# Hakin9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

Adobe® PDF Magazine Version

# ID THEFT

## GUARDING AGAINST IDENTITY THEFT

## THE BEST WAY TO LEARN AND APPLY CRYPTOGRAPHY

## ANALYSIS OF A SCAM

## SECURE ENV FOR PT

## KNOWING VOIP – PART III

## BLUETOOTH MICE CAN LEAK YOUR PASSWORDS

## CHOOSING AN IDS/IPS ENGINE

Vol.6 No.3
Issue 03/2011(39) ISSN: 1733-7186

PLUS

IDENTITY PROOF YOUR PERSONAL DATA
BY JULIAN EVANS

## Thinking of advancing your IT Security career?

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

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

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

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

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

### A CEH AND LPT KILLER?

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

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

CEH and LPT refer to *Certified Ethical Hacker* and *Licensed Penetration Tester* respectively, both the gold standards for penetration testing in the industry.

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

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

### REAL WORLD APPROACH USED BY PENTESTERS

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

### HOW TO BECOME A HIGHLY SOUGHT AFTER PENTESTER

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

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

"Absolutely. The training aspect is key. We start with our e-learning slides and videos which explain every aspect of web application, system and network security testing. We then follow up with labs and practical exercises. Instead of a multiple choice certification exam, ours is an actual penetration testing exercise. We are not just interested in testing theoretical knowledge. Candidates are required to conduct their own penetration tests on a given target and submit an actual test report for grading."

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

### IS THIS FOR YOU?

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

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

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

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

HAKIN9 team

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

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

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

**Proofreaders:** Justin Farmer, Michael Munt

**Top Betatesters:** Rebecca Wynn, Bob Folden, Shyaam Sundhar, Steve Hodge, Nick Baronian.

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 Dudzic
*ewa.dudzic@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*



*Dear Readers,*

*People always try to protect their personal or sensitive information from others. However, in today's world – in the era of the Internet- there are numerous options to obtain this data. Looking at the recent attack on Facebook, WikiLeaks scandal, click frauds or Night Dragon operation we can see how often and, in some way, how easy it is to get secret information. Very often these attack become unnoticed for a long time, like it was with Night Dragon -discovered after 2 years. That is why we devote this issue to one of the most commonly seen fraud – identity fraud.*

*Our ID fraud expert, Julian Evans prepared for you a glance at the methods to protect your personla information and prevent the misuse of these data.*

*Gary Miliefsky also touches the topic of identity theft. In his article Guarding Against Identity Theft he shows you the best practices, tools and technologies to protect personally identifiable information.*

*Hopefully, the advice from our experts will trigger a more responsible actions when you will click a strange link or provide your personal information next time..*

*Enjoy your reading*
*Karolina Lesińska*
*Editor-in-Chief*

## REGULARS

# BASICS



# ATTACK



# DEFENSE

## Malware hijacking Facebook user accounts

Facebook is under attack again from the cyber criminal community. Lolbot.Q malware is using Facebook to hijack user's accounts and we've just seen Asprox.N (we do love the names the security vendors give new malware), is a nasty trojan that comes attached to an email as a downloadable file which is targeting Facebook users.

The trojan sends a message that informs you that your Facebook account is being used to spam other Facebook accounts and that your password has been changed.

In order to retrieve the information you have to open the attached file. The attached file is labelled *Facebook_details.exe* which when opened allows the virus to send spam to your various friends.

*Source: ID Theft Protect*

## Overall click fraud on the rise

The number of online advertising campaign clicks that were fake – known as *click fraud* – declined in the fourth quarter of 2010 to 19.1%, compared with 22.3% in the third quarter of 2010. While that's an improvement, overall click fraud levels are still higher than the rate of 15.3% seen just one year ago.

Those findings come from Click Forensics, which tracks the quality of online advertising campaigns by researching who – or what – is clicking on links. To do that, it studies advertising traffic as it flows over a variety of Web sites, including search engines, shopping engines, online publishers, and social networks.

*Source: ID Theft Protect*

## UK government targeted by Zeus botnet

The UK government, fell victim to a cyber attack using the notorious information-stealing Zeus malware in late December, according to foreign secretary William Hague. Speaking at the high-profile Munich Security Conference on Friday, Hague revealed that the attack was part of an international effort to infect systems.

*In late December a spoofed email purporting to be from the White House was sent to a large number of international recipients who were directed to click on a link that then downloaded a variant of Zeus*, he explained.

*The UK government was targeted in this attack and a large number of emails bypassed some of our filters. Our experts were able to clear up the infection, but more sophisticated attacks such as these are becoming more common*.

*Source: ID Theft Protect*

## Waledac botnet cracks 500k email acounts

Security researchers have discovered that a botnet known as *Waledac* has successfully cracked nearly 500,000 email accounts, and is likely to start using them to vastly increase its spam activity. This makes the spam more likely to evade modern filtering techniques, such as IP blacklisting, as the messages will appear to originate from legitimate users.

Researchers from security firm Last Line also found the botnet had details of 124,000 FTP accounts, which can be used to upload files which then redirect users to infected sites. These sites can be used to serve malware, placing the user's machine under the control of Waledac. Waledac is the successor to *Storm*, once one of the largest botnets in the world. Although Waledac is currently far smaller than Storm, given the scale of information at its disposal, this could be set to change.

*Source: ID Theft Protect*

## Zeus and SpyEye combining elements

A new online banking worm combining elements from Zeus and SpyEye appears to be in circulation. The malware has a mechanism which is capable of bypassing the Rapport security software, which is promoted by many European and US banks. The malware allows a hacker to remotely target a victim's PC using Microsoft Remote Desktop Protocol.

Malware developments are nothing new, but cyber criminals appear to be researching using hybrid malware kits. This is a dangerous development for security vendors and end users. Fortunately right now, it appears that very few cyber criminals are using this hybrid malware kit.

*Source: ID Theft Protect*

## Latest from WikiLeaks

The WikiLeaks war is fought on many lines. Internally to the organization: new books authored by former WikiLeaks members are announced every day to reveal their truth and how Assange is a megalomaniac, paranoic *emperor*. Externally, where a few countries are hoping for Assange extradition before the so scary revelations on the banking industry come out.

Daniel Domscheit-Berg is a former member of the organization who has decided to write his truth about WikiLeaks, in the book named *Inside WikiLeaks – My Time with Julian Assange at the World's Most Dangerous Website*. The book reveals how he and a fellow members had hijacked the document submission system in order to avoid about 3500 documents to fall in Assange's hand.

According to Daniel they took material from Assange because *children shouldn't play with guns*.

The book depicts Assange as a megalomaniac and even discusses Assange's sexual preference for *young women*. Due to this and the revelations about the documents seizure, Assange Lawyers have accused Daniel of sabotage and are considering possible actions.

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

## Google to use One-Time-Passwords for Gmail

Google has demonstrated over time to be very serious about Gmail accounts safety, rolling out more and more effective features mitigating the number of stolen email accounts.

One time password are nowadays spread among Internet banking websites where the so called OTP token generates a new password every 30 seconds and adds more security to the username and password pair.

Google approach to the OTP is slightly different. It does not replace the user's login credentials but it adds a further layer of security to it, providing random security passwords through your landline phone, mobile phone or even Skype.

The option can be enabled under Google Accounts Personal Settings and it's named *Using 2-step verification*. A mobile application named Google Authenticator will run on the major smartphones (iPhone, Android, BlackBerry, iPad) to show the one time password in seconds (3 seconds according to tests) .

Another great feature is the possibility of creating ad-hoc accounts for non-web browser applications that need to login to your Google Account. This is very common with mobile phones accessing your Google Reader or your other Google services. Application-specific passwords will shrink the attack surface and increase the control you have over your account.

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

## SQL Injection strikes back

OWASP Top 10 2010 featured SQL Injection at the first place, surpassing XSS after a long time as the most risky web application vulnerability. The same vulnerability that caused eHarmony, one of the biggest online dating websites in the world, to recover from a serious breach.

Company has assured that the main website had not been affected and that only eHarmony Advice website has been breached exposing users logins. Unfortunately, it is well known how users tend to choose the same login for many websites, above all when these websites are under the same umbrella.

Bottom line is most of the login credential used at the minor websites were the same as the ones at main website.

It is also curious how the company stated that they *protect [their] networks with state-of-the-art firewalls, load balancers, SSL and other sophisticated security approaches*, as if firewalls, let alone SSL or load balancers, might mitigate SQL injections.

Security researcher and blogger Krebs has reported that the eHarmony database was on sale on underground forums for $2000. And all happened during the Valentine's days.

Not the best days to get bad publicity for a dating company.

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

## Night Dragon, Chinese target western Oil Companies

Night Dragon operation is the name given to the latest uncovered cyberwarfare operation undertaken by Chinese hackers against western companies. Hackers this time targeted major Oil companies whose names are still secret, stealing *very sensitive* information such as contractors bids and other rated top secret documents.

McAfee team took credit for the discovery of the large scale hack, that at first glance looks less targeted and sophisticated if compared to last year's Operation Aurora, where custom malware and 0-days were in use. This time hackers have managed to infiltrate companies networks through SQL injection vulnerabilities that allowed to further remote control of the vulnerable servers.

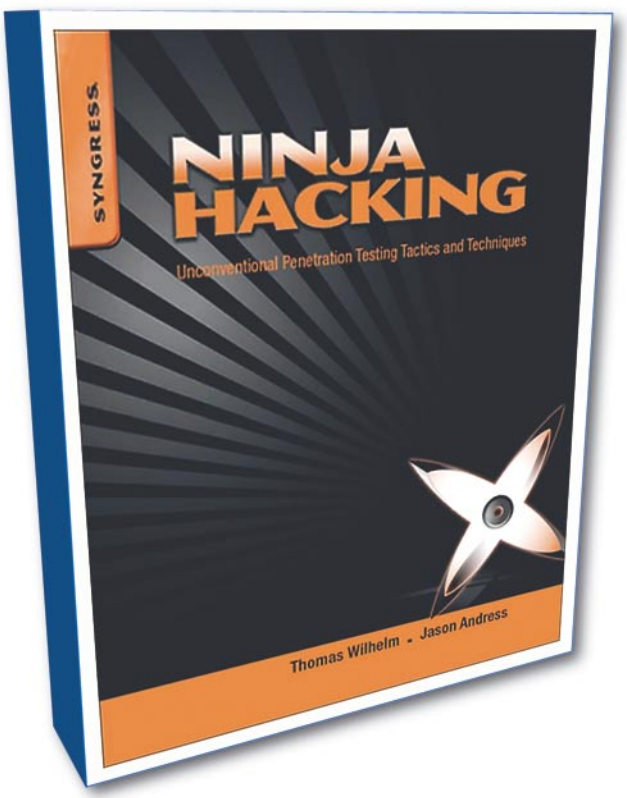
Hackers then used readily available remote administration tools to maintain access to the servers and move towards companies executives workstations.

There is no evidence at now, that the attack was sponsored by the Chinese government, however, it is proven that command and control servers originated from China.

The most scary part of the story, however, is the date of the hack: 2 years ago.

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

# Ninja Hacking:
## Unconventional Penetration Testing Tactics and Techniques




RRP: £30.99
Publisher: Syngress
ISBN-10: 1597495883

This is an unusual title for a book that is being aimed at the Security community and when I first looked at it i thought it was someones attempt to bring some humour into the IT Security arena, then as I started to go through each chapter I started to understand why it lives up to its name.

The first chapter covers the historical history of the Samurai and the Ninja clans. The comparison of these two legendary types of people is actually very applicable to the modern day especially in IT security. System administrators are the Samurai, rigidly sticking to their code and not thinking outside of the box. Whereas the Ninja are the complete opposite, no rigid thinking and using any method that is of use to get to their end goal... a successful mission.

In the third chapter you are shown the importance of laying plans and overall strategy and how the famous book The Art of War also still has applications in today's modern society when preparing for a test.

As you read through the book you will find yourself immersed in a world of historical fact intermingled with up to date technical information on tried and tested techniques in the modern day corporate world. Something I did find interesting is that the different Ninja clans actually had specialisations that they were known for, a bit like IT security people as we all have certain areas that we love to dabble in and absorb all information concerning it.

The chapters are well structured and allow you to jump to specific areas of interest and then allow you to read the other sections as and when required. Each chapter has an excellent summary in my opinion as it goes over in brief detail on what you have learnt and provides good reference links for those of you that wish to explore that particular part of interest and these are not just the technical side of things, you are also given the Ninja side of things as well.

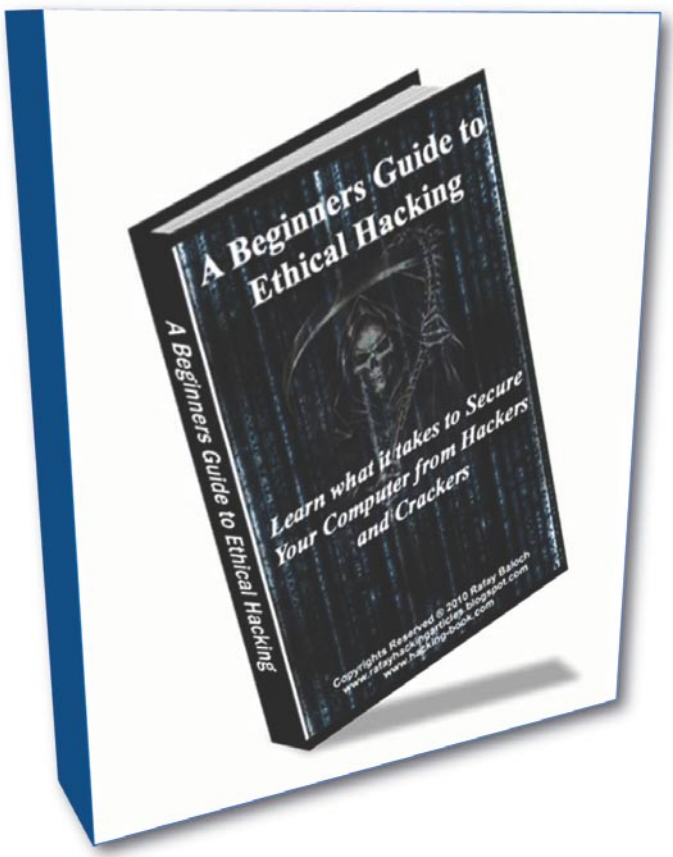
The main emphasis throughout the book is to instruct the reader on how to look at things from a totally different perspective so that the target is unlikely to be prepared for attacks from that vector. Some of the tools and techniques being explained would be more at home in the cyber warfare of small governments than in the toolkit of a corporate penetration tester, but this goes to show that if you learn to think outside of the box and become a true Zukin (Ninja Hacker) you would actually use these type of techniques if you were allowed to.

By going into detail on how each technique should be used through to a successful conclusion you can potentially prepare yourself and your clients on how to defend against these type of attacks, although having some guidance on how to build a policy to prevent this sort of thing would be a whole new book in itself as there is so much to cover.

I thoroughly enjoyed the book and have delved into it on many occasions so far and I am sure I will continue to do so. With the good blend of historical techniques and its modern day application there is something in here for everyone. I always thought that being a Ninja would be cool when I was young, now I can get to become one... without the black pyjamas! :)

**MICHAEL MUNT**

# A Beginners Guide to Ethical Hacking




URL: www.hacking-book.com
Author: Rafay Baloch
Cost: $20

A Beginners Guide to Ethical Hacking is a great resource for people interested in ethical (white-hat) hacking. It is targeted at „beginners", but some „intermediate" users may find value in this book as well.

Some people think that there is nothing ethical about hacking – I think that there is nothing ethical about attacking, but hacking can almost always be done ethically. Hackers are thinkers who seek to determine their limitations through challenging their skills, and this book serves to educate readers about how they can challenge themselves in an ethical way.

The book starts by defining the ethical boundaries of hackers – what the cognoscenti considers *too far*. It then quickly jumps into the realm of programming and how code-writing can be leveraged to achieve the readers' goals. Some might argue that programming or reverse-engineering is *old school*, and the *new school* is all about root, but just like in school, you have to start with the *Introduction to* classes before you can move on to the *Advanced* ones. A solid foundation makes for a sturdy building. Programming doesn't mean learning a coding language from scratch, it means finding the resources you need, when you need them. And this book does just that.

The author then moves on to hacking and cracking of passwords, Microsoft Windows OS, Wi-Fi, and websites. In the website section, the author details the web-application side of hacking, then covers malware and virii. This book not only helps you learn the hacking (or *offense*) side of information security, but also the anti-hacking (or *defense*, or *counter-measures*) side of the coin, detailed in the last chapter. By providing a good balance of both offense and defense, the reader is presented with the tools needed to make accurate and educated decisions regarding not only ethical hacking, but also how to properly secure themselves when doing business online.

Overall, I give this book a thumbs-up!

**SHYAAM SUNDHAR**

# The best way,

## to learn and apply cryptography

The CrypTool project is about making the sometimes daunting subject of cryptography more accessible and easy to understand. It is the most comprehensive cryptography learning tool worldwide.

**What you will learn…**

- Cryptography's place in modern communications
- CrypTool project history
- Available CrypTool versions and some features

**What you should know…**

- Basic understanding of mathematics
- Basic understanding of cryprography
- Using the Internet

We would like to introduce to you CrypTool (CT1) and the two successors, CrypTool 2 (CT2) and JCrypTool (JCT), using in each case a very small extract of their capabilities. Each project is open-source and available for free.

The history of cryptography goes back more than 2000 years; secret communication has always been important – mostly for military and political reasons. The breakthrough of cryptography followed the broadening usage of the Internet. In modern days cryptography has evolved into a mathematically characterized science that most people use everyday without even realizing it. Cryptography is used in our mobile phones, in ATM cards, Pay TV, secure e-mail or online shopping and much more. The four objectives that cryptography is addressing today are confidentiality, authentication, integrity and non-repudiation of digital data. Applications fulfilling these objectives ease our everyday lives, such as secure online banking or non-reproducible digital signatures that verify and protect important documents. This allows us to save time or to further eliminate bureaucracy. Cryptography has become such a vital technology in modern communications and is nevertheless barely known to most people.

