

# (IN)SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 15 - February 2008

## malware

APPLICATION SECURITY  
SOCIAL ENGINEERING  
VISUALIZATION TOOLS  
INTERNET TERRORISM  
FRAUD MITIGATION  
INSIDER THREAT

# SECURITY AS A SERVICE

NOW AVAILABLE AT A BROWSER NEAR YOU

Software-as-a-Service (SaaS) has been described as the most disruptive delivery model to ever face the enterprise software market for one simple reason: ***it works***

Qualys is the first company to deliver an on demand solution for security risk and compliance management. QualysGuard® is the widest deployed security on demand platform in the world, performing over 150 million IP audits per year — with no software to install and maintain.

**For a free trial, go to a browser near you.**

[www.qualys.com/SaaSTrial](http://www.qualys.com/SaaSTrial)



# TABLE OF CONTENTS

- Page 05 - Corporate security news
- Page 09 - Proactive analysis of malware genes holds the key to network security
- Page 13 - Advanced social engineering and human exploitation, part 1
- Page 18 - Free visualization tools for security analysis and network monitoring
- Page 26 - Latest additions to our bookshelf
- Page 30 - Web application vulnerabilities and insecure software root causes: solving the software security problem from an information security perspective
- Page 39 - Internet terrorist: does such a thing really exist?
- Page 44 - A dozen demons profiting at your (in)convenience
- Page 50 - Weaknesses and protection of your wireless network
- Page 61 - Fraud mitigation and biometrics following Sarbanes-Oxley
- Page 71 - Events around the world
- Page 73 - Interview with Andre Muscat, Director of Engineering at GFI Software
- Page 77 - QualysGuard visual walkthrough
- Page 81 - Application security matters: deploying enterprise software securely
- Page 87 - Hiding inside a rainbow
- Page 93 - The insider threat: hype vs. reality
- Page 97 - Security software spotlight
- Page 98 - How B2B gateways affect corporate information security
- Page 102 - Reputation attacks, a little known Internet threat
- Page 105 - Italian bank's XSS opportunity seized by fraudsters
- Page 107 - The good, the bad and the ugly of protecting data in a retail environment

## EXPERTS CORNER: BURNING QUESTIONS ABOUT MALWARE

- Page 122 - Mikko Hypponen, Chief Research Officer for F-Secure
- Page 125 - Richard Jacobs, Technical Director of Sophos
- Page 129 - Raimund Genes, CTO Anti-Malware at Trend Micro

# Welcome to (IN)SECURE 15

## the digital security magazine



It's February and the perfect time for another issue of (IN)SECURE. This time around we bring you the opinions of some of the most important people in the anti-malware industry, a fresh outlook on social engineering, fraud mitigation, security visualization, insider threat and much more.

We'll be attending InfosecWorld in Orlando, Black Hat in Amsterdam and the RSA Conference in San Francisco. In case you want to show us your products or just grab a drink do get in touch. Expect coverage from these events in the April issue.

I'm happy to report that since issue 14 was released we've had many new subscribers and that clearly means that we're headed in the right direction. We're always on the lookout for new material so if you'd like to present yourself to a large audience drop me an e-mail.

Mirko Zorz  
Chief Editor

Visit the magazine website at [www.insecuremag.com](http://www.insecuremag.com)

### (IN)SECURE Magazine contacts

Feedback and contributions: Mirko Zorz, Chief Editor - [editor@insecuremag.com](mailto:editor@insecuremag.com)

Marketing: Berislav Kucan, Director of Marketing - [marketing@insecuremag.com](mailto:marketing@insecuremag.com)

### Distribution

(IN)SECURE Magazine can be freely distributed in the form of the original, non modified PDF document. Distribution of modified versions of (IN)SECURE Magazine content is prohibited without the explicit permission from the editor.



# Corporate security news

## Qualys releases QualysGuard PCI 2.0

Actions: Delete Apply

View Edit Title

Initial Options (default)

Payment Card Industry (PCI) Options

Qualys Top 20 Options

SANS20 Options

Qualys announced the availability of QualysGuard PCI 2.0, the second generation of its On Demand PCI Platform. It dramatically streamlines the PCI compliance process and adds new capabilities for large corporations to facilitate PCI compliance on a global scale.

QualysGuard PCI 2.0 brings a new refined user interface making it easy to navigate through the process of scanning, remediating and e-filing customers' compliance status to multiple acquiring banks. ([www.qualys.com](http://www.qualys.com))

## Open Source Vulnerability Database 2.0

OSVDB announced a major milestone in the cataloging, classification, description and management of software and hardware security vulnerabilities - the release of OSVDB 2.0, a complete rewrite of the web site using Ruby on Rails, provides substantial performance and reliability improvements for both developers and researchers.

Vulnerability Classification			
Location	Attack Type	Impact	Solution
<input type="checkbox"/> Physical Access Required <input type="checkbox"/> Local Access Required <input type="checkbox"/> Remote/Network Access Required <input checked="" type="checkbox"/> Local / Remote <input type="checkbox"/> Duplex Access Required <input type="checkbox"/> Wireless <input type="checkbox"/> Mobile Phone <input type="checkbox"/> Unknown Location	<input type="checkbox"/> Cryptographic <input type="checkbox"/> Denial of Service <input type="checkbox"/> Hijacking <input type="checkbox"/> Information Disclosure <input type="checkbox"/> Infrastructure <input type="checkbox"/> Input Manipulation <input type="checkbox"/> Misconfiguration <input type="checkbox"/> Race Condition <input type="checkbox"/> Other <input type="checkbox"/> Unknown	<input checked="" type="checkbox"/> Loss of Confidentiality <input type="checkbox"/> Loss of Integrity <input type="checkbox"/> Loss of Availability <input type="checkbox"/> Unknown	<input type="checkbox"/> No Solution <input checked="" type="checkbox"/> Workaround <input type="checkbox"/> Patch <input type="checkbox"/> Upgrade <input type="checkbox"/> Change Default Setting <input type="checkbox"/> Third Party Solution <input type="checkbox"/> Discontinued Product <input type="checkbox"/> Solution Unknown

