attacker only needs to seek out known or likely E\*TRADE users and contact them. The result of the attack is that the attacker will have the user's username and password. This will allow the attacker arbitrary access to the account, including banking, securities trading, and other valuable access.

Link: <http://www.net-security.org/text/bugs/969714869,69820,.shtml>

### MULTIPLE VULNERABILITIES IN CISCOSECURE ACS

Multiple vulnerabilities have been identified and fixed in CiscoSecure ACS for Windows NT Server:

- The CSAdmin software module can be forced to crash by sending it an oversized URL.
- CiscoSecure ACS for Windows NT Server can be placed into an unstable state by sending it an oversized TACACS+ packet.
- The enable password can be bypassed to gain unauthorized privileges on a router or switch when CiscoSecure ACS for Windows NT Server is used in conjunction with an LDAP server that allows users to have null passwords.

Link: <http://www.net-security.org/text/bugs/969635524,66062,.shtml>

### DOS IN BROWSEGATE (HOME) V2.80

Delphis Consulting Internet Security Team discovered that it's possible to cause Browsegate to crash with an invalid read error.

Link: <http://www.net-security.org/text/bugs/969580439,75618,.shtml>

#### RED HAT LINUX - GLINT SYMLINK VULNERABILITY

If a specific symlink exists in /tmp, glint will open it and write to it when run by root - so destruction of any file is possible. Note that glint does not work with RPM 3.0 or higher. If you have RPM 3.0 or higher installed, just uninstall the glint package to remove this vulnerability.

Link: <http://www.net-security.org/text/bugs/969580219,81985,.shtml>

#### EXTENT RBS DIRECTORY TRANSVERSAL

Extent RBS allows users to register a new subscription via Credit Card through their web browser. The problem is that the web server does not check for directory transversal when reading image files. Thus any file available on the same partition (in WinNT or any file on the \*NIX system) which Extent RBS has permissions to read, can be read by a malicious user.

Link: <http://www.net-security.org/text/bugs/969579949,36863,.shtml>

#### EXPLOIT USING EUDORA AND THE GUNINSKI HOLE

Eudora saves all attachments in a single directory upon receiving the mail; a mail message need not be open for its attachment to be decoded and saved in that common directory. An intruder need only send an e-mail with a trojaned DLL as described in the Guninski advisory, along with or followed by an e-mail containing a Word document.

Link: <http://www.net-security.org/text/bugs/969408551,99330,.shtml>

#### WINCOM LPD DOS

A continuous stream of LPD options, sent to the LPD port (default TCP port 515) on the host running WinCOM, will eventually consume all the memory on that host. Systems Affected: WinCOM LPD V1.00.90 for Windows NT

Link: <http://www.net-security.org/text/bugs/969406272,66800,.shtml>

#### DIGITAL UNIX KDEBUGD REMOTE VULNERABILITY

The kdebug daemon can be exploited by remote users to open and display the contents of any file on the system. It can also be used to write to the beginning of any file on the system overwriting data which was previously there. Affected: Digital UNIX 4.0F, other versions believed to be as well but untested.

Link: <http://www.net-security.org/text/bugs/969406252,65377,.shtml>

-----  
Security world  
-----

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

#### ----- DIGITAL: CONVERGENCE EXPERIENCES SECURITY BREACH - [20.09.2000]

Internet technology company Digital:Convergence Corporation experienced a security breach that may have exposed certain members' names and email

addresses. The company was alerted of breach efforts by Peter Thomas at Securitywatch.com. The company has secured the site and is conducting a thorough security examination.

Press release:

< <http://www.net-security.org/text/press/969275944,52786,.shtml> >

---

#### XCERT PROVIDES SECURITY FOR SMART VISA PLATFORM - [20.09.2000]

Xcert, a leading provider of software products for securing Internet transactions and communications, announced that its Sentry CA public key infrastructure software is being offered as part of Visa U.S.A.'s newly introduced smart Visa Technology Platform. Xcert's technology, a component of the smart Visa Access application provides the foundation for secure Internet access using a smart Visa card.