Today, cryptography is not only interesting for business and commercial use. Recent political developments like the inspection of laptops or other electronic devices while crossing state borders make cryptography more and more interesting for each and everyone of us that value and cherish our rights of privacy. The technology to ensure privacy is there – it's free and it's secure. On the other hand, it is almost impossible to have a one hundred percent secure computer system due to it's complexity and ever evolving technologies. Cryptography applied correctly, can secure valuable data so it is impossible to be accessed by a third party. This includes yourself if you forget your password. It is important to understand that a lost password may mean to loose valuable data. Cryptography gives us the tools to write secure e-mails and secure our private conversations in social networks or instant messengers, but is rarely used by private persons.

The past has shown that security through obscurity and proprietary cryptography can't really be trusted. Many cryptography researchers agree that only if a cryptographic algorithm is open and available to the cryptographic community it can be analyzed and tested

### MysteryTwister C3 – Level I challenge number sequence

What is the next number in this sequence?
1 – 2 – 4 – 6 – 10 – 12 – 16 – 18 – 22 – 28 – 30 – 36 – 40 – ?
How did you find the solution?
Visit the MTC3 homepage to discuss and for more challenges: *http://www.mysterytwisterc3.org/*

to verify that it is really secure. Otherwise, a proprietary closed algorithm may contain serious flaws that, when exposed later, will require significant costs to eliminate the security risk. An example of such a situation is the MIFARE chip, which was used in millions of devices in the transportation industry before being compromised. Another example is the encryption used in wireless (DECT) phones – now your neighbor may find out when you complain about him.

Because many cryptographic algorithms are open, everyone has access to modern cryptographic technologies and all of us have the chance to learn about them and how to use them correctly.

The goal of the CrypTool project is to help and encourage people to understand cryptography and the underlying technologies. It demonstrates current state-of-the-art cryptographic technologies, as well as cryptanalysis and known attacks against cryptographic systems.

The CrypTool project is also trying to consolidate research and software implementations that has been done by individuals mostly from universities and companies, so others can learn from it. It gives their students a unique opportunity to contribute their code (e.g. software written for a thesis) to a project where it is maintained and used by others around the world rather then just disappearing into the ether.

The CrypTool project started in a large financial institution in 1998. It's original purpose was internal training, to raise awareness about cryptography and encourage developers to use standardized cryptographic libraries instead of self made *looks secure to me* software. It was also used as a reference to confirm other software implementations.

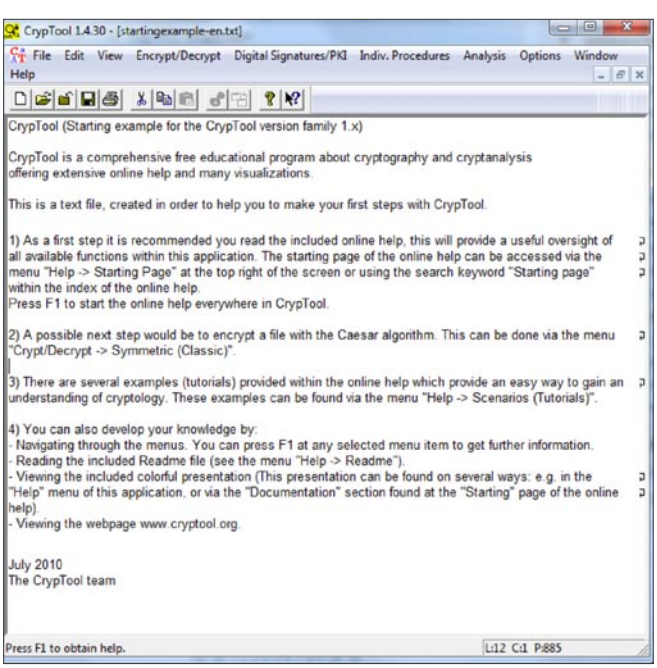



**Figure 1.** *CrypTool 1 – main window*

After the company-internal project ended, and thanks to the efforts of Prof. Bernhard Esslinger and the support of board member Hermann-Josef Lamberti, it was handed over to the Internet community and first released as freeware in the year 2000. In 2003 it became open source hosted by the University of Darmstadt. Since then, the CrypTool project evolved into the most comprehensive cryptography e-learning platform available today. Additionally the CrypTool programs can be used as well proven encryption programs. The project is ever-evolving and has now diversified into three software implementations, each with unique abilities, objectives and technologies behind them. For each project we put the numbers of it's downloaded setup files for 2010 (containing the whole package) into the Tables 1, 2 and 3.

## CrypTool 1

(Requirements: Windows XP or later)

CT1 is currently the most complete and mature CrypTool variant, implementing nearly all state-of-the-art cryptography functions and offering a comprehensive online documentation. CT1 is written in C++ and and runs only under Win32 OS.

Each function implemented is using a simple graphical interface. The online help is understandable without a deep knowledge of cryptography. It also contains a learning tool for number theory, a secure e-

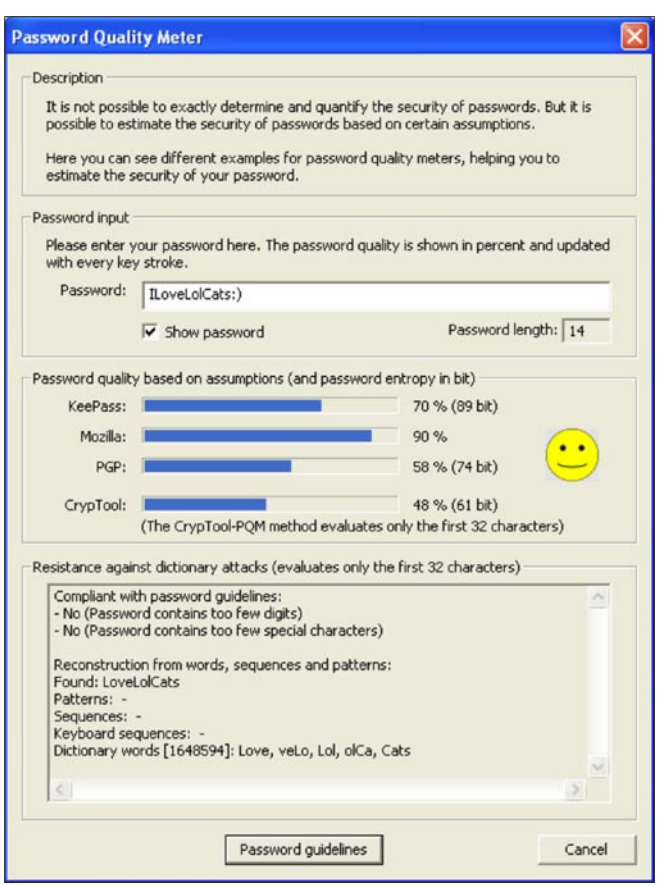



**Figure 2.** *CrypTool 1 – password quality meter*

**Table 1.** *CrypTool 1 – Downloaded around 67000 times in 2010*

| CT1 | |
|---|---|
| Month | Downloads |
| Jan 2010 | 5,496 |
| Feb 2010 | 5,628 |
| Mar 2010 | 6,978 |
| Apr 2010 | 6,128 |
| May 2010 | 6,070 |
| Jun 2010 | 4,550 |
| Jul 2010 | 4,440 |
| Aug 2010 | 4,962 |
| Sep 2010 | 5,122 |
| Oct 2010 | 6,300 |
| Nov 2010 | 5,978 |
| Dec 2010 | 5,297 |
| Sum 2010 | 66,949 |

mail demonstration and visualizations of many different encryption algorithms. CT1 is available in 5 different languages: English, German, Polish, Serbian and Spanish. One feature in CT1 that is useful for almost anyone to try is the *password quality meter* (PQM see Figure 2). There are tons of similar tools that can be found online, but most of them ask you to share your password and send it to a server. Potentially you risk that someone is logging your passwords for later use. The PQM built into CT1 keeps everything locally on your computer and does more than simply counting how many characters you enter and calculate statistics. It also checks the entered passwords against a dictionary (that can also be configured).

You may ask yourself what a password check has to do with cryptography. Even if you use the best encryption algorithms there today, they often rely on a secure (hard to guess/find) password, large prime or random numbers to reach their full potential of being unbreakable.

In 2007, the requirements of the CT1 user community were gathered in a big survey and the preferences of

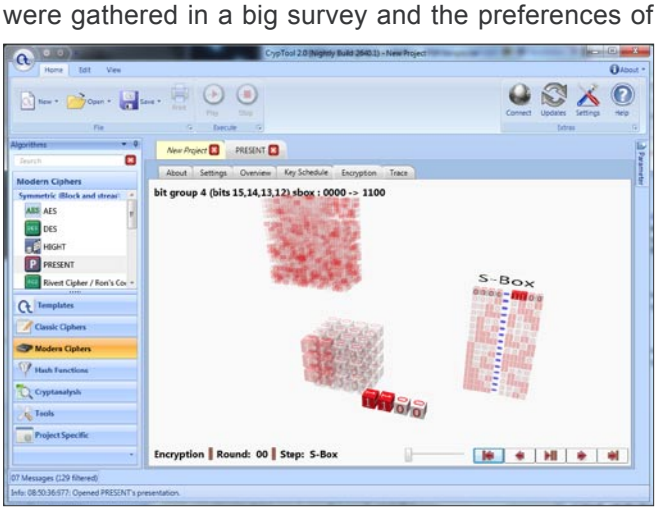



**Figure 3.** *CrypTool 2 – PRESENT cipher visualization with WPF*

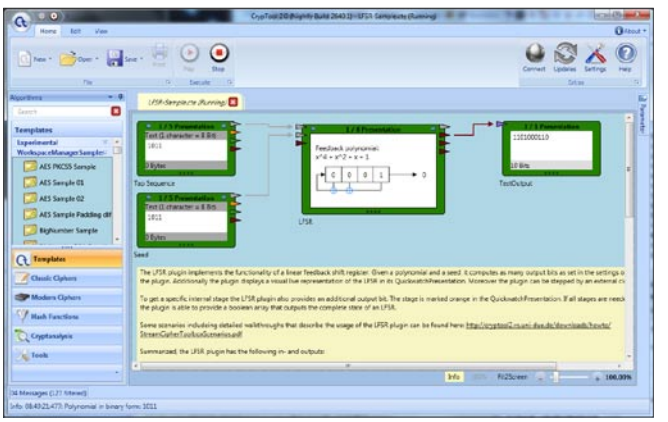


**Figure 4.** *CrypTool 2 – workspace with a linear feedback shift register*

the potential developers were looked at. The result was that the two successors of CT1 both are based on a pure-plugin architecture – one using .NET and C#, and the other using Eclipse, Java and RCP.

## CrypTool 2

(Requirements: Windows XP or later, .NET 4.0)

CT2 is the first modern successor that uses state-of-the-art development techniques and goes a completely new way in didactic learning. CT2 follows the model of visual programming and offers all components using Microsoft's Office 2007 user interface design guideline, providing a consistent and rich user experience. The visual programming model enables the user to combine an extended set of functions instead of being limited to just one function at a time. The vector-oriented GUI design is based on the *Windows Presentation Foundation* (WPF) and gives users the ability to scale the current view at will. It is being hosted by the University of Duisburg. The development is lead by Dr. Arno Wacker.

One very interesting function that has been implemented recently is the support for distributed computing. CT2 is able to establish ad-hoc peer-to-


**Figure 5.** *JCrypTool – main screen*

**Table 2.** *CrypTool 2 – Downloaded around 44 000 times in 2010*

| CT2 | |
|---|---|
| Month | Downloads |
| Dec 2010 | 5,496 |
| Nov 2010 | 5,161 |
| Oct 2010 | 4,377 |
| Sep 2010 | 3,681 |
| Aug 2010 | 2,664 |
| Jul 2010 | 2,480 |
| Jun 2010 | 2,427 |
| May 2010 | 3,231 |
| Apr 2010 | 4,612 |
| Mar 2010 | 3,863 |
| Feb 2010 | 3,492 |
| Jan 2010 | 2,233 |
| Sum 2010 | 43,717 |

peer networks in order to speed up computing intensive tasks. If you are interested in prime numbers, CT2 has a standalone function build in, which dynamically visualizes different attributes and properties about primes. One feature that we would like to introduce to you is CT2's modular design. It offers a toolbox with basic functions on the left side. These functions can be combined in projects to implement cryptographic protocols, build work-flows and test them against different analysis tools. CT2 can execute these workflows step by step. Teachers can use this to prepare tasks for their students, thus better utilizing the limited time available in a class. CT2 is currently available as beta 3 in German and English.

In CT2, more than 100 template-projects are deployed to illustrate how the functions can be used. Figure 4 shows how a pseudo-random number stream can be generated using the LFSR functions.

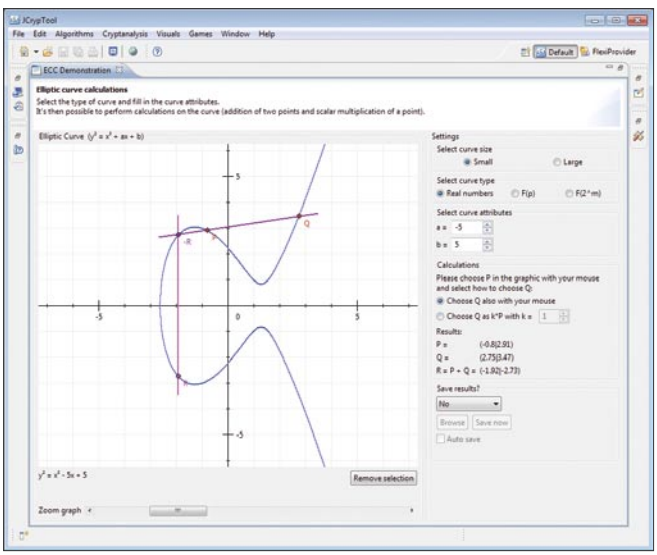



**Figure 6.** *JCrypTool – elliptic curve cryptography visualization*

## On the 'Net

- *http://www.cryptool.org/* – Homepage of the CrypTool project;
- *http://jcryptool.sourceforge.net/JCrypTool* – Developer homepage of JCT;
- *http://www.cryptool2.vs.uni-due.de* – Developer homepage of CT2;
- *http://www.cryptool.org/download/CrypToolPresentation-en.pdf* – Project presentation;
- *http://www.cryptool-online.org/* – Homepage of the browser variant;
- *http://www.mysterytwisterc3.org/* – International crypto cipher challenge MTC3.

## JCrypTool

(Requirements: Java run-time environment 1.6 or later)

JCT is CT2's sibling. It's also a successor of CT1, but with other objectives than CT2. The main requirement that it fulfills is platform independence, so it runs under Windows, Linux as wells as under MacOSX. JCT is also being developed as an open-source project. It is based on the *Eclipse Rich Client Platform* (RCP). It enables students, teachers, developers, and anyone else interested in cryptography to apply and analyze cryptographic algorithms in a modern and easy-to-use application. It uses both BouncyCastle and FlexiProvider as crypto providers. Thanks to FlexiProvider, it offers not only the algorithms which already passed the standardization, but also some current research algorithms mainly from the post quantum research field. JCT Release Candidate 4 (RC4) is currently available in German and English. It is hosted on SourceForge – project lead is Dominik Schadow. JCT's average ranking on SourceForge is in the top 700-3000 (of the 180,000 registered projects).

JCT supports combining algorithms in cascades in order to check and invent new variants of ciphers. One of the currently 15+ visualizations build into JCT is the *elliptic curve cryptography* (ECC) demonstration. ECC is an interesting technology that can use much smaller keys than RSA while being as secure (512 bits with ECC equals the security of a 15,260 bit RSA key).

**Table 3.** *JCrypTool – SourceForge statistics*

| JCT | | | | |
|---|---|---|---|---|
| Month | Rank | Total Pages | Downloads | Proj. WebHits |
| Dec 2010 | 1,479 | 7,519 | 835 | 24,774 |
| Nov 2010 | 1,512 | 16,424 | 922 | 26,884 |
| Oct 2010 | 810 | 25,495 | 905 | 29,268 |
| Sep 2010 | 719 | 9,267 | 745 | 23,518 |
| Aug 2010 | 477 | 5,032 | 558 | 21,103 |
| Jul 2010 | 829 | 2,523 | 689 | 22,960 |
| Jun 2010 | 652 | 3,561 | 784 | 21,673 |
| May 2010 | 1,019 | 7,552 | 867 | 26,155 |
| Apr 2010 | 1,674 | 8,751 | 870 | 26,514 |
| Mar 2010 | 1,664 | 6,960 | 1,002 | 30,185 |
| Feb 2010 | 1,032 | 5,196 | 838 | 26,377 |
| Jan 2010 | 376 | 8,485 | 845 | 26,673 |
| Sum/Avg. | 1,020 | 106,765 | 9,860 | 306,084 |

This is especially interesting for devices that don't have enough storage for large keys, e.g. in wireless sensor networks. The concept behind ECC operations is shown on the screen shot in Figure 6 with real numbers, but you can also use elliptic curves on other sets like the discrete field over p and the field over `2^m`.

## Related projects CT-Online, MTC3 and CT-Mobile

The CrypTool project is a great success story and good example for what open source and cooperative work of different universities and companies can achieve. There are further related projects like *CrypTool-Online*, which offers all ciphers and functions directly in the browser without any local installation. *CrypTool-Mobile* provides this front-end for modern smartphones.