OSVDB 2.0 enhancements include: greater detail about the overall nature of a specific vulnerability, a "Watch List" service that provides alerts for new vulnerabilities, consolidating external blogs by vulnerability, and new reporting metrics. ([www.osvdb.org](http://www.osvdb.org))

## Firestick Pico ultra-portable security USB device

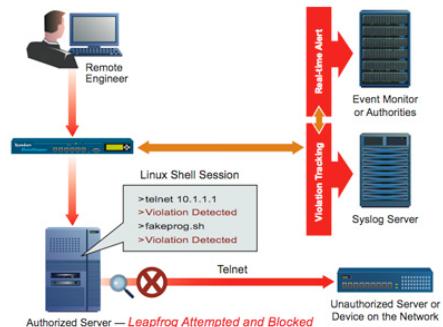


Yoggie Security Systems has introduced a unique, ultra-portable USB key-sized hardware-based firewall solution to protect PCs from malicious attacks. The Firestick Pico places a physical barrier between PCs and the Internet to ensure that threats never reach users' computers. It is a complete Linux-based 300 MHz computer with a dual flash memory mechanism that constitutes an 'untouchable operating system' running an independent firewall application. ([www.yoggie.com](http://www.yoggie.com))

## New GateKeeper prevents leap-frogging to unauthorized areas

Xceedium GateKeeper 4.0 delivers patent-pending LeapFrog Prevention technology, FIPS 140-2, Level 2 certification and other new feature enhancements.

It provides first-to-market technology that allows companies to protect critical infrastructure by restricting technical users to authorized areas only. Its patent-pending technology monitors and enforces policy at the socket layer and tracks all activities for these users. ([www.xceedium.com](http://www.xceedium.com))



## Biometric protection for Mac



UPEK launched Protector Suite for Mac, software that allows Mac users to increase both security and convenience with the simple swipe of their unique finger. Protector Suite for Mac in combination with Eikon Digital Privacy Manager, a USB peripheral fingerprint reader, enables Mac users to swipe their finger instead of typing passwords to login as well as access password-protected websites and secure preferences. ([www.upek.com](http://www.upek.com))

## RedCannon KeyPoint Solo Vault USB protection

RedCannon Security announced the RedCannon KeyPoint Solo Vault, a software solution to protect sensitive data stored on USB devices. It provides standards-based, military-grade software encryption that allows end-users to maintain productivity in the field with the assurance that the data they carry and use will not be compromised. KeyPoint Solo Vault extends the benefits of the RedCannon FIPS-certified portable encryption technology to any USB flash drive. The solution operates without a management server and requires no software installation on the host PC. ([www.redcannon.com](http://www.redcannon.com))



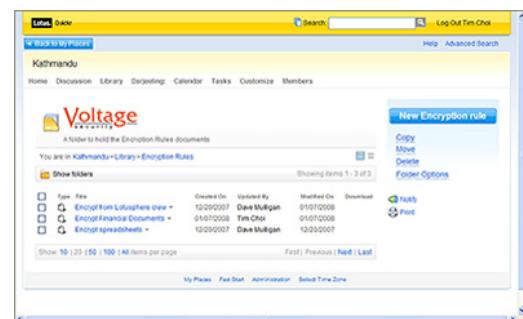
## Smallest form-factor data security card



Hifn announced Express DS 255, the industry's highest-performance, lowest-power and smallest form-factor data security card. Delivering the strongest industry-standard encryption for securing data-in-transit, the Express DS 255, easily handles today's encryption requirements and enables the next-generation network security applications. When applied to network security applications, the Express DS 255's accelerated performance can process SSL, IPsec and DTLS protocols at over 400K packets per second up to 2 Gbps. ([www.hifn.com](http://www.hifn.com))

## IBM Lotus Quickr file encryption solution

New Voltage SecureFile for IBM Lotus Quickr brings information encryption to documents within the Lotus collaboration environment. Voltage SecureFile for IBM Lotus Quickr offers several key benefits to customers that have deployed the IBM collaboration environment. The product enables businesses to secure information work-flows, protect the integrity of their brand reputation, ensure customer confidence, mitigate potential risk involved in a data breach and meet compliance regulations. ([www.voltage.com](http://www.voltage.com))



## Cisco ASA 5580 Series Adaptive Security Appliances

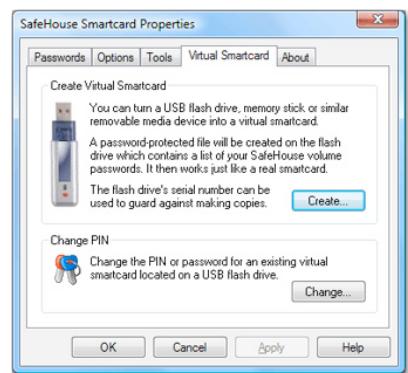


Cisco announced the availability of the Cisco ASA 5580 Series Adaptive Security Appliances, the company's highest-performing security appliance offering. The new Cisco ASA 5580 is a super-high-performance security platform equally well suited for deployment as a highly scalable firewall with up to 20 gigabits per second of throughput, as well as a 10,000 user remote-access concentrator for Secure Sockets Layer and IP Security based virtual private networks. ([www.cisco.com](http://www.cisco.com))

## SafeHouse 3.0 USB encryption

PC Dynamics announced the release of its new SafeHouse 3.0 data privacy and encryption software with dozens of new features including greatly-enhanced support for USB memory sticks. SafeHouse locks, hides and encrypts sensitive files and folders using passwords and super-strong encryption.