Press release:

< <http://www.net-security.org/text/press/969318536,94967,.shtml> >

---

#### INTEL BRINGS NETWORK SECURITY TO MOBILE PCs - [20.09.2000]

Addressing a gap in network security solutions, Intel Corporation announced the industry's first high-speed, security network adapters for mobile PCs. Intel also introduced updated LAN security connections for desktop PCs and servers. The new connections help protect confidential information, such as intellectual property, financial transactions, human resource records and customer demographics, transmitted across a local area network (LAN).

Press release:

< <http://www.net-security.org/text/press/969318710,4731,.shtml> >

---

#### PDS 2100 SECURITY APPLIANCE FROM INTRUSION.COM - [20.09.2000]

Intrusion.com, Inc., a leading provider of enterprise security solutions for the information-driven economy, announced a new class of low-cost security appliances targeted at small offices. The SecureCom PDS 2100 appliance series, designed for maximum flexibility and ease of use, will initially feature Check Point Software's VPN-1/FireWall-1 SmallOffice security software, also announced by Check Point, for a combined price starting under \$1,800.

Press release:

< <http://www.net-security.org/text/press/969318830,3134,.shtml> >

---

#### FREE SECURITY MANAGEMENT SOLUTION FOR LINUX - [20.09.2000]

Solsoft, Inc., the leading provider of policy management for e-Business security, announced immediate availability of the newest version of its free Linux security management solution. Following the success of its first release of Solsoft-NP-Lite for Linux in July, the new version, called Solsoft NP-Lite 4.0, offers robust

functionality including: a new visual interface for easier definition of the security policies, an enhanced compiler for optimized filters and performance, and a new Policy Audit function for a better view of defined policies and existing breaches.

Press release:

< <http://www.net-security.org/text/press/969378146,17801,.shtml> >

---

#### ICSA.NET ACQUIRES NTBUGTRAQ - [20.09.2000]

ICSA.net, the global leader in Internet security, has acquired NTBugtraq, the leading source for Microsoft-related security intelligence, and hired its owner, Russ Cooper, to continue managing the service. NTBugtraq is an Internet-based forum that encourages security technicians to discuss and notify other professionals about Windows-based vulnerabilities.

Press release:

< <http://www.net-security.org/text/press/969407614,32192,.shtml> >

---

#### PROTEGRITY ADDS PKI FUNCTIONALITY TO SECURE.DATA - [20.09.2000]

Protegrity, Inc., the leading provider of solutions that protect franchise data, announced at the Baltimore Technologies Global e/Security 2000 Convention that it has licensed Baltimore KeyTools to enable public key infrastructure (PKI) interoperability in its Secure.Data information-privacy solution.

Press release:

< <http://www.net-security.org/text/press/969409157,9537,.shtml> >

---

#### FIREWALL AND IPSEC COMPLIANT VPN FROM ELRON - [20.09.2000]

Cayman Systems, Inc., a global provider of broadband gateway solutions, announced a joint business initiative with Elron Software. As the first step in the initiative to offer value added services, Cayman adds Elron's Internet Manager Firewall(TM) and IPSEC compliant VPN security software to its 3220 and 2E500 gateway product families, further strengthening the security capabilities already packed into the products.

Press release:

< <http://www.net-security.org/text/press/969409232,14973,.shtml> >

---

#### SYMANTEC ANNOUNCES PRODUCT SUPPORT FOR WIN2000 - [20.09.2000]

Symantec Corp., a world leader in Internet security, announced product support for the new Windows Millennium Edition operating system. With the new OS focusing heavily on the connected consumer experience, many of Symantec's best-of-breed solutions will provide users the safety and protection they require while surfing the Internet. The following Symantec solutions are Windows Me compatible: Norton SystemWorks 2001, Norton SystemWorks 2001 Professional Edition, Norton Internet Security 2001, Norton Internet Security 2001 Family

Edition, Norton Personal Firewall 2001, Norton AntiVirus 2001, Norton Utilities 2001, Norton CleanSweep 2001 and Norton Ghost 2001.