Another related project that just started is the online crypto contest *MysteryTwister C3*, where you can check your cryptography skills against others, get listed in a global hall-of-fame and discuss your attempts in a moderated forum. Currently around 1800 users are registered. The challenges come from different authors, currently from Europe and the US.

## An open call to everyone interested

Cryptography is all around us and I hope that we can encourage more people to learn about this fascinating science. Visit the official CrypTool website and take a look at the project presentation to learn about all the capabilities built into CrypTool. The CrypTool project deeply appreciates any further contribution, constructive criticism and feedback regarding our current releases. You are welcome to join! Currently more than 50 individuals world wide support the project (some of the individuals were willing to offer information about themselves publicly, see the map of contributors: *http://www.cryptool.org/index.php/en/contributors-aboutmenu-36.html*). The project will continue its evolution and hopefully help more people to learn about cryptography.

**ARKADIUS C. LITWINCZUK**

***The author works as an IT-Security consultant and developer in the area of cryptography.***

***Contact the Autor:***

***Arkadius.Litwinczuk@gmail.com***

NETCLARITY
PREEMPTIVE, PROACTIVE PROTECTION

2G INTRUSION DEFENSE SECURED

# The only 2nd Generation NAC solution in the world.


## NACwall 2G:

- Manages the Unmanageable
- Fits any IT budget
- Easy to Deploy & Manage
- Scales to any Network Size
- Agent-less, non-invasive, non-blocking
- EasyNAC Cloud Update Service provides real-time intrusion prevention
- *All in a 1 RU single appliance!*

**Real-time Defense Against Today's Most Devastating Threats**

- Over 80% of Network Security Breaches are Internal
- More than 95% of these Exploit known Vulnerabilities

**Now Available from Partners Worldwide**

**www.netclarity.net**

# Analysis of a Scam

It's all to often that we hear about being scammed on the internet especially when using Craigslist – the popular website for selling and buying almost anything on the internet. But it seems as though the majority of the website has become devoted to messages warning us of the potential for getting scammed.

**What you will learn…**

- How to analyze email scam
- How to trace an email's IP address

**What you should know…**

- Basic internet skills

Recently, I received multiple such emails and one of them was quite believable. Because there is such a high possibility that we will end up dealing with email scams in the course of our internet use, this article is devoted to the analysis and steps necessary to determining whether or not you should even waste your time replying. We will start by analyzing the content of such emails and will end with pointing out just where to look in the email's header in order to determine the originating IP address and subsequent physical location of that IP address.

## Off to the Sp3ll!ng B33

For the most part, the easiest way to tell whether or not an email is worth actually reading is by looking for some obvious details. These details include the email's formatting, spelling, grammatical usage, and punctuation. Figure 1 shows a portion of one of the emails I received.

The text in Figure 1 is peppered with errors of all kinds. Notice that some words are capitalized while others are not at the start of each sentence. Also notice that some of the words are not even the right word or word tense. If you attempt to read it all the way through, the text really doesn't make much sense and you have to ask yourself the question, why would someone be attempting to rent an apartment from another country without going through a broker or real estate agent.

Figure 2 lists the actual information that the *landlord* needs in order to determine our ability to rent the apartment. Yet while the information seems standard, most real estate agents don't ask the question *Are you Married?*

Furthermore, looking at the information we are being asked to supply, it's obvious that the scammer is attempting to indirectly gather identity information. Worse yet, questions six and seven could be used as recovery questions for passwords. This is where it becomes dangerous to reply to these emails, especially if you are new to experiencing scams. For example, if you happened to reply to the email with all your personal information without asking the question *why?*, you have potentially put the security of your identity, usernames, and passwords at risk.

Having looked at an email that resembles an obvious scam, let's now turn our attention to an email that is a little more believable.

Am very glad for your interest in my apartment. This home is extensive with an area and a living room,1 bedroom,bathroom. the cabinets extended in kitchen and the site of the laundry, screen door that slipped of order in the lateral entrance. It includes the guarantee. The home is under 3 years of construction. We have each convenience that you could always wish. We have a friendly community of neighbors.. Portions of activities such as passages, bingo, Clutch of the coffee, divided groups that roll and for every holiday. The restaurants, supermarket, the post office and the warehouses are within distance that walks. But now am in christian mission in a country called west Africa,Nigeria and that's the main reason for which we are looking forward to give out this apartment for rent to a family who can take good care of our house as his own I will like to solicit for your absolute maintenance. and also please fill in the rent details and get back if you are really interested in having our apartment so that i can know all about you.

**Figure 1.** *The story*

In Figure 3 the first indicator is that it's written with better English in that there are not as many glaring errors. The scammer is also attempting to let the reader know why they didn't respond right away.

RENT APPLICATION FORM
1)Your Full Name:
2)Your Full Address & Phone Number:
3)How old are you?:
4)Are you married?:
5)How many people will be living in the house?
6)Do you have a pet?:
7)Do you have a car?:
8)Your Occupation?
9)How many months will you like to leave there?:

**Figure 2.** *The information*

Moving on, Figure 4 shows what could be considered the core of the email. You'll notice that in Figure 4 the author says we can't view the property and gives a potentially valid reason – it having been vandalized in the past. But while this seems like a valid reason, this is just another attempt to indirectly get information about our identity. At the same time, what makes this scam more dangerous – and more believable – is the fact that the author is asking that we use a website to create a credit report. Without having analyzed the website, its difficult to say if its legitimate or not but it's a safe bet to say that the website they recommend is probably not something you should use let alone submit your personal information to.

## Taking Steps To Protect Yourself

Dealing with just the email is not always a clear indication as to whether or not your dealing with a scam, simply because a well designed website is all you need to disguise a phishing attack. But that being the case, there is one piece of information that can be used to make a determination once and for all about what your dealing with, that's the originating IP address of the email. To figure this out, we have to dig deeper into the email and track it down through the email's header information.

```
Email header information
Received:
from zap-server (**********@173.224.219.130 with login)
```

I apologize for not responding to you earlier, I have been extremely busy the last few days!

The good news is that the rental is still available! We had handshake agreement from the first person we showed it to, but now it seems that they changed their mind, so we need to lease it as soon as possible. You were the second one to email me about it.

**Figure 3.** *A more believable approach*

We know you will want to do a walkthrough of the property, but my husband doesn't want me to advertise the address as a measure of safety. Last time we did that without verifying people, the empty property was broken into and vandalized. We don't want that to happen again! You will be responsible for cable, internet, and phone, if you decide to have these services. Just to confirm, we DO allow pets at this property.

The rental term is 12-month lease, but can be switched into a 6-month lease if preferred. We just ask that you give us fair notice if you are moving out.

If you would like to set up an appointment, go to the link below and request the free-copy of your rental report. We use this site for all the properties we manage. Just fill out the form and indicate that you want the free report. The actual scores aren't important to us, it's more of a formality to have it on file, to make sure there are no previous property related issues.

**Figure 4.** *A more believable story*

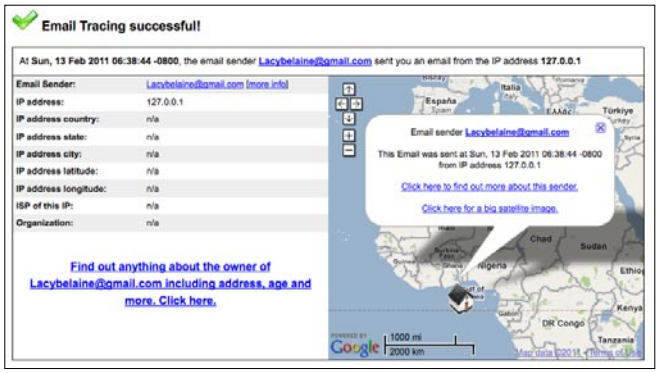



**Figure 5.** *Tracing results*

Above you can see the originating IP address of the email and in order to find this we need to look for the very last IP address which tends to be closest to the bottom of the header information. To do so simply click on *Actions* and then *View Full Header* if you are using Yahoo! Mail or click the down arrow in the upper right hand corner of the email and then *Show original* if using Gmail. Now that we have obtained the originating IP address we can use a website to trace it back its physical location. There are many websites that can be used to do this but for demonstration purposes we have used ip-adress.com.

Figure 5 shows the end result of our trace as well as the originating destination of the IP address.

Looking at the output in Figure 5 we see that the email originated from Western Africa and most likely Nigeria or the like. Knowing this information, we can now make better decisions as to whether or not we should supply our personal information or even bother replying to the email.

## Conclusions

As is usually the case, the best way to prevent such attacks is to avoid giving out your personal details in the first place. It should also be noted that you are almost never asked for personal data through email. If you should be asked for personal information make sure to verify with the person who is asking for your information before filling out any web forms or submitting attached *rental applications*. And if it happens that the email looks plausible, take the time to track down it's originating IP address and check where the email actually came from. Following the analysis we went through as well as the steps to tracing the email's original location will help you avoid having your identity stollen and will add a layer of protection to your personal information.

**RICH HOGGAN**

***Rich Hoggan is currently pursuing a bachelors degree in Computer Science and plans on specializing in information and cyber security. In his spare time, Rich enjoys writing music, photography, and creating visual art with the Processing programming language.***

# Bluetooth Mice Can Leak Your Passwords!

In this article, we will introduce a hidden vulnerability in Bluetooth mouse communication that may leak critical information including passwords.

**What you will learn…**

- A hidden vulnerability leaking your passwords in Bluetooth mouse communication
- How to sniff Bluetooth mouse communication
- What is Mouse Acceleration and how is it implement

**What you should know…**

- Basic knowledge of Bluetooth communication
- Basic knowledge of Operating System
- Basic knowledge of Mouse principle

Bluetooth mouse communication is generally unencrypted. By sniffing raw Bluetooth mouse communication, we are able to reconstruct the mouse trajectory on screen with default mouse acceleration enabled. Therefore, if passwords are typed through a software keyboard, the sniffed mouse movement will expose the passwords. We observed perfect mouse trajectory reconstruction under Linux and near-perfect results under Windows and Mac.

## Introduction

Bluetooth mouse communication is generally unencrypted. It appears that the computer mouse manufacturers, e.g., Logitech, believe that encryption is an overkill. We don't, fortunately! In this article we shall show how someone can learn your password(s) and computer usage patterns with a Bluetooth sniffer even when he/she is 30 meters away, and all this by simply recording your mouse movements and clicks.

The sniffer we use is a commercially available FTS4BT Bluetooth Protocol Analyzer [5]. With this sniffer, we are able to obtain an (unencrypted) hexdump/trace of transmitted raw mouse movements passively. Such a trace, although seemingly barren, has potential of being mined to reveal users' passwords by re-constructing their on-screen mouse pointer movements. Consider a scenario where Alice has typed (actually, clicked) in her banking credentials using a soft keyboard such as the web-based one used by HSBC Bank [6]. If Alice's activity was being sniffed, a trace of her password, essentially a set of on-screen positions of mouse clicks at different locations, may be hidden in the sniffed raw mouse movements. An appropriate mapping of raw movements to relative positions of pointer on-screen may lead to a perfect replication of her password. Thus, we believe wireless communication over Bluetooth/RF mouse must be encrypted. Otherwise, it may lead to significant intrusion of users' privacy.

We have achieved moderate success so far in our attempt to sniff passwords. Specifically, we are able to perfectly predict passwords under a Linux system, while reconstructing partial passwords under Windows and Mac OS X. A major challenge here is the (short) range limitation of Bluetooth communication, since it is impractical to assume that a victim would necessarily be in vicinity. To this end we applied a software defined radio USRP2 with custom antennas that can sniff Bluetooth communication over 30 meters of its range. Figure 1 demonstrates the actual versus predicted movements of a Bluetooth mouse pointer under Linux, Windows and Mac OS systems. It can be clearly observed that we can perfectly predict the real mouse pointer movements in Linux. As we shall discuss later, the imperfections under the later two systems are caused by their special strategies of mapping raw movements to pointer position, i.e., mouse acceleration.

To the best of our knowledge, the aforesaid hidden vulnerability in wireless communication over Bluetooth mise was previously undiscovered; or at the least largely ignored. For example, Logitech in their white paper published on July 7, 2009, mentioned *Since the displacements of a mouse would not give any useful information to a hacker, the mouse reports are not encrypted*. Thus, we intend to sound a warning bell to the industry that unencrypted communication over Bluetooth mouse may be detrimental to users's online privacy and security. We would like to appeal to the Bluetooth/RF mouse manufacturers to encrypt its data and enforce use of more secure device pairing mechanism.

In the rest of this article, we introduce techniques involved in mapping raw movements to pointer position in more details.

## Sniffing Bluetooth Communication

Bluetooth has been designed to divide the 2.4GHz frequency into 79 channels. Two synchronized bluetooth devices will hop through these frequencies for information communication. At each frequency, a device dwells for 625 microseconds, denoted as dwell time. The sequence of frequencies is called hopping sequence. The frequency-hopping scheme may avoid interference from other signals in noisy radio frequency environments.

We initially used a commercial Bluetooth sniffer, which is a USB pluggable device, by Frontline [5]. It outputs the sniffed data in format of hexdump. To perform sniffing, the FTS4BT tool has to glean the agreed frequency hopping sequence between a Master and Slave Bluetooth devices. It can start sniffing only when it synchronizes its clock with the Master device – usually, the mouse. However, to enable sniffing from farther distance, we may use multiple software-defined radio (SDR), GNU Radio and Universal Software Radio Peripheral 2 (USRP2). This has enabled us to sniff Bluetooth communication from a distance of 30 meters. A full sniffer with USRP2 is still under development. We focus on reporting results from the use of Frontline sniffer in this article.

## Raw mouse movements to On-screen pointer movements

To reconstruct on-screen mouse-pointer movements from sniffed raw movements of a mouse, it is necessary to have a precise understanding of implementation of *mouse acceleration*. Mouse acceleration, alternatively termed pointer acceleration, is a feature available with most of the prominent operating systems today, mainly Linux, Windows, and Mac OS X. This feature defines the relationship between the motion of mouse-pointer on the screen and the physical/raw movement(s) of the mouse. It provides users with the ability to effectively navigate screens with high resolution with minimal physical movement of a mouse. In addition, it allows users to exploit pixel-level precision of high-dpi (dots-per-inch) screens. Note that the widely-used term *resolution* is abused to mean pixel-dimensions of a computer screen. Resolution is actually measured in terms of pixels-per-inches or dots-per-inches.

The specifics of mouse acceleration implementation vary for different operating systems (OS); from being simplistic to acutely complex, or having been implemented in application or kernel layers of the OS. In the following sections we provide details of mouse acceleration features for different operating systems.

### Mouse Acceleration in Linux

Mouse acceleration in Linux is simplistic: *If the mouse is reported to have physically moved for over T number of threshold units, then amplify those units separately over X and Y axes by M to obtain corresponding mouse-pointer movement in pixels*, where T, M are integers. It is important to note that T is compared against the manhattan distance of the reported mouse movements. For example, if a mouse reports a movement of 3, 4 then the corresponding pointer movement will be 6, 10 when T = 6 and M = 2 on X and Y axes respectively.

Mouse acceleration in Linux can be easily configured from the Mouse and Keyboard option in the personal Configuratio menu. Alternatively, it can set from Terminal program using following command: `xset m acceleration`

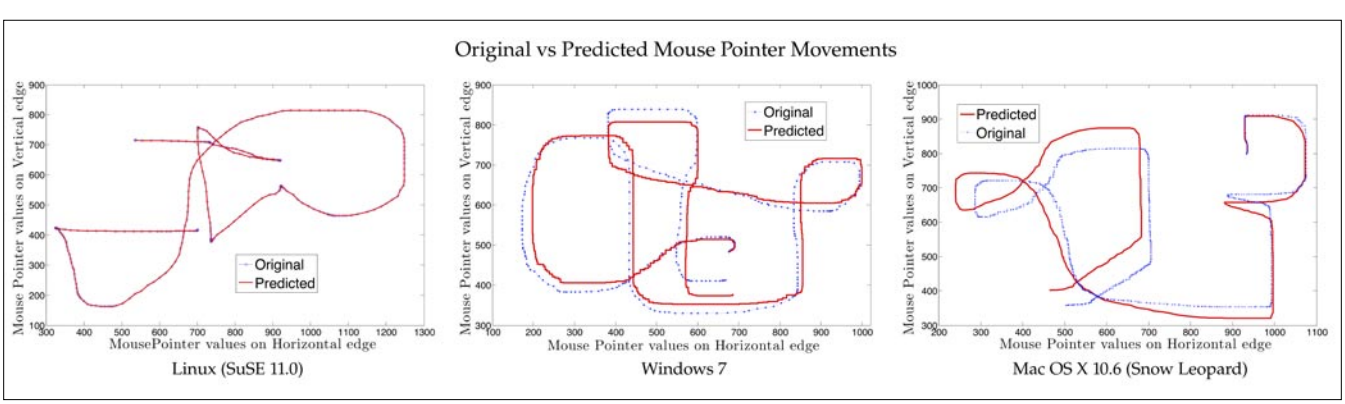



**Figure 1.** *Tracing the path of Mouse Pointer Movements on Linux, Windows and Mac OS systems*

`M threshold T`. Other mouse related configuration setting can be found in *InputDevice* section in `/etc/X11/xorg.conf`.

### How do application receive mouse events in Linux?

Figure 2 shows Linux input driver stack. Applications in Linux, e.g., X11 system, communicate with the devices via nodes or device files located in the `/dev` directory. In specific, `/dev/input/mice` is used for all the attached mice to the system. The mousedev (PS2-emulator) driver creates these device files, while the evdev generic input event driver that facilitates the aforesaid communication. Both these drivers along with the generic input driver and (generic) HID driver for USB input devices, i.e., usbhid form the most important part of *Input Subsytem* or *Input Core*. The format of raw mouse movement data available to all applications is as per the PS/2 standard [3]. In specific, for a 5 button mouse, which is generally used, the Intellimouse extension to PS/2 standard is employed. References – BlueZ [1], Linux Device Drivers [4], Essential Linux Device Drivers [7]. The attached devices in Linux can be accessed in user-space via special called as device file. One can simply use the `cat` command on these file to receive the data transmitted by the device on computer's bus.

