FIFA WORLD CUP 2010 - NETWORK SECURITY ADVISORY

Hakin9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

Vol.5 No.6
Issue 6/2010(31)
1733-7186

SECURING VOIP

WEAKNESS, EXPLOITS AND PROACTIVE DEFENSES

BIRTH OF AN EVIL TWIN
- TAKING SOCIAL ENGINEERING TO THE SOCIAL WEB

HACKING THE BAD GUYS

HIJACKING SSL - SSLSTRIP ON WINDOWS

GPS TRACKING WITH MOBILE PHONE

DISCLOSURE POLICIES

PLUS

MANAGING YOUR FACEBOOK PRIVACY IN 2010
BY JULIAN EVANS

Safety and Security vs Freight Mov

There is no advertisement like reputation

"While the CEH certification program served as a launching point for students, into the various realms of security, I found it didn't go to the depths that eLearnSecurity's program has reached, on the technical portions of penetration testing. While CEH had numerous tools and usage details, eLearnSecurity's training really dove deep into the underlying concepts beneath such tools."

Timothy E. Everson | Novell, Inc.

"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.
eLearnSecurity's course is easy to follow the whole way through with appropriate breaks for video and sprinkled exercises at every turn.
I am very impressed by the product as a whole and congratulate Armando and Team in an exceptional first run of the course"

Jason Haddix | EthicalHacker.net

"If you are just starting out I think the course and the certification will definitely have a positive effect on your career.
It goes into a lot more depth than courses like CEH and can really benefit your skills.
The way in which the material is presented is a lot more interactive and interesting than many other courses out there with a good mix of words, images and videos plus a good theory/practical mix too.
I wish there was something like this in 1999 when I was starting out."

Shaolin Tiger | Darknet.org.uk

Amen.

www.elearnsecurity.com

Hakin9 team

Editor in Chief: Karolina Lesińska
karolina.lesinska@hakin9.org
Advisory Editor: Ewa Dudzic
ewa.dudzic@hakin9.org

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

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

Proofreaders: 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: Paweł Marciniak

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

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

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

Subscription: Iwona Brzezik
Email: *iwona.brzezik@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

EDITOR'S NOTE

Dear Readers,

We receive from you lots of comments and opinions, most of them positive especially after going online. We are very happy that this decision was enthusiastically welcomed! The point of this change was to make Hakin9 magazine available for everyone having access to the Internet and not limit the audience to US only. And well, the numbers are saying everything:) It was worth to do it!

But coming back to this issue...As you've seen on the cover this issue is partially devoted to VoIP and its security, as it was one of the hottest topics lately.

Also, there is a lot of talking about Facebook security in the last days. That is why for this issue, Julian Evans, our ID fraud expert, wrote a great article about Facebook privacy in 2010. Don't worry - we did not forget about soccer fans! Derek Manky, Cyber Security & Threat Research at Fortinet, gives you a brief view on SEO attacks on FIFA World Cup 2010.

Enjoy!
Karolina Lesińska
Editor-in-Chief

REGULARS

BASICS

ATTACK

DEFENSE

More Twitter hacks and one Twitter hacker arrested

He's 24 years old and not a hacker at all. He had just successfully guessed the answer to the password reset secret question of Obama and other celebrities Twitter accounts. The Frenchman has been arrested thanks to the cooperation of the French police and the FBI and will have to face jail time and a fine of up to €30,000. The young man who, according to Mr. Coquillat, French state prosecutor, had no training in computer, did not post anything on behalf of the hacked personalities and did not try to profit financially of his hack, dated back to April 2009. The Frenchman, whose name is still not public, living in his parents house in Puy-de-Dôme and not even having a lawyer, is a low hanging fruit, but a fruit that had made a lot of noise at the time of the hack. Twitter hacks, however, have been going on and the latest to fall victim is Tory MP Therese Coffey, newly elected member of the British parliament. This time the hacker, who goes by the handle of thegh0st, has posted offensive twit messages on behalf of the deputy targeting prime minister's wife Samantha Cameron. Miss Coffey has readily apologized from her blog but she's still trying to get her Twitter back in control.

Source: Armando Romeo, www.elearnsecurity.com

EFF and Tor project team up to bring HTTPS Everywhere

No script and Tor are two add-ons that the cybersecurity savvy cannot do without during web browsing. The first provides protection from a number of script injection and phishing threats, the latter allows the browser to tunnel the connection through a number of nodes that make the originator of the request virtually untraceable. Until now, the use of an encrypted channel was a choice left to the website: Google uses SSL for Gmail but still not for the Search. Same thing happens with Wikipedia or a number of other sites that do not default to an encrypted connection. EFF, The Electronic Frontier Foundation and the The Tor Project have now announced the availability of the beta version of HTTPS Everywhere. The project aims at redirecting you to the secure versions of each of the major websites on the net (Google, Wikipedia, Facebook…) by rewriting the links in the page towards their secure version. The most visible example of the case addressed by the joint-venture is Google, defaulting its search to HTTP but still providing an HTTPS version of the same feature.

The add-on works through a rule-set that the user can easily beef-up with additional websites not covered in the off-the-shelf Add-on package available from the Eff.org/https-everywhere webpage.

Source: Armando Romeo, www.elearnsecurity.com

AT&T exposure of 114,000 iPad users emails – Hacker arrested

In early June a breaking news of a hacking group who had exposed over 114,000 emails from At&t hit all the security websites, magazines and TV. Only 20 days after the author of the hack, or at least the representative of the hacking group responsible, has been arrested and then released after posting $3,160 bond on felony drug possession charges. Andrew Auernheimer, is a 24 years old exponent of the Goatse Security group that had uncovered a small but effective hack in At&t website. Cocaine, Ecstasy and LSD was found in Auernheimer's house on an FBI's search that has not yet been clarified if related to the At&t hack or not. The hack gained the group 114,000 email addresses of iPad 3G Subscribers including a number of military officials, politicians among which New York Mayor Michael Bloomberg and White House Chief of Staff Rahm Emanuel. The group at the time of the hack realized that by providing the SIM card serial numbers to a webpage of the At&t website, allowed gaining the correspondent email address. Since these serial numbers are released in sequential order, running a very simple tool allowed the group to enumerate thousands of emails in no time. Immediate warning was given to the Telco company that admitted and immediately fixed the issue. Although the only information to be gained was the email address related to the iPad user, the hack could *allow someone who does the proper research to possibly target iPad 3G users and take over their iPads, and they could sniff traffic, they could act as the user of the iPad* according to Goatse analyst Jim Jeffers.

Source: Armando Romeo, www.elearnsecurity.com

Apple quietly secures your Snow Leopard

There's a common misbelief among non-Windows users: my OS is immune from security threats, malwares and viruses. While this could have been true, at some extent, many years ago, now it just sounds arrogant and anachronistic. Malware for Mac OS does exist and it's becoming more and more widespread. In particular OSX/Pinheard-B, as categorized by Sophos, and better known as HellRTS is a malware that gives complete remote control of the infected OS-X machine: you can take snapshots, send emails, transfer files and log keystrokes from the victim. Apple, however, seems to be pleased by this misbelief and doesn't do anything to wake up its users to the malware call: an update to Snow Leopard included a silent update to Xprotect.plist. XProtect is, in the words of Graham Cluley Senior Security Consultant at Sophos, a *rudimentary file that contains elementary signatures of a handful of Mac threats*. Starting from version 10.6, OS-X users are warned when suspicious files are downloaded and executed from Entourage, Safari, Mail, Thunderbird and other browsing

tools. This kind of protection is rather sloppy as malware can get through by means of Skype, BitTorrent or other tools that are currently unsupported by Mac OS-X builtin signature-based malware protection.

Source: Armando Romeo, www.elearnsecurity.com

Secure calls and text messages with Moxie's RedPhone

Moxie Marlinspike is a Pittsburgh hacker and security researcher author of papers and famous tools such as sslstrip, presented at BlackHat DC 2009 and sslsniff. His last venture is a startup, Whisper Systems, that has one precise scope: securing mobile phone calls and text messages storage. RedPhone, the solution proposed by Moxie, is an Android app that uses Phil Zimmerman's ZRTP encryption protocol to secure VOIP calls on the fly making them hard to eavesdrop. Any two phones with this app installed are enabled to secure communication without ever noticing the app running: as stated by Moxie *Our main aim is to make this [secure communication] as easy as possible*. The app allows confidentiality by means of encryption and also authentication by means of a passphrase generated from the two peers keys: it is easy, from a user point of view, to verify that no man-in-the-middle is there. The other application, TextSecure addresses the need for having a secure storage of one's SMS's. The two applications, still in beta version, will likely remain free, while premium versions could be released for small fees.

Source: Armando Romeo, www.elearnsecurity.com

Fake YouTube pages continue to be a threat

A leading internet security company has identified more than 700,000 web pages which look like they are real YouTube pages (including the YouTube logo to add authenticity). In fact they are fake pages delivering malware to users computers. The malicious pages claim to contain a *hot video* associated with the Gulf oil spill, NBA Playoffs, Harry Potter and other popular topics. If a user inadvertently plays the video from one of the fake pages a pop up appears informing them that they need to download and install a media codec file. If the user clicks *OK* the users browser will be redirected (see: browser redirector) to a malware infected website. The malware infected website promotes scareware and rogue antivirus software. The malware is being propagated using poisoned search results.

World of Warcraft detected as malware

Symantec admitted recently that their Norton Internet Security Suite labels files associated with World of Warcraft as malicious. The security suite deleted the files it thought were malware, causing the game to stop working and computers to crash while booting. Symantec have highlighted that the Norton Internet Security Suite suffers from ten to forty false positives per month – which unfortunately also included World of Warcraft. False positives are looked at by humans, so it's easy to see why the error occurred. The updated World of Warcraft file (*svchost.exe*) was analysing the system which made it appear as a suspicious file. Sometimes security products accidentally delete important system files due to false positives but it doesn't happen that often. There is of course a failsafe in most if not all security software which will not allow removal of critical system files.

Malware targets Windows Mobile

Scammers are distributing apps for Windows Mobile-based smartphones that have malware hidden inside that makes calls to premium-rate numbers across the globe, racking up expensive bills unbeknownst to the phone's owner. The apps – 3D Anti-Terrorist game, PDA Poker Art and codec pack for Windows Mobile 1.0 – are being distributed on as many as nine popular download websites, including DoDownload, GearDownload and Software112, according to John Hering, chief executive and founder of mobile security provider Lookout. Someone has copied the programs and repackaged them with the malware inside, he said. Once the app is installed the virus wakes up and starts dialing premium-rate numbers like in Somalia and the South Pole, Hering said. He added that victims may not know about the problem until they get their phone bill and see that it is $50 (£35) or $100 higher than it should be.

Hacker finds serious SQL injection flaw with website

An attacker has discovered a serious flaw in a website set up to encourage the use of smart cards for public transportation in the Netherlands, resulting in the leakage of personal information of more than 168,000 travelers.

The website offered a coupon for a free trip using the OV smart card system and was set up to promote the new system which is being slowly rolled out throughout the region. According to Webwerld, a tech publication based in the Netherlands, the names, addresses and telephone numbers of individuals who signed up were publicly available as a result of the flaw. Information about the flaw was exposed by an anonymous hacker who gave the magazine a video demonstrating the error using a SQL injection attack. The hacker told the magazine that he made the flaw publicly available because there is no excuse for simple website mistakes. The website has since been taken offline. In this instance, the hack appears to have orchestrated with the interests of exposing poor security, rather than stealing users' data and identities.

Source: ID Theft Protect

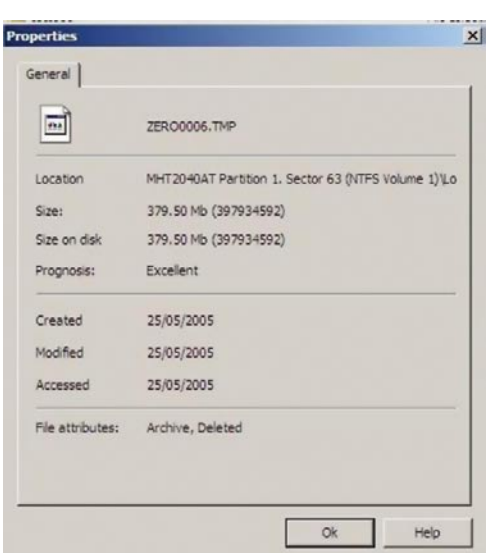
NTFS Mechanic Disk & Data Recovery for NTFS Drives

Items Tested:
40GB External USB HDD that has had an extensive amount of files written to it, and then randomly deleted, approximately 16GB in total and has intermittant connection issues to the point that the local machine doesn't actually register the drive is there.

Once I had the software installed it was time to see how it performs. I plugged the external drive in and then powered up the software. It saw my drive straight away, but it didnt actually state what disk format the drive actually was. This might be due to the fact that the operating system didn't actually find the drive itself, so it was a pleasant surprise that this program did indeed find it.

You are able to configure what types of files you actually want the program to be searching for during the recovery process, for this test I just left everything as default which means everything was selected.

I selected my external USB Drive and it scanned the partitions first to ensure that it can actually see the drive correctly. Once this part of the process has been completed it then requests that you allow it to scan the whole partition that you have selected, this appears to be a very cpu intensive program so I would suggest to just leave it running on its own if possible. It took just over an hour to scan through a 40GB hard drive. Once it was finished NTFS Mechanic provides all the data thats on the drive, deleted and non-deleted files. You can select in the right hand menu to only see the recovered files, which makes it a lot easier to see what the program has actually found.



Pricing
Standard $99.95
Business $199.95
Professional $299.95
Prices are in US Dollars

If you look at the properties of the files and folders that have been listed as being recovered, you can actually see the prognosis of each file if you decided to proceed and recover the file completely.

The process for recovery couldn't be much easier, it's simply a case of going through the folder list and selecting the files you want to recover and then just say where you want them to be stored.

The program performs really well and managed to recover data from a disk that hasn't been seen by any of my machines for a little while now which quite impressed me.

I noticed that there were a few area's within the program that could do with some QA work as there were non english characters in use and some screens weren't actually needed in my opinion but they arent detrimental to the product.

I would gladly have this tool in my toolbox.

http://recoverymechanic.com/ntfs_recovery/ntfs_mechanic.php

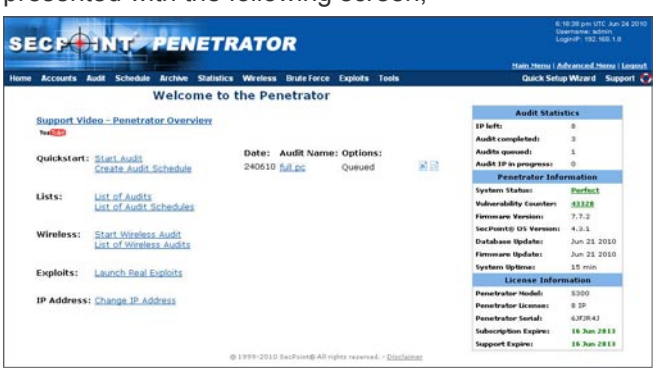
Partition Recovery
Hard Drive Recovery
Recover deleted files

by Michael Munt

Secpoint Penetrator

by Michael Munt

The Secpoint Penetrator S300 comes in a small form factor Dell Optiplex unit. All you need to do is plug it in as the operating system and programs etc are already pre-configured for ease of use. Just connect to the system via your local machines' browser and you're ready to go. Once you are logged in you are presented with the following screen;



Auditing

There are two options available to use when auditing; a quick audit or a full scan with an option to schedule your scans. Ideal for those who want to put it into the server room and then to perform a monthly audit of the servers or certain parts of the network. This is also an excellent option for those of you that want to be able to offer this as a managed service to your clients. You are also able to see trends on the audits by comparing each scan against the others that have happened in the past.

Quick Audit

This is a small basic audit that scans the known TCP ports and then performs checks against 20 known vulnerabilities to see if your system is susceptible.

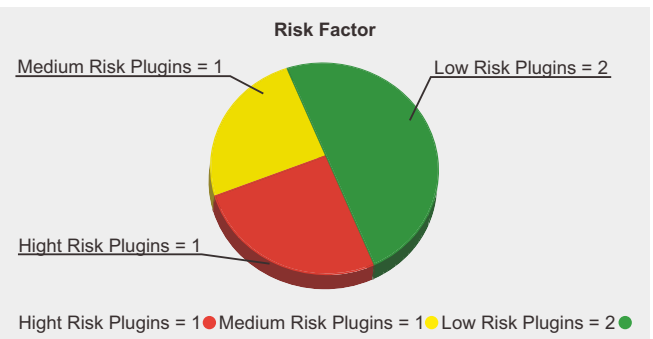
Full Scan

The full scan option will perform an assessment of your requested systems, you have the option to enhance this audit by allowing the system to actually deliver the payload against the machines in question. The Penetrator database of vulnerabilities is currently in excess of 42,000 and is continually growing, as you receive updates throughout the day. Once the audit has completed you are presented with the options on how you would like to view the results.

Reporting

There are two main report options available to you; the Executive summary or the full report (including solutions to the vulnerabilities it has identified). The Executive summary is aimed at the management types and provides enough information concerning the audit, including graphical detail and the amount of vulnerabilities found. The full scan goes into a lot further detail with information on each vulnerability found and a resolution on how to prevent this from being exploited in the future.

An overall risk factor graphic is provided which gives you an immediate indication as to how secure or insecure you are.



You are able to customise and personalise the reporting so that you can insert your own company logo etc which will enable you to sell these to your customers (this is permitted within the licencing of the unit).

Overall Impressions

Whether you are a professional tester or just starting out this unit is a complete solution for testing your own or your customers' networks. Its ease of use is a serious advantage as you wouldn't need to spend time and effort in configuring the system up etc apart from the initial wizards. Once you have scheduled all your audits, you can tuck it away somewhere and forget about it, although you could have it sitting under your desk and would never know it was there, as its almost silent operation had myself checking on more than one occasion to ensure it was turned on.

The sensible clear layout of the menu's makes it so simple to use, that even complete beginners will be using this within 15 minutes. The help documentation provided is of first rate and clear about what you need to do for each section. If you're not the "manual" type each section has a video tutorial attached to it as well.

Finally I have to say something about the support I received when I had some difficulties with my unit. I can some it up in one word. Superb! They were very quick on their initial response and kept me up-to date throughout the issue. Even offering to remote in to the machine to double check that I hadn't made a simple mistake. Once it was all resolved, they still followed up the next day to ensure I was still working properly. This has got to be one of the best levels of support I have received in a very very long time.