It is completely transparent to the way users work and is compatible with all Windows applications by masquerading as a password-protected Windows drive letter. ([www.pcdynamics.com](http://www.pcdynamics.com))



## New SafeWord 2008 two-factor authentication tokens



Secure Computing announced the immediate availability of SafeWord 2008, their new two-factor authentication solution. These easy-to-use tokens provide highly secure and cost effective access protection for information assets and applications through Citrix applications, VPNs, Web applications and Outlook Web Access. SafeWord 2008 is designed for the latest 64-bit

Windows environments, including Vista and Windows 2008 Server, with seamless integration to Microsoft Active Directory. ([www.securecomputing.com](http://www.securecomputing.com))

## Mobile security for UIQ devices

F-Secure released its Mobile Security product for the UIQ platform. F-Secure and Sony Ericsson are partnering on supplying mobile security to Sony Ericsson's smartphones. A trial version of the F-Secure Mobile Security 3.3 for UIQ will be available in selected Sony Ericsson UIQ devices. The companies will cooperate closely together in the area of mobile security to make sure that smartphones will continue to offer a safe and rich mobile computing experience. ([www.f-secure.com](http://www.f-secure.com))



## Remotely "murder" your stolen laptop



Alcatel-Lucent has developed a laptop security and management system – the OmniAccess 3500 Nonstop Laptop Guardian – that remotely secures, monitors, manages and locates mobile computers. If a laptop is reported lost or stolen, the solution can automatically destroy all data held on the device, even if the computer is turned off. The core technology of the solution

consists of a secure, 'always on' computing system residing on a 3G broadband data card which includes a completely separate secure operating system and battery, and operates over any broadband, 3G or WiFi network. ([www.laptopguardian.co.uk](http://www.laptopguardian.co.uk))

## WatchGuard upgrades software on its appliances

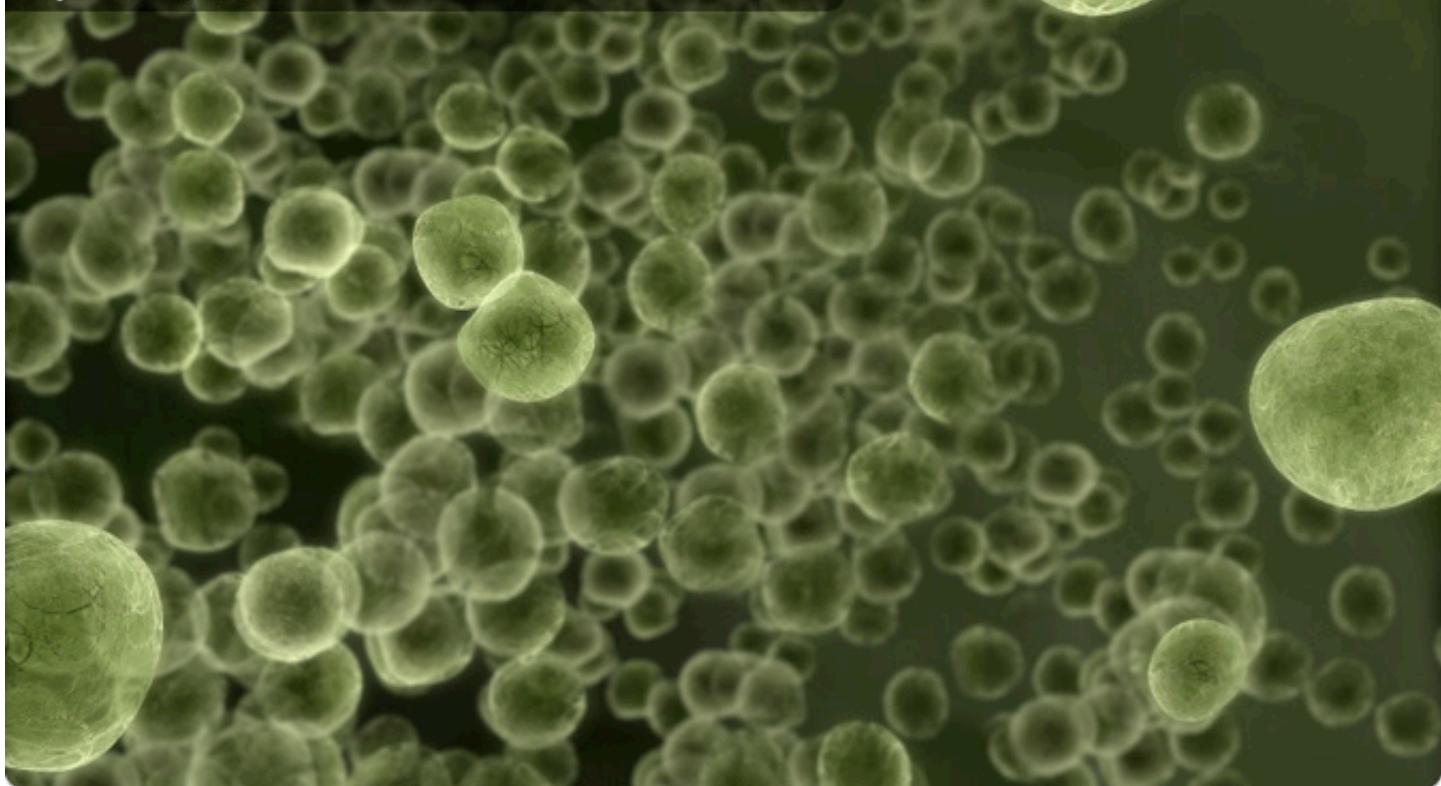
WatchGuard released the latest version of network security software for its Firebox X Peak, Core and Edge unified threat management appliances. Version 10 includes a myriad of new features to keep users securely connected to their network. For instance, Fireware 10 and Edge 10 now integrate SSL VPN functionality.

Further addressing secure mobility needs, both operating systems will support Mobile VPN for Windows Mobile devices, and for workers who use voice over IP or video conferencing, Fireware 10 and Edge 10 support SIP and H.323 connections. ([www.watchguard.com](http://www.watchguard.com))



# Proactive analysis of malware genes holds the key to network security

By Mark Harris



**During the last few months of 2007, some new entrants into the security market made a lot of noise about the impending death of the signature based virus detection offered by traditional anti-virus vendors.**

However, the reality is that this type of protection has already been dead for a long time, with the 'traditionalists' themselves killing it off in the early 90s, when viruses and malware stopped having distinct signatures. Since then, cybercriminals have continued to shift their focus from one-dimensional virus writing to multi-faceted malware creation, which is capable of infiltrating all possible routes into a company's corporate systems. These complex attacks mean that ever more proactive methods of detection and protection have been evolved in order to protect the integrity of corporate networks.