### Semantics of Bluetooth raw mouse data

The semantics have been understood by reverse engineering. The hexdump shown here is taken from the Bluetooth Packet Logger tool in Mac OS X. However, these hexdumps have consistent structure for all the sniffer/logger tools. It is important to note here that the discussion below focuses on constructing raw mouse movements and not the on-screen pointer movements from the sniffed Bluetooth data.

Microsoft Bluetooth Mouse 5000

Hexdump – `[ACL RECEIVE]2E 20 0B 00 07 00 41 00 A1 11 00 {01 FE} 00 00`

The fields in curly brackets give the X and Y movement of mouse, respectively. This data is expressed in two's complement form. Thus the corresponding movement will be 1,-2 i.e a unit movement on right and two units in the upward direction.

Logitech V470 – Cordless Laser mouse

Hexdump – `[ACL RECEIVE]2E 20 0C 00 08 00 41 00 A1 02 00 {F3 FF FF} 00 00`

Here three fields in curly brackets are used to calculate mouse movement. Following rules are applied to get the movement: Let the first field be X_raw (F3), second be Y1_raw (FF) and third be Y2_raw (FF). X_mouse and Y_mouse represent raw mouse movements on X and Y axis respectively, in decimal.

### Algorithm to reverse engineer mouse pointer movements from raw data

We now present our algorithm to reconstruct raw mouse movements from the hexdump for Logitech V470 in Figure 3. It must be noted here that the aforesaid reconstruction is much more complex in this case as compared to Microsoft Bluetooth Mouse 5000.

In specific, the hexadecimal values A-F may not necessarily represent the (regular) decimal values 10-15. Whenever A-F do not represent 10-15, we would refer to HASH, a key-value set-associative pairs container.

The Bluetooth HID profile leverages the universal definition of a HID device for the existing class devices [2]. The HID profile describes how to discover a HID class devices feature set and how a Bluetooth enabled device can support HID services using the L2CAP layer. The syntax and semantics of the raw (hex) data initially exchanged between a device and host is called as *descriptor*.

## Discussion

We have also discovered the mouse acceleration strategies under Windows and Mac. They are more complicated than the one under Linux. We designed the corresponding algorithms to reverse engineer mouse pointer movements from raw data for Windows and Mac. From the mouse movement construction results in the figure of *Tracing the path of Mouse Pointer Movements on Linux, Windows and Mac OS system*, we can see that the predicted trajectory under Windows and Mac does not perfectly match the real trajectory. We believe that the small discrepancy here is caused by the strategy of residue calculation in Windows and Mac. In Linux, the mouse event is processed event by event without any residue carrying over from one event to another.

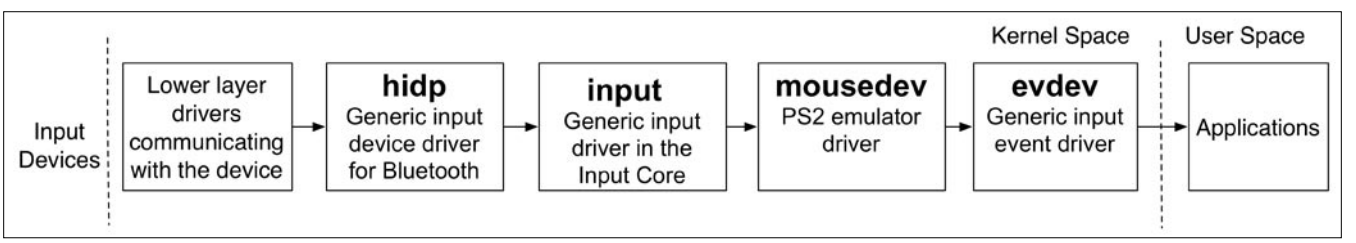



**Figure 2.** *Linux Input Driver Stack*

## On the 'Net


- *http://www.bluez.org/.* Bluez: Official linux bluetooth protocol stack [1].
- *http://www.usb.org/developers/.* Device class definition for human interface devices [2].
- *http://www.computer-engineering.org/ps2mouse/.* Ps/2 mouse interface [3].
- J. Corbet, A. Rubini, and G. Kroah-Hartman. Linux Device Drivers, 3rd Edition. O'Reilly, 2008 [4].
- *http://www.fte.com/products/fts4bt. aspx* Frontline Test Equipment, Inc. FTS4BT bluetooth protocol analyzer and packet sniffer, 2010 [5].
- *http://www.banking.us.hsbc.com/personal/demo/cam/cam demo.htmHSBC.* Security key demo, 2010 [6].
- S. Venkateswaran. Essential Linux Device Drivers. Prentice Hall, 2008 [7].


In Windows and Mac, however, the mouse acceleration algorithms may calculate the mouse position from a batch of mouse events (with residue from a previous event taken into account in the processing of the next one) – this leads to a small error on our trajectory prediction because, as a third-party, we have no knowledge as of which events are processed together in the same batch. We leave the rigid verification of this reasoning as part of the future work.

## Conclusion and Future Work

In this article, we delivered a clear message about the existing vulnerability in Bluetooth mouse communication and how it can be exploited by a malicious adversary. In particular, our research showed:

- Hidden and largely ignored, but detrimental, vulnerability in unencrypted Bluetooth mouse communication. It leaks user passwords in the air! The attacker just needs passive sniffing.
- The indirect, but well-pronounced, presence of mouse pointer movements in the raw hexdump of Bluetooth mouse communication.
- The concept of *mouse/pointer acceleration* and how it can be used to reconstruct the screen coordinates of the mouse pointer under three different OSes. We believe that all unencrypted RF mice are subject to the proposed attack.

The current state of work demands that the initial position of pointer be known. As ongoing and future work, we have been investigating if a starting position of the pointer can be (near perfectly) estimated based on pattern of movements, e.g., a popular Windows operation of clicking the Start Button and then scrolling up vertically to select an application. If a perfect prediction of initial pointer position is not possible then we intend to generate a set of most probable key sequences based on the distance between successive key presses. In addition, we intend to perform testing with other popular Bluetooth mice.

**Algorithm 1** Reverse Engineering the Mouse Movements from Raw Hexdump for (*Logitech V470*)

**Require:** HASH = ( F → 16, E → 32, D → 48, C → 64, B → 80, A → 96);

1: **if** ($X_{raw}$ >= 127 in decimal) # left movement **then**
2: $X_{mouse}$ = HASH[first digit of $X_{raw}$] - second digit of $X_{raw}$;
3: **else**
4: $X_{mouse}$ == $X_{raw}$; #right movement
5: **end if**
6: **if** (first digit of $Y2_{raw}$ == F) # top movement **then**
7: $Y_{mouse}$ = HASH[second digit of $Y2_{raw}$] - first digit of $Y1_{raw}$;
8: **else**
9: # down movement
10: **if** ($Y2_{raw}$ == 00) **then**
11: $Y_{mouse}$ = first digit of $Y1_{raw}$;
12: **else**
13: $Y_{mouse}$ = decimal result of concatenating second digit of $Y2_{raw}$ with first digit of $Y1_{raw}$;
14: **end if**
15: **end if**

**Figure 3.** *Algorithm to reverse engineer mouse pointer movements from raw data*


### ANIKET PINGLEY

***Aniket Pingley is a PhD student in the Department of Computer Science at the George Washington University in Washington DC. He received Bachelors and Masters degree in Computer Science from Nagpur University, India in 2005 and from the University of Texas at Arlington in 2008, respectively. His research interests include privacy and security in wireless networks.***

### XIAN PAN

***Xian Pan is a PhD student in the Department of Computer Science at University of Massachusetts Lowell. Her research area is security and applied cryptography, including security and privacy issues in bluetooth networking.***

### NAN ZHANG

***Dr. Nan Zhang is an Assistant Professor of Computer Science at the George Washington University, Washington, DC, USA. He received the B.S. degree from Peking University in 2001 and the Ph.D. degree from Texas A&M University in 2006, both in computer science. His current research interests span security and privacy issues in databases, data mining, and computer networks, including privacy and anonymity in data collection, publishing, and sharing, privacy-preserving data mining, and wireless network security and privacy.***

### XINWEN FU

***Dr. Xinwen Fu is an assistant professor in the Department of Computer Science, University of Massachusetts Lowell. He received B.S. (1995) and M.S. (1998) in Electrical Engineering from Xi'an Jiaotong University, China and University of Science and Technology of China respectively. He obtained Ph.D. (2005) in Computer Engineering from Texas A&M University. Dr. Fu's current research interests are in network security and privacy, network forensics, computer forensics, and information assurance.***

# Secure Env for PT

Security awareness guideline about establishing a controlled environment to conduct technical security testing and assessments in order to protect companies and professionals from possible legal implications.

### What you will learn…

- security awareness, mitigating impact and implication of security tests in terms of possible trade secrets, privacy concerns and government classified information leakage;
- guide line to setup a secure environment when conducting security tests;

### What you should know…

- Goals of a security tests, including Vulnerability Assessment and Penetration Test;
- Basics of *nix and networking;

I think it is good to start this paper by introducing a word: *ethics*. A quick Internet search (Google Search: *define: ethical*) reveals its meaning: conforming to accepted standard of social or professional behavior; a matter of moral principles that govern a person's behavior or the conducting of an activity. In the world of ICT, when specifically talking about security it's quite common to hear an expression like *Ethical Hacking*. As more and more companies needs to be aware of security, security tests had been introduced. This kind of service is well described as *analysis conducted as a potential attacker, by means of security vulnerabilities exploitation; usually done by a vulnerability assessment and penetration test*. In this kind of job the most needed people are technicians called *Penetration Testers*, *Ethical Hackers*, *Analysts*, *Assessors* etc. Let's call this role from now on a PenTester. Why *Ethics* is such an important point is strictly linked to confidentiality and privacy. Let's imagine the impact of the test results performed against the company being made publicly available. Figure 1 shows the classification of confidentiality according to NSTISSC (*National Security Telecommunications and Information Systems Security Committee*).

By the same awareness, for a professional PenTester, there is always the impact of being unfairly accused of stealing information, abusing system access, etc., while conducting security tests. Either way, the trust relationship between tester and customer must be addressed in some way. My research tries to address this aspect, so that working within what I call a *controlled environment for security tests* either companies and penetration testers can be sure that this critical and necessary *mutual trust* cannot (or at least is almost impossible) be circumvented.

## Guideline

First of all, I have started my research reading the *Technical Guide to Information Security Testing and Assessment* by the *National Institute of Standards and Technology* (NIST). This guide discusses if *it is beneficial to gain an external perspective on the organization's security posture by giving outsiders access to the organization's systems which can introduce additional risk*. Of course, the same problem arises when giving the internal team access to the organization's systems

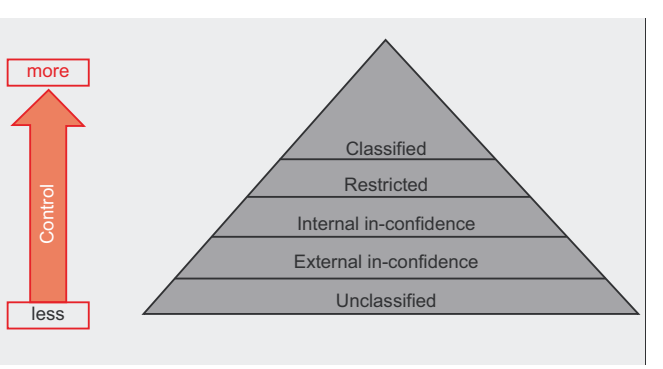



**Figure 1.** *nist*

while conducting any security tests. Either way, the trust relationship between tester and customer must be addressed in some way. While I strongly recommend this reading I will jump right to the Data Collection section of the guide, pointing the focus to the following:

*Assessor Activities. Assessors should keep a log that includes assessment system information and a step-by-step record of their activities. This provides an audit trail, and allows the organization to distinguish between the actions of assessors and true adversaries. The activity log can also be useful in developing the assessment results report.*

There is also an additional consideration related to big companies, where there are usually tasks handled by the SOC (*Security Operation Center*), which is a division playing the role of the controller that interacts with the penetration testing team. Basically, they are able to track and record the penetration testing activity to distinguish between the actions of PenTesters and true adversaries. However, this approach leaves room for the following discussions:

- what are the do's and don'ts when conducting security tests for a company without a SOC division?
- how can the PenTester and/or company be sure that collected data, if in place, has not been tampered with, hence trustable?
- what are the do's and don'ts, if PenTesters are called to perform a *covert penetration testing* oriented to audit the SOC Incident Handling process, hence with a potential missing of data collection?

Continuing the NIST guide reading, it is reported the following:

*Use of a keystroke logger on an assessor's system can create a step-by-step log of many tester actions, although it will not capture mouse clicks and certain other actions. For automated tools, assessors can maintain the audit logs from each tool that is used. While assessors may choose to dump the output of the keystroke logger or tool audit log onto a separate system to create a centralized storage and auditing capability, an alternate manual approach is an activities log that tracks each command executed by assessors on the network. This approach is time-consuming for the assessors, and leaves room for error. If an activities log is used, it should include at a minimum the following information: date and time, assessor's name, assessment system identifier (i.e., IP or MAC), target system identifier (i.e., IP or MAC), tool used, command executed, and comments.*

These considerations lead to the necessity to have a controlled environment for technical security tests and assessments, in order to be sure that every precaution has been adopted. Surely, all performed tests are to be collected by the team and/or controllers throughout the assessment. Also, it's important to handle the data appropriately considering it could be classified as sensitive. This also comes in handy when there is the necessity to prove that queries against the databases had been done with a *LIMIT* and that a complete database dump had not been done unsure of what this means or the relevance. This controlled environment is also useful if a PenTester is unfairly accused of being the origin of a denial of services attack that triggered loss of revenue, having the possibility to prove the opposite.

## Design Consideration

The possible legal impact of this discussion makes me think about forensics methodology, which means the solution put in place must be forensically accepted. The general idea up to now is to do the following:

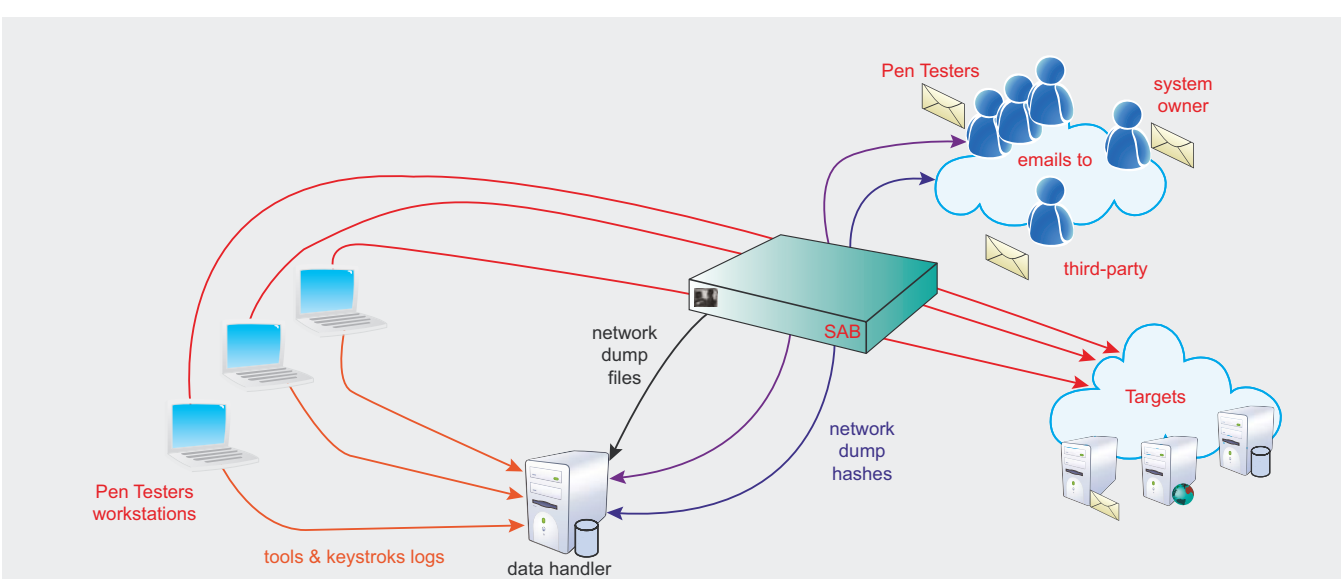



**Figure 2.** *Black box flow*

- provide the PenTester with a notebook equipped with all necessary tools, including a keystroke logger. Configure all tools to send logs to a third system with the designated role of data handler (log collector). Include a HIPS such that the workstation is also scrutinized if being used as bridge to the targets;
- insert a *black box* between PenTester and targets, in order to record and hash all traffic routinely, this is to ensure that it is at least as trustworthy as who created the dump and the hashes;
- configure the *black box* to check out if systems not in scope are accessed as error or intentionally;
- continuously send the computed hashes by email to PenTester, system owner, and the third-party not directly involved into the security tests.

The flows involved into the process, are illustrated in Figure 2.

## Implementation

It is time now to jump a little into the details of this controlled environment, defining how to implement this tailored *black box*. First of all, it must be compact such that transportation is not a problem and have at least four ethernet interfaces. Of course you can choose whatever you want as operating system (OpenBSD might be a good choice). Two ethernet network interfaces are setup in bridge mode (Layer 2, one interface is connected to PenTesters network, the other goes to the targets networks) to capture all network traffic, by means of a *tcpdump* session. The generated dump file needs to be hashed as stated before; a third network interface is setup with a public IP address such that the black box can communicate with the outside world. The fourth interface is utilized to access the box for management purposes and to let the box to communicate with the data handler system. The overall schema of the proposed black box is showed in Figure 3.