URL: *http://www.secpoint.com/penetrator.html*
Product SP-S300-8-1YB
Price (Euro's)949.00

Elcomsoft iPhone Password Breaker

Items Tested

Elcomsoft's new tool iPhone Password Breaker provides a quick reliable and light weight password breaker. It can be purchased and downloaded from *www.crackpassword.com*

Although they do have a free version on the website it does have limitations. It supports password protected backups to iPhone 2G,3G,3GS, and iPod Touch 1st 2nd and 3rd Gen devices.

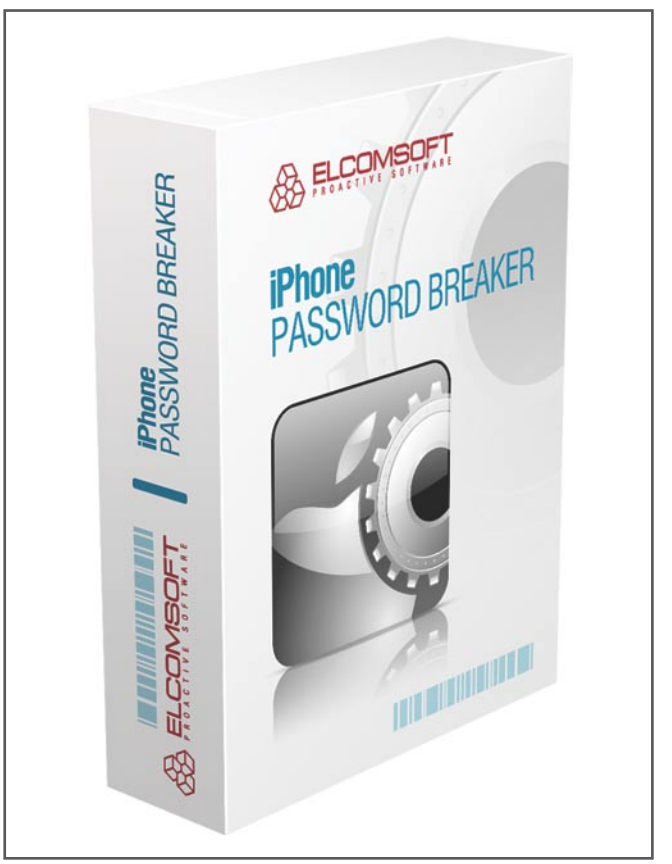
I recently tested this software on a Windows XP machine on a iPhone 3G encypted backup. The installation process was quick and to the point. Upon startup you will have to browse for the encypted iPhone backup file. In Windows you should be able to find it under C:\Documents and Settings\ YourUserName\Application Data\Apple Computer\ MobileSync\Backup. If you are unable to find it there I would suggest you do a search for "Manifest.plist".

On another note, if you select a file that isn't encrypted then it will not work and you will get an error message that tells you the backup isn't encypted. Once you have found your encypted plist file you will then select a password breaking option either a Brute Force attack or a wordlist attack with the ability to specify a text or dictionary file.

When it comes to wordlist it will depend on how good your password list is, however, if you are doing a brute force on a numbered passcode then it will find it within a matter of seconds if not sooner. It found my

4 digit passcode in 0.83 seconds. In the real world an outright brute force attack against anything with upwards of 5 characters including symbols and upper and lower case characters will take substantially longer but with the iPhone password breaker you will be well on your way to finding that encrytped password. Password Breaker also gives you the ability to select multiple processors under the Recovery --> Options Tab. Here you can select multiple processors to work on your job or select only one if you are in need of the resources for something else.

All in all a great tool and one that I highly recommend adding to your toolkit.



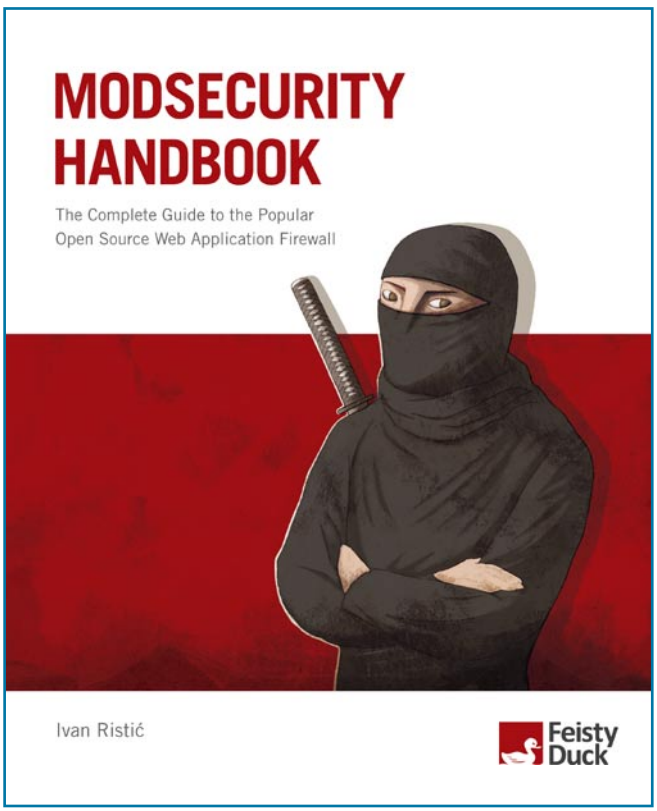
URL: http://www.elcomsoft.com/eppb.html
Cost:
Home Edition 79€
Professional Edition 199€

WARDELL MOTLEY JR.

Wardell Motley is a Systems Administrator for a Large clothing Manufactures in Dallas Texas.

He is a member of the ISSA and InfraGard and in his spare time works as freelance IT security researcher.

Modsecurity Handbook



URL: https://www.feistyduck.com/
Author: Ivan Ristic
ISBN-10: 1907117024
ISBN-13: 978-1907117022
Cost: L29.95

For those of you who have never heard of Modsecurity, it is in essence an Open Source Web Application Firewall, but this is just a small part of the complete toolkit of what this application really is. Ivan himself refers to it as a HTTP Intrusion Protection tool but admits this still isn't a true description of what it can do and he should know as he started working on the project in 2002 and still has his hand in today.

I haven't used this application myself, so I was a bit apprehensive in the beginning especially when I looked at the table of contents (all 14 pages of it, and the book is only 340 pages in total length!) Looking very much like a large manual I was pleasantly surprised at how easy the book was to read, the technical sections are fully explained and well thought out with plenty of examples throughout the book, which are really useful to ensure that the information is retained and understood correctly.

The book is broken down into sections which enable you to either delve into area's that you need to without having to read it from cover to cover (which you should really do as even the most experienced Modsecurity users will find something new in here I am sure). Right from the beginning of the book you are taken step by step on how to install and configure your Modsecurity setup all the way down to the little details. When the application is updated and we all know software is updated all the time, the publishers have promised to keep the book information upto date with an electronic online version which I believe is a unique feature for a technical book, and keeps things in touch with the Open Source mindset. This book has actually given me enough enthusiasm to want to go setup and install Modsecurity itself on a system somewhere to have a play and put some of the information imparted to me to some good use.

It was a pleasure to read this book, and I wish there were more authors like this that have such passion about a particular subject that it infects the reader!

by Michael Munt

Disclosure Policies

How to proceed with researched vulnerabilities and what or how much information regarding it should be disclosed, has always been a controversial topic and double-edged sword.

What you will learn…

- basic approaches in terms of researched vulnerabilities and their (dis)advantages

What you should know…

- for this article no special requirements are needed

A questions to which there seems to be often no right or wrong answer, and often requires further investigation before a certain pattern can be followed strictly. Although various approaches addressed to this topic exists, none was yet established, which could please all parties involved. The following will therefore explain the most common methods in more detail and takes up some of the advantages and disadvantages, which occur frequently within discussions on this topic.

Full Disclosure

In Full Disclosure all information regarding a certain vulnerability are disclosed and made publicly available. Here not only the information itself is published, namely that a specific vulnerability was discovered in a particular product and version of it, but also detailed information regarding discovery and exploitation. This way companies and developers should be forced to release a patch or another solution as fast as possible. Otherwise concerned systems are not only longer vulnerable for exploitation, but also a considerable reputation damage and so thoroughly a customer and money loss are likely to happen. Security should therefore be increased, as the time period in which a system is vulnerable, gets shortened.

In Full Dosclosure it's often assumed, that black hats are already aware of a certain vulnerability and exploit it actively. By disclosuing all details to the public, each party can respond early and prepare their own arrangements, which hinder further exploitation of their systems, as long as no patch is available. This may include such measures as disabling an affected service or changing configuration files, depending on the scenario and vulnerability. Ideally, full disclosure should also lead software manufacturers to invest more effort and time into quality assurance, rather than using end customers as their final instance of beta testing.

Opponents of full disclosure often critizice the fact, that developers are only informed about a vulneraility at the same time as the general public, which results in an enourmous pressure towards companies and developers. As everyone get the information at the same time, a guaranteed time window is created in which a system is vulnerable to exploitation, even when

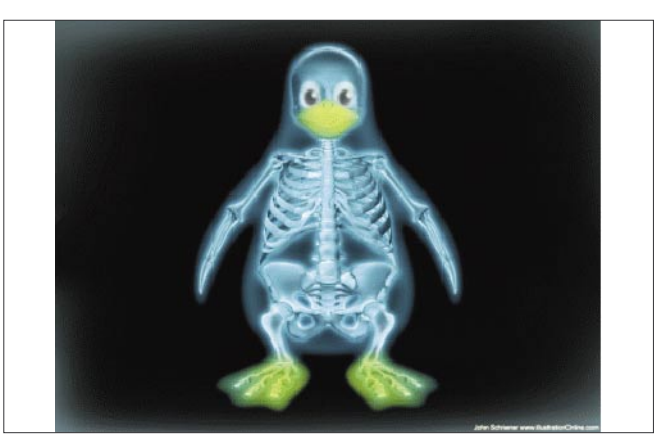


Figure 1. *How much should be disclosed? (Source: John Schriener, http://illustrationonline.com/)*

working immediatley after announcement on a solution. Additionally often together with the announcement or shortly after, automated exploitingtools are published, which enables also scriptkiddies to successfully exploit a vulnerable system, even if the background and functionality is not understood.

Non-Disclosure

Non-Disclosure is essentially the opposite of full disclosure. This means that an approach is pursuied, where found flaws in software are kept private, and at best only in a selected circle, often within an internal group, are shared.

In the past it was shown that some vendors and researches have pursued this philosophy and still do, although they have received harsh criticism because of it. From a developer's perspective it's thereby attempted to keep a vulnerability secret until a patch was developed which closes the flaw. Here, however, a big problem arises, which is about the selection of people who should be notified. Is it sufficient that only internal developers are aware of the vulnerability, or should e.g. also operators of critical systems be informed about it (such as hospitals, nuclear plants, etc.)? Who guarantees that the shared information are kept private and are not shared by anyone or published, or even worse, used for one's private benefit?

It may also not be assumed that no one else has already found the same vulnerability, only because nothing was published regarding it. If both, developers and researchers don't publish any information in general, the real problem is not solved and system administrators won't be able to protect their systems. Unfortnately some companies imply that it's sufficient to close a security vulnerability only if it was found by others and further details were released among with it.

Limited Disclosure

Limited Disclosure pursues firstly a similar approach as non-disclosre, though it is tried to disclose all details of a vulnerability to the stakeholders. Mostly this includes the researcher herself, the manufacuterer or developer of the affected product and sometimes an independed third-party, which acts as an intermediary between researcher and developers. To the public it's only announced, that a vulnerability was found in a specific product, but further details are not disclosed. Usually, a precise explanation of all the details is even then not disclosed, after a fix was supplied by the manufacturer.

The goal of limited disclosure, then, is to publish only those information, which are essential to know in order to protect a system. In the view of limited disclosure the publication of further and more detailed information would in the first place only serve black hats, which is the reason why it's simply disclaimed.

Bibliography and further ressources:

- *http://www.schneier.com/crypto-gram-0002.html#PublicizingVulnerabilities* – Crypto-Gram Newsletter, February 15, 2000, Bruce Schneier
- *http://www.schneier.com/crypto-gram-0111.html#1* – Crypto-Gram Newsletter, November 15, 2001, Bruce Schneier
- *http://www.wiretrip.net/rfp/policy.html* – RFPolicy v2.0
- *http://www.securityfocus.com/columnists/66 – Responsible Disclosure* Draft Could Have Legal Muscle
- *http://www.sans.org/reading_room/whitepapers/threats/define-responsible-disclosure_932* – How do we define Responsible Disclosure?
- *http://labs.idefense.com/vcp/* – Vulnerability Contributor Program
- *http://www.zerodayinitiative.com/* – Zero Day Initiative
- *http://www.securityfocus.com/archive/* – BugTraq
- *http://www.cve.mitre.org/* – Common Vulnerabilities and Exposures
- *http://osvdb.org/* – The Open Source Vulnerability Database
- *http://secunia.com/* – Secunia
- *http://oss-security.openwall.org/wiki/mailing-lists/vendor-sec* – vendor-sec
- *http://wikileaks.org/* – WikiLeaks
- *http://en.wikipedia.org/wiki/Full_disclosure#History* – Full disclosure history

Using this disclosure philosophy leads to similar problems as within other disclosure methods. First it has to be assured that the information are only disclosed to ethical people who don't utilize the newly gained knowledge for their personal gain. Also there is too little pressure on the developers to fix the flaw in the shortest possible time, as the general publih is not initially informed about the vulnerability. Since only a very vague announcement is made, many system administrators may not be able to secure their systems until a patch or solution from the vendor is provided. Ultimately here again it can not be assumed that the black hat community is not already aware of the specific vulnerability and exploiting it actively.

Responsible Disclosure

A commonly used policy is known as responsible disclosure. Here the developer or vendor is contacted first, before the full information is released into the public. This should ensure that developers are granted a specific time period in which they can take care of the problem, but the public still gets all the details, even if it's somewhat delayed. In contrast to full disclosure, however, an attached exploit-code is often missing; general information, technical details and ideally a patch but are still published.

How much time is allocated to such an ultimatum differs from case to case, common are often several weeks to months though. Regardless of the time limit given, it should not be extended continously, as some vendors try to delay it as long as possible, often with the goal, to push it so long away until it becomes no longer relevant or another solution has shown; so to say that it is not handled as their primary goal to close the security flaw.

Unfortunately some developers and vendors consider it as a personal insult or attack if a vulnerability or security flaw in one of their products is reported to them. As a result of this it often happens that such messages are just ignored or worse, that the discoverer gets threatened with legal actions. That those two approaches can't be purposeful may be obious to many readers, but unfortunaly this happens in reality quite often and can be seen over and over. In this case the information is then usually just published to the public without further caring of the vendor.

The concept of responsible disclosure, therefore, is to notify first the vendor so that a patch can be provided as quickly as possible, and only with some delay, the general public. Published information should still include all the details necessary to safeguard ones system, ideally already together with a patch supplied by the developers itself.

Conclusion

The market for exploits and their acquisition, especially for 0-day-exploits, seems to enjoy a steady growth and it can be assumed that it will still increase by a multiple. A standardized policy, which addresses all the needs from all involved parties, would be appreciateable, but seems to be possible in an utopia only.

Which disclosure policy is executed at the end has to be decided by everyone on their own. Many of the existing methods seem to have a right to exist and for some scenarios, some methods are probably not even come into question.

The initial problem, namely the existence of security flaws and breaches, could already be significantly reduced if companies and developers would put more effort into *secure programming* and a better *quality assurance* (or often even could). The implementation seems, however, often difficult, although all parties involved would benefit from a more secure and error-free software.

MICHAEL R. HEINZL

Michael R. Heinzl is engaged with it-security and related areas for some years, especially with penetration testing and reverse code engineering. Contact is possible through http://awesec.com or through the Austrian security website https://defense.at.

Burp Scanner. Don’t trust the monkeys.

GPS Tracking

with mobile phone

Sometimes I like to do mountain excursion, going through new paths.

What you will learn…

- the use of a GPS application for your mobile phone
- how to see the points received from the GPS of your mobile phone on pc
- how to integrate applications from different systems (mobile phone, pc, web server)
- introduction to Android development and GPS handling (for the advanced part)
- how to parse xml files with php (for the advanced part)
- how to use Google Maps (for the advanced part)

What you should know…

- how to install an application on the mobile phone
- how to read the mobile phone uSD from pc
- what is an xml file
- programming understanding of java/php/javascript (for the advanced part)

Sometimes, back home, I tried to understand which course I did looking at a map, but with 100 doubts on where and when I was exactly. Now, luckily, there are satellite navigators, but not all offer the possibility to keep track of the traveled route and have details on exact traveling times.

What do you say about using a mobile phone to collect time/position data and visualize the route on computer later on?

Requirements:

- a mobile phone android with GPS and a uSD memory
- a computer with SD reader and an internet connection
- an adapter from uSD to SD

The software to install on mobile phone is GPSLogger, available for free at: *http://www.androlib.com/android.application.com-mendhak-gpslogger-ipxp.aspx* or *http://apps.doubletwist.com/GPS-Logger-for-Android/-2727505723369031487*.

After starting the application go to *Menu>Settings* (see Figure 1) and select *Log to GPX* (in this way logs will be saved on files with *.gpx* extension inside the uSD memory), then select a value for *Time before logging*, so that position will be saved with the preferred frequency (I use 60 seconds and 0 meters as *Distance before logging*).

Few minutes before going outside home click on *Start logging*. You'll notice that logging needs a bit of time to start, so be patient. The application is trying to detect

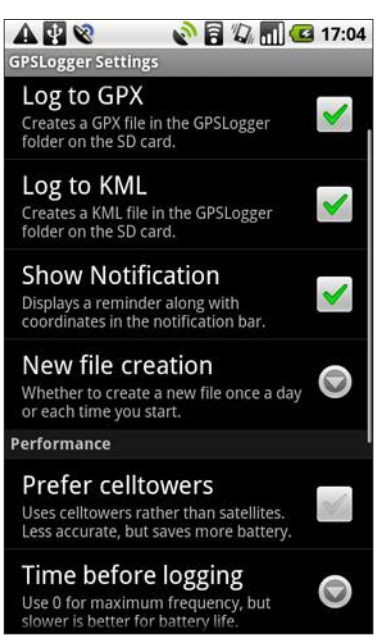


Figure 1. *GPSLogger settings*

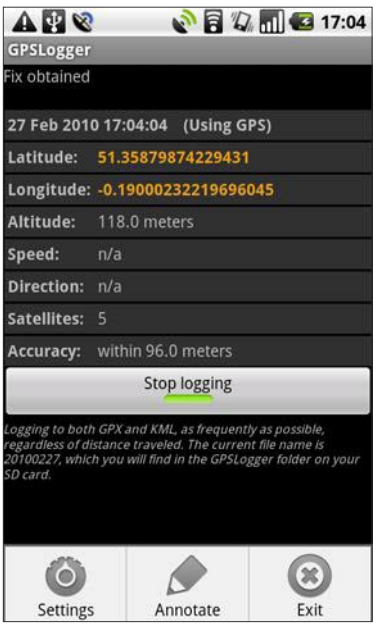


Figure 2. *GPSLogger getting the current position*

the starting position looking for a GPS signal on many satellites. The more it will find, the better the accuracy will be. You should begin to see the coordinates of your position as shown on Figure 2.