The growth in malware wheedling its way onto business networks has come about for one key reason – money. The days of awkward adolescents stowing themselves away in their bedrooms, feverishly inventing headline-grabbing viruses to gain notoriety and respect from their peers are long gone. Now, cash is the motivator, and cybercriminals are con-

stantly trying to create the next piece of malware that, instead of making the news, will slip through the net unnoticed. Hackers are therefore carrying out far more targeted attacks, which by their very nature are harder to detect, so dictate that a much more sophisticated approach to IT security must be adopted.

Another factor to consider is that the ubiquity of computers in the 21st century. Almost all businesses now rely on PCs and most homes have at least one computer. PCs are used for everything from business correspondence and social networking, to shopping and gambling and the sheer volume of confidential information now disclosed online offers rich pickings to cybercriminals. As most businesses now recognize the importance of protecting their data, cybercriminals have had to become more inventive in the methods they use to break through ever-tightening IT security defences and dupe innocent users.

One common tactic is to write as many variants of the same malware as possible. This makes it quick and easy to create and send out new attacks and the slight change in the code and behavior of each variant mean that it is much more likely to avoid detection by IT security solutions. The potential success of such tactics is clearly illustrated by the Pushdo Trojan horse. First detected in March 2007, Pushdo caused relatively little trouble for computer users until August when the authors started spamming out around four new variants every day. For the last five months of 2007, Pushdo consistently ac-

counted for around one fifth of all email-borne malware detected by Sophos.

### Signature based security is dead

Traditional anti-virus detection techniques look for patterns of code that are unique to known malicious executables. While this sort of detection by itself no longer offers sufficient protection against cyber attacks, most security solutions still rely on these malware signatures in part to identify different types of threats in order to defend networks against intrusion.

## A HOST INTRUSION PREVENTION SYSTEM (HIPS) IS THE KEY TO MORE RIGOROUS NETWORK DEFENSE

Anyway, these signatures can take many forms and are usually based on several sections within the program. For example, a signature might look to match three 50-byte areas of code, at specific offsets or locations within a file. The challenge when creating such signatures is to ensure that the areas of code detected as malicious by the security solution, are not in fact part of common libraries. Such a mistake could result in legitimate programs being labeled as malicious and not being allowed to run.

The disadvantage of this form of protection is therefore that no proactive detection of any sort can be offered. Fast paced, malicious malware, including zero-day threats which are released into the wild before security vendors can issue protection against them, can therefore sometimes slip through the net, resulting in infection of the corporate network, the consequences of which can range from corporate ID theft, to embarrassing headlines and hefty financial penalties.

### The HIPS solution

To comprehensively defend against all threats, it is therefore necessary to implement proactive security solutions that can protect and defend against attacks as soon as they are released; that is before a specific detection update can be written to secure the software against attack and, crucially, before the malware is even allowed to execute. Without this level of defense in place, fraudsters will con-

tinue to find success targeting business operation systems and applications.

A Host Intrusion Prevention System (HIPS) is the key to more rigorous network defense, and will effectively complement reactive solutions. These proactive solutions have been designed to stop malware before a specific detection update is released by monitoring the behavior of applications. Traditional HIPS systems achieve this by monitoring and looking for unusual or malicious behavior once applications are running.

Nevertheless, these solutions can fall down. As with signature based detection, it can be a challenge to distinguish between legitimate and malicious applications, as the simpler the malware the harder it is to identify it as such. This can cause problems because the HIPS solution will monitor code as it runs and will intervene as soon as code that is deemed to be suspicious or malicious is detected. Therefore, if malicious code is even allowed to run, it can wreak havoc on the corporate network before it is even detected. Furthermore, if a suspicious, but ultimately clean, application is monitored, any modifications that are made may have an adverse effect on the operating system. Stopping the execution could cause further problems. Another drawback is that this type of run-time analysis can only occur at the desktop or endpoint, and therefore offers no protection against malware entering via the email or web gateways.

## Beyond HIPS

Traditional HIPS systems then are a big step in the right direction, but further proactive protection needs to be put in place in order to ensure IT security solutions are able to effectively deal with all malware threats, both known and unknown. The next stage should therefore be to implement pre-execution scanning to determine what the functionality of the application is and what behavior it is likely to exhibit before allowing the program to run.

In addition to analyzing run-time behavior, with such a solution it is also possible to determine and assess static characteristics which can also be indicators of malicious behavior. For example, resource information such as details of the software publisher – strings embedded in the application – can be used to ascertain the validity of some programs.

## The gene building alternative

One way of implementing effective pre-execution scanning is to effectively identify each individual characteristic as a gene. Whilst in biological terms, genes are the building blocks that make up individual species, in technology terms, they are the building blocks of executable programs.

Using behavioral genotyping solutions, businesses can be safe in the knowledge that their data and networks are protected from attack, as all files will be rigorously scanned, with hundreds of genes extracted for microscopic analysis. Rather than looking for individual characteristics, these solutions identify combinations of genes to enable the classification of new malware. By extracting genes from existing malware, it is possible to identify the common characteristics and the combinations in which they are used in malware. This knowledge enables security experts to pinpoint new genes that have never previously appeared, therefore ensuring they can be quashed before future attacks are attempted.

Still, to ensure precision, the best solutions will also look at the genes that are seen in known safe files; these are executables that are known to not be malicious. By comparing the combinations that are found in malware but that never appear in clean files, the risk of

incorrectly identifying a file as malicious when it is actually safe, can be dramatically diminished.

## Giveaway genes

A key benefit of adopting of this behavioral genotyping approach is that there are some giveaway genes, which can be used to quickly identify the presence of malicious code. For example, it can be used to decode ‘packer’ tools, which are frequently used by cyber-criminals to disguise the contents of their attacks. Packers are compression tools that reduce the size of executable files, thereby enabling fraudsters to compress and hide the contents of these files in an attempt to bypass security applications.

This method also has the added benefit of making the files easily modifiable, making traditional signature-based detection methods ineffective and redundant. While sophisticated signature-based detection will eventually decode the packing algorithm, enabling the solution to descramble the contents of the file, by the time this happens, malware authors will more often than not have already moved on to the next packing algorithm.

The way in which an application is packed can be a strong indication that its content is malicious – Sophos research has shown that 21 percent of all malware it detects is packed, but only one in every 100,000 clean files are packed. Packing is one ‘gene’ that is assessed during the scanning and analyzing process. Other genes include which programming language is used, the ability to access the internet, copy files, add registry entries or search for publisher information. Simply put, if an application is packed, written in Visual Basic, accesses the internet and contains references to banking websites, there is a significant chance that it is a banking Trojan horse.