What's highlighted here is the way the dump file is hashed while being generated; this is the focal point and where a difference resides comparing this way to go against a simple and generic dump capture done during a security test. Another session is limited to alert and/or drop packets in case of *out of scope* traffic.

## Tools and some Tests

### Dump and hashes sessions

In order to capture the traffic and perform hashing, two tools are necessary. The first tool is the well-known *tcpdump*; the other is perhaps more well known to the forensic community and is *dcfldd* (*http://dcfldd.sourceforge.net*). This tool is an enhanced version of *dd* (to copy the standard input to the standard output) with features useful for forensics and security, such as non-repudiation. For instance, hashing the dump as it is being captured helps to ensure data integrity. As soon as network traffic is captured two text files (*md5.txt* and *sha256.txt*) are generated and continuously updated with the computed hashes of the at-that-time pcap blocks of bytes, these files are sent continuously (let's say every 10 minutes) to the third party email addressees. The receivers of these

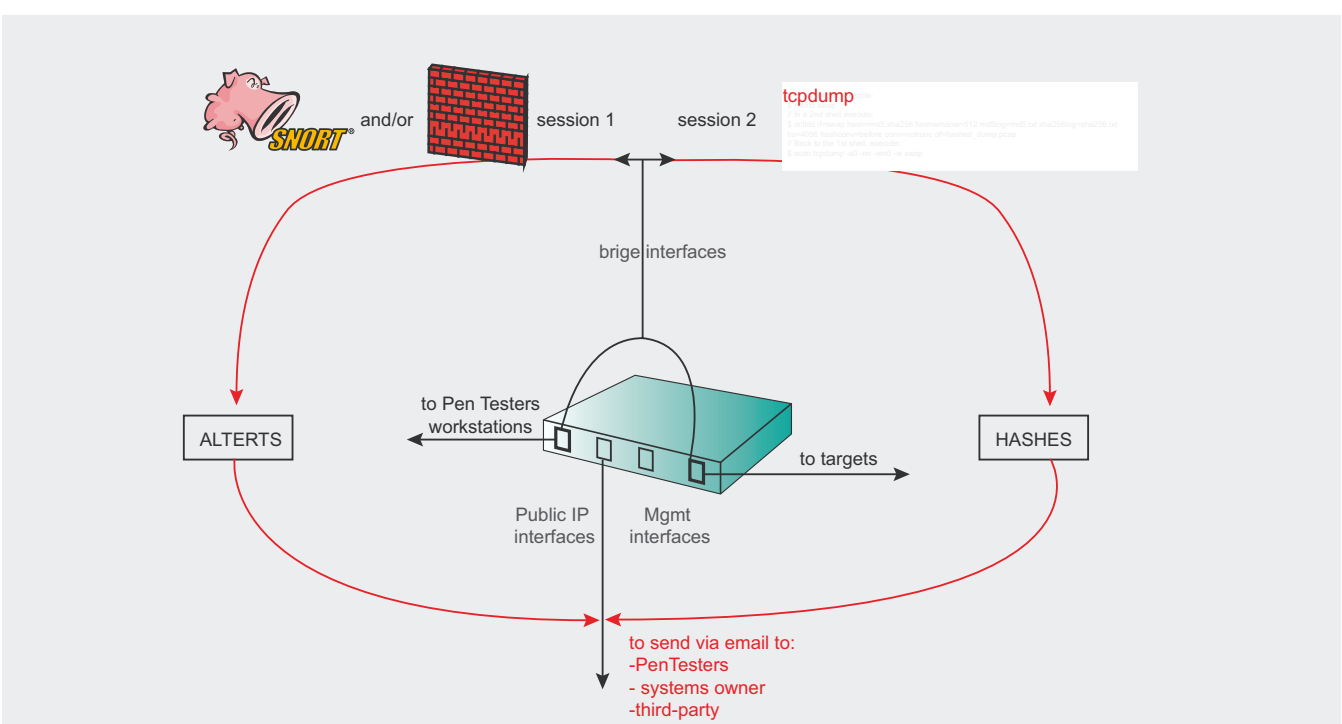



**Figure 3.** *ni*

files will have the hashes of each block of the pcap file (*hashwindow* parameter), and the last email will contain all the blocks of hashes along with the total hash of the final pcap. Basically in this way nobody can carve out packets related to an *attack* or *unethical behaviour*. If this were possible, all the computed hashes after that carving would not be valid. A way to illegally bypass these controls in place would be next to impossible, because there would be several things to bypass including: the PenTester's workstation, applications, and keystroke logging which is useful in case an encrypted tunnel is being used between the PenTester(s) and target(s) (TLS, SSL). Even still, a black box bypass would raise suspicions from email recipients who would be warned because of altered email timelines and hashes. Anyway, it is important that the following checks, all together, are in place:

- the bridge feature of the black box, works if and only if the *tcpdump* session is working properly otherwise traffic is not allowed to reach the targets;
- the bridge feature of the black box, works if and only if the box is able to send email, otherwise traffic is not allowed to reach the targets. (Emails might be sent with the subject line: *Computed Hashes security tests code #XXXX*);
- logs generated by the black box regarding networks and running processes are sent via email separately. (Emails might be sent with the subject line: *System logs security tests code #XXXX)*.

Of course, the overall obviousness that everything has been done correctly is achieved by meshing all of the countermeasures put in place. Hence, even if a problem arises on the black box in terms of a malfunctioning of the applications logs, the keystroke logs, emails etc. there should still be enough to build a timeline and prove the correctness of what actions did or did not occur. Now let's do a quick example and let's suppose we decided to generate hashes and send an email every 512 bytes of captured data. Based on this example, 3 hashes have been computed

**Listing 1.** *tcpdump and dcfldd steps*

```
// In a 1st shell, execute:
$ mkfifo swap

// In a 2nd shell execute:
$ dcfldd if=swap hash=md5,sha256 hashwindow=512 md5log=md5.txt sha256log=sha256.txt bs=4096 hashconv=before
                    conv=notrunc of=hashed_dump.pcap

// Back to the 1st shell, execute:
$ sudo tcpdump -s0 -nn -ien0 -w swap

// When the job is done Ctrl-C the tcpdump session, so that you have available
// the hashes files:
$ cat md5.txt
0 - 512: a03a9953daf04749fb2344d2caf67a27
512 - 1024: e2de92733868fc48236abf7c93c91e40
1024 - 1336: 612b3c6d3ab55ce0fa83c54233ff1f93
Total (md5): 2258dcb5b95436cf2c245ef52083fbd0
$ cat sha256.txt
0 - 512: df7d0ff6143f5e64d696921ed30cdbc35ea84c3a6531d74ad69710a817872d52
512 - 1024: bef6eba7bfa4ceca8873cb064134570317ed25df9013612e59815c918497bcfa
1024 - 1336: b731c4e321f0b2b442bf1e1a8e748eccab56cf4fd0dbc7bbbbfb7860ea361e30
Total (sha256): f6b4e82252780c40bfc645a3a887d5e74f5919dd7c0806ebc45e3710b745c9ec

// Of course you can verify the matching of hashes:
$ openssl dgst -sha256 hashed_dump.pcap
SHA256(hashed_dump.pcap)= f6b4e82252780c40bfc645a3a887d5e74f5919dd7c0806ebc45e3710b745c9ec
$ openssl md5 hashed_dump.pcap
MD5(hashed_dump.pcap)= 2258dcb5b95436cf2c245ef52083fbd0
```

**Listing 2.** *Snort session*

```
# PT sensor - rules to be used with '-o' flag to Snort
# Define variables
var ANALYSTS [192.168.10.5, 192.168.10.6]
var TARGETS  [156.54.23.25, 156.54.23.26]

# Start with pass rules
pass tcp $ANALYSTS any: <> $TARGETS any

# Catch-all rule, recording the session

var SESSION_TTL 60 # How long do we keep the session for?

alert tcp $ANALYSTS any -> !$TARGETS any ( msg: "Out of scope - disallowed outgoing traffic" tag: session,
                    $SESSION_TTL, seconds; \ rev:1; )
```

**Listing 3.** *Firewall session*

```
# ipfw -q add allow all from $ANALISTS to $TARGETS via bridge0


// don't forget to send firewall logs, at least, to the data handler
// (/etc/syslog.conf)

security.*            @192.168.20.20:32350
```

hence, the addressee will receive three emails; the last one will include all the hashes of the bytes blocks and the total hash of the overall pcap file; basically, the same content of the output given from commands *cat md5.txt* and *cat sha256.txt* at the end of the recorded traffic. Now if someone had performed something bad during the test, let's say between bytes 512 and 1024, nothing could be done to cloak it. Carving out packets from byte 512 to 1024 will compromise all subsequent computed hashes already received by the addressee, so game over. On the companion website *www.securityindepth.org* you will find a more detailed description of this example. The dump steps are illustrated in Listing 1.

### Out of scope sessions

In order to be warned of an out of scope session, accidental or not, there are two possibilities: first, a simple alerting mechanism that could be detected with a Snort session. Basically, there is no filtering at the IP level. The following configuration is a minimal ruleset which means I am ignoring a number of Snort features, such as plugins and signature sets. Basically, the session isn't performing any Intrusion Detection, instead it is just alerting us of any out-of-scope traffic. Listing 2 shows a possible snort configuration.

The second possibility is by means of a firewall, hence filtering at IP level. Configure a firewall delimiting the perimeter, dropping any disallowed outgoing connection. Listing 3 shows a possible ipfw firewall configuration.

## Conclusion

I hope the reader found this discussion interesting. Of course all the considerations done, are just in the early stages. I would really appreciate any feedback in term of advis, tips, or simply additional considerations. I still have a couple of points under discussion such as data retention and sensitivity. Basically, the dump of the traffic might contain sensitive information and needs to be managed appropriately. Still in case of a wireless penetration test, the black box should be positioned between the AP and the internal network. A web application would be of great help, such that all necessary steps might be handled via browser, (e.g., set the targets lists, email addressees, hashwindows, logging parameters, etc.).

**ANTONIO MEROLA**
***www.antoniomerola.info***


# EMERGING THREATS PRO

*the* comprehensive ruleset

emergingthreatspro.com

## *The* complete ruleset, focused on malware just like you are.

- **Complete Ruleset**
- **The Best Malware Coverage**
- **Suricata and Snort Versions**
- **Cost Effective**
- **Site Licensing**
- **Customization**

**The Emerging Threats Pro is a complete, stand-alone ruleset** that draws upon numerous sources of intelligence as well as the EmergingThreats.net open source project to provide up to the minute rules for your network. The rules are updated daily as the threats are identified. No delays, no obfuscated rules.

**Emerging Threats Pro will detect more malicious content in your network.** Every network has some and most IDS rulesets don't cover it well. The research required to keep up to date on the bots and command and control channels in use is massive. But we've been doing that for ten years now...we've got you covered.

**Snort and Suricata versions.** We're not tied to any one platform or engine, so we don't have to make the choice not to cover a threat to avoid making a platform perform poorly. We know you can manage your sensors, so we let you make the decision as to which threats are most important.

**Customized Rulesets.** Every network is different, and for most organizations all the coverage they need can be found in the Pro ruleset. But for others, the threats they face are very specific and require custom rules to be developed specifically to meet those needs. The in-house Pro research team specializes in creating custom rulesets and working with clients to create optimum network security.

**We offer site licensing discounts for larger sensor networks.** We know you need a predictable cost per year and nobody wants to spend time counting sensors. Let us know about how many sensors you have and we will work out a competitive price you can rely on.

## If you need comprehensive coverage for the vulnerabilities and malware that threaten your network then Emerging Threats Pro is the ruleset for you.

| | Emerging Threats | Emerging Threats Pro | The Other Guys |
|---|---|---|---|
| Suricata Support | YES | YES | — |
| Snort 2.4 to Curretnt Sutpport | YES | YES | — |
| Serious About Malware | YES | YES | — |
| CnC/Data Exfiltration Focus | YES | YES | — |
| Community Intel/Support | YES | YES | — |
| Hardware/Platform Neutral | YES | YES | — |
| Load Rated Rulesets | YES | YES | — |
| Complete Major Vuln Coverage | — | YES | YES |
| Known Bad IP Lists | — | YES | — |
| IP Reputation Support | — | YES | — |
| Full Time Research Team | — | YES | YES |
| Research Partnerships | — | YES | YES |
| 24x7 Email Support | — | YES | — |
| 24x7 Phone Support | — | YES | — |
| Custom Rulesets | — | YES | — |
| Other Formats | — | YES | — |
| Site Licensing | — | YES | YES |

emergingthreatspro.com • 765-807-8630

# Knowing VoIP

## Part III

In previous chapters we have talked about the marvelous world of VoIP, what it allows us to do, accomplish and so on. Now, let's focus on the dangers that we need to be aware of and the countermeasure as well.

**What you will learn…**
- Ways VoIP are weak
- Securing VoIP networks

**What you should know…**
- Knowing VoIP part I
- Knowing VoIP part II

There is a famous saying that I would like to reference here: *If you know the enemy and know yourself you need not fear the results of a hundred battles.* (Sun Tzu in the Art of War)

### Ways VoIP are weak

The security risks of VoIP deployments are very broad. To ensure the best possible protection against current and emerging threats to this technology, companies must understand that risk exists and auditing of current security practices to address vulnerabilities that could allow the system to be exploited is a must. The following is a summary of the current major threats to VoIP deployments.

### Phone Fraud

Crafty hackers can get into a business VoIP network to carry out various nefarious activities, including: attacking the company's system to make free phone calls, infecting the network with viruses, and steal sensitive company information (i.e., billing information). This means all personal and delicate information are unprotected. Despite the lack of authentication in an IP-based network, you can assign access privileges on specific phone lines. However, it is easy for an individual line to be kidnapped and to make calls as that person or to obtain access to a line with authority or duties on the main system without proper authentication of end users. The potential risk associated with any of these situations can lead to damage of reputation, legal implications, or simply be of valuable information to someone.

### Theft of bandwidth

There are many ways in which attackers can impact the corporate bandwidth by exploiting the VoIP network. Many of these can have catastrophic consequences for the overall operations. Attackers can launch internal *denial of service* (DoS) attacks that have different impacts on the bandwidth of network. For example, a denial of service attack against the IP network can point specifically to the voice network, flooding the system with calls, or you can direct traffic affecting the quality of service to legitimate users.

### Limited Encryption

In a VoIP system, calls are standard open text, making it easier for a nefarious individual to intercept call setup and content of information to get, the important information in a given conversation. It is important that organizations find ways to mitigate this risk with a high-security encryption, especially for certain telephone lines during which confidential information is exchanged (i.e. conversations between the CEO and CFO).

As you already know, nothing in life is completely secure, especially electronic devices. This simple fact means that there are many more ways that VoIP is vulnerable either due to lack of knowledge, processes, technology, etc.

**Table 1.** *VoIP & Telecom Abbreviations*

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

## Securing VoIP networks

Most organizations have developed best security practices and policies, but these policies (often) do not cover the protection of VoIP network. Because there are specific issues to be addressed to ensure adequate protection for VoIP, companies should also conduct a risk audit, which will provide the information necessary to secure the VoIP network.

Today, there is an excellent guide available to CSOs and CISOs of standards bodies (ANSI, 3GPP, ETSI, ISO), industry associations (VoIP Security Alliance) and Government agencies (NIST) on how to define and enforce current practices in security to support VoIP and other session types (instant messaging, video) in a company. In many cases, best practices and processes may be working, and additional investments can be as simple as extending the existing corporate security policy. Additionally, based on the vulnerability assessment results of the VoIP network, this could mean a change to the company's network infrastructure (i.e., switches, routers, firewalls, etc.). Once a policy is created or updated and the associated risks are identified, there are several routes for information security managers to take in order to achieve their goal.

## What are the options?

As in the world of data, VoIP security can be achieved either through internal sources or managed through outsourcing. Carriers are beginning to offer customers of all sizes the option of outsourcing the supply, deployment, and monitoring of VoIP equipment. Often this is simply a question of scope, cost, and resource constraints by the customer.

It's important that companies that manage the internal security to maintain a layered approach (defense-in-depth) if extending the existing infrastructure. The first component often deployed is a certain element of next generation IP, such as a switch in the network border. The border switch is the evolution of session border control due to integration of security, call control, support media, scalability, and performance.

The border switch provides the enterprise with its first line of defense on the perimeter. These elements must not only defend the main corporate network from VoIP intrusions, but also provide policy-based control over VoIP sessions, basic signaling protocol (SIP, H323, SIP-I), QoS (quality of service) for bandwidth management of media streams and advanced communication services such as audio codec transcoding and support FAX.

The role of boundary switch becomes even more important as companies with multiple locations are more vulnerable to denial of service through interconnection via the public Internet to carry company VoIP traffic both internally and externally instead of dedicated connections. This display can be used to protect the VoIP network, similar to solutions used to secure Web server farms and data base systems to DoS attacks.

As one seeks to protect the network from the inside out, it is important to recognize that while IP-based VoIP network elements such as delivery systems, billing systems, SIP servers and IP PBX share common vulnerabilities with non-VoIP counterparts. This is because these systems are based on elements such as operating systems commodity (Solaris, Linux, Windows) running on general purpose computers. COTS (Common Off The Shelf) components may use other protocols besides TCP/IP that equipment manufacturers embed within their proprietary platforms. As such, vulnerabilities may exist, but protection against intrusions and vulnerabilities can be mitigated by proper curing, as with their non-VoIP counterparts are provided today.

In addition to these traditional weaknesses, VoIP-specific vulnerabilities such as SIP, may also exist. These threats can be mitigated by many of the same techniques as the overall protection that is used on the bottom layer. Given the nature of SIP sessions an organization needs a class of device aware of more than what a firewall or ACL can provide on the edge; if not already in place, the company should consider an IDS/IPS.