Press release:

< <http://www.net-security.org/text/press/969409302,92874,.shtml> >

---

#### SMARTGUARD RELEASED BY V-ONE - [20.09.2000]

V-ONE Corporation, a leading provider of Virtual Private Networks, released the latest version of its award-winning SmartGuard Security Appliance, which now includes Secure Multiple Unit Management over the Internet and IPSec for Site-to-Site using IKE. These features enhance the robust VPN capabilities already included in SmartGuard version 1.0

Press release:

< <http://www.net-security.org/text/press/969409654,65302,.shtml> >

---

#### WATCHGUARD LIVESECURITY SERVICE - [20.09.2000]

Further expanding the reach of its LiveSecurity Service, WatchGuard Technologies announced that its Internet security software and services will be automatically available in wired homes using Leviton's new Vestal Router. Leviton will market the Vestal Router to builders and contractors nationwide, as well as to individual homeowners doing remodeling projects or upgrading their homes to support computer networks and Internet access. WatchGuard will operate the LiveSecurity Service, delivering firewall protection to owners of these "wired homes."

Press release:

< <http://www.net-security.org/text/press/969450519,49878,.shtml> >

---

#### CYLINK SECURES BLUETOOTH WIRELESS NET TECHNOLOGY - [20.09.2000]

Secure e-business pioneer Cylink Corporation announced that its SAFER+ encryption algorithm is being used for user authentication within Bluetooth, a protocol that is rapidly growing in use for wireless communications. More than 1,700 companies support the Bluetooth protocol. With Bluetooth-enabled devices, a wireless personal area network (PAN) for mobile commerce can easily be created using peripheral devices, notebooks or handheld computers, smart telephones, and even vending machines. The SAFER+ algorithm is one section of the Bluetooth protocol. The algorithm enables one user to send a test message to a recipient for encryption and compare the returned encrypted message with his own encryption of the test message. A perfect match verifies the recipient's authenticity.

Press release:

< <http://www.net-security.org/text/press/969460501,25978,.shtml> >

---

#### SECURE COMPUTING SECURES ERICSSON R380 SMARTPHONE - [21.09.2000]

Secure Computing and Ericsson today announced that the Ericsson R380

smartphone is available on GSM markets with Secure Computing's SafeWord authentication token. Now, SafeWord users can use the R380 smartphone to authenticate to networks and applications protected by SafeWord.

Press release:

< <http://www.net-security.org/text/press/969549592,49689,.shtml> >

---

#### WATCHGUARD RECEIVES COMMON CRITERIA CERTIFICATION - [21.09.2000]

WatchGuard Technologies, Inc., a leader in Internet security solutions, announced that its LiveSecurity System and the Firebox II firewall appliance have been awarded Common Criteria Certification. WatchGuard's Firebox II is the first firewall appliance for the small to medium size enterprise market to receive this certification. Some U.S. government agencies and certain countries require that Internet security products they purchase meet Common Criteria Certification.

Press release:

< <http://www.net-security.org/text/press/969549687,31372,.shtml> >

---

#### ONLINE CREDIT CARD FRAUD-ELIMINATING TECHNOLOGY - [22.09.2000]

What is the biggest barrier to the growth of e-commerce and the Internet and prevents more than half of the world's Internet users from making an online purchase? Fears of online credit card fraud and security and privacy issues. iShopSecure, Inc., a privately-held company based in Davie, Florida, has launched a patent-pending technology and business process that eliminates credit card fraud and allows consumers to shop from more than 750,000 web sites without putting their credit card or other personal information online.

Press release:

< <http://www.net-security.org/text/press/969585687,91319,.shtml> >

---

#### IDENTIX COMBINES TWO SECTORS INTO SECURITY DIVISION - [22.09.2000]

Identix Inc., a worldwide leader in providing user authentication, security and identification solutions, Friday announced that it has established a new organizational structure for its commercial market products, combining its Physical Access and IT divisions into one division, Security.

Press release:

< <http://www.net-security.org/text/press/969635824,19544,.shtml> >

---

#### PRIVACY FOUNDATION'S OPINION ON CUECAT ISSUE - [23.09.2000]

Marketers of the :CueCat, a new consumer electronics device that attaches to PCs and TV sets, should disable a personal tracking feature and disclose more details about how information collected will be used, the Privacy Foundation requested today. "The Privacy Foundation has serious privacy concerns with the :CueCat," said Richard M. Smith, chief technology officer of the foundation.

"We are asking the company to fix the service now, before it is in widespread use."