## Key advantages of proactive techniques

This method of gene detection is flexible enough to adapt as malware authors’ techniques evolve. When authors implement a new method, it is frequently identified as a new gene, and security experts can then analyze it in conjunction with existing genes

to effectively detect many new variants of a malware campaign, rather than simply the original attack. This type of examination also has the added benefit of offering protection at the email and web gateway, as well as at the desktop, since analysis can be carried out without even executing the code. Furthermore, sophisticated HIPS systems can also detect and prevent zero-day threats without the need for signature updates, ensuring that these attacks are stopped in their tracks before they can cause serious mayhem.

### The Storm worm example

A good example of modern sophisticated proactive detection at work is given by the Storm worm outbreak that started in October 2006 and is still continuing to cause infections. There were hundreds of variants, including the prolific Dorf and Dref worms, and in one fell swoop, a single behavioral genotype identity detected nearly 5,000 different, unique variants. Using traditional signature-based, reactive techniques would have taken considerable resources and energy – not to mention time. The time saved ensured that the variants created by the hacker were able to gain ac-

cess to far fewer systems than if signature-based testing alone had been implemented.

### Conclusion

Proactive detection is already central to the most effective security solutions, but organizations need to be aware that not all HIPS technology is the same. It is crucial to implement a solution that examines code before it executes as well as when the application is running. Without this dual method of analysis, malware could slip through the net, and network issues could arise if a file has incorrectly been identified as malicious when it is actually safe.

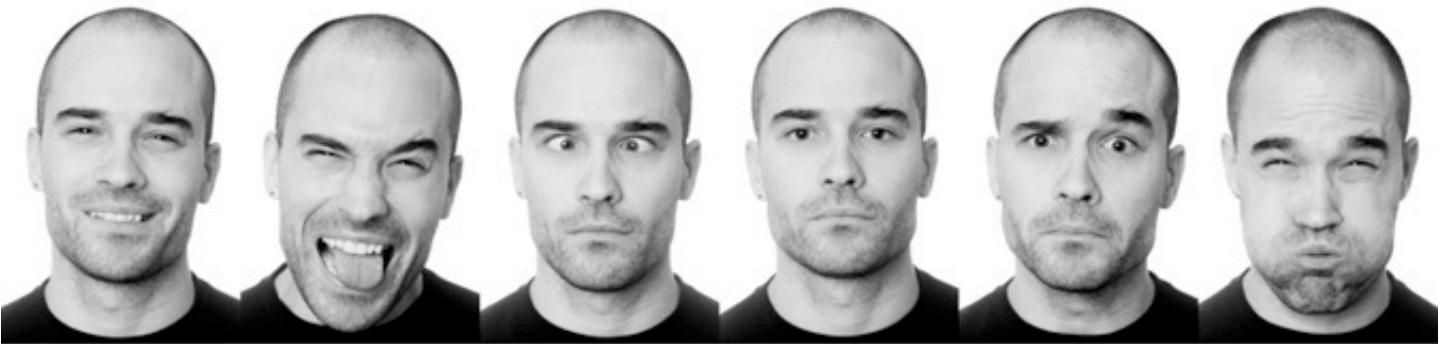
If IT managers are aware of the breadth and cause of threats silently trying to infiltrate corporate networks every minute of the day, they will have a clearer understanding of what action needs to be taken. If businesses take control of their security and realise the importance of proactive detection methods, they will reap the benefits, resting safe in the knowledge that they are doing everything in their power to thwart malware attacks of all kinds.

Mark Harris is the Global Director of SophosLabs. Based at Sophos's global headquarters near Oxford, UK, Mark manages the company's worldwide threat analysis teams, which deliver round-the-clock anti-malware protection to the company's worldwide customer base. He joined Sophos in 2005, prior to that he was Director of Engineering at McAfee.

**Hacking naked since 2005 - [www.pauldotcom.com](http://www.pauldotcom.com)**

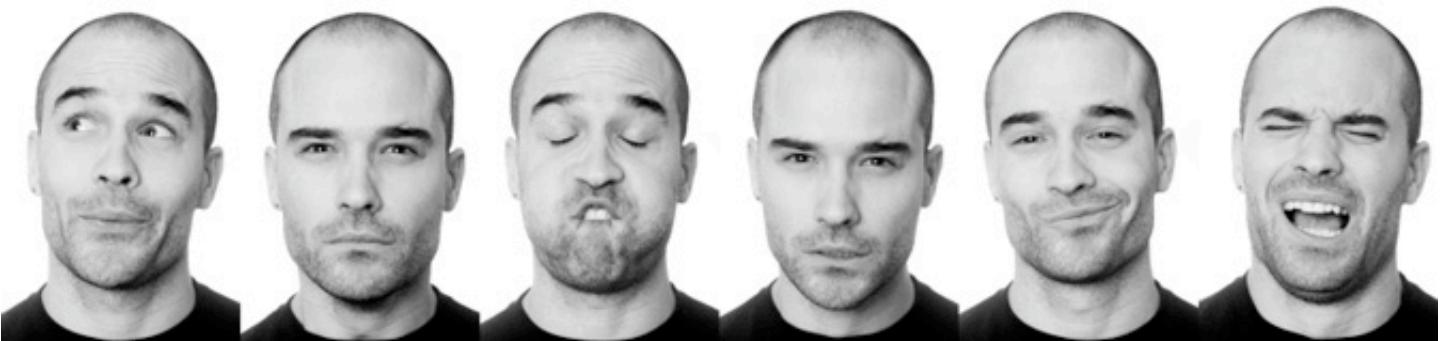


**PaulDotCom Security Weekly: A podcast covering the latest security news, vulnerabilities, and research.**



## Advanced social engineering and human exploitation, part 1

By Mike Murray



**When I go out in the world and talk about social engineering, many people are amazed by what kinds of influence are actually possible on the people around them. And, yet, when I read the common books and online resources about social engineering, two basic messages are repeated over and over again:**

***"If you want success as a social engineer, just ask for what you want"***

***"If you want to be successful, just pretend to be somebody obvious who can't be verified (like a help desk or IT guy)"***

I repeatedly read this, and I find it discouraging. I talk to some of the luminaries in the security field or read their blogs and the things that they hold up as the “pinnacle” of social engineering are the simplest and the most ridiculous attacks I have seen. It’s as though we, as an industry, look at social engineering the same way that the major media looks at DDoS attacks and website defacements; the simplest and least impressive technical attacks are heralded as a big deal. And it is the same sort of ignorance that leads to the current state of knowledge about social engineering.