Once back home extract the uSD memory from mobile phone and insert it in a uSD to SD adapter (see Figure 3). Then put the adapter inside the SD slot of the computer. This memory uses a vfat file system, it should be automatically detected (on OpenSuse it's mounted on `/media/disk`). You'll notice a file like `/mount_dir/GPSLogger/20100413.gpx` where the file name matches the data `yearmonthday.gpx` when logging.

gpx is an xml file with this format

```
<?xml version="1.0"?>
<gpx … >
  <time>2010-04-13T16:22:05+02:00</time>
  <bounds />
  <trk>
    <trkseg>
      <trkpt lat="44.35" lon="12.15">
        <ele>121.0</ele>
        <src>gps</src>
        <sat>4</sat>
        <time>2010-04-13T16:22:05+02:00</time>
      </trkpt>
...
```

where each point (called also track point or in short: trkpt) is saved with 2 attributes `lat=latitude`, `lon=longitude`, and other information is presented as child elements (time, elevation, speed etc)..

To visualize easily these files I made a php script that you can access on my server *http://g1ld0.is-a-geek.net/gps_track/*.

Table 1. *Definition of track points, <gpx><trk><trkseg><trkpt>*

Attribute	Child Element	Meaning	Mandatory
lat		latitude	yes
lon		longitude	yes
	ele	elevation [m]	no
	course	direction	no
	speed	speed [m/s]	no
	src	gps or wifi data	yes
	sat	number of satellites	no
	time	time	yes

Just upload the file, the script will parse the xml file and extract for each node time, logitude, latitude and, if present, also elevation and speed, and the path is built as you can see in Figure 4.

I've noticed when browsing the sources that the author foresee to deliver a new version of the application with the possibility to visualize the map directly on the mobile phone. For the moment, however, this option is not active. Also, from the sources it seems that the user/password authentication will be required to use this service.

How the code works

Dalvik

Majority of the applications for Android are written in Java. Not every standard java class is available, but you can find many adjunctive classes that allow to develop easily applications using mobile hardware features (like fotocamera, bluetooth, telephony, SMS, GPS, touch screen etc.).

The virtual machine interpreting these applications is called Dalvik. If someone is interested in the development there is an eclipse plugin allowing easy development of applications for Android and an emulator to run and test applications on pc without the need of a connected phone.

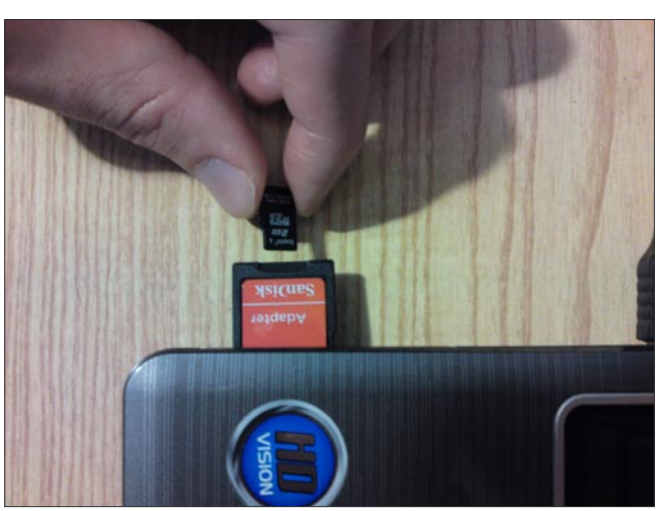


Figure 3. *The adapter for uSD card to read it from pc.*

Listing 1. *How the telephone acquires GPS positions*

```
android.location.LocationManager gpsLocationManager;
gpsLocationManager = (LocationManager) getSystemService(Context.LOCATION_SERVICE);
gpsLocationManager.requestLocationUpdates(LocationManager.GPS_PROVIDER,minimumSeconds * 1000,minimumDistance,
                    gpsLocationListener);
gpsLocationManager.addGpsStatusListener(gpsLocationListener);
```

Let's see very quickly how GPSLogger uses the GPS functionality. I used the class android.location. LocationManager is needed to request updates on the current position. Updates on position are sent to a class `GeneralLocationListener` implementing the interface `android.location.LocationListener`. Roughly speaking the code asking updates is this: see Listing 1.

During the logging the function `onLocationChanged(Location loc)` (*http://developer.android.com/reference/android/location/GpsStatus.Listener.html#onGpsStatusChanged(int)*)of object `gpsLocationListener` will be automatically called with new data on current position inside paramter loc.

For anyone interested, the official documentation of `android.location.LocationManager` can be found here: *http://developer.android.com/reference/android/location/LocationManager.html*.

PHP Script

In the PHP script for paring the xml file on the web server, once read file content inside string `$data`, I've created an `$xml` object with the function `simplexml_load_string()`. Then, I read each `<trkpt>` node in this way:

```
  // create xml object
$xml = simplexml_load_string($data);
  // look for each node <gpx><trk><trkseg><trkpt>
foreach ($xml->trk->trkseg->trkpt as $node)
{
  $lat=$node['lat'];   //latitude
  $lon=$node['lon']; //longitude
…
```

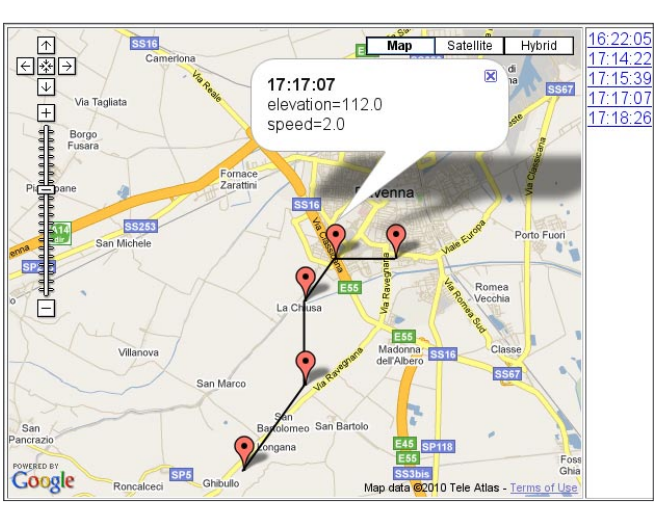


Figure 4. *Screenshot of the track of traveled path*

JavaScript and Google Maps

To represent the path with Google Maps, for each node found the php script prints these JavaScript lines (simplifying a bit):

```
// create the point with latitude lat and longitude lon
point = new GLatLng(lat,lon);
// create the point marker
marker = new GMarker(point);
map.addOverlay(marker);
path.push(point);
```

Also clicking on the track points the JavaScript lets us open a small frame with information such as elevation and speed (if available).

In the end, in order to draw the path with a polyline the Google Maps Api provide the function `GPolyline()`, that takes as first mandatory argument the array `path` with track points filled before:

```
var polyline=new GPolyline(path,'#000000',2,1.0);
map.addOverlay(polyline);
```

Conclusion

In the first part we have seen how to use GPSTrack to save the information on the travelled path on the uSD memory of the mobile phone and how to view it on the browser of the pc.

The second part instead deals with programming details of all the components mentioned, from the Android application to the server side script creating the Google Map.

A short description of GPSLogger allowed us to introduce a powerful framework for the development of Android applications. After that we looked on server side at the handling of the generated xml file performed with few lines of Php. This occasion was taken to spend few words also on the usage of the Google Maps Apis to show the travelled path on the web page.

MAURO MENEGHIN

Italian Mechanical Engineer, age 31, actually working as high school teacher. Hobby: software programming and hacking from 10 years.

Passware

Passware Password Recovery Kit Forensic 10.0

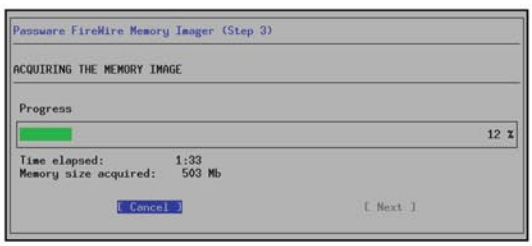
A Complete Password Recovery and E-Discovery Solution for Computer Forensics

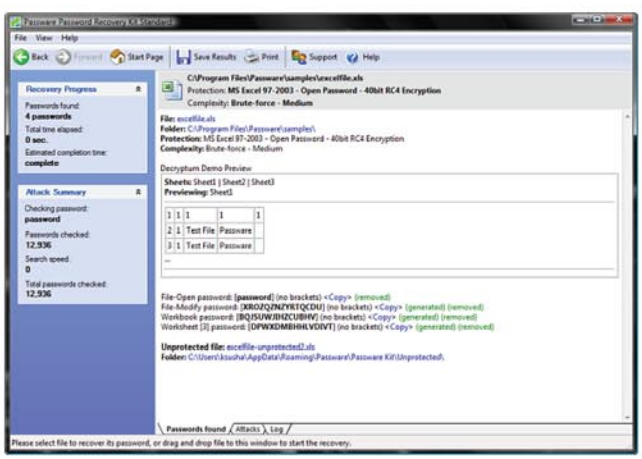
Now with Distributed Password Recovery and instant TrueCrypt decryption!

Passware Kit Forensic includes over 30 password recovery tools, Encryption Analyzer Professional, Search Index Examiner, FireWire Memory Imager, and a Portable Version to provide immediate password recovery for any protected file detected on a PC or over the network while scanning. It recovers or resets passwords for more than 180 different types of files, as well as decrypts hard drives, PGP archives, and unlocks Windows 7 Administrator accounts. Many types of passwords are recovered or reset instantly.

Key Features

- Scans computers and network for password-protected files
- Recovers passwords for **180+ file types**
- Unlocks hard drives protected with **BitLocker** and **TrueCrypt** New!
- Retrieves electronic evidence in a matter of minutes from a Windows Desktop Search Database
- Includes **Portable Version** that runs from a USB thumb drive and recovers passwords without installation on a target PC
- Acquires memory images over FireWire New!





> *Let me just say "well done" . Excellent software, excellent support. I have watched this software evolve over the past six year. World class stuff.*
>
> **Craig Vogel, myComputerGuy, inc.**

> *After losing my password to important encrypted documents, I thought it was the end of the world. Thanks for saving my work, Passware.*
>
> **Conor LaHiff, LaHiff & Company.**

Advanced Features

- Instant recovery for many password types
- Acceleration with distributed computing **(Distributed Password Recovery)** New!
- Multiple-core CPUs and nVidia GPUs acceleration
- **Tableau TACC** hardware acceleration
- 8 different password recovery attacks (and any combination of them) with an easy-to-use setup wizard
- Detailed reports with MD5 hash values

5 editions for consumers, small business, professional, corporate, and forensic users.

Starting from **$49!**

For additional information, please visit:
www.lostpassword.com/kit-forensic.htm

Pass ware In c.
800 West El Camino Real, Suite 180
Mountain View CA 94040

Contacts
Nataly Koukoushkina
media@lostpassword.com
Phone: +1 (650) 450-4607

30 DAYS MONEY BACK GUARANTEE

Hijacking SSL

SSLStrip on Windows

This article is about a demonstration of SSL hacking using the SSLStrip tool.

What you will learn…

- What is NULL prefix attack
- How SSLStrip exploits it to carry out SSL hijacking
- How to run SSLStrip on Windows machine
- How to mitigate the problem with SSL certificates

What you should know…

- Basics of SSL and Certificates

It discusses the weakness in the SSL certificate signing request which gets exploited for making fake certificates. Finally, the article shows how to run the SSLStrip tool on Windows and hijack the SSL successfully.

What is SSLStrip

The SSLStrip works by watching http traffic, then by acting as a proxy when a user attempts to initiate an https session. While the user believes the secure session has been initiated, and SSLStrip has connected to the secure server via https, all traffic between the user and SSLStrip is http. The SSLStrip replaces all links with *https://* in the page with *http://*. Warnings usually displayed by the browser don't appear and the session appears normal to the end-user. Login details can then be harvested.

The author of the tool Moxie Marlinspike says: *This tool provides a demonstration of the HTTPS stripping attacks that were presented at Black Hat DC 2009. It will transparently hijack HTTP traffic on a network, watch for HTTPS links and redirects, and then map those links into either look-alike HTTP links or homograph-similar HTTPS links. It also supports modes for supplying a favicon which looks like a lock icon, selective logging, and session denial*.

An https padlock logo can be spoofed in the URL bar, to further lull the user into a false sense of security.

While SSL is generally accepted as being secure, security researchers have claimed SSL communications can be intercepted. Researcher Mike Perry said he had been in discussions with Google regarding an exploit he planned to release, which would allow a hacker to intercept a user's communications with supposedly secure websites over an unsecured Wi-Fi network.

Weakness of SSL in practice

The main weakness with conventional SSL certificates is that there are no standards for their issuance, nor any rules for what the fields in them are supposed to mean and which are required for authentication. Marlinspike's SSLStrip attack demonstrated the combination of several attack techniques to exploit the above weaknesses and fool users/client applications into thinking they were using a trusted site/server, when in fact they were using a fake version of that site/server. He combined a number of techniques; including *man-in-the-middle*, fake leaf node certificates and the null character attack.

SSL heavily rely on X509 certificate structure to prove authenticity. For the SSL it is the *common name field* of the X509 certificate that is used to identify authentic servers. For example, Paypal will use *www.paypal.com* in the common name field. The signing process heavily relies on the above convention. The Certificate Authorities will sign *www.paypal.com*, they don't care whether you are

requesting for *anything.paypal.com* or *something.anything.paypal.com* – as long as you prove that you are *paypal.com*.

X509 certificates are commonly formatted using ASN.1 notation. ASN.1 supports many string types but all of them are represented as some variations of PASCAL. In PASCAL character string the NULL characters are treated as normal characters. They don't have any special meaning.

So NULL characters can be included into the common name field of X509 certificates. So a signing request like *www.paypal.com\0.fakeorganization.com* will be treated valid. The Certificate Authority will ignore prefix and sign the root domain *fakeorganization.com*.

Now the thing is most contemporary SSL/TLS implementation treat the field in X509 as C strings. And in `C '\0'` (NULL) means end of the string.

So *www.paypal.com\0.fakeorganization.com* and *www.paypal.com* will be treated as identical.

Thus the owner of the certificate for *www.paypal.com\0.fakeorganization.com* can successfully present his certificate to the connections intended for original *www.paypal.com*.

Here MITM happens on SSL.

You can sign your own certificates using the valid certificate you got from Certificate Authority. *Actually there is field in X509 certificates which needs to be set FALSE in order to restrict domain owner to act as a Certificate Authority (see Figure 1).*

Most CA's didn't explicitly set basicConstraints:

```
CA=FALSE
```

A lot of web browsers and other SSL implementations didn't bother to check it, whether the field was there or not. Anyone with a valid leaf node certificate could create and sign a leaf node certificate for any other domain (see Figure 2).

The *blueanarchy.org* can create a valid certificate as *paypal.com* and use it.

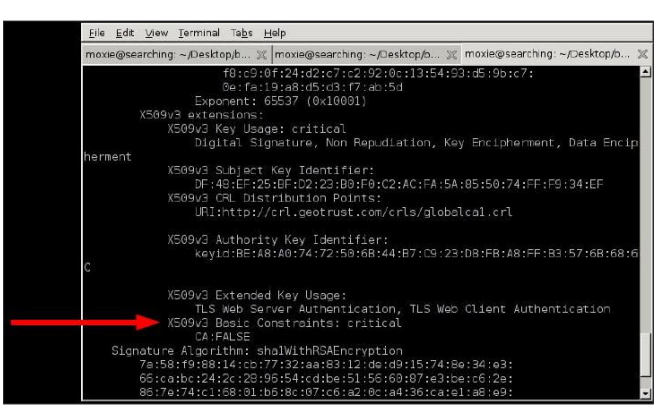


Figure 1. *The field CA=FALSE must be specified to restrict generating new certificates*

How SSLStrip works

- It does an MITM (*Man-In-The-Middle*) on the HTTP connection.
- It replaces all the HTTPS links with HTTP ones but remembers the links which were changed.
- Communicates with the victim client on an HTTP connection for any secure link.
- Communicates with the legitimate server over HTTPS for the same secure link.
- Communication is transparently proxied between the victim client and the legitimate server.
- Images such as the favicon are replaced by images of the familiar *secure lock* icon, to build trust.

As the MITM is taking places all passwords, credentials etc are stolen without the Client knowing.

Performing the Hijack on Windows

The process of using SSLStrip on Windows machine is almost similar to Linux machine. Linux has Firewall management tool iptables for enabling Port Forwarding. The port forwarding utility actually accepts traffic on one port of the machine and redirects to another port on the same machine. Windows machine doesn't have any inbuilt mechanism for port forwarding.

There are mainly fours steps to perform the experiment:

- Turn your machine into IP forwarding mode.
- Setup iptables to redirect HTTP traffic to sslstrip.
- Run sslstrip.
- Run arpspoof to convince a network they should send their traffic via your machine.

Prerequisite: Install Python as SSLStrip is a Python based tool. You need two machines running Windows on same LAN- one for attacker, another for victim.

The scenario: see Figure 3.

Attacker's machine is the machine where the SSLStrip runs. Also this is the machine where you will

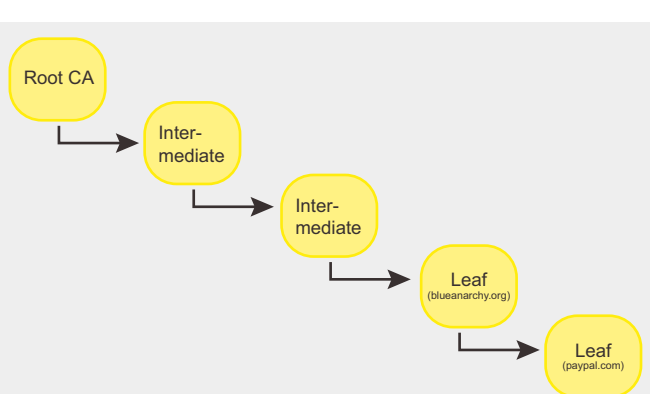


Figure 2. *The fake Paypal certificate created*

run the arpspoof command to spoof the traffic from Vitim machine. The port forwarding utility needs to be run on this machine as well.