Press release:

< <http://www.net-security.org/text/press/969715210,80941,.shtml> >

---

#### VISA PARTNERS WITH SECURIFY - [24.09.2000]

Securify, a leading eSecurity services provider, announced its appointment by Visa U.S.A. to manage smart Visa Access, a key component of the smart Visa Technology Platform. The smart Visa Technology Platform is a new payment card platform with multi-function capabilities powered by cutting edge chip technology. The smart Visa card enables Visa financial institutions to combine the purchasing power of traditional payment cards with smart chip technology to offer added security, utility and convenience to consumers. The smart Visa Access system, a critical component of the smart Visa Technology Platform, authenticates Visa cardholders, thus allowing banks to offer secure, personalized services delivered through the Internet.

Press release:

< <http://www.net-security.org/text/press/969750752,5714,.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.

---

#### ISSUES: HIRING HACKERS, THE FINE LINE BETWEEN CULT AND CRIMINAL by Thejian

Obviously there are a lot of technically talented individuals running around in the hacking scene nowadays. There always have, it's the root of its existence. This has given birth to another interesting issue. Besides hacking being marketable and trendy, the underground today has the full attention of the corporate world where the skills are recognized (in some) and could be put to good use as well. In short, hiring hackers, if not good for profits at least is the trendy thing to do. And looking at the security problems some companies are having that definately is a good thing. However, it also raises the question of trust.

Article:

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

---

#### SECURING A REDHAT LINUX 6.2 MACHINE (BASICS) by bokuden

This article covers the basics of making a virgin redhat install more or less secure before putting it on the internet. Remember all of this work should be done before the box is put online, as machines can be rooted in minutes of being on the net.

Article:

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

---

#### THE SECRETS OF SNOOP by Lance Spitzner

How to best leverage the network sniffer snoop, with various command line examples. Included are examples on how to analyze network traffic and improve your network security.

Article:

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

---

#### DETECTION OF AN UNKNOWN VIRUS by Kaspersky Lab

In this chapter we discuss the situations which user faces when he suspects, that his computer is infected, but none of the anti-viruses known to him tested positive. How and where to look for virus? What tools are needed for that, what methods to use and what rules to follow?

Article:

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

---

#### VIRUS ALGORITHM ANALYSIS by Kaspersky Lab

"To my mind the most suitable object for keeping and analyzing the virus is a file containing the virus body. In practice to analyze the file virus it is convenient to have several infected files of different, but not too large, size. Except that it is desirable to have infected files of all kinds (COM, EXE, SYS, BAT, NewEXE) that this virus can infect..."

Article:

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

---

#### RECOVERY OF AFFECTED OBJECTS by Kaspersky Lab

In most cases of viral infection the procedure of recovery of infected files and disks means running a suitable anti-virus capable of disarming the system. However, in the virus is not known to any anti-virus, it is enough to send the infected file to anti-virus developer companies, and in some time (usually several days or weeks) receive the cure updates for this virus. But if time presses, you will have to disarm the virus yourself.

Article:

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

---

## PACIFIC BELL ALERTS CUSTOMERS TO 90# SCAM

Pacific Bell is alerting consumers and advising them how to protect themselves from a telephone scam that is once again generating e-mail traffic on the Internet. If consumers receive a call from someone claiming to be a telephone technician, seeking to test the phone line and requesting that consumers dial 90#, consumers should hang up immediately without dialing the requested numbers. Residential and business customers are targeted.

Article:

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

---

## ANTI-VIRUS PROGRAMS by Andrew Krukov, AVP Team

I would like to point out that there are no anti-viruses guaranteeing 100 percent protection from viruses. Any declarations about their existence may be considered to be either an advertising trick or a sign of incompetence. Such systems do not exist because for each anti-virus algorithm it is always possible to suggest virus counter algorithm, making this particular virus invisible for this particular anti-virus (fortunately the opposite is also true: for any anti-virus algorithm it is always possible to create an anti-virus).

Article:

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

---

## KASPERSKY LAB MAKES LINUX EVEN MORE SECURE

Kaspersky Lab, an international anti-virus software development company, announces a new version of Kaspersky Anti-Virus (AVP) for Linux. This latest version combines unique functionality, significantly simplifying the program's use and the world's first anti-virus solution to integrate into the popular e-mail gateways Sendmail and Qmail.