Most of what is on the news and in the books on social engineering is really the “script kid-die” version of social engineering. In most cases, it is no more impressive than someone downloading a ‘sploit off of PacketStorm and running it against a bunch of websites. While

this stuff works against truly easy or unprepared targets (exactly like most canned exploits), it tends to fail against truly hard targets.

Unfortunately, this tends to give everyone a false sense of security. A friend of mine likes to say that penetration tests are ultimately tests not of the organization’s security, but of the skill of the penetration tester. Nowhere is this more true than in social engineering: and the state of skill of most social engineers is truly dismal. Even the greats of the industry have incredible natural talent but little understanding of how and why they are successful.

I hope, through this series of articles, to expand what you see as possible. And, hopefully, that enhanced awareness will push the bar higher in the industry - for all social engineers to see a need to upgrade their skills

in influence, so that when organizations test their security by employing social engineers, they are actually finding the places in the organization where there is resistance to a genuinely skilled attacker.

## What real social engineering looks like

*"ABC Drug franchise help line. How can I help you today?"*

Thus began a social engineering engagement that remains legendary to this day (to the 10 or so people privy to the details). The company had been engaged to work with a major drug store chain whose business was a franchise operation. And, like most franchise operations, their crown jewels were all contained in the manuals and business processes a store uses to operate.

This company had invested a huge amount in protecting this information electronically. Encryption, access control, least privilege - they had done it right. And they were confident that the consultant that they hired to test their security would be unable to get the information.

Then they met Christine (not her real name). She picked up the phone one night and called the help line that was available for those who were legitimate franchisees.

*"Umm... hi", she started. "So, uh.... like, yeah... my boss got a franchise, and I had the kit sent to the wrong address. He's going to kill me."*

From there, through the course of a half-hour call, she didn't just obtain a copy of the franchise kit, she convinced the help line person to enter an entirely new franchise into the system. She was **given** a drug store.

Normally, a drug store franchise for this company is priced in the multiple six-figures. In 30 minutes, she convinced him to give her one. Suffice it to say, the client was happy. And scared.

Note that she didn't get the franchise by "just asking for it", nor pretending to be someone in the right position. Sure, she used both tactics. But most social engineers couldn't have dreamed of pulling it off. She did it by using

the skills of a really advanced well-trained social engineer.

## Social engineering - a definition

First, I should define what "social engineering" really is. The definition that fits best is a simple one: "the use of skills of influence and misdirection to obtain information or access that is generally inappropriate". While there are more complex definitions, this one cuts right to the heart of the matter.

Note that this type of activity can happen in ANY media. While most think of the social engineer as someone who is using face-to-face methods or phone calls, a phishing attack or an exploit triggered by getting a user to a website all fall under the same definition. Indeed, many of the most sophisticated social engineering engagements that I have been involved in have included some measure of technological exploitation to extend or enhance the use of influence or misdirection.

## The three defining skills of a social engineer

So, what are these skills of influence and misdirection that I keep referring to? When you observe and analyze the work of many social engineers, you can ultimately describe every engagement and every act of social engineering in terms of only three skills:

- 1. Language:** The ability to use words artfully
- 2. Awareness:** The ability to understand the effect of one's actions on other people
- 3. Framing:** The ability to manipulate contexts or "frames".

These three skills are present in every great social engineer. In every case, the better a social engineer is, the more complete their skill sets are in these areas. A social engineer who is deficient in any of the areas will have difficulties in many engagements.

The rest of this article is going to describe the skills in each of these areas. The lessons here are going to be drawn from a variety of disciplines. First, my experience in social engineering, but also training and experience with psychology, hypnosis, neurolinguistic programming, neuroscience, economics, and stage

magic. With some smattering of marketing, sales and PR (because who else is better at getting their ideas in to people's heads?).

## Language - a model of reality

*"Language can both represent reality and shape it."* Linda Ferguson and Chris Keeler, NLP Canada

Language is not real. While that may seem like an obvious statement (as you know the difference between an apple and the word "apple"), most of us often treat language as a very, very close analogue to reality. In fact, as pointed out by the quote above, language often can affect reality, especially when used artfully. If it couldn't, there would be very little reason for you to be reading the words on this page right now - my words are shaping your version of reality as you read this.

The reason that language shapes reality is that language acts as a mental model of the world. In fact, the mind actually processes language as though it is real. As you hear or read, your mind processes the language into a representation of the experiences being described. Neuroscience has shown that what is vividly represented in the mind is actually processed by the mind *as though it is actually happening*. As an example, if I vividly describe to you the experience of eating an apple, your mind will engage many of the same neurons as would be engaged if you were actually eating the apple.

This ability is the basis of the human ability to process language. It is also the basis of the ability of one person to influence another. But more on that in a minute...

## The reason that language shapes reality is that language acts as a mental model of the world.

First, there's a big problem. Language is an utterly incomplete model of reality. The use of the term "model" is an apt one - much like a model of a race car is similar to the actual race car, the linguistic representation of an experience is similar to the actual experience. But it has a different scale, has things left out, and is distorted in particular ways. When building a model race car, there is also a purpose - namely, to be able to keep the race car on your shelf rather than in your garage.

With language, the reasons for these distortions are similar - language would be incredibly burdensome if you tried to make an even moderately complete version of the most trite experience.

For example, back to the idea of eating an apple: imagine making a complete description of even one bite of the apple: how it felt to open your mouth, the feeling of your lips on the apple, the pressure on your teeth as you start to bite in to the apple, then the feeling of saliva being excreted and the feeling of each set of taste buds, etc. And that wasn't even close to a description, as it left out the sounds, the smells, sights, etc.