Step 1:
Enable IP forwarding on Attacker's Machine
Get the hacker machine into acting as a router as it needs to forward all the traffic coming to it to outside internet.

- Start Registry Editor (*Regedit.exe*).
- In Registry Editor, locate the following registry key:
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`
- Set the following registry value:
- Value Name: IPEnableRouter
- Value type: `REG_DWORD`
- Value Data: 1
- A value of 1 enables TCP/IP forwarding for all network connections that are installed and used by this computer.
- Quit Registry Editor. Restart the PC.

Step 2:
Set a firewall rule that forwards HTTP traffic from the victim to hacker's machine for modification
This was most challenging and time consuming part of the experiment as I was unable to find single command, tool or utilities to do that. In Unix the an IPtables command would do that-

```
sudo iptables -t nat -A PREROUTING -p tcp --destination-
                    port 80 -j REDIRECT --to-port 10000
```

It tells all HTTP traffic from victim, coming on port 80 of hacker's machine to redirect it on port 10000 on the same hacker's machine. Port 10000 is used by SSLStrip tool by default.

Tired of not finding any equivalent firewall utility for Windows to perform above rule fortunately I stumbled upon blog of Kenneth Xu (*http://kennethxu.blogspot.com*) and I finally found the following nice Java based TCP/IP port forwarding utility – (Download here *http://code.google.com/p/portforward/downloads/list*)

```
C:\>java -classpath commons-logging.jar;portforward.jar
                    org.enterprisepower.net.portforward.
                    Forwarder 80 localhost:10000
```

This command forwards all HTTP traffic received on port 80 of Hacker's machine to port 10000 of the same machine. SSLStrip runs on port 10000 by default.

Step 3:
ARP spoof the target traffic to redirect to hacker's machine
Suppose the Victim machine's IP is 192.168.1.10 and IP of the gateway is 192.168.1.1. It will poison the victim machine (192.168.1.10) MAC table and instead of sending the traffic to Gateway (192.168.1.1) it will send to the hacker's machine falsely assuming it as the real gateway.

Run the following command on attacker's machine

```
arpspoof -t 192.168.1.10 192.168.1.1
```

It will update the ARP table on Vitim's machine with changed gateway IP of attacker's machine.

Step 4:
Run SSLStrip on hacker's machine
Run the following command on Hacker's machine

```
python sslstrip.py  -f lock.ico
```

You can see the log file in the SSLStrip installation folder for logged credentials.

The SSLStrip will log all the traffic coming from Victim's machine and strips the all the SSL link (*https://*) to *http://* between the Victim and Hacker. Thus the traffic between the Victim to Hacker is transparent and in clear text: see Figure 4.

Various options available with the SSLStrip:

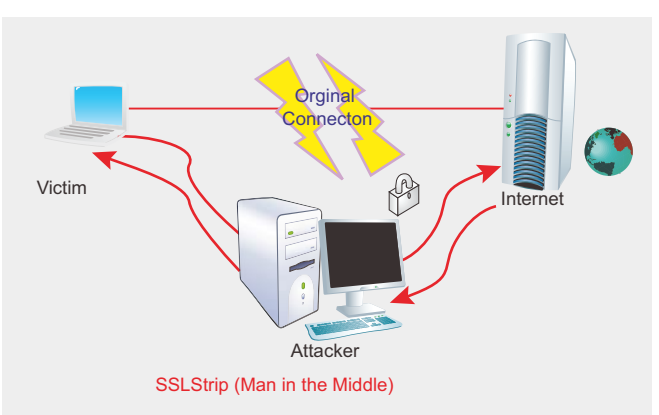


Figure 3. *The actual scenario*

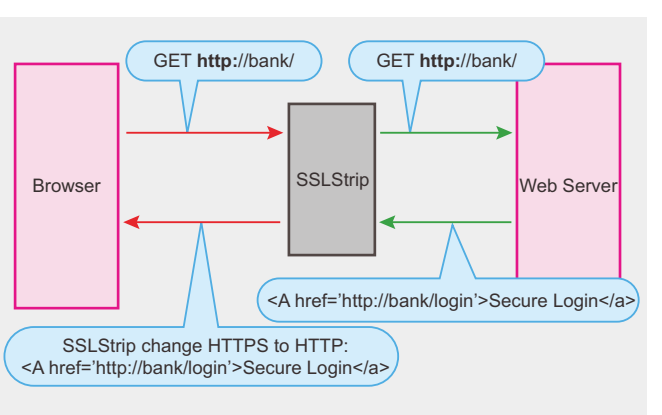


Figure 4. *The HTTPS links are converted to HTTP*

Figure 5. *LinkedIn login page on http*

Figure 6. *The ebay login pages being served on http*

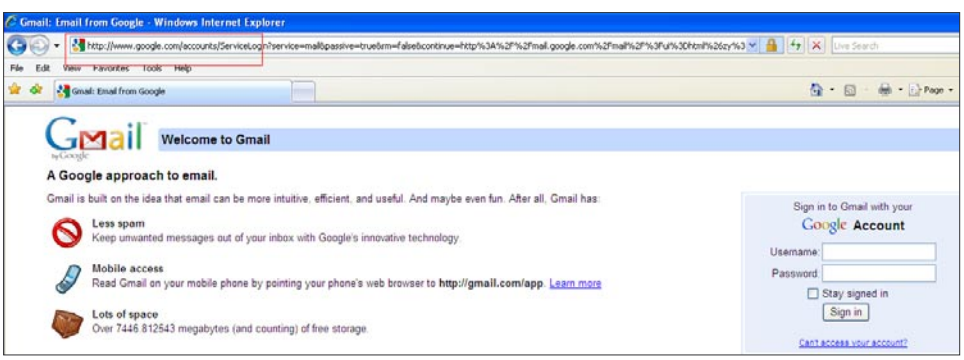


Figure 7. *Gmail on http*

Figure 8. *The log of all traffic which contains Passwords in clear text*

Options:

- w `<filename>`, `--write=<filename>` Specify file to log to (o
- p, --post Log only SSL POSTs. (default)
- s, --ssl Log all SSL traffic to and server
- a, --all Log all SSL and HTTP traffic to and from server
- l `<port>`, `--listen=<port>` Port to listen on (default 10000)
- f, --favicon Substitute a lock favicon
- k, --killsessions Kill sessions in progress
- h Print this help message.

Real life examples

The following page appears on *https://* in normal situation but here it is as *http://* see Figure 5.

View page source can also reveal that links are stripped of SSL: see Figur 6.

Gmail on http: see Figure 7.

An example of Log file of SSLStrip, Passwords logged: see Figure 8.

Mitigation

User Education: User should be educated to always use https while requesting any sensitive page. As user only type domain.com that is redirected to *https://domain.com* may be vulnerable to SSLStrip.

EV SSL Certificates: There is no reliable information to back up the authentication of the domain name. To address this critical problem, certificate authorities and software companies joined to form the CA/Browser Forum and promulgate a new standard called EV SSL for Extended Validation SSL. For instance, they must validate that the organization exists as a legal entity, that any organization names are legal names for that organization, and that the applicant is authorized to apply for the certificate.

SSLStrip tool:
http://www.thoughtcrime.org/software/sslstrip/
NULL Prefix attack on SSL Certificates:
http://www.thoughtcrime.org/papers/null-prefix-attacks.pdf
Black Hat presentation:
http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf

NILESH KUMAR

Nilesh Kumar is working as an Engineer-Security Analyst with Honeywell Technology Solutions, Bangalore, India. He is primarily focused on Application Security ranging from Code Review to Black Box Testing. Apart from that he shows interest in Network Security and Reverse Engineering.
(Blog: nileshkumar83.blogspot.com)

Birth of an Evil Twin

Taking Social Engineering to the Social Web

I'd hate to wake up some morning and find out that you weren't you. this quote from the 1956 movie Invasion of the Body Snatchers has more relevance today than ever.

What you will learn…

- Definition of an Evil Twin
- Using an Evil Twin for Social Engineering
- What an Evil Twin can do

What you should know…

- How to use a search engine
- How to sing up for a social network

Evolving Web of Trust

When an email says that it is from one of our friends, we rarely second guess the origin. That mentality has directly followed us from email to social networking, where the claimed identity of an individual is never challenged. Today with the prevalence of blogs, Twitter, Facebook and LinkedIn we are putting data about ourselves on the Internet for anyone to see.

While we are caught up in the self-publishing culture that is fueling Web 2.0 sites, we forget that each piece of information we put out to the world is a data point that can be used against us. In this article we will explore how an attacker can turn our Social Media against us manifesting in an Evil Twin that can be used against us, our family or employer.

An Evil Twin attack, as defined in Seven Deadliest Social Network Attacks by Carl Timms and James Perez, is when a rogue user poses as a legitimate user. This is not new, it has been happening for years on forums and chat rooms where users change their identity to appear as someone else.

Where an Evil Twin gains momentum is from Social Networking sites where the claimed identity of a user is assumed to be true. If I start a Facebook profile and claim that my name is William George, would people who did not know me in person disagree that my name is William George. On the internet a person can be anyone they want – that is part of the appeal of the internet, it is a chance to reinvent yourself. An Evil Twin occurs when I create a Facebook page for William George with the intent to collect information about the real William George's family, friends, coworkers, etc… Using an Evil Twin, you claim the identity of a legitimate person in an attempt to gather information, infiltrate a circle of trust (the friends of a specific person), spread malware (via Facebook Applications) or whatever other motivation you can imagine.

Does this sound like Social Engineering to you? It is! An Evil Twin is a tool for Social Engineering. The definition of Social Engineering according to Kevin Mitnick's Art of Deception :

Social Engineering: using influence and persuasion to deceive people by convincing them that the social engineer is someone he is not or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology.

The description of an Evil Twin falls directly into this definition. The Evil Twin is a hybrid of using technology to pose as someone else while also collecting information about the target to facilitate the Evil Twin's believability.

Creating an Evil Twin is the means to an end, whether that end is spreading malware, discovering information or defamation of character, the Evil Twin is an enabling tool for a Social Engineer.

Social Networking sites are the engine that runs an Evil Twin with Social Media sites being the fuel. Just to be clear on definitions, a Social Networking site is one that allows users to connect to other users and share parts of their profile (examples: Facebook, LinkedIn, Bebo). A Social Media site is one that allows users to self publish content to the web (examples: Blog, YouTube, Twitter).

While there is a gray area between the two, social networking sites are about connecting while social media sites are about content for the purposes of this article. Many of these sites have privacy settings that will allow your content and information to stay hidden from anonymous or users outside of your circle of trust, but these controls are not always turned on by default. Social Media sites fuel the Evil Twin by telling the attacker all the information they need to know to create a believable persona for the target individual. A Twitter feed that frequently talks about golfing can tell an attacker that this individual is a golfer which can go on the Evil Twin profile as an *Interest*.

The Evil Twin attack examined

Recently I worked with a company we will call GroundTrans Corp (all names have been changed) to execute an Evil Twin attack and determine how far we could go using Social Networks and Social Media of employees to extract secure data about the company. Throughout the rest of the article we will be examining how I implemented the concepts presented. As a word of warning, being an Evil Twin violates the User Agreement of most Social Networks and Social Media sites. Being the Evil Twin of an unwitting person can land you in serious legal trouble. Do not try this at home without the express permission (written, documented and archived) of the person you are impersonating and the organization you are testing against.

Step 1:
Determine the goal

Before anything, you should have a goal in mind. Why are you doing the Evil Twin attack? The motivation can be extremely diverse from defamation of character, spying, spreading malware, market manipulation, disinformation, and the list could go on. The goal drives everything else that you do for the Evil Twin attack and beyond, so make sure you have a clear vision of where you want this thing to go. In my example I will be attacking for access credentials to the system. As a semi-technical hacker, my goal will be to obtain login credentials to access the system remotely which I will eventually use to steal money from the target's financial system.

Step 2: Determine the Target

The first thing to do in an Evil Twin attack is to determine the target. Who are you attacking for the end game? The target could be an individual or an organization/ company. If the target is an organization, then you will need to select a person to attack the organization through.

Ask the following questions about your target to assess it's quality:

- Does your target have some existing Social Media: Try to pick a target with some information already out on the internet. This will make starting your Evil Twin much easier.
- Does your target lack a Social Networking presence: It is ideal for a target to not have a Social Networking site but if they do, simply select a different Social Network and invite the target's friends. It is not uncommon for people to have multiple Social Networks or profiles on a single network. You can also go with the *My other account go hacked* method where you siphon connections to a new account.
- Could your target achieve your goal: Make sure the target you choose would be able to achieve your goal. If your goal was physical access codes to an office building in Baltimore, do not select a target in London that probably does not have the Baltimore access codes. Although, the door code might not be a secret within the company, best to focus your efforts on targets that are most likely to be able to obtain the information you seek.

In my Evil Twin attack, GroundTrans Corp is the target and my goal is to get access credentials to steal money from the financial system. Since my target is a company, I need to determine who I am going to impersonate. After reviewing GroundTrans' website and examining the corporate bios, I cross reference executive bios against LinkedIn to see who has a LinkedIn account. From the group that had LinkedIn accounts, I then looked to see who had their LinkedIn status updates set from Twitter. That narrowed down my selection to two executives of which I chose the CIO, Steve Partmen. Now I had the target to impersonate and knew three places I could pull from for my Evil Twin (the Executive Bio page of GroundTrans' website, LinkedIn and Twitter).

Step 3:
Collect information about the Legitimate User

After you have a target, collect all the information that you can on him/her. What information is important

depends on the Social Network you will be building your Evil Twin in and who your target is. The best place to start is Google. Type in the person's name and see what comes up. Make sure that you collect information about the correct person as there could be many Steve Partmen's in the world. Using sites like Blogger, Twitter, LinkedIn, Facebook, etc.. can yield a lot of information. Twitter for example, is used to do updates about what the person is doing or thinking about. You can discover a lot of information by looking at Twitter posts.

The key for collecting data is in the aggregation of that data, not the individual data points. For example, users of Twitter treat each post as a separate entity. In their mind, one post is one piece of information. When you look at all posts and derive information based on not only the total of the user's Twitter posts but keeping those posts in mind as you explore their other Social Media such as their blog or YouTube postings. If a Twitter user talks about going to play golf often in their posts and you find helpful golf swing hints as a reoccurring section of their blog, you can determine that this person really likes golf and it is more than just a simple hobby for them.

To keep track of all data I find about a user, I place it in matrix represented by Table 1.

This matrix allows you to place items into categories and then specify the frequency of the item. As you discover an item, you place it in the proper row and analyze how often it appears to determine whether it is Often, Average or Rare. Notice golf is placed as an Interest that appears Often because it is throughout the Twitter posts and appears repeatedly. Rare pieces of information are the most valuable because they represent things that few people know about the individual. These are the data points that will make your Evil Twin the most believable.

In our GroundTrans Corp attack, where the person I was impersonating was Steve Partmen, I analyzed his executive bio on the GroundTrans site. It said that he use to work for SeaTrans prior to GroundTrans but this did not appear in his LinkedIn profile so I labeled it as Work Information, Average. As I was Googling Steve I found a website for a small karate school where he was listed as one of the instructors. This was found on page 8 of the Google results so I put it as a Hobby/Rare due to not being able to find it anywhere else and that it was so buried in the Google results. From his LinkedIn page, I took note of each position Steve has had and any data points that could be found in the Education, Interests and recommendations. With a basic list of items I went to his Twitter page and read through all of his posts marking down interests as I came across them. Golf stood out as one, as did hiking and mountain climbing. He also, according to his Twitter account, did a yearly trip to do some mountain climbing in Canada in arctic conditions.

Checking on Flickr, I found pictures of Steve and his friends climbing in arctic Canada. I saved those pictures and then did a search for some golf pictures. While I could not find pictures of Steve playing golf, I did find a lot of poor quality pictures of people who looked sort of looked like Steve from a distance. These would be good enough; while not perfect their lack of quality would add some authenticity. Having these pictures would be a great addition to Steve's Evil Twin because who else would have these photos…right?

Table 1. *Gathered information matrix example for Steve Partmen*

Item Category	Frequency	
	Often	Average
Personal Information	Name: Steve Partmen Birth Date: August	Married Very Social
Work Information	GroundTrans Corp	SeaTrans Corp
Education Information		ABC University
Hobbies		Model airplanes Ice/Mountain climbing
Interests	golf UFC	Sports cars Motorcycles

Step 4: Connection pooling

We have our target, we have our person to be impersonated, and we have our data now we need to know who our Evil Twin is going to be connecting to. It is not difficult to find connections online. Social Networks thrive on the interconnecting of individuals in their site and display this information either explicitly or implicitly. With LinkedIn, you can hide your connections and only expose them to people you are connected with. When this feature is enabled, only people you have approved can see your connections. Turning this feature off would allow anyone to see your connections which would an example of explicitly displaying your connections. LinkedIn has another feature that is handy, *Viewers of this profile also viewed...* which is an example of implicitly exposing one's connections. While this feature is helpful to see where people went from a specific user, it also suggests a link between the users. An implicit connection does not mean the two are definitely connected, but there is evidence that a user was able to go from this profile to one of the *also viewed* profiles. Think of it like Amazon.com's *people who bought this also bought…*, it does not mean that people always purchased the items together, but a few people did. In my own experience, *also viewed* profiles tend to

Table 2. *Connection listing*

ID	Name	Company	Relationship	Social Links
1	Bob Jones	GroundTrans	CFO	None
2	Carol Partmen	AT&T	Wife	http://social.com/blah?ID=124
3	Dona Far		Daughter's friend's mom	http://social.com/blah?ID=23
4	Frank Haim	GroundTrans	IT manager	http://social.com/blah?ID=2

be connected to the profile you are viewing and that assumption has worked well for me in the past.

Any time you encounter a connection for the target take note. The connections you discover now will be people to add for your Evil Twin later. For listing connections I use the table format in Table 2. This allows me to keep a single list of all the connections I find for an individual and how they are related to the target.

Once you have a fairly large list of connections, use Table 3 to examine the nature of the relationship and the frequency in which the connection appears. This will later be how you decide who to connect to. Remember, the goal of the Evil Twin is to gain trust. Differentiating between family, friends and business associates will be important so that you can focus on your target. If you are attacking an organization, you will focus on business contacts while spying could be more focused on family and friends. Use the numbers from your previous list to save some typing and space.