Article:

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

---

## "JAVANIZATION" OF MOBILE PHONES: A GREEN LIGHT FOR MALICIOUS PROGRAMS?

On 19 August, Sun Microsystems and some of its partners announced the shipment of Mobile Information Device (MID) standard, based on the Java programming language (Java™ 2 Platform Micro Edition – J2ME) for use on mobile phones. At the same time, Motorola, one of the biggest companies for the development of wireless technologies, released an application programming interface (API), allowing for the development of additional programs for its wireless devices.

Article:

< <http://www.net-security.org/text/articles/viruses/javanization.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](mailto:staff@net-security.org)

---

### ENHANCED IP SERVICES FOR CISCO NETWORKS: A PRACTICAL RESOURCE FOR DEPLOYING QUALITY OF SERVICE, SECURITY, IP ROUTING, AND VPN SERVICES

The book provides a useful and instructive breakdown of each enhanced service: what it is, why you need it, how it works, how to deploy it, how to validate it. This book offers a practical guide to implementing IPsec, the IOS Firewall, and IOS Intrusion Detection System. Also included are advanced routing principles and quality of service features that focus on improving the capability of your network. A good briefing on cryptography fully explains the science that makes VPNs possible. Rather than being another routing book, this is a guide to improving you network's capabilities by understanding and using the sophisticated features available to you in Cisco's IOS software.

Book:  
< <http://www.amazon.com/exec/obidos/ASIN/1578701066/netsecurity> >

---

### JAVA SECURITY

This book is extraordinary both for its technical depth and its readability. It provides the Java programmer with a complete overview of the Java security architecture and security classes, plus a wealth of detailed information and code examples for specific implementations. The following chapters look in depth at the elements of the Java security architecture: language rules, class loaders, the security manager, the access controller, and permission objects. All these chapters provide detailed information on implementation, as well as an excellent explanation of the role of each feature within the entire security picture. The second half of the book covers cryptographic features in the Java security package and how Java programs work with code that performs authentication and encryption. Here, you'll find detailed chapters on message digests, keys and certificates, key management, digital signatures, and the Java Cryptography Extensions. Anyone who needs to understand Java security, but especially those who will implement security features in Java applications, will want this book.

Book:  
< <http://www.amazon.com/exec/obidos/ASIN/1565924037/netsecurity> >

---

## JAVA 2 NETWORK SECURITY

Rather than focusing on how a Java system can be broken, the authors show managers, network administrators, developers, and security professionals how Java can be made secure and how to exploit its strengths. Topics include the pros and cons of each Java security alternative; architectural techniques for maximizing security; securing Web and intranet applications; deploying or limiting Java across firewalls; integrating Java and SSL; and using Java's Cryptography APIs. The disk contains source code and links to Java security Web sites.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0130155926/netsecurity> >

---

## LINUX SYSTEM SECURITY: THE ADMINISTRATOR'S GUIDE TO OPEN SOURCE SECURITY TOOLS

The introduction of Linux System Security acknowledges that there's no magic bullet as far as security is concerned. Security-minded system administration is a process of constant revision. It promises, though, that "if you follow the procedures outlined, you will certainly reduce your level of vulnerability." The book delivers on that promise in spades. Using Red Hat Linux as the demonstration environment, the authors explain how to use a suite of publicly available tools to analyze, protect, and monitor your machines and networks. They approach the subject from a practical standpoint, emphasizing software and its use while referring the reader (using copious bibliographic notes) to more specialized works for detailed information on cryptography, firewall configuration, and other subjects.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0130158070/netsecurity> >

---

## IMPLEMENTING AS/400 SECURITY

A concise, practical guide to implementing, evaluating, and auditing an AS/400 security strategy. This edition (first was 1992) brings together the fundamental AS/400 security tools and experience-based recommendations, and includes the security enhancements available in OS/400 Version 3 Release 1.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1882419782/netsecurity> >

---

## Security Software

---

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

---

### AMAVIS 0.2.1-PRE3

AMaViS (A Mail Virus Scanner) scans e-mail attachments for viruses using third-party virus scanners available for UNIX environments. It resides on a UNIX (Linux) machine and looks through the attached files arriving via e-mail, generates reports when a virus is found and sets the delivery on hold.