What you would probably say, most of the time, is: "I bit in to the apple." Behind that statement, you have left out a **huge amount** of information. Imagine, for a second, what level of information is deleted with a statement like "I'm happy."

## The two acts of language

Language is treated as real by the mind. And it's horribly incomplete. These are two of the most important things for any social engineer to know, because it is the ability of the mind to treat language as real that enables you to actually influence people and get the access you want. It is the incompleteness that creates the opportunities to use language in artful ways to create that influence. But there are two different sets of rules - one for each action of language. Every linguistic act can be isolated into one of two purposes: the act of information transfer and the act of influence.

Information transfer is what you probably spend most of your time doing when using language. Most of the time, you are either telling someone something or requesting that they tell you something - pulling information

from people or pushing information to them. Nearly every statement in this article has been an act of information transfer (including this sentence). Most sentences are designed to provide a piece of information to you that you can assimilate and remember.

The rest of your time, you spend working to influence someone to change their opinions or positions on something. In that case, you are not conveying nor requesting information, but

attempting to change the thinking of another. Note that these linguistic acts are not usually the province of logic or rationality. This is the domain of the emotions (neurologically speaking, the amygdala). I am not speaking of a logical argument - much of the time, logical debate comes down to information transfer. True acts of influence attempt to influence the decision-making machinery in the brain through the altering of the model of a person's reality.

## **When making statements, the aim is to make statements as precise as required for the purpose of the communication.**

### **Information transfer**

The act of information transfer is, as I intimated above, bidirectional. Information can be transferred to someone with what you say (by telling them), or you can request information from them. Above all, the goal is to overcome the incompleteness of the language that the person is using. For example, imagine the following exchange:

Target: "*I can't tell you my password.*"  
Social Engineer: "*Why can't you?*"  
Target: "*It's against policy.*"  
Social Engineer: "*Which policy?*"  
Target: "*The information security policy.*"  
Social Engineer: "*You have an information security policy? What does it say?*"  
Target: "*It says not to reveal passwords to unauthorized staff.*"

Note that, for each of the questions asked by the social engineer, she is requesting a piece of information that was left out of the previous statement that the target made in order to make the information more precise. This is the fundamental rule of information transfer: precision. When making statements, the aim is to make statements as precise as required for the purpose of the communication. And when requesting information, the goal is to obtain information at the level of precision that is appropriate for the purpose of the conversation.

### **Influence**

While information transfer is important, influence is the true domain of a great social engi-

neer. Where precision is the fundamental concept of information transfer, the fundamental concept of influence is agreement. This is not agreement in the sense of logical, rational or conceptual agreement, but the act of ensuring that your language creates a situation where a statement (or set of statements) is not possible to disagree with. One of the major defense mechanisms in the mind is that of disagreement - if I say something that you can disagree with, you are immediately aware of the content of the sentence. If, however, I were to say something that you couldn't disagree with, the content in the statement will slip in to your mind completely intact.

This is easier to show through example. Which of these statements do you agree with?

*"I could imagine that you have a sensation in your hand."*

*"I know that you have a stabbing pain in your right hand."*

Even if you happen to have a stabbing pain in your right hand at this moment, you are definitely in agreement with the first sentence. And, as you read the first sentence, you probably became (even though only momentarily) aware of the sensation in one of your hands. While, in the second statement, your reaction was probably a more simple one: "Nope, no pain."

It is this "artful vagueness" that is repeatedly mocked in business speak or "market-ese", but the reason that this language is used is that it is impossible to disagree with.

For example, what company in the world could not use this as a mission statement:

*"We aim to be the value-added leader in business solutions."*

While this language seems ridiculous, this same language is used to allow you to create representations in your mind while always remaining in agreement with the social engineer (or marketer). For example, imagine that you and I are on a social engineering engagement and I am trying to convince you to give me your password (or a drug store franchise). I could say something like:

"I know it could seem strange for me to ask this of you. But you can imagine that it is difficult for me to be asking and how it would feel to be under the pressure that I'm under from

my boss and how much I need your help right now, and how it would be for you to need my help so badly. And you could imagine that in the same situation, your human kindness will be a wonderful benefit and how great that will make you feel!"

Note that I used a few patterns in that example that made the statement impossible to disagree with ("It could seem...", "You can imagine...") - this makes the statement a wonderful exploit for the human mind.

While I could talk about this in far greater detail, this article is getting long. Next time I'll go into detail about the other two skills of social engineering - awareness and the ability to create a frame. And how to put this all together in to a social engineering engagement that really works.

Mike Murray is an experienced social engineer, trained hypnotherapist, and long-time information security professional. He currently is the Director of Neohapsis product testing lab, and is the author of the upcoming book "Social Engineering: Advanced Human Exploitation". Read his blog at [www.episteme.ca](http://www.episteme.ca).



# OWASP

The Open Web Application Security Project

**JOIN US!** OWASP is a free and open community dedicated to improving application security for everyone.

You'll find free tools, books, articles, best practices, mailing lists, conferences, and local chapters around the world to help you build secure code.

[www.owasp.org](http://www.owasp.org)

# Free visualization tools for security analysis and network monitoring

By Sam Abbott-McCune, A.J. Newson, Robert Ross, Ralph Ware, and Gregory Conti



**Whether you are a security analyst, system administrator or technical manager, chances are you are confronted with an overwhelming sea of security related data. Typically, we analyze this data with textual reports, command line scripts, or simple pie graphs and bar charts. However, there are much richer ways to analyze and explore the data using information visualization techniques. Information visualization systems attempt to create insightful and interactive graphical displays that exploit the human's extremely powerful visual system.**

If done correctly, users will be able to examine more data, more quickly and see anomalies, patterns and outliers in ways that textual data simply cannot provide and machine processors cannot detect.

In this article, we present a number of free visualization systems that you can use to help find insight in your data. Where applicable, we've also included links to other tools you may wish to explore. In order to provide a broad overview of available options, we've sought out tools across a number of security related domains, including: network visualization, packet visualization, network management, and port scan visualization, as well as general purpose tools that can be used with many types of security data.

## Network visualization

The Interactive Network Active-traffic Visualization (INAV), see Figure 1, is a monitoring tool that allows network administrators to monitor traffic on a local area network in real-time without overwhelming the administrator with extraneous data. The visualization tool can effectively perform a variety of tasks from passively mapping a LAN to identifying reoccurring trends over time.