For our attack on GroundTrans, I found Steve Partmen's LinkedIn page. As my goal is to spread malware, I am going to use Facebook as my Social Network. Looking through LinkedIn I find a series of contacts that I list in my Contact List table. I took special note of profiles that were *Popular Profiles* on LinkedIn. As I reviewed each possible connection, I keep the end goal in mind: *Financial gain*. With each possible connection I ask myself, will this user have access to the necessary elements for me to access the financial data? With this question in mind I focus on connections listed in the Finance and Accounting department as

Table 3. *Relationship Matrix*

Category	Frequency		
	Often	Average	Rare
Business Contacts	At Work	1	4
	At Other Compaines		
Personal Contacts	Friends		
	Family	2	

I know these people will have access to the resources I need. After listing all the connections, I cross reference who exists on Steve's Twitter page as well. Users that are both LinkedIn connections and Twitter followers I mark as appearing Often. Users that only appear on LinkedIn I mark as Average while followers on Twitter are Rare.

Step 5: Build the Evil Twin

This whole time we have been preparing to build the Evil Twin, now we will actually go and do it. The first step in construction is to select the Social Network you are going to use. Which you select depends on your over all goals. If malware distribution is your goal (as in our example) then, Facebook is a great option. Their application framework makes it easy to distribute malicious code to a large user group and collect their Facebook information while doing it. LinkedIn is a great choice for focusing on a professional network (perhaps to do PR damage to a company) and is ideal for building a professional reputation for your Evil Twin. You might decide that you want to go outside the normal Social Networks and use an up and coming service. This can lend credibility to your account as you could be the only Steve Partmen in this new system. A benefit of using an emerging social network is that you can invite connections, again leading the connection to think, who else but Steve would specifically invite me?

Once you have selected the Social Network, you will need an email account to use for it. For this you can select any of the free online email services such as: Gmail, Hotmail, Yahoo Mail, etc… When creating your account you might want to consider mimicking the impersonated person's real email address. For instance, if you know Steve has *spartmen@hotmail.com*, try *spartmen@gmail.com*. Users might not even notice the change or, if they are similar enough, think that Steve has moved to a new email provider.

With new email address ready, simply go to your Social Network of choice and register. This process is simple and using the tables we built in previous steps, will allow you to create a very believable Evil Twin. In both Facebook and LinkedIn registrations, you will need to answer a few questions about interests, birth date, etc… If you do not know the answer, put in a ridiculous answer. If you do not know the person's birth day and they are a young person then enter something outlandish such as 12/2/1928. Many users of Social Networks do not pay attention to the details and while we want to get the Evil Twin as accurate as possible, a little ridiculousness could lead to an online personality for your Evil Twin. Keep in mind that research is a key element to a believable Evil Twin but, an Evil Twin is not just a culmination of facts…it must

have a personality too. Your research should give you a glimpse into the impersonated person's personality, emulate it but infuse some of your own. A believable Evil Twin is a person, not a list of facts.

Once your Evil Twin is out in the wild you can expect some organic connections, connections that seek you out. Organic connections are a powerful thing as they will, without any effort on your part, open new connection opportunities for your Evil Twin. The more connections that your Evil Twin amasses, the more organic connections you will be able to leverage.

For Steve Partmen's Evil Twin I selected Facebook for the application ecosystem. My eventual plan is to spread malware through that ecosystem to my *friends*. I setup an email account in Hotmail as *spartmen@live.com* and register in Facebook. Using my Interest table from Step 3 I entered any interests, movies, books, etc… that I found about my person. Once completed I wrote a message on my wall: *Finally joining this Facebook thing*. Next, I connected my legitimate Facebook account to Steve's to show that he has at least one friend. Using the pictures I found in Step 3 I upload a few and enter in some witty captions. All those items fleshed out Steve's profile so that the Evil Twin was more than just a blank profile. The next day I sent out Friend Requests to the connections in my Connection Matrix marked Often. With each request I added a message: *Please keep this under wraps at work. I have some people already irritated that I'm not sending them friend requests so please don't talk about my Facebook account at work*. While it might sound strange, users who received this message often wrote back, *Same here* or something to denote that they did not want to talk about Facebook at work either. This is perfect for encouraging users not to talk about the Evil Twin to the real Steve Partmen.

Results

In total, Steve Perlman's Evil Twin was able to connect with twenty-five people in under twenty-four hours. Only seven of those connections were friend requests that I sent. The other eighteen were people who found Steve's Evil Twin through another connection. Once the Evil Twin started connecting it was able to go viral spreading amongst other users all trusting that Steve was the real Steve. Connections found Steve through other connections which increased the Evil Twin's credibility (often these types of connections are a result in connection 1 trusting the connections of connection 2).

Using the Facebook API, I was able to build a small HTML application called *I love GroundTrans Corp* and sent it to the connections. Twenty accepted it (discovered in post experiment interviews). The application was just an image tag on the screen but could have been anything from a CSRF to XSS attack. The application is where I would have distributed the malware to extract credentials to my target users' systems. There have been numerous articles written about distributing malware through social networks, the key is leveraging the trust the user has in the social network.

In the post experiment interviews, where I discussed what happened with all the Friends who added Steve's Evil Twin, none of the users ever second guessed Steve's identity in the application. Most did not even notice that his birth date was set to 1930 (Steve is 40 years old). In the end, all uses accepted Steve's identity based on some pictures and believable wall postings.

Escalation opportunities galore!

From the Evil Twin experiment one can see the opportunities to take the attack to a whole new level. As stated previously, an Evil Twin is the means to an end, not the attack itself. Some of the attacks an Evil Twin can facilitate are spreading malicious applications, phishing, cyberbullying or just simple defamation of character. Any of these attacks can be damaging to an individual or organization and are all enabled by the inherent trust that we provide to our connections through our Social Networks.

Conclusion

While Social Media allows us to self publish any content imaginable, it also exposes our data to an unfriendly internet. Social Networks allow us to keep in touch with people who have moved or we have not seen in years but, it also exposes our personal information. The Evil Twin attack exploits our interests in Social Media and our desire to stay connected in Social Networks. Vigilance and offline confirmation is your only defense against this growing threat. As Social Networking is embraced by more corporations we will see the Evil Twin threat grow. Take care to verify your social network connections because one day you might wake up and realize your connections…are not who you thought they were.

TIM KULP

Tim Kulp (CISSP, CEH) is an Information Security professional in Baltimore, MD. He specializes in secure software development and penetration testing web applications. In recent years, Tim's focus has been working with development teams on updating applications to utilize secure coding practices and studying the security impact of Social Media.

Securing Voice Over Internet Protocol (VoIP)

Understanding Weakness, Exploits and Proactive Defenses for Deploying VoIP

If you think your telephone is safe from hackers, think again. With wireshark, a *tcp/ip dump file* and vomit (voice over misconfigured ip telephony) you can play back conversations from your own local area network that took place earlier today – and play these wave files in the privacy of your own home. This is a problem. And in VoIP it's only the tip of the iceberg.

What you will learn…

- The Basics of VoIP
- Types of VoIP Attacks
- VoIP Vulnerabilities
- Hardening Your VoIP Deployment

What you should know…

- Basic VoIP setup
- How to Sniff Network Traffic
- How to Configure a Firewall
- How to Test Vulnerabilities

The way we do business has changed dramatically since the advent of the Internet. Now, with new protocols for communication, enter the world of *Voice over Internet Protocol* (VoIP), which will forever change the way telephone calls are made. Just look at the numerous offers for Vonage, a VoIP system designed to replace your standard telephone service by using the Internet to make local and long distance phone calls.

Or look at SKYPE, which is a software version of VoIP that rides your existing Internet connection to allow you to make calls to fellow SKYPE users anywhere in the world at no charge. VoIP turns your analog audio signals into digital data that can be easily transmitted over the Internet. That's why there are millions of users of SKYPE making millions of Internet-based telephone calls daily, using their desktops or laptops, a microphone, headset, their built-in sound card, the Windows operating system, and the SKYPE peer to peer (P2P) software.

Your first question might be – how useful is VoIP? and your second question might be – is it safe? The answers to both questions are that yes, VoIP can be very useful and very inexpensive, but it also has a very high risk of being attacked, especially by eavesdropping and denial of service exploits – not good when you need to place an emergency phone call or when you are giving your credit card information out to make a purchase using your VoIP telephone.

First, let's take a look at how VoIP works.

How VoIP Works

When you want to place a call using VoIP, you can do it in one of three different ways:

- Through an Analog Telephone Adaptor
- Through an IP (Internet Protocol) Telephone
- Through Peer to Peer VoIP

The first and easiest way to make a VoIP call is through an ATA (*Analog Telephone Adaptor*), which are sometimes called *Gateways*. These ATAs let you use your existing *old fashioned* analog telephone. All you have to do is plug your antiquated handset into the ATA and then connect the ATA to your Internet Connection (Cable modem or sometimes directly into your computer) and you are ready to place calls. A Gateway takes the analog signal from your dusty old phone and turns the sound waves into digital signals that can be easily transmitted over the Internet. Some of the Gateways come with additional software that is loaded onto your personal computer, enabling you to configure it for VoIP and monitor VoIP status.

Another way to do VoIP is to use an IP (*Internet Protocol*) telephone. These telephone handsets look just like normal handsets, however, they have an RJ45 Ethernet connector instead of the standard RJ11 connector. These phones are just like *micro* computers and have all the software and hardware built-in to them to get an IP address to be online for making

and receiving telephone calls. Because they connect directly to your Internet connection, they are very fast to setup, install and use, just like an old fashioned telephone.

Finally, as we've seen with *Peer to Peer* (P2P) systems like SKYPE, you can do computer to computer VoIP. All you have to do is install the software, configure it properly and begin using your microphone and headset attached to your PC. SKYPE promises to be *free forever* and other services are coming online that will offer the same price – not bad. So what is the catch? You might want a VoIP call to be forwarded to your cell phone when you are away from your computer or might want voice mail and other features – these *options* are not free, so there's the catch. The more options you want, such as Caller ID, Voice Mail, Inbound Fax, Call Forwarding, Call Waiting, etc., the more you will pay for systems like SKYPE.

Computer to computer – This is the easiest way to make use of the VoIP technology. There are many companies offering cost effective software that you can use for this type of VoIP. Usually the only charge you pay is the monthly one from your Internet service provider, even for long distance calls. All you need is a microphone, speakers, a suitable sound card, and a fast Internet connection.

There's a high probability that you've already made a VoIP call without even realizing it. Maybe you've called your local bank and the branch manager who answered the phone was on a VoIP telephone. Most major telephone carriers are already using VoIP to route thousands of long distance calls through a circuit switch and into an *Internet Protocol* (IP) Gateway. Your call is received by a remote IP Gateway at the other end and then routed into a local circuit switch on the other side. As more companies install VoIP phone systems, the technology will grow and reach a disruptive state, becoming a commodity, available everywhere – this is happening as you read this document. Disruptive and powerful new technologies usually catch on like wildfire. VoIP is one of them.

VoIP Features

One of the best features of VoIP is portability – can you take your old fashion home telephone into your doctors *office waiting room or your accountants* office and make a telephone call from your phone number? Nope. But with VoIP, you can make calls from anywhere that you can plug into an Internet jack (RJ45 connection) and make calls as if you were home. If your VoIP rings, someone has dialed your local VoIP telephone number, even if it is ringing from your hotel room in Hawaii – now that's really cool technology.

If you are using a soft-phone (VoIP software such as SKYPE), then you can make and receive calls wherever you run this software – if it is on your laptop, then your phone number is now Mobile – wherever you have access to the Internet, including a coffee shop or the airport, your telephone is moving with you. Most old-fashioned telephone carriers charge you for all those extra features you love but with VoIP accounts they usually come standard, unless you are using a free soft-phone like SKYPE. These are the kinds of standard features you can have access to with your VoIP telephone service:

Standard Features of VoIP Phone

1. Call Waiting
2. Caller ID
3. Call Transfer
4. Repeat Dialing
5. Return Last Call
6. Three-Way Dialing

There are even additional features available from some VoIP service providers. These additional features allow you to decide how calls to a specific number can be automatically handled or *filtered* by using Caller Identification (ID). They include:

Special Filtering Features of VoIP

- Send the call directly to voicemail
- Forward the call to a particular number
- Give the caller a busy signal
- Play a *not-in-service* message

With most VoIP services, you can check your voice mail over the internet or have it sent to you as an email attachment that you can play as a sound file (like you would play in Windows Media Player).

VoIP Benefits

There are many cost saving benefits that arise from flattening out your network architecture – for example, your phone system and your internet access can all come from the same network and service provider.

If you are Network Administrator or *Information Technology* (IT) Professional, this technology holds the potential of a streamlined communication system – instead of managing two networks (the telephone system) and the Internet/intranet, you can manage one network. The portability of VoIP systems is excellent for improving communications and ease of access to sales staff, partners, customers, and fellow VoIP users. If you are the Network Administrator and you need to make changes to voice mail for new hires, it can be done right over the Internet/intranet using a web browser with simple point and click software.

If you have many branch offices, you might want to flatten out how your corporation appears – a call made far away to a branch in California can be routed to a branch in New York without the caller even knowing this routing took place. You can benefit from a flatter, easier communication environment with:

- One receptionist for all calls
- Auto attendant features for all calls
- Corporate-wide Voice Mail managed from one location
- Updates to the phone system executed across the entire organization at once

Choosing a VoIP System

If you have decided that a VoIP phone system is the right move for your company, next you need to determine how much of your existing telephone equipment you are able to keep. The potential cost savings associated with retaining any existing digital equipment are huge. Many digital phone systems can be IP enabled using minor hardware additions and software upgrades.

When shopping around for potential systems you need to be certain of the features each VoIP supplier provides as standard and the features that are optional cost extras.

You also need to be certain of exactly what is included with the system. Many suppliers claim to include everything you need, but standard components can vary from one company to the other. So you need to sure you are comparing equivalent systems when approaching potential suppliers. You will also need to:

- Inquire about the compatibility of existing equipment. The technology used in many VoIP systems may affect the implementation of any existing telephone hardware.
- Ensure that any existing devices, such as fax machines, credit card processors, security systems, and the like, can be integrated into your new VoIP phone system. Make any potential vendor aware of such devices so they can provide you with a suitable phone system for your requirements.

A note of caution: Do not try to save money by buying used VoIP phone systems. Remember VoIP is a new technology, so even last year's equipment is outdated. Also the installation cost will still apply whether the system is new or second hand, and the service costs with a used VoIP may even be higher due to reliability issues. Used VoIP systems just aren't worth the hassle. The higher secondary costs will wipe out any potential saving. The next section details some of the potential threats and vulnerabilities in a VoIP environment, including vulnerabilities of both VoIP phones and switches.

VoIP Security Flaws

This discussion is included because the variety of threats faced by an organization determines the priorities in securing its communications equipment. Not all threats are present in all organizations. A commercial firm may be concerned primarily with toll fraud, while a government agency may need to prevent disclosure of sensitive information because of privacy or national security concerns.

Information security risks can be broadly categorized into the following three types:

- Confidentiality
- Integrity
- Availability

You can remember these categories with the mnemonic *CIA*.

Additional risks relevant to switches are:

- Fraud
- Risk of physical damage to the switch, physical network, or telephone extensions.

Packet networks depend for their successful operation on a large number of configurable parameters: IP and MAC (physical) addresses of voice terminals, addresses of routers and firewalls, and VoIP specific software such as Call Managers and other programs used to place and route calls. Many of these network parameters are established dynamically every time a network component is restarted, or when a VoIP telephone is restarted or added to the network. Because there are so many places in a network with dynamically configurable parameters, intruders have a wide array of potentially vulnerable points to attack.

Vulnerabilities described in this article are generic and may not apply to all systems; however, investigations by NIST and other organizations have found these vulnerabilities in a number of VoIP systems. This list is not exhaustive; as systems may have security weaknesses that are not included in the list. With each potential vulnerability mentioned there are some recommended actions to eliminate or reduce the risk of compromise.

Confidentiality and Privacy

Confidentiality refers to the need to keep information secure and private. For home computer users, this category includes confidential memoranda, financial information, and security information such as passwords. In a telecommunications switch, the risk of intruders eavesdropping on conversations is an obvious concern, but the confidentiality of other information on the switch must be protected to defend against toll fraud, voice and data interception, and denial of service

attacks. Network IP addresses, operating system type, telephone extension to IP address mappings, and communication protocols are all examples of information that, while not critical as individual pieces of data, can make an attacker's job easier. With conventional telephone systems, eavesdropping usually requires either physical access to tap a line or penetration of a switch. Attempting physical access increases the intruder's risk of being discovered, and conventional PBXs have fewer points of access than VoIP systems. With VoIP, opportunities for eavesdroppers increase dramatically, because of the many nodes in a packet network.

Switch Default Password Vulnerability

It is common for switches to have a default login/password set, such as admin/admin, or root /root. If no one changes this default, it becomes a vulnerability that allows wiretapping of conversations on the network with port mirroring or bridging. Once an attacker has access to the switch administrative interface, the attacker can mirror all packets on one port to another, allowing the indirect and unnoticeable interception of all communications. Preventing use of this vulnerability may seem straightforward, but failing to change default passwords is one of the most common errors made by inexperienced users. Another way to close this vulnerability is to, if possible, disable remote access to the graphical user interface to prevent the interception of plain text administration sessions. Some devices provide the option of a direct USB connection in addition to remote access through a web browser interface, another accessway you can close. You should also consider disabling port mirroring on the switch.

Classical Wiretap Vulnerability

Attaching a packet capture tool or protocol analyzer to the VoIP network segment makes it easy to intercept voice traffic. How can you prevent such interception? A good physical security policy for the deployment environment is a general first step to maintaining confidentiality. Disabling the hubs on IP Phones as well as developing an alarm system for notifying the administrator when an IP Phone has been disconnected will allow for the possible detection of this kind of attack.

ARP Cache Poisoning and ARP Floods

Because many systems have little authentication, an intruder may be able to log on to a computer on the VoIP network segment, and then send ARP commands corrupting ARP caches on sender(s) of desired traffic. The intruder can then activate IP. An ARP flood attack on the switch could render the network vulnerable to conversation eavesdropping. The act of broadcasting ARP replies blind is sufficient to corrupt many ARP caches. By corrupting the ARP cache, the attacker can now re-route traffic to intercept voice and data traffic. To prevent this type of attack, use authentication mechanisms provided wherever possible and limit physical access to the VoIP network segment.

Web Server Interfaces

Both VoIP switches and voice terminals are likely to have a web server interface for remote or local administration. An attacker may be able to sniff plain text HTTP packets to gain confidential information. This action would require access to the local network on which the server resides. To prevent such an attack, if possible, do not use an HTTP server. If it is necessary to use a web server for remote administration, use the more secure HTTPS (HTTP over SSL or TLS) protocol.