Another technique that companies must take into account is the placement of VoIP phones on separate VLAN's to guarantee protection against unauthorized devices that can hear the internal communication and lead to theft or fraud. For added protection against these violations, incoming and outgoing VoIP traffic should be isolated so that it can easily be controlled by a call handler. Companies should also implement encryption technology to protect calls that travel over public networks to prevent fraudulent use of VoIP, including exploitation and theft of authentication.

As with other technologies, it is crucial to understand that the implementation of enterprise VoIP security lies in the company's ability to protect its entire network, not just a segment. Again, this implies the need for a documented security policy of VoIP (architecture and technology selection) to create a layered, defense-in-depth approach. Together, these characteristics are the basis of any comprehensive security solution claims that all VoIP companies are properly protected from threats and future network modifications.

So far, this is the end for VoIP, but do not be afraid, I will come back with a fascinating and interesting new article for you to enjoy it. In the mean time, please memorize and learn the terms in Table 1 that are very important not only for VoIP but for networks as well.

**WINSTON SANTOS**

# Data CENTER

FOR IT PROFESSIONALS

MAGAZINE

Want to have all the issues of Data Center magazine?
Need to keep up with the latest IT news?
Think you've got what it takes to cooperate with our team?

Check out our website and subscribe to Data Center magazine's newsletter!

Visit: *http://datacentermag.com/newsletter/*

# Guarding Against Identity Theft

**Best practices, tools and technologies to protect personally identifiable information (PII)**

In my last article I made predictions on the ever growing and dynamic landscape of cyberwar and cybercrime – bottom line, some of my predictions are already coming true this year so it's time to become even more vigilant to guard your personal identity and for your organization to do the same.

**What you will learn…**

- How serious is the Identity Theft problem
- How individuals and businesses are targeted
- Finding vulnerabilities in network equipment

**What you should know…**

- Why proper forensic review is important
- How to watch for behavioral patterns
- How to enable and centralize logging

Over the past decade, we've experienced the transformation of world economies as they have evolved around the Internet as a center for innovation, communication and commerce. It's become the lifeblood of daily business worldwide. With this paradigm shift we see incredible potential – for new experiences that are profoundly uplifting and enabling, coupled with the risks associated with a more open and easily accessible information infrastructure. Coupled with this opportunity for great reward, we are also at risk of tremendous loss. It comes in many forms through lost productivity, less profit, poor image, reduced moral and less free time when anyone with a computer and a network connection can steal your identity or disrupt your business.

Identity Theft is on the rise. The thing the cyber criminals want the most is your idendity and those of others – by gaining access to key PII variables, they can take on your financial persona – stealing money through credit card fraud, wire money from your bank account or cause small transactions to happen across thousands of accounts, gaining millions of dollars in a single effort.

If they can be you – take on your identity – your electronic persona, then they have stolen your identity and maybe cleaned out your bank account. However, most identity theft focuses on collecting massive databases full of the identities of many individuals – not just you or me but tens of thousands of us. They want our names, our addresses, our dates of birth, our credit card numbers, our government identifiers such as tax identifiers or social security numbers and even our passwords if they can get them.

With information technology enabling virtually every major business function, technology expenditures being

the single largest capital expense for all enterprises, it's critical now, more than ever, that you become more vigilant to secure yourself and your organization against identity theft.

It is easy to be mislead about what's required to secure your company. First, you should understand that security is a process to be managed, not a product or solution you install or purchase.

Outsourced security guards at the front desk may help you sleep well at night but are they well trained? What is their specific role in protecting your assets beyond the perimeter? You may have been told *just purchase a firewall* and that will solve all your problems. Or perhaps you have invested resources in setting up a *Virtual Private Network* (VPN), like a tunnel through which only your employees, armed with the domain name and an assigned login/password, can access their office computers.

True security is not about turning on alarms or firewalls or other products or solutions – it's about managing risk in an always-changing world. You need to take stock of the entire picture. Be sure you've thought about all the issues. This is the first step.

## Move from One or Two Factor to Three Factor Authentication

So, let's work on the first step to protect *personally identifiable information* (PII). One or two factors of authentication for accessing data is not enough – from now own, you should be more vigilant and employee three factors of authentication. According to NIST.gov, best practices in protecting our personally identifiable information include implementing systems that require us to provide something from all three of the following categories:


1. Something you know: like a password or pin code;
2. Something you have: such as a drivers license or ID badge or physical token;
3. Something you are: such as your biometric retina scan, fingerprint scan or facial scan.

Systems that incorporate all three factors of identification are stronger than those thatonly use one or two factors of authentication. However, when was the last time you did online banking using your web-cam for a facial orretina scan? Most likely, you've encountered a one or two factor authentication which is simply not enough.

If you think two factors is enough, just take a look at all the PII data theft that has taken place in the united states alone – visit *PrivacyRights.org*.

## Log Everything and Backup the Logs Regularly

Some of the best cyber criminals have deployed malware that is so intelligent and malicious – it may open URLs using a malware callback URL (MALCON), it may probe the local computer and also open ports looking for peers to attack, or install additional threat code into data files on file servers by using the SMB (structured message block) protocol. All of these actions could be properly detected if local computer behavior and network traffic activity were logged into a central logging server using the SYSLOG format.

By logging everything, even if you don't have the time or resources to proactively stop an identity theft breach, in advance, you will have taken the right steps for forensic analysis. Reviewing logs regularly for anomalies can help you determine if you left the front door open on your firewall, or the backdoor opened on executive laptops.

## What Constitutes Personally Identifyable Information (PII)?

Your personal information is more than your name, address and Social Security number. It includes your shopping habits, driving record, bank account information, medical diagnoses, work history, credit score and much more. The right to privacy refers to having controlover this personal information. It is the ability to limit who has this information, howthis information is kept and what can be done with it.

Unfortunately, personal privacy is lost, unknowingly forfeited, purchased or stolen every day. Here are some of the methods used to obtain consumer-based PII:

1. Behavioral Targeting
2. Social Media Websites
3. Smartphones
4. eBook Readers
5. Wireless Networks

**Behavioral Targeting**
Behavioral Targeting will continue with double-digit growth through 2014 as more and more consumers increasingly go online. A majority of the consumers around the globe already use the Internet. Behavioral targeting usesdata collected from your computer to deliver *targeted* advertisements. The concern is that marketers can track your online behavior, such as the links you click on and how long youspend on a page, without your knowledge. Since marketers often sell and trade data, they caneasily build a detailed profile on you over time.

**Social Media Websites**
Let's look at Facebook, for example. Facebook alone connects more than 500 million people-more people than in America and Brazilcombined. On Facebook, people store massive amounts of personal information, including birthdates, photos, phone numbers, and more. Not only is this information a gold mine formarketers and unscrupulous individuals, but it may also be used against you by current and future employers.

**Smartphones**
Smartphones are the fasted growing segment of the mobile phone market, with half of Americans expected to own one by the end of 2011. Built-in GPS capability allows you to share your location through photos and apps. It might seem harmless, but criminals can use location data to track your movements or find out where you live. Another problem is when smartphone apps sell data about you-such as your phone number, current location and name-tothird-party marketers without your knowledge or consent.

**eBook Readers**
The ownership of eBook Readershas tripled in less than two years and eBook sales already account for 10% of U.S. consumer book sales. Like your smartphone, eBook readers collect and track data. For example, reading devices may track what books you search for, the exact pages being read, and any annotations you make. How is that information being stored and shared?

## How Many Databases Contain Your PII?

Few people even suspect how much of their personal information is available in numerous public and private databases. Read on to learn about some of the ways this information is collected, traded and sold – often without an individual's knowledge or consent.

**Specialty reports**
Specialty reports – are used by companies that may be considering offering you a job, renting you an apartment or providing you with an insurance policy. These companies feel a need to assess their *risk* in dealing with you – by using specialized *consumer reports* tofind out more about you.

**Credit reports**
Credit reports – A credit report is a record of your credit and loan activities – how you pay your bills, and whether you've been sued, arrested, or filed for bankruptcy. It contains your name and any name variations, your address, and previous addresses, telephone number (including unlisted number), Social Security number, year and month of birth, and employment information. Learn how to understand your credit report and make corrections to inaccuracies.

**Public and Government Records**
Public and Government Records – These public and government records can be accessed by anyone – including future employers –without your knowledge or consent. Find out what might be included in these public records about you or your organization, before others do. Online information brokers comb through public records for personal information – including your name, address, and even your Social Security number and sell this information online at minimal costs.

**Wireless Networks**
Wireless Networks – We're constantly hearing stories about government agencies, airlines and transit authorities, retailers and financial institutions being exploited daily by remote attackers. What most people don't understand is that wireless encryption is a complete fallacy. There are only a few ways to properly secure a wireless network and most people do not know how to do this. Turning on WPA or WEP encryption just slows down the exploit for a few seconds to about ten minutes. Hacking tools like WEPCrack and KISMET are among the thousands of ways to break into wireless networks.

The wireless network is the new frontier for attacks which lead to access to PII – just read my article in Hakin9 about the Greatest Breach in Cyber History – over 100,000,000 consumer records (credit card transactions, names, addresses, etc.) all stolen by the cyber criminals through their initial exploit of the target merchant's wifi networks.

Why is this such a serious issue for Identity Theft? Because attackers can be sitting many blocks away either on a rooftop or in their car. This is called Wardriving. It is typically viewed as the act of searching for Wi-Fi wireless networks by one or more hackers in a car using a laptop and a Pringles can to extend and focus the antenna or a simple PDA. Wardriving tools are freely available on the Internet, notably NetStumbler for Windows, Kismet or SWScanner for Linux, FreeBSD,

NetBSD, OpenBSD, DragonFly BSD, and Solaris, and KisMac for Macintosh. There are also homebrew wardriving applications for handheld game consoles that support Wi-fi, such as sniff_jazzbox for the Nintendo DS, Road Dog for the Sony PSP and Stumbler for the iPhone. There also exists a mode within Metal Gear Solid: Portable Ops for the Sony PSP (wherein the player is able to find new comrades by searching for wireless access points) which can be used to wardrive (*source: Wikipedia*).

The notion of a wireless network being secure is nearly impossible because it does not require physical connectivity by a wire through the network. This has been devised as a convenience and to help us *untether* ourselves and our new internet enabled devices (such cell phones, pdas, laptops, bar code scanners, front door locks, cameras, printer servers and much more). So, what methods have been made available to protect our wireless networks and why are they failing?

Initially, good security was to password protect your wireless network. That was easily hacked by simply sniffing the password in clear text over the wireless traffic. The next step was to encrypt wireless communications by adding keys, passphrases and fully encrypted traffic between wireless routers and end-users. Also, intrusion detection packet sniffers looking for traffic-based exploits was added to these wireless routers. All of the above have resulted in customers having a warm-and-fuzzy good feeling that they were secure, until ten minutes later, they were hacked.

How can a hacker breach these multiple layers of wireless security in ten minutes or less? It's simple. Because wireless traffic flows over the airways, there is simply no way to protect public and private key encryption properly. Within 10 minutes of logged encrypted traffic, tools like WEPcrack can obtain these keys. Most of the new attacks are not traffic based but they are asset based. So, instead of sending malicious traffic to a wireless router, which could set off the intrusion detection alarm, most hackers only send good traffic to the router which will not set off the alarm.

So, one might use an additional layer of security by only allowing trusted assets onto their wireless network. The way to do this is to limit access to a list of devices based on their MAC address. The problem with this approach is that a MAC address can be spoofed. In fact, Microsoft Windows allows you to change your MAC address on your Ethernet card with a few mouse clicks and keystrokes.

Either you disable and remove all wireless access to your network, or if you must use wireless for business purposes, you take ever step possible to harden your wireless routers by removing their vulnerabilities and find some way to prevent intrusion on these devices either through an intrusion prevention system or a network access control system designed to protect wireless networks.

## Dramatically Reducing Risks– Get Rid of Wireless or Get More Proactive

The real answer to solving much of this problem comes in two parts – 1) get rid of wireless networks (and we doubt anyone would accept this solution in the long haul, based upon the conveniences we derive) or 2) take a radically different, more proactive approach to wireless security by focusing on the wireless router and those assets which connect to this router. Does the wireless router have any known vulnerabilities that are remotely exploitable? You can visit *http://nvd.nist.gov* and look them up. Then, see if there is a way to close these holes and remove these exploitable weaknesses either through a patch upgrade or a trade-in for a newer model.

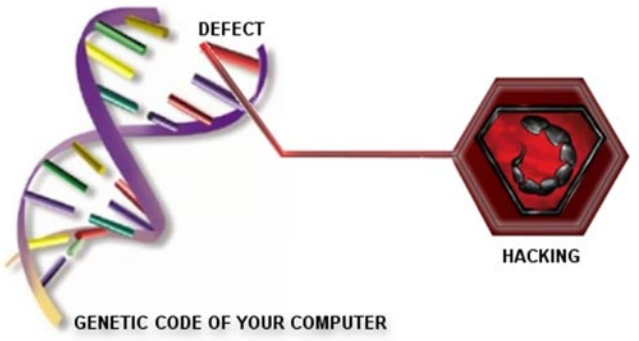
## Track and Control All Access to Your Network

Ultimately, if you can track all the assets that are truly allowed to connect to your wireless router, you can do the same thing to them, harden them against exploit and ensure that only those who are allowed to connect to your wireless router are on your trust list. If someone attempts to connect to your wireless router and you are certain they are not on your trust list then you should boot them off immediately. There are numerous ways to boot someone off your wireless router – one is to log into the router and remove them from the access list, the second is to limit the number of wireless connections allowed – if you have 10 employees who use the wireless router, why would you allow an unlimited number of connections, which is the usual default? Finally, you can turn the tables on the attacker and deny them service. The best way to automate this process is to find an agent-less *network access control* (NAC) solution that works with your wireless router so this NAC solution can do all of the above and act on your behalf and provide you with a more controlled, trusted wireless network.

## Reducing Identity Theft Breaches – Proactively Protect and Harden Your Systems

First, you need to understand the defects in the genetic code of your computer and how cyber criminalstakes advantage of those defects to infect your systems and steal confidential records, causing massive PII breaches.

According to my research, every computer and every piece of networking equipment (VoIP telephones, wireless routers, laptops, desktops, servers, firewalls, managed switches, etc.) has its own genetic code. For example, the genetic code of your office computer might read as follows:




1. Ethernet (NIC) Card, Ethernet Driver – for Internet access
2. Bios – for hard drive, operating system (OS) and peripheral device access
3. CPU – the brain, with RAM, memory
4. Operating System – Windows, Macintosh, Linux, Novell or Unix, etc.
5. Device Drivers – loaded into memory and used to access your devices such as your monitor, floppy drive, CD-ROM, etc.
6. Services or Background Tasks – such as your printer queue, anti-virus scheduler, software updater, instant messenger listener, etc.
7. Applications – such as your favorite word processor or e-mail program or web browser.

These seven components make up the Genetic Code of your office computer. Within each component, there may reside a Defect that is exploitable by a hacker – in particular, the cyber criminal who wants access to one or more PII records.

The cyber criminalmight use this defect to install a worm or backdoor on your computer, take control of your system, change or delete your files, remotely, over the internet or from within your internal network. The number of defects that has been uncovered in the genetic code of computer equipment has been growing exponentially. These defects are also known as *Vulnerabilities*.

As a result of so many defects, literally thousands, the volume of successful Identity Theft attacks by exploiting those holes or *defects* continue to rise dramatically. So the malware and the real-time cyber criminal attacks are successful when they take advantage of a weakness at the heart of your computer – your genetic defects. These defects, known as Vulnerabilities are more accurately called CVE®s, which stands for *Common Vulnerabilities and Exposures*.

If you didn't know that CVEs are what allow Hackers to be so successful, you are not alone. Most people are unaware that CVEs, rather than viruses, are at the root of 95% of all security breaches. Firewalls can't stop most CVE Exploiters. Anti-virus software can't get rid of CVEs. Anti-virus software only cleans up viruses, while doors and windows are still open to attack because of CVEs.

Cyber criminalsand their automated tools are CVE Exploiters – taking advantage of the Defects in your Computer's Genetic Code. So, you are probably wondering, how hard is it toexploit your CVEs? Just look at the following steps a cyber criminal hacker took at an online bank:

- The Hacker found an online bank web site running a version of Microsoft IIS (Web Server) that contained a genetic Defect.
- The Defect is in the printer service, which is turned on by default. By sending a simple message over the Internet, with too much data, the printer service crashes, allowing an attacker to gain root privileges and take remote control of the bank server.

## How Do Cyber Criminals Exploit CVEs to Steal Personally Identifyable Information (PII)?

All hackers and the automated tools they have created use the same methodology. The amount of damage they may cause depends on how far they or their tool goes and the CVEs they find and exploit:

1. Footprint your servers, desktops and network infrastructure.
2. Scan for numbers of computers, open ports, services running.
3. Enumerate those servers and services they can find.
4. Penetrate those systems that have high-risk CVEs.
5. Escalate their privileges to become a super-user or administrator.
6. Pillage your information and customer records.
7. Get interactive including installing helper software to let them in later.
8. Expand influence by replacing trusted programs with backdoors.
9. Cleanup their tracks including firewall and server logs.

   And if they want to disrupt your business, they will perform:
10. DoS (*Denial of Service*) attacks against you or others, using your resources.

Sometimes they install software known as Zombies, which are used as remotely controlled or preconfigured DoS attacking tools that use your resources against another target, such as another online bank.

You would think that the online bank would be more secure or could have *patched* the problem. A patch is exactly that – it's a Band-Aid that may or may not work.