Link:

< <http://net-security.org/various/software/969754025,36384,.shtml> >

---

### PHPSECUREPAGES 0.19B

phpSecurePages is a PHP module to secures pages with a login name and password. It can handle multiple user groups (each with their own viewing rights), store data in a MySQL database or a configuration file, and be used to identify your Web site viewers. It also has multiple language support and session support for both PHP3 and PHP4.

Link:

< <http://net-security.org/various/software/969753951,18916,.shtml> >

---

### KILL THE SPAMS V.1.03

From the developer: "Kill The Spams is anti-spam software using a unique algorithm to detect unsolicited emails. If you're tired of unsolicited commercial e-mail clogging your inbox, you're not alone. Surveys have proven again and again that most Internet users detest it. The main goal is to filter your e-mail box without the pain of building complex filters. Unlike other similar products, KTS does not need to maintain a list of spammers."

Link:

< <http://net-security.org/various/software/969380297,16138,.shtml> >

---

### SPAMMOTEL V.1.2

This is a Web-based antispam program that gives you complete control of your email address without using filters. SpamMotel lets you attach reminder notes each time you give out an email address online, so you'll know exactly when and where the spammer got your email address, and then lets you stop spam from that sender. This free program works with your existing email account. A small downloadable interface makes access easy, and requires no installation on your computer. A handy online Log Page lets you view all your SpamMotel activity. This program is also useful in organizing your email folders more effectively.

Link:

< <http://net-security.org/various/software/969379780,9260,.shtml> >

---

### PC DOORS GUARD V.1.0.1.6

PC Doors Guard is a complete anti-Trojan solution for your office and home PCs. The program consists of three main utilities, which can provide you with stable and reliable protection. A Trojan needs to get through this three-folded barrier in order to infect your PC. While online updates keep PC Doors Guard up to date, the built-in heuristic analyzer can detect a Trojan without using any virus database. The Monitor utility constantly verifies the files you download, get via ICQ, or receive by e-mail; the Executor checks any file before it is executed; and the Scanner provides you with a virus search engine so that stealth, phantom, and worm viruses do not get away.

Link:

< <http://net-security.org/various/software/968808468,3315,.shtml> >

-----

#### INTERSCAN WEBPROTECT V2.2

InterScan WebProtect is a real-time virus scanning package that works with Microsoft Proxy server. It protects proxy server traffic from computer virus infections and malicious JAVA and ActiveX code. It auto-cleans infected files transferred via HTTP or FTP. WebProtect has additional security features that let you selectively control the type of material that are downloaded from the Internet.

Link:

< <http://net-security.org/various/software/968808271,26573,.shtml> >

-----

#### Defaced archives

-----

[18.09.2000] - Sandia National Laboratories

Original: <http://samt4831.sandia.gov/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/18/samt4831.sandia.gov/>

[18.09.2000] - Idaho State Government

Original: <http://www.sapd.state.id.us/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/18/www.sapd.state.id.us/>

[18.09.2000] - Gujarat (GOV)

Original: <http://mail.gujarat.gov.in/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/18/mail.gujarat.gov.in/>

[19.09.2000] - The Temple of Yehwe

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/19/www.vodou.org/>

[20.09.2000] - The Colorado Springs Gazette Telegraph

Original: <http://www.appeal-democrat.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/20/www.appeal-democrat.com/>

[20.09.2000] - The Orange County Register

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/20/www.freedom.com/>

[21.09.2000] - Ministry of Foreign Affairs, Albania

Original: <http://www.mfa.gov.al/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/21/www.mfa.gov.al/>

[21.09.2000] - Journal des Finances

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/21/www.jdf.com/>

[22.09.2000] - Planet Quake (Germany)

Original: <http://www.planetquake.de/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/22/www.planetquake.de/>

[22.09.2000] - Sigma Computer Training & Consulting, Inc.

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/22/www.sigmacomputerc.com/>

[23.09.2000] - NetAgent

Original: <http://www.crack-contest.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/23/www.crack-contest.com/>

[23.09.2000] - The George Washington University Hospital

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/23/www.gwhospital.com/>

[23.09.2000] - National Library of Ireland

Original: <http://www.nli.ie/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/23/www.nli.ie/>

[0.09.2000] - University of USA

Original: <http://www.usa.edu.ph/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/09/23/www.usa.edu.ph/>

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

Help Net Security staff

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

<http://net-security.org>