IP Phone Netmask Vulnerability

An effect similar to the ARP Cache Vulnerability can be achieved by an attacker assigning a subnet mask and router address to the phone. The attacker crafts those addresses so that most or all of the packets the phone transmits will be sent to the attacker's MAC address. Again, standard (1q aware) IP forwarding makes the intrusion all but undetectable. Setting up a firewall filtering mechanism can reduce the probability of this attack. Remote access to IP phones is a severe risk.

Extension to IP Address Mapping Vulnerability

An intruder can readily discover the IP address that corresponds to any extension. All it requires is calling that extension and getting an answer. A protocol analyzer or packet capture tool attached to the hub on the dialing instrument will see packets directly from the target instrument once the call is answered. Being able to find out the IP address of a particular extension is not a compromise in itself, but makes it easier to execute other attacks. For example, if the attacker is able to sniff packets on the local network used by the switch, it will be easy to pick out packets sent and received by a target phone. Without knowledge of the IP address of the target phone, the attacker's goal may be much more difficult to reach and require much more time, possibly enough time that the attack could be foiled. While disabling the hub on the IP Phone will prevent this kind of attack, it is a rather simple task to turn the hub back on.

Integrity Issues

Integrity of information means that information remains unaltered by unauthorized users. For example, most users want to ensure that bank account numbers cannot be changed by anyone else, or that passwords are changed only by the user or an authorized security administrator. Telecommunication switches must protect the integrity of their system data and configuration. The richness of feature sets available on switches provides

an attacker with plenty of tools. A hacker who can compromise the system configuration has opened the door to a variety of potential hacks. For example, a hacker could reassign an ordinary extension into a pool of phones that the hacker can then eavesdrop on the same way that supervisors can legitimately listen in on or record conversations for quality control purposes. Another action the intruder can take is to damage or delete information about the IP network used by a VoIP switch, producing an immediate denial of service.

The security system itself provides capabilities for system abuse and misuse. Compromise of the security system not only allows system abuse but also allows the abuser to eliminate all traceability,(covering his tracks) and insert trapdoors for future intruders to use on their next visit. For this reason, the security system must be carefully protected. Integrity threats include techniques that can result in system functions or data being corrupted, either accidentally or as a result of malicious actions. Misuse is not restricted to outsiders, and may often involve legitimate users (insiders performing unauthorized operations) as well as outside intruders.

A legitimate user may perform an operations function incorrectly, or take unauthorized action, resulting in deleterious modification, destruction, deletion, or disclosure of switch software and data. This threat may be opened up by several factors, including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.

Intrusion

There are a number of serious intrusion threats the intruder may carry out. By masquerading as a legitimate user, an intruder may access an operations port of the switch. Or the intruder may use the permission level of the legitimate user and perform damaging operations functions such as:

- Disclosing confidential data
- Causing service deterioration by modifying the switch software
- Crashing the switch
- Removing all traces of the intrusion by modifying the security log

Insecure State

At certain times the switch may be vulnerable due to the fact that it is not in a secure state. For example:

After a system restart, the old security features may have been reset to insecure settings, and new features may not yet be activated. (For example, all old passwords may have reverted to the default system-password, because new passwords are not yet assigned.) The same may happen at the time of a disaster recovery.

At the time of installation the switch may be vulnerable until the default security features have been replaced.

DHCP Server Insertion Attack

It is often possible to change the configuration of a target phone by exploiting the DHCP response race when the IP phone boots. As soon as the IP phone requests a DHCP response, a rogue DHCP server can initiate a response with data fields containing false information.

This attack allows for possible man in the middle attacks on the IP-media gateway and on IP Phones. Many methods exist that give the hacker the potential to reboot the phone remotely, for instance, utilizing *social engineering*, ping flood, MAC spoofing (probably SNMP hooks and the like).

A preventive strategy would be, if possible, to use static IP addresses for the IP Phones. This implementation will negate the necessity of using a DHCP server. Further, using a state based intrusion detection system can filter out DHCP server packets from unauthorized IP Phone ports, allowing this traffic only from the legitimate server.

TFTP Server Insertion Attack

It is possible for a hacker to change the configuration of a target phone by exploiting the *Trivial File Transfer Protocol* (TFTP) response race when the IP phone is resetting. A rogue TFTP server can supply spurious information before the legitimate server is able to respond to a request. This attack allows an attacker to change the configuration of an IP Phone. Using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing such traffic only from the legitimate server. Organizations looking to deploy VoIP systems should look for IP Phone instruments that can download signed binary files.

Availability and Denial of Service

Availability refers to the notion that information and services will be available for use when needed. Availability is the most obvious risk for a switch. Attacks exploiting vulnerabilities in the switch software or protocols may lead to deterioration in service or even denial of service or denial of some functionality of the switch. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages, causing severe deterioration (possibly denial) of service. A voice over IP system may have even more vulnerabilities when it is connected to the Internet.

Because intrusion detection systems (IDS) fail to intercept a significant percentage of Internet based attacks, once attackers circumvent the IDS, they may be able to bring down VoIP systems by exploiting

weaknesses in Internet protocols and services. Any network can be made vulnerable to denial of service attacks simply by overloading the capacity of the system. With VoIP the problem may be especially severe, because of its sensitivity to packet loss or delay.

CPU Resource Consumption Attack without any account information

An attacker with remote terminal access to the server may be able to force a system restart (shutdown all/restart all) by providing the maximum number of characters for the login and password buffers multiple times in succession. Additionally, IP Phones may reboot as a result of this attack.

In addition to producing a system outage, the restart may not restore uncommitted changes or, in some cases, may restore default passwords, introducing the possibility of intrusion vulnerabilities. The deployment of a firewall disallowing connections from unnecessary or unknown network entities is the first step to overcoming this problem. However, there is still the opportunity for an attacker to spoof his MAC and IP address, circumventing the firewall protection.

Default Password Vulnerability

Just as switches have a default login/password sets, VoIP telephones often have default keypad sequences that can be used to unlock and modify network information.

This vulnerability opens up the prospect of an attacker taking control of thenetwork topology remotely, allowing for not only complete denial of service to the network, but also for a port mirroring attack to the attacker's location. The mirroring attack would give a hacker the ability to intercept any other conversations taking place over the same switch. Further, the switch may have a web server interface that the hacker can use to disrupt the network without advance knowledge of switch operations and commands.

In most systems, telephones download their configuration data on startup using TFTP or similar protocols. The configuration specifies the IP addresses for Call Manager nodes, so an intruder could substitute a different IP address pointing to another call manager that would allow eavesdropping or traffic analysis. This kind of potential for intrusion means changing the default password is crucial. And disabling the graphical user interface is also required to prevent the interception of plain text administration sessions.

Exploitable Software Flaws

Like other types of software, VoIP systems have been found to have vulnerabilities due to buffer overflows and improper packet header handling. These flaws typically occur because the software is not validating critical information properly. For example, a short integer may be used as a table index without checking whether the parameter passed to the function exceeds 32,767, resulting in invalid memory accesses or crashing of the system.

Exploitable software flaws typically result in two types of vulnerabilities:

- Denial of service
- Revelation of critical system parameters

An intruder can implement a Denial of Service remotely, by passing packets with specially constructed headers that cause the software to fail. The goal is to get the system to crash, producing a memory dump that the intruder can search to find IP addresses of critical system nodes, passwords, or other security-relevant information. In addition, buffer overflows that an intruder can use to introduce malicious code exist in VoIP software, just as they exist in other applications. These problems require action from the software vendor and distribution of patches to administrators.

Clever intruders are on top of the issues; they monitor announcements of vulnerabilities, knowing that many organizations will require days or weeks to update their software. Being sure your organization regularly checks for software updates and patches is essential to reducing these vulnerabilities. Automated patch management can assist in reducing the window of opportunity for intruders to exploit a known software vulnerability. This window of time during which organizations are vulnerable is also known as the *vulnerability gap* – a gap all organizations can close by being up-to-date on patches, usually using automated systems.

Account Lockout Vulnerability

An account lockout vulnerability is a situation where an attacker can attempt to access an account several times using an incorrect login at the telnet prompt until the account becomes locked out. Once the account is locked out, no one may connect to the machine for the set lockout time period. The effect is a denial of service. Because this problem takes advantage of a feature common to most password-protected systems (as part of trying to prevent attackers from making repeated login attempts until the correct password is found), it is difficult to circumvent. If such an attack occurs and if remote access is not available to legitimate users as a result, this problem can be solved with physical access control.

Securing Your VoIP

Properly securing your Voice over IP system is a complex process because VoIP is the integration of data and voice into a single network. Your network may be subject to daily attacks by hackers, viruses, and worms. With your old fashion phone system you you would never consider worrying about these types of attacks taking place.

There are nine steps that the *National Institute for Standards* (NIST) recommends you take to secure your VoIP network:

- Develop appropriate network architecture for voice and data communications.
- Examine the risk around deploying VoIP for voice communications.
- Take special precautions for ensuring Emergency 911 (E-911) services.
- Deploy physical controls are especially important in VoIP security.
- Consider additional power backup requirements to ensure continued VoIP availability during power outages
- Find, evaluate, and deploy VoIP-ready firewalls.
- Avoid using 'softphone' solutions, as they are harder to manage and secure.
- If mobile devices are part of your VoIP deployment, make sure they are secured using WPA and not WEP and lock down all the MAC addresses AND limit total connected devices
- Review regulatory requirements regarding privacy and record retention.

Develop Appropriate Network Architecture

Separate voice systems from data systems by putting each on a logically different network if feasible. Different subnets with separate RFC 1918 address blocks for voice and data traffic and with separate DHCP servers for each will ease incorporation of intrusion detection and VoIP firewall protection.

At the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or other VoIP protocols from the data network. Use strong authentication and access control on the voice gateway system, as with any other critical network component. Strong authentication of clients towards a gateway often presents difficulties, particularly in key management. Here, access control mechanisms and policy enforcement may help. A mechanism to allow VoIP traffic through firewalls is required. There are a variety of protocol dependent and independent solutions, including application level gateways (ALGs) for VoIP protocols, Session Border Controllers, or other standards-based solutions when they mature. Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call. (This may not be practical when multimedia protocol inherent security or lower layer security is applied; for example, H.235 Annex D for integrity provision or TLS to protect SIP signaling.)

Use IPsec or *Secure Shell* (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system. If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for IPsec tunneling. Since some VoIP endpoints are not computationally powerful enough to perform encryption, placing this burden at a central point ensures all VoIP traffic emanating from the enterprise network has been encrypted. Newer IP phones are able to provide *Advanced Encryption System* (AES) encryption at reasonable cost.

Note that *Federal Information Processing Standard* (FIPS) 140-2, Security Requirements for Cryptographic Modules, is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

Examine the Risk Around Deploying VoIP

It is important that you examine the issues with deploying VoIP to ensure that the organization can acceptably manage and mitigate the risks to information, system operations, and continuity of essential operations when deploying VoIP systems.

An especially challenging security environment is created when new technologies are deployed. Risks often are not fully understood, administrators are not yet experienced with the new technology, and security controls and policies must be updated. Therefore, organizations should carefully consider such issues as their level of knowledge and training in the technology; the maturity and quality of their security practices, controls, policies, and architectures; and their understanding of the associated security risks.

VoIP can provide more flexible service at lower cost, but there are significant tradeoffs that must be considered. You can expect VoIP systems to be more vulnerable than conventional telephone systems, in part because they are tied in to the data network, resulting in additional security weaknesses and avenues of attack. Confidentiality and privacy may be at increased risk in VoIP systems unless strong controls are implemented and maintained.

An additional concern is the relative instability of VoIP technology compared with established telephony systems. Today, VoIP systems are still maturing and dominant standards have not emerged. This instability is compounded by VoIP's reliance on packet networks as a transport medium. The public switched telephone network is ultra-reliable. Internet service is generally much less reliable, and VoIP cannot function without Internet connections, except in the case of large corporate or other users who may operate a private network. Essential telephone services, unless carefully planned, deployed, and maintained, will be at greater risk if based on VoIP.

Special Considerations for 911 Services

Special consideration should be given to E-911 emergency services communications, because E-911 automatic location service is not available with VoIP in some cases.

Unlike traditional telephone connections that are tied to a physical location, VoIP's packet switched technology allows a particular phone number to be anywhere. This is convenient for users, because calls can be automatically forwarded to their locations. But the tradeoff is that this flexibility severely complicates the provision of E-911 service, which normally provides the caller's location to the 911 dispatch office. Although most VoIP vendors have workable solutions for E-911 service, government regulators and vendors are still working out standards and procedures for 911 services in a VoIP environment. Organizations must carefully evaluate E-911 issues in planning for VoIP deployment.

Physical Security for the VoIP System

Organizations should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.

Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices with a VoIP many more points exist where anyone can connect to a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis and determine the parties that are communicating. You should, therefore, ensure that adequate physical security is in place to restrict access to VoIP network components.

Physical securities measures, including barriers, locks, access control systems, and guards, are the first line of defense for the VoIP system. Organizations must make sure that these physical countermeasures are in place to mitigate some of the biggest risks such as insertion of sniffers or other network monitoring devices. Otherwise, practically speaking, this means that installation of a sniffer could result in not only data being accessed, but all voice communications being intercepted.

Costs for Additional Backup Systems

Evaluate costs for additional power backup systems that may be required to ensure continued operation during power outages. Conduct a careful assessment to ensure that sufficient backup power is available for the office VoIP switch, as well as each desktop instrument. Costs may include electrical power to maintain UPS battery charge, periodic maintenance costs for backup power generation systems, and cost of UPS battery replacement. If emergency/backup power is required for more than a few hours, electrical generators will be required. Costs for these include fuel, fuel storage facilities, and cost of fuel disposal at end of storage life.

VoIP-Ready Firewalls and VoIP Security Features

VoIP-ready firewalls and other appropriate protection mechanisms should be deployed. Organizations must enable, use, and routinely test the security features included in VoIP systems.

Because of the inherent vulnerabilities (such as susceptibility to packet sniffing) when operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. Organization security policy should ensure that these features are used. Additional measures, described in this document, should be added. In particular, firewalls designed for VoIP protocols are an essential component of a secure VoIP system.

Restriction of Softphone Systems

If practical, *softphone* systems, which implement VoIP using an ordinary PC with a headset and special software, should not be used where security or privacy are a concern, because worms, viruses, and other malicious software are extraordinarily common on PCs connected to the Internet, and very difficult to defend against.

Well-known vulnerabilities in web browsers make it possible for attackers to download malicious software without a user's knowledge, even if the user does nothing more than visit a compromised web site. Malicious software attached to email messages can also be installed without the user's knowledge, in some cases even if the user does not open the attachment.

These vulnerabilities result in unacceptably high risks in the use of *softphones*, for most VoIP site installations. In addition, because PCs are on the data network, a softphone system conflicts with the need to separate voice and data networks to the greatest extent practical.

Protection of Mobile Systems on the VoIP System

If mobile units are to be integrated with the VoIP system, use products implementing *WiFi Protected Access* (WPA), rather than 802.11 *Wired Equivalent Privacy* (WEP).

The security features of 802.11 WEP provide little or no protection because WEP can be cracked with publicly available software. The more recent *WiFi Protected Access* (WPA), a snapshot of the ongoing 802.11i standard, offers significant improvements in security, and can aid integrating wireless technology with VoIP systems.

NIST strongly recommends that the WPA (or WEP if WPA is unavailable) security features be used as part of an overall defense-in-depth strategy. Despite their weaknesses, the 802.11 security mechanisms can provide a degree of protection against unauthorized disclosure, unauthorized network access, or other active probing attacks. However, the Federal Information Processing Standard (FIPS) 140-2,

Security Requirements for Cryptographic Modules, is mandatory and binding for Federal agencies that have determined certain information must be protected via cryptographic means. As currently defined, neither WEP nor WPA meets the FIPS 140-2 standard. In these cases, it will be necessary to employ higher level cryptographic protocols and applications such as *secure shell* (SSH), *Transport Level Security* (TLS), or *Internet Protocol Security* (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms to protect information, regardless of whether the nonvalidated data link security protocols are used.

Compliance with Privacy/Record Retention Statutes

Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

Although legal issues regarding VoIP are beyond the scope of this document, readers should be aware that laws and rulings governing interception or monitoring of VoIP lines, and retention of call records, may be different from those for conventional telephone systems. Organizations should review these issues with their legal advisors.

The Magnitude of VoIP Vulnerabilities

Everyone knows that VoIP has been experiencing rapid growth. Even still, you might be surprised to learn that over 30% of all voice traffic is now transmitted with VoIP technology (IDC). The mass deployment of this new technology brings along with it many challenges – one area the security of your network.

Because IP networks are subject to sophisticated, automated attacks, voice traffic on those networks is more vulnerable says David Fraley, author of *Cyberwarfare: VoIP and Convergence Increase Vulnerability*.

In fact, the UK's *National Infrastructure Coordination Centre* (NICC) has released findings that equipment from many vendors who have implemented the H.323 protocol standard for IP Telephony contains flaws attackers can exploit. (for more detail, visit *http://www.uniras.gov.uk/vuls/2004/006489/h323.htm*)

According to tests commissioned by NICC, these vulnerabilities can leave products open to:

- Denial-of-Service (DoS) attacks
- Buffer-overflow attacks
- Insertion of malicious code into the compromised equipment

According to CERT Advisory Number CA-2004-01 (visit the *http://www.cert.org/advisories/CA-2004-01.html* location), companies affected by these vulnerabilities include:

Cisco	Stonesoft
Check Point	WatchGuard
NetScreen	3COM
Nokia	AT&T
Microsoft	D-Link
Nortel	Extreme
Avaya	Foundry
Alcatel	Fujitsu
F5	Hitachi
Secure Computing	Intel
Cyberguard	Juniper
Symantec	NEC

As just one example, Cisco alone has many products that contain vulnerabilities in processing H.323 messages.

All Cisco products that run Cisco IOS software and support H.323 packet processing (*http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml#process*):

- IOS Firewall
- IOS Network Address Translation
- Call Manager
- Conference Connection
- 7905 IP Phone
- BTS 10200 Softswitch
- Internet Service Node
- H.323 Gateway, H.323 Gatekeeper
- ATA18x Series Analog Telephony Devices

In some cases, Cisco does not plan to fix the vulnerabilities that have been identified.

To help you deal with VoIP's inherently vulnerable nature, you should be aware that there are a number of possible attacks that can be more readily perpetrated against a VoIP than against a standard network. The next section presents some of those attacks.

Possible VoIP Attacks

You should be alert to the types of attacks on your VoIP that CVEs can make it vulnerable to, including:

- Man in the Middle (eavesdropping and altering)
- Denial of Service (DoS)
- Compromise of Gateways
- Compromise of Endpoints – Impersonation

QoS and Security Issues

Quality of Service (QoS) refers to the speed and clarity expected of a VoIP conversation. QoS attacks are easier to pull off than other attacks, without a hacker going to extremes – no longer is it necessary for a hacker to *take down* an entire network; the hacker can merely *slow down* traffic.