In fact, many patches open up new Vulnerabilities. Here are some other interesting Hacker attacks that caused embarrassment and billions of dollars in damages:

*Paris Hilton's cell phone was hacked because of a CVE. How? Hackers used a CVE (Common Vulnerability and Exposure) to break into T-Mobile's user website for Hilton's Sidekick phone-computer and stole her personal data.*

*Sasser is another intruder that takes advantage of a CVE. The truth is that Sasser uses a CVE that was around long before the worm was born. It caused an incredible amount of network downtime and business activity losses.*

*Even Stuxnet (not designed for PII breaches but for cyber terrorism) takes advantage of a CVE. The truth is that Stuxnetexploits four CVEs which can be found in the NVD.nist.gov's website. As a result, many nuclear sites are doing hardware upgrades.*

**You may never know your data has been stolen**

You may never know your data has been stolen. The only way to be sure your network is safe is to lock the doors-eliminate the Vulnerabilities-the CVEs – the weak spots – before the attackers strike.

## Defend Against PII Breaches – Detect and Track All Network Assets

Do you have policies and systems in place to track all of your network-based assets? Do you allow laptops in and out of the office? Are laptops a company asset or a personal computer that can be used at home? Do you require firewall, antivirus, antispyware and patches to be installed on each host and up to date? 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.

## Defend Against PII Breaches – Audit Your Entire Network For CVEs

Find a tool you like. Google *Laptop Auditor* or *Security Auditor* 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 to pick a tool that doesn't take any assets offline and scans and reports on CVEs.

## Defend Against PII Breaches – Lock the Doors Against CVE Exploiters

Your firewall is your best countermeasure. Make sure to review logs – look for suspicious traffic. Also make sure you setup the VPN interface properly and know who's using it and if they are coming in through a secure tunnel on an insecure or *sick* computer. By reconfiguring your rules table around CVE Exploits, you might be one step ahead of the hackers. For example, why not block ports for all inbound/outbound traffic that you don't use – 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 to fix and what port is it on? Update your rules table until it is fixed. Don't trust all patches. Reinspect for same or new CVEs and the affected ports and services. Keep repeating this process, daily.

## Defend Against PII Breaches – Cleanup Your CVEs

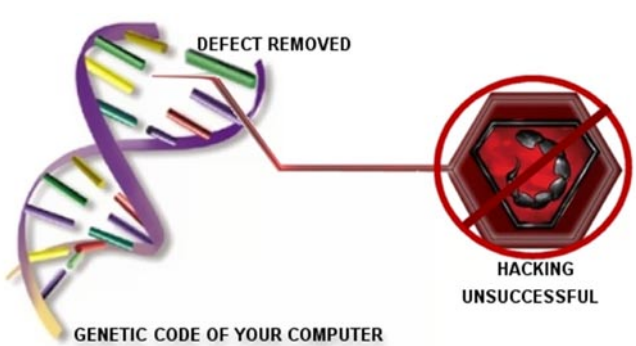
Does your vendor offer patches? Did the patch fix the CVE? Yes, good. No? Then, why not shut off the service or feature that harbors the CVE – one quick configuration change and no CVE to exploit. Some CVEs can be patched while others require intelligent reconfiguration. Cleanup your CVEs on the most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

## Best Practices for Defending Against Identity Theft – Repair Your CVEs

CVEs can be repaired. Through continuous detection and remediation, you can do for your computer and network equipment, what Science has not yet been able to do for humanity – you can remove your genetic Defects – your CVEs – from most and possibly all of your computers and networking equipment. Quarantine & Repair of your CVEs should cure your network of most risk against successful hacker, virus or worm attacks.

Three types of solutions that claim to help you harden your assets are:

1. Configuration Management
2. Patch Management
3. Vulnerability Management



Every day there is a new CVE so keep an eye on *http://cve.mitre.org*. As you now know, this website at MITRE is the homepage for helping you stop cyber criminalsand harden your assets. Why? By knowing the CVEs, if you find a system with a CVE, then you can find a way to block an exploit that would impact this asset.

## Defending Against Identity Theft – Device and Network Security Best Practices

It is crucial today to prevent Vulnerabilities across the enterprise and remove your Genetic Defects. Knowing what they are, where they are on your network, and how to remove them is more important than sniffing packets and listening for burglars.Take this opportunity to harden your network assets by using the following formula:

1. Visit *http://cve.mitre.org*
2. Keep an eye on the CVEs contained on the SANS/ FBI top 20 list *http://www.sans.org/top20/*
3. Test for the latest CVEs on a daily basis
4. Report on your CVEs on a daily, weekly or monthly basis (DUE DILIGENCE)
5. Remove all CVEs that you possibly can (DUE CARE)
6. Block at the Firewall and at the Managed Switches (INCREASE UPTIME)
7. Deploy Network and Host-based Intrusion Prevention Systems (SECURING THE DATA)
8. Watch for User and Traffic Behavior Anomalies by reviewing your device and network logs (CATCH THE DATA THIEVES)

Today's networks are at risk. Not just because hackers are out there, but also because in a mobile world, any device can pick up a virus or Trojan or have a vulnerability that opens just enough of a window to your network that a cyber criminalcan exploit it to gain access to personally identifyable information (PII).

Just one CVE® in your network and you may be in trouble. CVE is the Standard by which all information security professionals will be judged and the litmus test against regulatory compliance including GLBA, HIPAA, 21 CFR FDA 11, NERC/FERC, SOX-404 and many more.

## Understanding the Red Flag Rules – A US-based Model on Identity Theft

The Red Flags Rule requires many businesses and organizations to implement a written Identity Theft Prevention Program designed to detect the warning signs – or red flags – of identity theft in their day-to-day operations. On December 18, 2010, President Obama signed into law the Red Flag Program Clarification Act. The new law limits the circumstances in which creditors are covered by the Red Flags Rule. The FTC is revising the materials on this site to reflect the change in the law. If you are not in the USA, you can still learn from this model and implement similar in your own local government or organization.

## Defending Against Identity Theft – Documenting Policies for Compliance

Not only should you document your CVEs and show that you are fixing them, you should also have a corporate security best practices document – something which you update as needed, roll-out to your executives and employees. You want them to signoff on your best practices model – this could include Triple Factor Authentication, When to Change Passwords, Acceptable Use of Network Resources and much more. Looking at the most successfully deployed international standard – ISO 27001, you should consider visiting *http://www.iso.org* and get your own copy of this standard to help you begin to create your own *living* document on your corporate security best practices policies. Others such as COBIT are also helpful. Find a model you like and start using it. Here are the areas you would look to document:

1. *Security Policy* – To provide management direction and support for information security
2. *Organizational Security* – To manage information security within the organization
3. *Asset Classification and Control* – To maintain proper classification and protection of organizational assets
4. *Personnel Security* – To reduce the risk of human error, theft, fraud or misuse of your company or organization
5. *Physical and Environmental Security* – To prevent unauthorized access, damage and interference to business premises and information
6. *Communications and Operations Management* – To ensure the correct and secure operations of information processing
7. *Access Control* – To control access to information
8. *System Development and Maintenance* – To ensure security is built into information systems development and maintenance processes

## Resources

There are some really excellent resources out there to help you understand how serious an issue Identity Theft has become and how to start combatting it:
ISO: visit *www.iso.org* to obtain best practices security policy models such as the ISO27001.
ISACA: visit *www.isaca.org* to obtain the best practices security policy model called COBIT.
If you need to prove to your executives how serious an issue this is, here's where you can find current statistics on PII data breaches (mostly in the USA but the statistics can be used as a sampling to show the severity of the problem, no matter where you are in the world):
Data Loss Database: visit *www.datalossdb.org* to see the latest data breaches tracked by month.
Privacy Rights: visit *www.privacyrights.org* to see an entire chronology of data breaches tracked by type of breach and industry.
Don't forget to start hardening your systems:
CVE: visit *http://cve.mitre.org* to learn about the common vulnerabilities and exposures program.
NVD: visit *http://nvd.nist.gov* to learn about and search the national vulnerability database.
NIST: visit *http://csrc.nist.gov/groups/SMA/fasp/areas.html* to learn about best practices for hardening systems.
These resources should be an excellent start on your path to being more diligent against identity theft.

9. *Business Continuity Management* – To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters otherwise known as BCP/DRP
10. *Compliance* – To avoid breaches of any criminal and civil law, statutory, regulatory or contractual within your business model and government guidelines

By now you should realize how important it is to find and fix your holes (CVEs), take a more proactive approach to hardening your network resources – start at the database and file servers where you store the most critical PII and work your way out, across the network. You should also consider that the daily removal of high-risk CVEs may protect you from hackers, downtime and regulators. In seizing control of a server, security experts say, a hacker can also modify any trusted applications to perform malicious operations. An attack that manipulates such internal applications is more likely to escape notice by the network's electronic guards. *Intrusion-detection systems only spot known attacks or behaviors that indicate a certain class of attack*, said the expert. *Attacks against a server might be detected, but a complex application-based attack might look like normal behavior.*

## In Summary

It's time to be even more vigilant than ever – both personally and professionally – to protect your own identity and those critical, confidential records stored and utilized by your organization. This information is so important to cyber criminals because all it takes is one identity theft to create a compliance breach, upset a customer and damage your organization's reputation in the marketplace.

Knowing that security and compliance are processes, not products, you should put the proper policies in place that help document what tools and techniques you are using to ensure a safer, harder network to breach. Start with the weakest links – the database and file servers, all their touchpoints and your mobile devices. Make sure you can control what gets on the network and if you have to deploy wireless for business purposes, you should also consider intrusion prevention or network access control around your wireless router and related policies. You don't want someone sitting in a parking lot or garage next door, *invisible to you*, but able to find their way into your network because of one CVE on one wireless router.

Finally, with proper due care and due diligence, you will mitigate most risk and breaches and by logging for forensic purposes, if a breach occurs, you'll be able to find how it happened with more pinpoint accuracy.

**GARY S. MILIEFSKY, FMDHS, CISSP®**

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

# Identity Proof Your Personal Data

Information is being collected about us every second of every day without us ever realizing what happens to it. Most of us don't really care what happens to our personal data as long as it isn't misused. So let's go up close and personal by taking a brief glance at how you can protect your personal data if you are a UK citizen.

Worth remembering, your data held in the UK is also shared with other countries, mainly the English speaking world i.e. Canada, New Zealand, USA, South Africa and Australia to name a few. The credit reporting agencies share this data with these countries and in particular when people migrate to these countries. Every country has its own data protection laws but for the benefit of this article we will concentrate on the UK.

## UK data regulation

Regulating our personal data is more important than ever these days, especially given the sensitive nature of the data that is collected. The first attempt at a data protection law was with the *Data Protection Act* (DPA) 1984 which started by authorising organisations to take accountability for your personal data privacy. Check any UK registered website and they should highlight the DPA 1984 and 1998 (amendment). The 1998 amendment tightened the DPA which now allows everyone to see the data that is stored about them on either hardcopy (paper) or a computer.

The personal data held by third parties is used in many instances to make key life changing decisions without you ever realizing it – i.e. credit referencing agencies, people tracking websites, banks, mortgage lenders, employers etc. I will discuss this in more detail later. The DPA provides a safeguard for people so people can ask for the data held about them and dispute any inaccuracies. The way the data is collected and used is also covered under the DPA 1984/1998 Acts. As is the case with most laws, it's there as a protection but that doesn't stop data breaches or inaccurate data being held about people.

## Keep in mind

You can use the DPA to request information from a financial provider if you suspect for example that the data about you is inaccurate. It doesn't have to be your data that stops you from being accepted for a new loan or credit card. It can also be where you live and who you live with. More often than not people fail to tick or un-tick the *do not receive any marketing communication from a company or its third parties* box.You should always remember to *opt-out* if you value your privacy.

## The Electoral Register

There are many instances of people applying for credit cards and loans being refused simply because they are not recorded on the electoral roll. The electoral register should highlight your current address, so it's important you make sure it's up to date if you have recently moved. The names and addresses of all UK citizens over the age of 18 registered to vote are kept on the electoral register *http://bit.ly/qcw51*. For the past few years organisations and individuals could obtain this information and use it for any legal purpose, but privacy concerns have meant that regulation was introduced in 2002.

The regulation introduced two electoral registers. The full register lists everyone who is entitled to vote. Only certain people and organisations (i.e. UK Direct Marketing Association *http://bit.ly/BMRXz*) can have copies of the full register, and they can only use it for specified purposes. These include electoral purposes, the prevention and detection of crime and checking your identity when you have applied for credit. The edited register leaves out the names and addresses of people who have asked for them to be excluded from that version of the register. The edited register can be bought by anyone who asks for a copy and they may use it for any purpose.

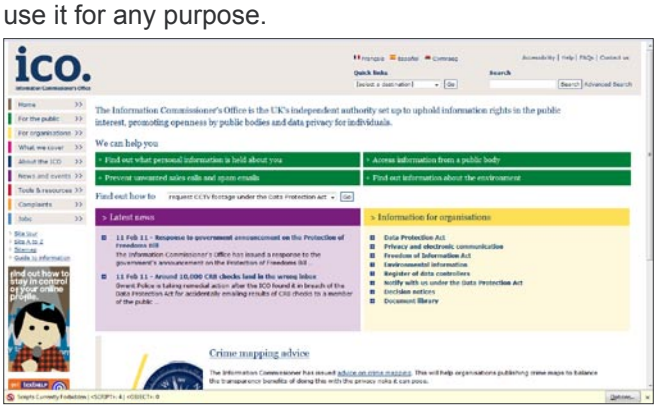



**Figure 1.**

Everyone on the full register goes on the edited version by default, but you can *opt out* this when you return the *Annual Voter* registration form. This means commercial organisations will not be able to have access to your name and address and on that year's register. Remember, that you will not be removed from the previous year's registers. Organisations may still have your personal details as well as the people you live with. If you want to stop cold calling, direct marketing mail and tempting credit card offers, this is a first positive step to protecting your personal data.

## Preference Services

Register with the free MPS (*Mailing Preference Service*) *http://bit.ly/3xksTZ* if you want to manage and control what marketing mail marketing telephone calls (includes silent calling) you receive. This list of people who don't want their publicly available details to be used for direct marketing purposes is administrated by the UK *Advertising Standards Authority* (ASA). There is though one small issue with this and that is organisations are not legally obliged to use it.

UK organisations can buy in the lists but should check the data against the Mailing Preference Service opt-out list. The problem is a number of organisations don't actually do this. That said if the organisation is a DMA member (and you can check to see if an organisation is a member of the DMA *http://bit.ly/7tzoa0*) they are bound by the code of practice, so must screen the data against the MPS database.

The Royal Mail also has an *opt-out* door to door service *http://bit.ly/UU3g6* which will stop all those unaddressed mail being posted through your mailbox. This service doesn't stop the mail addressed *the occupier* though. If an organisation continues to send you unsolicited marketing mail after you asked them to stop, that organisation will be in contravention of the Data Protection Act and ASA regulations, which means that the ICO and ASA can be asked to intervene.

Another really useful mailing preference service is *The Bereavement Register http://bit.ly/hmlbcW* which can help reduce the amount of direct mail sent to your address, stopping painful daily reminders. Unless companies are informed of a death, they will continue to send promotional mailings about their products and services. By registering with this free service the names and addresses of the deceased are removed from mailing lists, stopping most direct mail within as little as six weeks.

## Telephone marketing, silent calls and filling in forms

Telephone marketing calls are something we all have experienced. Sometimes having an ex-directory number can help as can signing up for the *Telephone Preference Service* (TPS) *http://bit.ly/qOsft* Organisations are not obliged to use the TPS list but it does help reduce the marketing calls from personal experience. If you are repeatedly hassled by these marketing and silent calls then complain to the ICO.

Cold calling that originate overseas can also be stopped, but only if those companies calling are UK registered/owned and are using foreign call centres to make these calls – so these companies will still be bound by the DPA code of practice. If you are still receiving cold calls then there is an EU Data Protection Directive *http://bit.ly/QqxGe* which the ICO routinely liaises with.

Silent calls are made by automated dialling systems that fail to connect the call when answered, however it might a good idea to register with a service called SilentCall-Gard: *http://bit.ly/eH5aG* – it's totally 100% free. In the UK, new legislation introduced by the regulatory body Ofcom (Independent regulator and competition authority for the UK communications industries) has just revamped the automated dialling systems. After February 2011, all automated calls must be connected within two seconds of the recipient speaking or there should be a recorded message that states the organisation's name and how to opt out of future calls.

Form filling is something we are all fond of – well not really. This is where we get caught out as so far as allowing others access to our personal data by forgetting to tick or un-tick a simple box. Be sure to tick the appropriate boxes when filling out any forms for goods and services. Look for opt-out statements which use euphemisms to confuse you. Read the opt-out a couple of times so you fully understand what you are opting out of and that you are actually not opting in. It's very important you have the opportunity to prevent your details being passed to third parties – but this is in your control. Consider this; magazine subscriber lists are routinely sold/rented as are our high level data from our credit files to marketing and other agencies (including people tracking websites). Form filling will never go away, whether it's online or a paper copy, so stay completely vigilant.


**Figure 2.**

**HINT**
Worth noting and not everyone knows this – third-party organisations are not legally allowed to sell on the details of consumers on these sold-on lists, unless that is they convert these consumers into consumers of their own.

## Checking your credit report

Under the DPA you can request information from a financial provider i.e. bank, credit card provider if you suspect the information about you is incorrect or has caused you problems when applying for a loan, credit card or opening a bank account for example. The Data Protection Act allows for you to obtain a *statutory credit report* from all the credit reporting agencies – Experian: *http://bit.ly/hNL28g*, Equifax: *http://bit.ly/fY7yZq* and CallCredit: *http://bit.ly/gRIv2c*. The information on credit reports is the most important information about you. Credit information is used to decide whether you are financially viable. In other words these agencies decide whether you can have a loan, mortgage, credit card and so on. Without a credit history (which takes time to build – and the only way to build this is to have credit in your name) you are unlikely to be able to borrow money.