QoS attacks are hard to defend against: Implementing proper security measures such as firewalls and encryption still leaves your VoIP vulnerable to latency and jitter.

Latency
Latency is the time from when words are spoken until they are heard at the other end. Latency greater than 150 milliseconds is unacceptable in most cases.

Jitter
Jitter is a series of non-uniform delays. Jitter requires buffering at the endpoints and application level reordering, which produces more latency. Increased jitter makes it hard to tell when a packet is missing or just late.

Packet Loss
VoIP is highly sensitive to packet loss. Loss Rates as low as 1% can garble communications.

Latency and Jitter can contribute to *virtual packet loss* as packets arriving after their deadline are as good as *lost*.

Firewalls, NAT Routers, and Encryption
The Old Stand-By's are not as reliable as they used to be: Firewalls, *Network Address Translation* (NAT) routers, and encryption suffer from these shortcomings:

- Cannot be Implemented in a VoIP network without special considerations – standard components are not built for VoIP's high rate / small packet traffic pattern.
- They degrade the Quality of Service (QoS) by causing Latency, Jitter, and Packet Loss.
- They obstruct the call set up process by blocking incoming calls.

Firewalls
Firewalls filter out malicious traffic based on a set of rules and are needed to protect networks from outside attacks. They also secure the internal barrier between voice and data networks.

Firewalls and QoS
Firewall traffic investigation adds latency to the system and heavy data traffic can introduce jitter, which reduces the *quality of service* (QoS).

To resolve this issue, implement firewalls with fast CPU's to handle the high rate of packet delivery. Use QoS-aware firewalls.

IPSec
In ESP Tunnel Mode, IPSec protects both the data and the identities of the endpoints. IPSec is the standard encryption suite for the Internet Protocol and will be fully supported in IPv6.

Problems with IPSec include:

- Encryption can be used to secure voice data and avoid the firewall problems.
- Encryption introduces latency/jitter
- Encryption/decryption process takes time
- Crypto-engine schedulers do not implement QoS

Solutions include packet compression schemes, which have experimentally aided performance. QoS-aware scheduling before and after encryption heuristically improves performance.

Network Address Translation (NAT)
Network Address Translation (NAT) is used to allow multiple terminals to share a single IP address. It allows security measures to be consolidated at the NAT router and hides information about the structure of the internal network.

The problem with NAT and Firewalls is that both can block incoming calls. To prevent them from doing so you can apply:

- Application Level Gateway
- Firewall Control Proxy

VoIP Call Setup Disruption
The two competing protocols for VoIP call setup are H.323and SIP. H.323 is a suite of several more specific protocols. It uses dynamic ports and binary encoding. SIP is a simpler protocol running over one port using a three way handshake. It uses a single port and text encoding.

Firewalls can block the call setup ports and NAT can change the IP address/ports being used internally. As a result they both disrupt the call setup process.

To prevent any such disruption, incorporate an ALG or FCP into the architecture that can manipulate the setup packet data.

What Should You Do Now?
Actions you can take now to protect your VoIP system include:

- Deploying Network Tools
- Protecting Voice Data
- Defending Against Registration Hijacking

Deploying Network Tools
You should create virtual LANs to separate voice and data traffic into distinct address spaces (physically unique networks are not required).

This protective measure helps to both reduce risk of data sniffers infiltrating the VoIP system and tune your IDS separately for voice and data.

Use firewalls designed for VoIP traffic.

At the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or MGCP connections from the data network.

Protecting Voice Data

Guidelines for protecting voice data as it travels over a VoIP network:

- Avoid PC-based *softphones* if practical
- Keeps voice and data networks separate
- Use access control and encryption where possible
- Use IPSec or SSH for all remote management and auditing access
- Do encryption at the router or other gateway, not the individual endpoints

Defending Against Registration Hijacking

The primary defenses against registration hijacking are to use strong authentication and to use VoIP-optimized firewalls to detect and block attacks.

At a minimum, all registrars should require MD5 digest authentication and selection of strong passwords. Passwords must not be *mechanically* generated (such as the extension with a prefix/suffix). These steps help to prevent dictionary-style attacks. Ideally, registrars should use strong authentication, such as that provided by the TLS.

The *Internet Engineering Task Force* (IETF)-approved security solution is to use the combination of TLS, MD5 digest, and strong passwords.

Registrations from the external network should be disabled if possible – or at least limited to a small set of external UAs (such as teleworkers), who have a valid need to register from the external network. Max-Forwards header limits (and other techniques) can be used to detect external attacks, but these limits not commonly enforced.

Of the numerous security issues unique to VoIP, registration hijacking is one of the more serious. An attacker who successfully hijacks registrations in your organization can block, record, and otherwise manipulate calls to and from your organization. This is a very real threat that you must counter.

Harden Your VoIP Against Attack

Consistent repair of your *Common Vulnerabilities and Exposures* (CVEs) is the litmus test that all information security professionals will be judged by regarding how successfully they are protecting their VoIP networks. Repairing vulnerabilities also helps you stay in compliance with related regulations, including GLBA, HIPAA, 21 CFR FDA 11, E-Sign and SOX-404.

CVE Management is the key to hardening your VoIP and removing defects from your computers and networking equipment. Three types of solutions that claim to help you harden your VoIP are:

- Configuration Management
- Patch Management
- Vulnerability Management

CVEs specific to VoIP are on the rise. By using an automated vulnerability management system to find and remediate them in a timely way, you can reduce the risk of your VoIP system being vulnerable to attack.

If you find a solution that helps automate this process for you, make sure it helps find and fix CVEs. If the solution you choose has not been vetted by MITRE, then it may not be compatible with the CVE standard.

MITRE is funded by the U.S. Department of Homeland Security to manage this industry standard – the database of exposures and weaknesses in all networking equipment and computers. Look for this logo to accompany the product or service in question verify it at *http://cve.mitre.org* and *http://nvd.nist.gov*. Every day there are new CVEs listed and you can find them on *http://cve.mitre.org*, the homepage for helping you stop hackers and harden your assets. By knowing the CVEs, you can find any CVEs your VoIP system may have, then you can find a way to block any exploitation of that CVE that would impact your VoIP.

Protect Against CVE Exploiters

There are four key things you can do to protect yourself against CVE Exploiters:

- Detect and track assets
- Audit your VoIP for CVEs
- Lock the doors against CVE Exploits
- Clean up your CVEs

Detect and Track Assets

Do you have policies and systems in place to track all of your network-based assets? You should have a policy on whether or not you allow laptops in and out of the office. For instance, you may require that all laptops allowed on the network be company assets, rather than a personal computer that can be used at home. Do all hosts have the required firewall, antivirus, antispyware, and patches installed so they are up to date and have minimal vulnerability to attack? What about wireless routers and *ad hoc* wireless LANs – have you sniffed the airwaves and port connections to see if there are any new wireless devices or servers connected to your network? Answering these questions is critical in the protection of these assets against CVE exploiters.

Audit Your VoIP for CVEs

Find a tool you like. Google *Security NACwall* or use similar keywords and you'll find companies and products in this marketplace. Do an evaluation of open source versus commercial products. If you built your

firewall from scratch, go for open source, otherwise find a company you can work with and trust. Make sure you pick a tool that doesn't take any assets off line, and one that scans and reports on CVEs.

Lock the Doors Against CVE Exploits

Your firewall is your best countermeasure. Make sure to review the firewall's logs – look for suspicious traffic. Also make sure you set up the VPN interface properly and know who's using it, whether they are coming in through a secure tunnel on an insecure or *sick* computer. By reconfiguring your rules table around CVE exploits, you can be one step ahead of the hackers. For example, why not block all inbound/outbound traffic for ports that you don't use – port 445 was exploited by MSBlast and Sasser. Do you need to keep this port open at the firewall? Look at the computers that have CVEs – how long will it take to fix those CVEs and what ports are they on? Update your rules table until it is fixed. Don't trust all patches. Reinspect your VoIP system the for same or new CVEs on the affected ports and services. Keep repeating this process, daily.

Clean Up Your VoIP's CVEs

Does your vendor offer patches? Did the patch fix the CVE? Yes, good. No? Then, why not shut off the service or feature that harbors the CVE – one quick configuration change like that and there won't be a CVE to exploit. Some CVEs can be patched while others require intelligent reconfiguration. Clean up your CVEs on the most important systems and highest risk of attack. Keep repeating this process, daily.

If you don't have time to do all this yourself, find a security appliance, service, or consultant who will do it for you. It's easy to find them, now that you know what to look for and where to look. It's a good idea to be sure that the security appliance or vulnerability management system, not only detects CVEs, but quarantines systems with CVEs until the issues are repaired in order to protect your VoIP network from intrusions. The system should then help with remediation and repair by providing some kind of tracking system.

CERT Recommendations

Carnegie Mellon University operates the CERT Coordination Center, a major reporting center for Internet security problems. CERT, founded by the *Defense Advanced Research Projects Agency* (DARPA), provides technical advice and:

- Coordinates responses to security compromises
- Identifies trends in intruder activity
- Works with other security experts to identify solutions to security problems
- Disseminate information to the broad community

The CERT/CC also analyzes product vulnerabilities, publishes technical documents, and presents training courses. In the CERT Advisory referenced above, recommendations are issued to help companies protect their networks from these vulnerabilities.

Among their recommendations are the following:

- Block access to H.323 services on devices that do not need to be exposed
- Limit access to only those machines that use H.323 for critical business functions
- Limit access of any type to only those areas of the network where it is needed
- Consider disabling application-layer inspection of H.323 packets by Firewalls
- Coordinate among telephony, application, network, and desktop staff to assess the threat in individual network segments

Summary

VoIP security requires adapting traditional network security measures for a high speed, dynamic environment.

Credits:
Thanks also to NIST and CERT for providing information on their web sites. Many thanks to the MITRE CVE team for their work in creating and standardizing CVEs, *http://cve.mitre.org*.

On the 'Net

For more information about VoIP, refer to the following resources:

- *Security Considerations for Voice Over IP Systems*, NIST *http://csrc.nist.gov*
- *Five tips for securing a converged net*, Computerworld *http://www.computerworld.com/securitytopics/security/story/0,10801,85844,00.html?SKC=security-85844*
- *Security in SIP Based Networks*, Cisco: *http://www.cisco.com/warp/public/cc/techno/tyvdve/sip/prodlit/sipsc_wp.pdfIP*
- Telephony Security in Depth–Cisco *http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safip_wp.htm*
- *http://nvd.nist.gov/*

GARY S. MILIEFSKY, FMDHS, CISSP®

Gary S. Miliefsky is a 20+ year information security veteran and computer scientist. He is a member of ISC2.org and a CISSP®. Miliefsky is a Founding Member of the US Department of Homeland Security (DHS), serves on the advisory board of MITRE on the CVE Program (CVE.mitre.org) and is a founding board member of the National Information Security Group (NAISG.org).

FIFA World Cup 2010

Network Security Advisory

High profile events such as the 2010 FIFA World Cup always lead to higher Internet search traffic. Maybe you're looking for tickets, the latest scores or video highlights from the day's games.

If you find yourself doing a FIFA search anytime during the World Cup, we urge you to be mindful of the search results links, because concentrated search traffic around one particular subject tends to bring out search engine optimization (SEO)-based attacks. The FIFA World Cup is no exception.

SEO attacks work by getting popular search engines to rank malicious Websites among a list of the top set of returned results following a gaming related keyword search. And it's happening to FIFA today. See the screen shot that identifies a malicious link embedded in a search results list (see Figure 1).

SEO attacks can be dangerous because they are often user-initiated, unlike many other solicited attacks seen in the wild. In addition to malware attacks, fraud is also a significant threat to be aware of. For example, FIFA issued a scam warning earlier this year that suggested sports fans be wary of ticket lotteries and any other communications from FIFA that ask for additional payments and/or personal information to secure tickets. New threat innovations allow hackers to carry out attacks such as the ones described above with such ease that it becomes essential to construct a formidable defense plan.

More on SEO

SEO attacks nowadays have become more sophisticated and dynamic. Automated processes (bot agents) can keep the SEO attack fresh and active with particular keywords. In the past, perhaps one of the most effective SEO attacks was using Google Trends. This attack capitalized on hot keywords, typically from major media outlets that users were searching for on a routine basis. In many cases, the malicious sites stole HTML templates directly from the legitimate sites they were mirroring, changing some code to redirect the victim to yet another malicious site serving attack code. (see Fortinet's blog post here). SEO attacks usually occur in two stages like this, with the intermediate *lure* site redirecting the victim to a secondary site. To achieve success, attackers typically use a high volume of primary sites (the ones ranked in search results), many of those are compromised and managed by automated processes. Remember to *think before you link* when clicking on those search results.

Protect your network

In a bid to stay safe online, enterprises need to educate employees on Web usage and define policies on Web content that is appropriate for the workplace. Even legitimate Websites can be compromised, making it difficult to completely avoid malicious code online. In a previous attack on the Super Bowl, Web traffic going to Dolphin Stadium was diverted to malicious sites using JavaScript that had been injected by attackers onto the stadium's site.

Fortinet's FortiGuard team recommends IT managers read the company's regular threat research blogs (available via RSS) to stay current with latest threat trends. Companies should also seriously consider putting in place an intelligent, layered security solution, such as Fortinet's Unified Threat Management (UTM) offerings. With Web 2.0, mobile

computing on the rise and a much more distributed and global workforce, companies are exposed to a greater than ever number of entry points into the corporate network.

DEREK MANKY

Derek Manky, Project Manager, Cyber Security & Threat Research at Fortinet

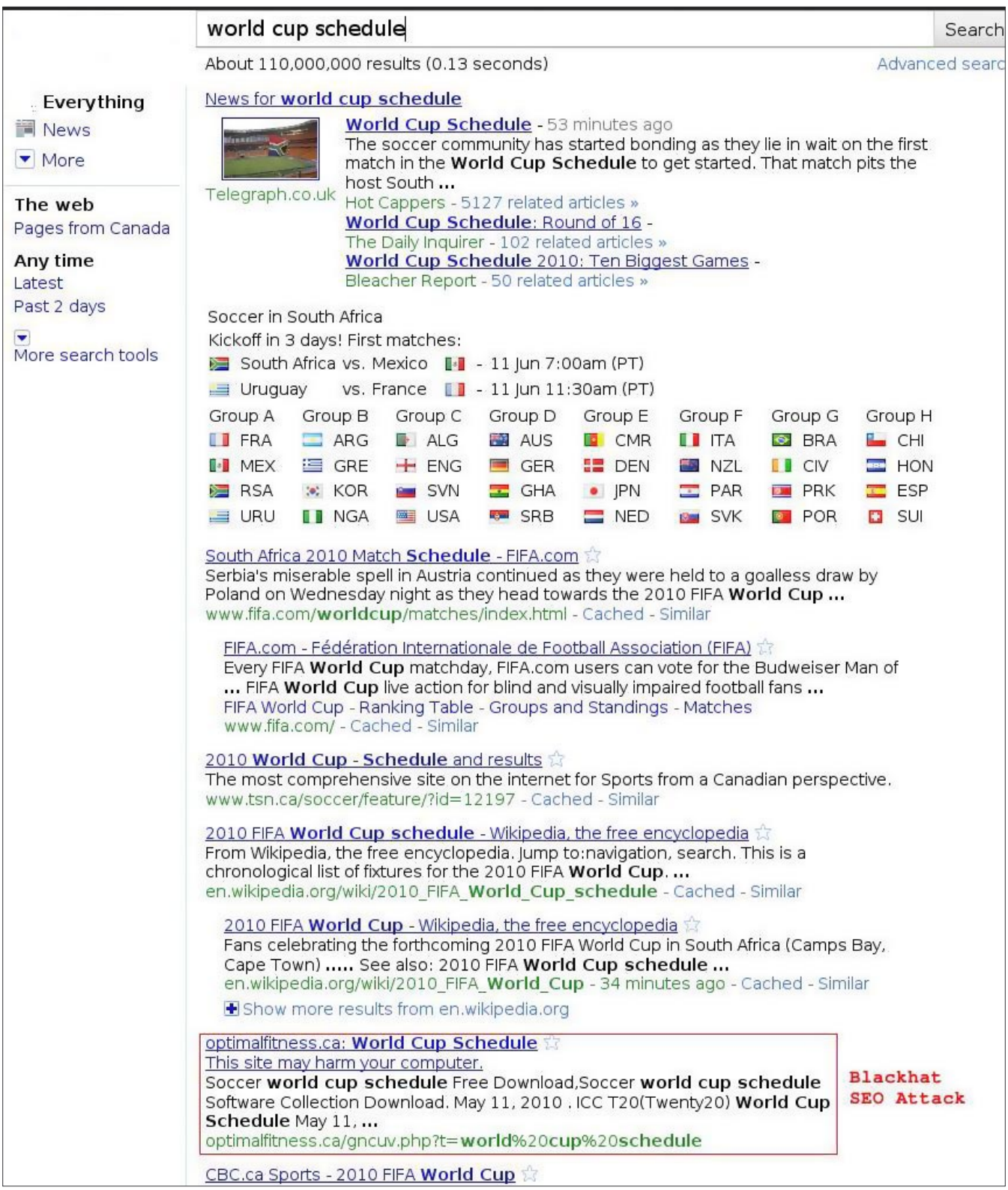


Figure 1.

Hacking the Bad Guys

A brief BBC article today about a presentation at Syscan by Laurent Oudot from Tehtri Security got me thinking. The presentation was about the security holes in common malware and web kits, and how the bad folks don't actually use the tools available to secure their own code. I didn't get to see the presentation, but the concept brings up a few interesting thoughts.

We all know it's an incredible pain to build secure software, and it'll never be completely secure especially when you have to rely on platforms and servers that themselves bring flaws and vulnerabilities. Most of us make a living securing, building, or breaking applications and networks. We know it's tough to do. Here we have some clear evidence that the bad guys, the ones that spend their time picking holes in our defenses, aren't so good at plugging their own holes either. It's reassuring really, maybe we actually are doing something better than the other team.

So I have to wonder. Why don't they use the tools we all build together to secure their own code? I have a few theories. As we all know, the world of bad guys is made up of 2% genius that can code, reverse engineer, build an exploit, and design a command and control protocol. The other 98% use the code these folks produce without understanding or inspecting. So the smart ones build proof of concept code, possibly not really intending it to be used in production and thus not considering how secure or stable the code is. The script kiddies grab it and assume it's ready to go.