Credit card companies are not that interested in people who don't rack up debt – so long as they can make money on your interest payments they are more than happy to give you credit to spend. To access your statutory report will cost L2.00 (correct as of February 2011) but this will not give you your credit score – which determines how risky you are to loan money too. All three credit reporting agencies will have some different information about you, so it's important to obtain the reports and credit score from all three.

If you spot an error, you should send the credit reporting agency a *correction* letter or if you notice that you have some late payments showing or you have an unpaid debt that was a result of an uncorrected billing error. You can also apply to the agencies for a *notice of correction* to your credit report which will clarify the in correction to future lenders.

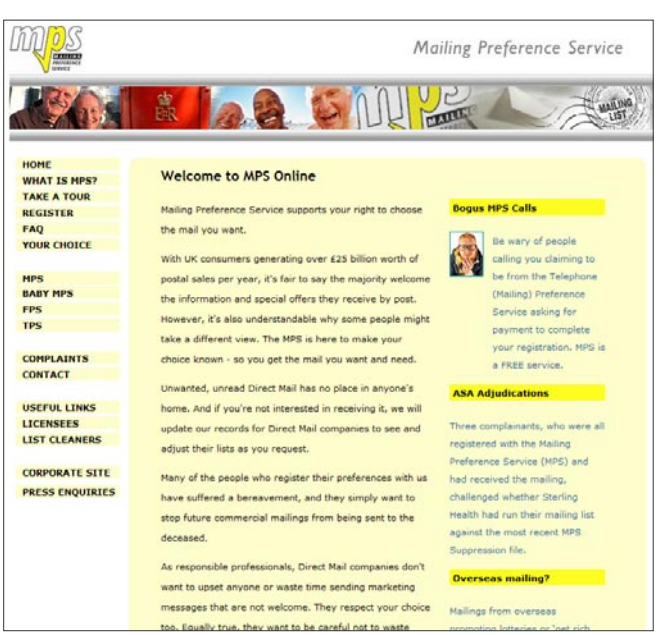


**Figure 3.**

If you have recently divorced or left your partner you should also *financially disassociate*. Once a disassociation has been created, lenders requesting your report no longer see details of the disassociated family member or members. You will need to notify each agency about the disassociation.

If you don't do this then your ex-partner may obtain a loan or credit card in your good name. It has happened and continues too, even when people are legally divorced. Here are the links for financial disassociation: Experian – *http://bit.ly/dIakAB* Equifax: *http://bit.ly/eoU9Ds* CallCredit – *http://bit.ly/hDm03Z*.

## Protecting your email address

Unsolicited direct marketing mail is not only sent to a letter box. As we all know well it is also sent to our mail inbox on our PCs. This unsolicited email is called spam. Since 2003 sending spam is a criminal offence, but beware it all depends on whether you remembered to tick or un-tick that box on the web form that asks you for permission to use your personal details for marketing purposes.

Savvy surfers use two email addresses – one for email communication and the other with everything else. Disposable email addresses are a must have if you value your email addresses. There are many but the general idea is that you open a web page and click a get link for a randomly generated email address that exists for a specified time period. Here are three popular websites: Guerrillamail *http://bit.ly/2LVUNc* Spamgourmet: *http://bit.ly/PcE9K* and Mailinator: *http://bit.ly/1WHWBe*.

Some of these sites only allow you to send and receive email using their webmail system – but some not all allow you to manage the spam and forward any relevant emails to your actual email address.

## Facebook and Google 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

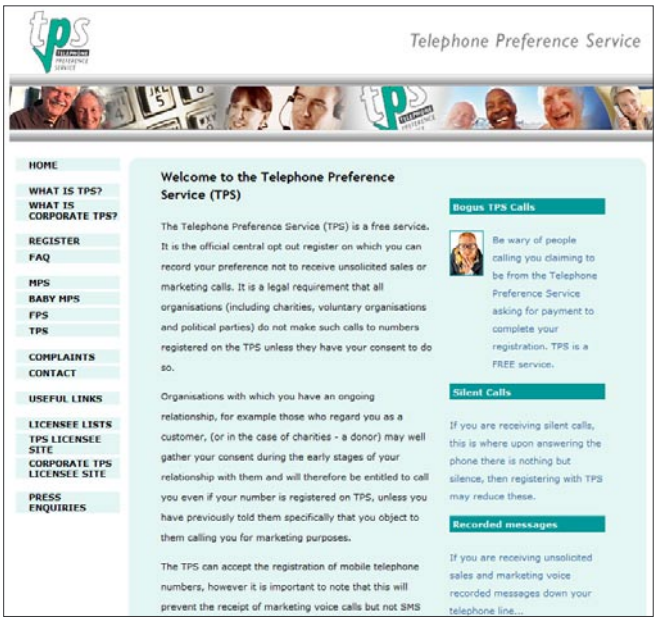



**Figure 4.**

now opt out 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.

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. See my blog entry regarding Facebook scraping *http://bit.ly/gWhq7W* for further information on this threat.

Facebook has recently addressed a major security issue – surrounding HTTPS. I wrote about this in *Managing your Facebook Privacy in 2010* June 2010 feature See my blog entry regarding how you can setup a HTTPS connection: *http://bit.ly/hVkkCB* – if we all value our data then we should all be using HTTPS.

## Protecting your identity and your personal data from identity theft

So – how do you go about protecting your good name, both in the cyber world and the offline world? I'm going to highlight the UK service options and then you can decide which service is best for you.

### UK Identity Theft Protection Service Options

Here is what you should look for if you are living in the UK:

- Credit reporting / scores i.e. providing single report or triple reports analysis*
- Computer protection i.e. anti-malware/firewall/anti-virus/password protection
- 24/7 access to trained ID Theft Resolution Specialists – includes identity recovery
- Identity theft Insurance (up to L50,000)
- Lost wallet/cards protection – will cancel and replace your cards/passport etc
- CIFAS Protective Registration – places a warning flag against your credit file(s)**

*If an application for credit is made in your good name you also have the option of receiving an EMAIL or SMS. The three leading credit reference agencies in the UK are: Experian, Equifax and CallCredit. **CIFAS Protective Registration can also be purchased separately for L14.10 for one year. Please check the CIFAS *http://bit.ly/hHORFO* website for further information. (December, 2010)

The average cost of UK identity theft protection services varies from L8-10 per month (this mainly applies to credit monitoring only). In the UK there is only one company that offers an identity protection service, similar to what is on offer in the US – called Garlik they charge L45 for a one year subscription for individuals to DataPatrol. Garlik DataPatrol *DOES NOT* offers an online credit monitoring service.

Worth remembering: If you do decide to purchase just a credit monitoring service you will have to pay extra for your credit score.

Worth remembering: Section 75 of the Consumer Credit Act 1974 protects consumers on any credit card purchases (this includes loss or theft) which cost over L100 and under L30,000. Note: This also applies when someone else fraudulently uses your credit card i.e. Chip & Pin fraud, *Card Not Present* (CNP) fraud etc.

If you are a UK citizen and value your personal data, I'm sure what I have written here will be of considerable interest. I hope to cover this feature for US citizens very soon...

**JULIAN EVANS**

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

# Choosing an IDS/IPS Engine

So this months article is all about what's on my mind. It's rare that there is something on my mind that makes much sense, so I figured I'd better take the opportunity to share while it seems coherent.

We are now publishing the Emerging Threats rulesets (both the open and Pro versions) in many formats, on many engines, and for many platforms. We have our flagship engine Suricata as well as Snort and shortly a couple of proprietary platforms for OEM use. We have four major version delineations in Snort back to 2.4, thankfully just one major version of Suricata, and the proprietary versions to support. Our goal is to be a single research organization (the community as well as our Pro resources) and make the information and protection available on any format possible. We believe this to be more effective and more efficient than every company doing the same research in parallel.

The point of this article isn't to complain, we do the multiple engine thing quite well, and we love it. That's why we exist, to tie the research together regardless of end product. We invested heavily in building a backend that makes this very streamlined and efficient. But a challenge is performance testing to tune each rule to be its best not only on each engine, but on each version of the engine, and then on each hardware platform for each version. We are doing this well also, but it's run us through some interesting hurdles. Let me explain...

It's not rocket science how to performance test a ruleset. You have four major variables that affect IDS/IPS performance. The actual physical capabilities of the hardware and capture (we lump os, hardware acceleration, and capture acceleration in here), the engine and its capabilities, the traffic you run by the sensor, and then finally the ruleset. So to performance test any of those components you have to treat all four as variables. You hold three of the variables constant and then test the fourth.

So what we do is run a number of static hardware platforms that are used for nothing but this and never change, we use a few terabytes of very representative traffic from universities and corporations and home users (this pcap does not change often, planning yearly rotation of pcaps), so we have left just the ruleset and the engine.

The ruleset of course changes daily for us, but for the sake of discussion here let's think about just a single day's ruleset. If we lock the ruleset by day then we have three variables stable and we can play with the last one, the engine.

For daily ruleset testing this actually shows us some very interesting things about the engines. I don't have all the data together yet in a publishable format, but we will soon. We can see especially in Snort the changes in how it handles different rules and traffic over the years through the versions of the engine we test. We can also see how other engines (ignoring the proprietary ones for now) do, such as Suricata. It does some things better than Snort, and vice versa.

But Suricata is multithreaded, so testing it against Snort head to head even on the same hardware is very unfair. Frankly, we couldn't find any hardware to use in our test lab that could process the traffic corpus quickly enough that wasn't multicore. To have a good test we need lots of traffic, and anything old enough to be single core just can't do that quickly enough to let us test twenty or more configurations in the few hour release timeframes we desire to meet. So since Suricata can use all the cores in the reference hardware but Snort can only use one, Suricata has a huge advantage.

Another example, Suricata checks dsize (payload size of the packet) before doing pattern matching. Snort checks it after pattern matching. So we have a lot of potential signatures we want to match on in small packets, and sometimes very small strings. Checking for a small string in all packets is very very expensive, but if for example we know the target packet is 16 bytes we can eliminate 99% of packets from matching just by checking dsize first. But Snort doesn't check dsize till after matching as it's more oriented toward extremely efficient matching and pre-matching, so you can have the same rule that will perform horribly on Snort and be nearly no load on Suricata but still hits on both just fine.

So this isn't a huge deal for our QA and performance testing because we are actually looking at the

differences between the ruleset from yesterday to today per engine and platform, not testing engines head to head. We use that data to identify the rules that don't perform well and tune them per engine. And in the case of Suricata we actually can make feature suggestions to the dev team to enhance the engine to allow us to get the detections we need.

We are often asked which engine to use if an organization is deploying the Emerging Threats rules in a new infrastructure. My answer here is generally that we can't compare Snort and Suricata and many other engines directly. And in most cases there just isn't a real reason to. If you have certain needs, or certain preferences you'll use one engine over the other. They do different things better. We cannot really have a good performance test apples to apples. But we do need to have good information in general testing one ruleset against another.

So there you have it. The answer to which engine to use.... it depends.

I'm very interested in what you think. Please send me your thoughts, *jonkman@emergingthreatspro.com*. Get your copy of the new ET Pro Ruleset, *http://www.emergingthreatspro.com* and support open source security!

**MATTHEW JONKMAN**

***Matt is the founder of emergingthreats.net, the only open and community based intrusion detection ruleset, CEO of Emerging Threats Pro, 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.***

# Weaponised Malware

## – how criminals could use digital certificates to destroy your organisation

***Jeff Hudson, Chief Executive Officer, Venafi***

The headlines which heralded the first story of the Stuxnet cyber attack on an Iranian nuclear facility were familiar: *New malware attack* but they did not tell the full story. This new virus has the potential to destroy physical objects – a major new departure for software – weaponised malware had been born. Should we really worry about it? It should worry all of us – and not just those in close proximity who were in danger of being blown into the next world by the actions of a computer virus.

Digital security threats and sometimes the hype surrounding them have become commonplace in our interconnected and IT-dependent world. However, this was no ordinary attack. Apparently malware was introduced into the Iranian nuclear facilities local area network. It entered between the internet and the internal network. The other possibility was a trusted insider who was an agent of the organisation which carried out the attack.

As researchers later discovered, the attack used four different Zero Day exploits on Windows platforms. In addition to the Zero Day attacks, the 'payload' included a stolen digital certificate that was issued by Verisign. The virus was self-propagating and spread to numerous machines. The mission of this virus was to auto-propagate in the wild (there was no back channel to a command and control host as this was an isolated network). It was then to locate and operate a valve or control module that was a critical part of the nuclear facility's infrastructure, with the intent of disabling or damaging the facility. In other words: to act as a weapon. This is a significant step forward in the development of malware.

The traditional, malicious approach to damaging the facility would have been to use a conventional weapon (i.e. a bomb). The astonishing difference is that this malware was attempting to do mechanical damage to the facility without supplying the destructive mechanical force on its own. In other words, this was malware designed specifically to accomplish the work of a weapon. It has therefore earned the dubious classification as weaponised malware.

This particular malware is estimated to have taken 10 man years of effort to develop. It is sophisticated. The tools used in development, the timestamps on the binaries, and the number of modules with different coding styles suggest multiple development teams. The origin of the malware has not been verified but the most popular theory is that it was developed by a nation state or states that were attempting to disrupt the Iranian nuclear program.

Iran has the largest percentage of known instances of the Stuxnet virus. However it has also been found on systems in many other countries. Experts predict that numerous, undetected instances are still active.

It is a well-established fact that many weapons developed by national military programs become available to non-nation state entities, such as terrorists, rogue nation states and criminal organisations. It is just a matter of time. Examples are; night-vision goggles, GPS systems, airborne drones, fully automatic rifles, Kevlar body armor and shoulder launched missiles, to name just a few.

The questions are, A) when will Weaponised Malware and its derivatives be used to destroy, disable or steal valuable assets and information from other nations, utilities, banks, or telecommunication companies, and B) what can we do about it?

The Stuxnet weaponised malware utilised multiple zero day vulnerabilities to infect, and employed a signed digital certificate to authenticate itself in the environment. The certificate allowed the malware to act as a trusted application and communicate with other devices. This is the first reported incident of the utilisation of a digital certificate in this type of attack, and is a very ominous and worrying development. The level of threat has moved from downtime and a damaged reputation because your certificate has expired to physical damage to you and your employees if the virus successfully makes a manufacturing or utility process go critical.

The use of four zero day vulnerabilities and a stolen digital certificate signals the beginning of a new era of cyber warfare and cybercrime. The implications

are enormous. This is not the first occurrence of this species. The Aurora virus was a first generation variant and Stuxnet represents a significant evolutionary leap in complexity and sophistication. Additionally the potential costs to the targeted organisation in the event of a successful attack are higher than ever.

Zero day vulnerabilities are by definition impossible to defend against. The use of unauthorised digital certificates by weaponised malware in a networked environment is another matter. There are steps organisations can take to significantly reduce the risk of a successful attack.

The first consideration is the knowledge of digital certificates that are active in a network. Most organisations do not know how many they have, where they are installed, who installed them, their validity, and the expiration date of the digital certificates in their network. Here's a parallel analogy in the world of physical security. This is exactly the same as not knowing which people in a secure building are authorised to be on the premises and which ones are unauthorised. Imagine a bank where no one knew which people in the building were authorised to be there or not. This is not an exaggeration. This is an unacceptable situation to anyone who takes security seriously. This is an unquantified risk. The only acceptable practice is to continually and actively discover certificates on the network.

Additionally those certificates must be validated that they are functioning as intended and that they are monitored throughout their lifecycle so that they can be expired and replaced as dictated by the security policies of the organisation. Most organisations are deficient in this regard. This is an unmanaged risk and can be easily brought under management. A failure to manage this kind of risk exposes organisations to increased vulnerabilities like the Stuxnet attack. This is not scaremongering – it is a real threat which will affect an organisation sometime soon.

Why are organisations exposing themselves to this unquantified and unmanaged risk? The reason is simple enough to understand. Before Stuxnet, the lackadaisical knowledge and management of digital certificates was viewed as acceptable. Additionally many board – level executives are not familiar with digital certificates, how they work, their role in security, and the management practices and policies. This has to change. There is not one board – level executive that misunderstands or underestimates the importance of ensuring that only authorised individuals can enter a secure building. Those same executives naively allow unauthorised or unknown certificates to enter and operate on their networks.

In summary there is unquantified and unmanaged risk that allows Stuxnet to propagate and operate on a network. This represents bad management practice of a critical part of a layered security model. Digital certificates are widely used to authenticate and identify entities in a network. Poor management practices render digital certificates ineffective for their intended purpose. In fact poor management in some cases creates an exploitation opportunity.

The Stuxnet Weaponised Malware is a very loud wakeup call as it has exploited the poor management practices of digital certificates that exist in many firms today. Implementing practices and policies for the management of digital certificates is an important and necessary component of a broad and wide security strategy. It is the one strategy that can detect the appearance of malware that utilizes digital certificates for authentication. Weaponised Malware has or will be aimed at every company in the Global 2000. The responsibility is to act before the weapon strikes.

*www.venafi.com*

**Jeff Hudson – CEO**

A key executive in four successful, high-technology start-ups that have gone public, Hudson brings over 25 years of experience in information technology and security management. Hudson has spent a significant portion of his career developing and delivering leading edge technology solutions for financial services and other Global 2000 companies.

Prior to joining Venafi, Hudson was the CEO of Vhayu Technologies Corp. Vhayu was the market leader for the analysis and capture of market data, and was acquired by ThomsonReuters. Prior to joining Vhayu, Hudson held numerous executive leadership posts, including CEO and cofounder of MS2, Senior Vice President of Corporate Development at Informix Software, CEO of Visioneer, and numerous senior executive posts at NetFRAME Systems and WYSE Technology. He started his career with IBM.

Mr. Hudson earned a B.A. in communications at the University of California, Davis.

# In the next issue of Hakin9 magazine:

## Cell Phones Attacks

## Smartphones Security and Privacy

Available on March 31st