This leaves us some very interesting possibilities of which we may not be fully taking advantage. Let's say you're a cyberwarrior proudly defending your nation's infrastructure and citizens. You spend your time gathering information about the infrastructure and vulnerabilities of the nations likely to attack. You plan first strikes and counter attacks, trojan their command and control systems, and monitor traffic and activity. Or if you're smarter you're tracking the vigilante groups that are evolving into professional hit squads, the ones more likely to be an attacker for hire in the next conflict. But that's a whole other article.

Looking for the weak spots in an economy is interesting and necessary on some levels as a cold war style mutually assured destruction deterrent. But it's just as likely, if not more likely, that the most significant attacks a nation state will have to defend itself against will not come from a state but from a terrorist group or organized crime syndicate. If law enforcement takes an effective and serious stab at the organized *Russkranian* criminal gangs they'll likely fight back. If these gangs are smart, which they have proven themselves to be over the years, they'll not fight back with reinforced steel doors and shotguns to hide behind, but with electronic attacks and sabotage. If part of the power grid near Washington DC were to go down after a threat from a group under siege, I suspect law enforcement would have to think twice about pushing further. Surely the political will behind a crime sweep would dwindle.

So there you are, proud cyberwarrior, suddenly realizing maybe you're only preparing for half of your potential enemies. And unfortunately what you're not watching are the half that are more likely to attack, and will do so without diplomatic warning or threats. So let's start looking at the bad guys that are not state sponsored. Conveniently about 90% of the botnets out there are using the same 10 or 20 codebases for their CnC, php shells, and tracking systems. Interesting for us as the good guys as most of these codebases have been compromised or are for sale on the market. Heck, if you want the code for a good php shell just

put up an old vulnerable version of php or phpnuke somewhere and wait a few minutes. Someone will upload several for you!

So we have an advantage over the bad guys. True, we run thousands of different applications and many different servers and operating systems which contain untold numbers of new bugs to be exploited. And the bad guys only have to have a hole in one of them to get us. But we also have an advantage. The bad guys use a small number of known tools to control their attacks against us, but we have the source for those tools.

The saying *the best defense is a strong offense* holds true here. If I know of a vulnerability in most of the major cnc packages likely to be used to attack me I am in a very strong position when that attack comes. I may have more points to apply pressure to, but if i know how to destroy my attackers control of his entire attacking force, I have a very significant chance of winning the war. We build our networks to survive attack, and not be vulnerable to a single point of failure. Our attackers aren't at that point yet with a few exceptions. We should be preparing to exploit that imbalance.

The same concept of offensive defense applies to private security and security contractors. We need to continue to improve how we code and how we secure our systems. But we also need to think offensively. Say for instance I have a bot infestation in the network of a large organization. If I can identify the cnc mechanism, but not necessarily every infection in my enterprise, my logical point to apply pressure to the problem lies in attacking the command and control protocols and infrastructure being used against me. If the bots can't report home then the infections are less of a threat and can be mitigated over time.

Lets take it yet another step further. If I have come to the realization that I will be a target, and I will get owned eventually, then I ought to be thinking about making responding that attack easier. What if I were to put together a really cool, super easy to use command and control codebase. Release it under the name l337c0d3rd00d and make a lot of noise about how much better mine is than the other l0s3rs out there. It'll get used by some set of last script kiddies.

But I don't do anything as obvious as backdooring or a super admin password. We intentionally give it buffer overflow flaws, or use php implementation idiosyncrasies to give us an avenue to attack and control or disable the entire network. And make sure it leaves the network in a way that makes recovering the bots impossible.

Important here of course is making sure that your use of the nuclear option isn't detectable by the bad guys. If they figure out that a codebase is intentionally able to be compromised, or that it just seems unstable, it won't be in use much longer. If we do this over and over the bad guys will be forced to use the SDLC to develop more secure code. Heck, maybe they'll develop some new tools we can all use!

My final thought on the matter. Back to our proud cyberwarrior. If you're not thinking ahead to where I'm thinking please let me guide you there. The talk of a cyber first strike is complete nonsense. We've suffered thousands of first strikes and we've not done anything to fight back other than the random law enforcement action. The bad guys actually discipline and attack each other more often and far more effectively than we do. So what would I like to see? Glad you asked, here's my best day ever:

We compile enough vulnerabilities and identify the major botnets out there. We coordinate among the certs and offensive cyber operations out there. And we pick a day, the day we shut down all the botnets. All of them. A couple years ago we shut down Atrivo and Mccolo and saw spam rates on the Internet drop by half for a week until they recovered their bots. Can you imagine how well the Internet will work if we shut down 90% of the crud out there?

I have reasons for wanting this other than the sheer pleasure of it. If the criminal organizations out there are out of business for a few weeks it's possible that legitimate businesses will be able to swoop in and provide these services and products at real prices. Maybe people will stop giving their credit card numbers to popup ads that promise to rid the 243 viruses the ad just magically found on their computer. And maybe, just maybe, some of these very bright individuals wasting their time taking advantage of the trusting nature of our fellow humans will actually find a productive use for their talents. So when the crime syndicates recover and rebuild perhaps they will be less powerful, and maybe fewer of them.

I can dream can't I?

MATTHEW JONKMAN

Matt is the founder of emergingthreats.net, the only open and community based intrusion detection ruleset, and is also president of the Open Information Security Foundation (OISF). The OISF is building Suricata, an next generation ids funded by the US department of homeland security.

Managing Your Facebook

Privacy in 2010

The Privacy and Authentication issues surrounding user profile data and third-party Facebook applications.

All of us know what Facebook is and most of us know someone who uses it. It's no surprise then, that Facebook is the largest social community on the planet. It currently has over 400m members (see Table 1) who are members of the website to contact friends, stay in touch with people and share their personal lives with people. It's the last point that conjures up the *celebrity* image whereby everyone wants to be famous. Facebook (much like YouTube) is allowing people to become famous just because they might have said or done something.

Andy Warhol said in 1968: "In the future, everyone will be world-famous for 15 minutes".

Note: *400m* isn't actual users – this number to likely to be much less.

The need to have friends and be famous has its own risks. The real concern has to be the ease at which people let others into their lives, especially because people are driven by *how many friends they have*. It's this last point that really causes the alarm bells to ring regarding privacy control and potential *data leakage*.

Table 1 – *Facebook company statistics – Facebook (c) 2010*

More than 400 million active users
50% of our active users log on to Facebook in any given day
More than 35 million users update their status each day
More than 60 million status updates posted each day
More than 3 billion photos uploaded to the site each month
More than 5 billion pieces of content (i.e. web links etc) shared each week
More than 3.5 million events created each month
More than 3 million active Pages on Facebook
More than 1.5 million local businesses have active Pages on Facebook
More than 20 million people become fans of Pages each day
Pages have created more than 5.3 billion fans

Facebook Protests

Facebook has drawn protest these last few months for amending its privacy and to some it's forgetting how it started – with users. The *user* community is largely being forgotten now, which is a little surprising considering how the website was built – with users of course. The biggest challenge facing most business – *how do you find people to sell to?* is now consigned to the trash can – the next biggest challenge for Facebook will be how they monetize this vast database of information.

Privacy versus Revenue

There is a fine line between privacy and making money. One way Facebook will make money is from the user profile data – it's not surprising with the vast amount of *personal* data that is being uploaded every second that this is going to be the most successful channel. Facebook is making hundreds of millions of dollars every month from advertisers who realize the revenue opportunity. It doesn't take a genius to work out that Facebook would be foolish to stop all data from being used for marketing.

The biggest problem will be how they handle user privacy. One way might be to remove default *safety* settings and get the user to be proactive – in other words users will get basic default privacy settings and it will be up them to stop

third party advertisers from collecting invaluable personal profile data by checking yet more privacy check boxes.

Facebook may in turn make it more difficult for users to find these settings as it's not in their interest for users to use them as they will be collecting the dollars from the advertisers. Naughty you might say, but then again the social world is a business and it has to survive somehow.

There is a fine line between protecting user profiles and making money from user profiles. Last month, Facebook had an internal meeting to discuss new Facebook functions that could well help it gain insights about millions of its members and help it sell more advertising. These functions will duly arrive in time, especially if Facebook wants to compete directly with power house Google.

It's been a rough last few months for Facebook. First their privacy policies were run through the wringer, and now there's another advertising scam doing the rounds, looking to poach user's sensitive information. According to security company Sophos, thousands have been hit by a malware attack disguised as a naughty video called *candid camera prank*.

The *candid camera prank* encourages you to click a thumb of a suggestive image of a woman exercising, which then leads to the option of downloading the *correct video software* to view the clip in question. The download turns out to be an adware installer that grabs all of your information and plagues your desktop with pop-ups/nagware.

Facebook Application Security

Facebook has also developed a comprehensive application network. The application network allows developers to develop third-party software with the use of the Facebook APIs. Facebook has been very busy recently with updates including a brand-new authentication scheme for applications, possibly affecting the sort of application attacks that have been reported in the press within the last year.

Facebook Application Authentication

The old authentication system: Facebook is actually phasing out its old authentication system. The old system generated a session by forwarding clients to a particular Facebook URL. If a user chose to authorize an application, Facebook would forward the user back to the application context, passing along a valid session key and session secret. The Facebook application then attempts to use the session key to generate the API requests by signing each with either the session secret or application secret.

The new authentication system: Facebook has recently rolled out OAuth 2.0 which is a lightweight model of OAuth 1.0/WRAP. Closer inspection of the specification and it clearly defines several models of authentication resources and how the Web Server Flow works.

How does this actually work? There are two major steps whereby the application forwards clients to a Facebook URL; however it does this with a list of specific permissions. The user has to grant the list of permissions to generate the session key to be able to use the given application.

So what is different? The real change from the previous authentication system is that the Facebook application must now use the session key to request an access token from Facebook. This particular step is done directly from the Facebook application server which also must be signed by the application secret.

New API Methods: Facebook has also introduced new API methods for accessing data. In the first instance, Third-party Facebook developers can now use a simple JSON interface to make requests using a valid OAuth access token. The downside here is Facebook is not forcing developers to move to this new interface – though most third-party developers appear to be still using the old REST API.

Facebook did announce on June 1st 2010 that they are requiring developers to use this new system (but it is not mandatory at present June 2010). Facebook developers will be using the new Graph API for access and publishing – developers should keep one eye open on this. In time Facebook will force developers from FBML tag-based applications and shift them to use iFrame – but this comes with obvious security implications.

Facebook Application Authentication Security Implications

The major problem with the OAuth 2.0 system is that it isn't *tried and tested*. It's relatively a young protocol which is under constant development – like anything under development there are security holes that need to be filled. The OAuth 2.0 protocol is currently handling third-party authentication for over 400 million users, so you'd expect security to be of high concern.

The really strong aspect of the new protocol is that the two step flow process makes it impossible to forge a request for an access token. A hacker might be able to hijack the first implementation process but getting an accessible token requires the application secret. If a hacker has cracked the application secret then they have access to the third-party application.

Application attacks using OAuth 2.0 is actually much easier than under the old system. Facebook is

advising all developers to move towards HTML-based applications rather than FBML which *exploits cross-site scripting* (XSS) holes. A hacker for example could take advantage of an FBML application by inserting the JavaScript.

Developers will find out that the new API requests make it easier for hackers to exploit – i.e. *cross-site request* (CSRF) attack would make it very easy for hackers to exploit. Another attack vector is once an application has a valid session an XSS attack would be able to hijack the session and issue requests back to Facebook using the Facebook applications access token.

Facebook has always been in the firing line with this type of attack vector – It has though made it a lot more difficult for this attack to work by introducing an access token and Graph API requests to replace the session secret to make the REST API requests.

As you will know this attack vector can only work if there is an XSS vulnerability in the third-party Facebook application – so this hijack method is more difficult to deploy than in the previous protocol. If you were to search the Internet you will find references which highlight over 9000 Facebook applications that have serious XSS or other security flaws.

Facebook Application Security Hints and Tips

Here are some simple measures that can help you identify or at least reduce the threat of having your Facebook profile hacked when using a Facebook application. We should all be very suspicious of any Facebook application that claims to let you do something that you cannot normally do – such as permitting you to see who is viewing your profile.

Applications cannot identify or pick up email addresses without first asking your permission. The simple message here is *be careful what you approve here*.

Facebook TIP

A friend might have signed up to a Facebook rogue application which harvests your profile data – so what can you do to stop this from happening?

- Go to *Account-Privacy Settings*
- Click *Applications and Websites*
- Click the settings for *What your friends can share about you*
- Deselect anything you wouldn't want a scammer not to see

Facebook applications do not reside on the PC, they are integrated into the Facebook website – so people are unable to run virus or malware scans on these applications to find out whether they are malicious are not.

Facebook TIP

Hiding your Facebook profile from appearing in search engines in two simple steps:

- Log into your Facebook account and navigate to *Privacy Settings* (see top right hand corner near *log out*) or use *http://www.facebook.com/privacy.php*
- Click on *Search* and where it says *My public search listing* uncheck the box. This will disable your profile from appearing in search engines.

Data Privacy

Facebook privacy has been the subject of much discussion in recent months. It isn't the only social website that is facing criticism.

Google, the world leader in Web search, has been in trouble recently for collecting information from unsecured wireless networks all over the world. This was done as specially equipped vehicles took pictures for the Google mapping feature called Street View. Google said it never meant to collect people's private information, like e-mails and passwords.

Some of the main problems have been linked to the default privacy settings in Facebook. Facebook now opts users in to allowing third party sites like Yelp to *personalise* a user's experience, and there are questions about how much information is being given away.

One suggestion here is to make instant personalization which exports users content to third-party Web sites, opt-in by default.

Another data issue circulating is the one concerning third-party applications Facebook currently stores the data for no more than 30 days and does not use it for advertising or selling to third-parties. One suggestion here is for Facebook not to keep data about user visits to third-party sites that use social plug-ins, such as the *Like* button.

The most important privacy issue has to be profile content control. Facebook recently reduced the amount of user information that is available to everyone it allows users (see Table 2) to restrict the visibility of their friends lists and pages they like. Why not give users control over every piece of their profile data, including their name and profile picture?

Considering the number of users using Facebook it is rather surprising they have not implemented an HTTPS connection. Facebook has mentioned it is testing SSL access and plans to provide this service as an option in the coming months.

Facebook does not impose any restrictions on users that prevent them from exporting the content that they have posted themselves on Facebook. A suggestion here would be to provide users with simple exporting tools so users can easily transfer their information to another social network.

Table 2. *Facebook User Statistics – Facebook (c) 2010*

Average user has 130 friends on the site
Average user sends 8 friend requests per month
Average user spends more than 55 minutes per day on Facebook
Average user clicks the Like button on 9 pieces of content each month
Average user writes 25 comments on Facebook content each month
Average user becomes a fan of 4 Pages each month
Average user is invited to 3 events per month
Average user is a member of 13 groups

Facebook does have open APIs that permit applications to export this information (but this may well be collected by the third-party application). Facebook does not allow exporting of content that is created by others because it doesn't respect the decisions users make on Facebook about how to share their data.

Facebook data privacy could also be enhanced if it was allowed to degrade or fade in time. The idea of *degrading* data about visitors isn't a new concept. A database could be developed that would gradually swap user details for more general information and help guard against accidental disclosure.

A research project has recently been carried out by a Dr van Heerde from the *Centre for Telematics and Information Technology* (CTIT) at the University of Twente in Holland. He looked into ways to change the way databases manage information about users and customers.

Dr van Heerde claims that the ability of those databases to gather information tempts companies and organisations to hoard information just in case it proves valuable – which is a very true statement considering the Facebook revenue model is based on ad targeting which directly correlates to user profile data. Facebook doesn't rent or sell user data directly, but if users use Facebook third-party applications, some or all user profile data can be captured and potentially shared back in reverse with Facebook.

The dangers of having all this data, is that thousands of third-party applications and Facebook have access to sensitive and very valuable personal content. The data can leak or be used for fraudulent purposes. Everyone makes mistakes including governments, so why not Facebook or a third-party developer? Don't forget we are talking about 400m records or more – which is more people than currently live in the US – 307m, so data protection is very much an important subject.

The US congress is also looking at privacy protections on Facebook and other social networks to decide whether more government regulation is necessary.

One suggestion Dr van Heerde had for overcoming the privacy debate, is to have a privacy policy that clearly states that user profile data will be surrendered and degraded over time. He goes on to say that an initial use to secure a transaction or get useful information from a search all relevant details might be stored.

Subsequently details would slowly be swapped for more general information.

In the case of a location-specific search information about a user's exact GPS co-ordinates could be swapped for a street name, then a neighbourhood and then just a city.

Facebook TIP

How to STOP search engines from accessing a user profile and any information visible to *Everyone*:

- Go to *settings*
- Then *privacy*
- Then 'search' and uncheck *Public search results*.

The public version of a Facebook profile that will appear in search results includes your name and photo by default. If the visitor is not logged into Facebook and listed among friends, they will need to become one before they can see your profile.

Final Thoughts

Facebook privacy will be an ongoing issue for privacy advocates (and for Facebook as well as Governments) until something is done which allows users to control what happens to their user profile data. The real problem lays in the control of user profile data not only with Facebook but also with the third-party developers and external marketing agencies and affiliates. Until something is done here, there will always be the risk of your data ending up being shared with multiple companies, sold on to marketing agencies and more importantly data leakage resulting in a user becoming an identity fraud victim.

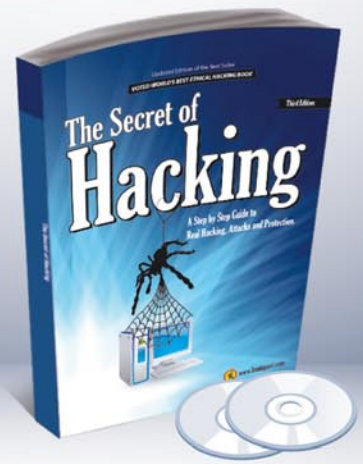
JULIAN EVANS

Julian Evans is an internet security entrepreneur and Managing Director of education and awareness company ID Theft Protect (IDTP). 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.

Order Online at: www.secrethacking.com

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

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



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%**)

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

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

Security Expert Average Salary 1,20000 USD
Source: payscale.com

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

8 BIG 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.thesecretofhacking.com

Now available on Amazon.com

Over 50,000 Sold!

:: Get Suprise Free Gift ::

www.thesecretofhacking.com

LEO IMPACT SECURITY

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

IS YOUR INFORMATION BEING GIVEN AWAY?

- Control who uses your content, what they can do with it, and how long they can use it for
- Stop unauthorized distribution, copying, printing, screen grabbing
- Expire content, and instantly revoke access to information
- Audit document usage, generate statistics and reports

PROTECT IT WITH LockLizard

www.locklizard.com