Currently, INAV supports Ethernet, IP, TCP, UDP, and ICMP. INAV is implemented using a client-server architecture that allows multiple administrators to easily view network traffic from different vantage points across the network.

Once established, the INAV server passively sniffs data from the network and dynamically displays activity between different nodes on the network while keeping statistics on bandwidth usage.

The current state of the network is stored and broadcast to the different INAV clients. The INAV client uses an intuitive, lightweight graphical user interface that can easily change views and orient on specific clusters of nodes. Once a node on the network is selected, the client highlights any node that has sent traffic to or from that location. The client receives the current state of the network with a variable refresh rate that is adjustable to limit INAV generated communications on the network. Installation of the tool is straight forward and its op-

eration is very intuitive. The INAV server runs on any Linux operating system with root privileges, while the client was developed in Java and can be run on most operating systems.

You can download INAV at [inav.scaparra.com](http://inav.scaparra.com) and a detailed white paper is available at [inav.scaparra.com/docs/whitePapers/INAV.pdf](http://inav.scaparra.com/docs/whitePapers/INAV.pdf). You may also wish to explore other network visualization systems including Afterglow ([afterglow.sourceforge.net](http://afterglow.sourceforge.net)), Doomcube ([www.kismetwireless.net/doomcube](http://www.kismetwireless.net/doomcube)), Etherape ([etherape.sourceforge.net](http://etherape.sourceforge.net)), FlowTag ([chrislee.dhs.org/pages/research/projects.html#flowtag](http://chrislee.dhs.org/pages/research/projects.html#flowtag)), and Packet Hustler ([shoki.sourceforge.net/hustler](http://shoki.sourceforge.net/hustler)).

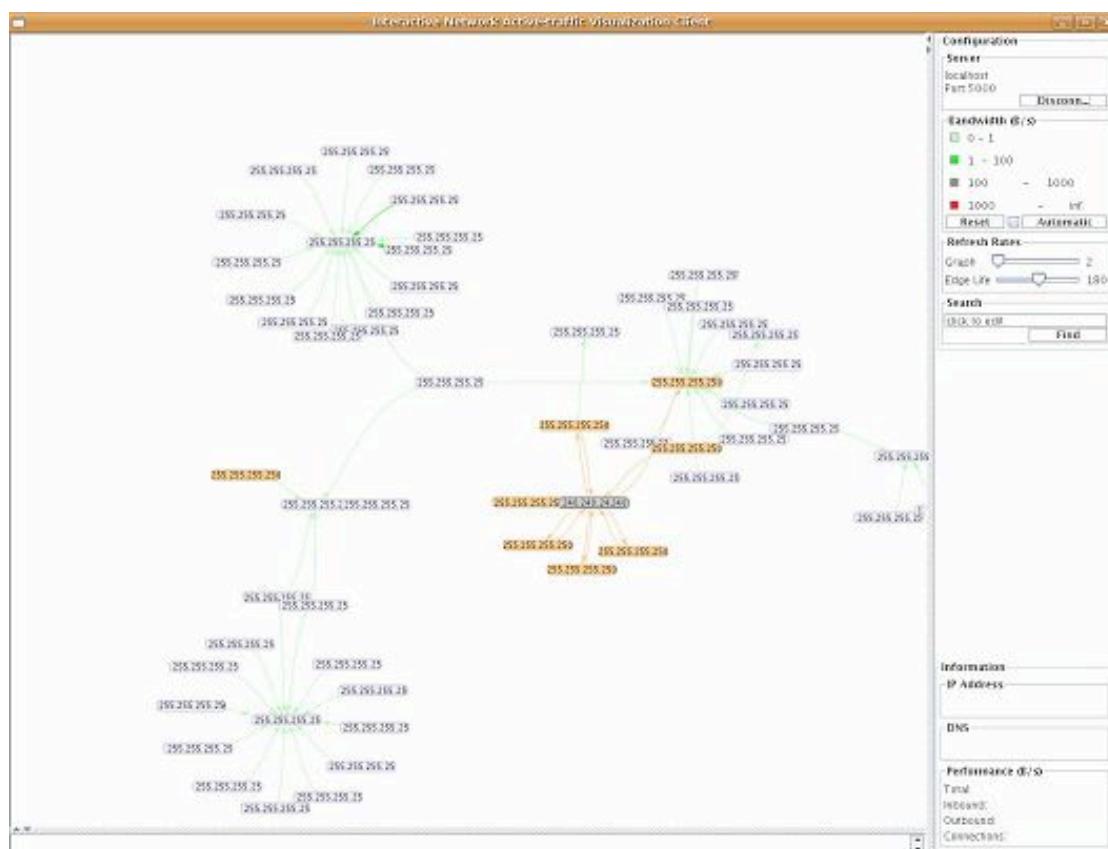


Figure 1: The Interactive Network Active-traffic Visualization (INAV) system passively sniffs network traffic and dynamically creates network graphs.

## Nmap visualization

The fe3d network visualization tool, see Figure 2, is an open source application that works in conjunction with nmap and presents scan results using a 3-dimensional cone tree visualization (see [citeseer.ist.psu.edu/308892.html](http://citeseer.ist.psu.edu/308892.html) for more information on cone trees).

Fe3d can be used with either imported nmap XML scan files or, alternatively, the user may launch and observe scans in real time. It also allows the user to routinely monitor network nodes for security issues such as open ports without requiring textual analysis. Fe3d gives the user the same scan results as command-line nmap, but in a very intuitive, easily understood 3-dimensional visual format by

graphically portraying the network node's operating system, IP address, and all open ports found on the node. This tool requires the following additional open source applications, Xerces-C++ XML parser ([xerces.apache.org/xerces-c/install.html](http://xerces.apache.org/xerces-c/install.html)) and wxWidgets([www.wxwidgets.org/downloads/](http://www.wxwidgets.org/downloads/)). We initially encountered difficulties interfacing the XML parser and wxWidgets on Linux op-

erating systems, but found Windows installation to be quite straightforward, although we recommend that you use a recent version of Microsoft Visual C++ for easier installation. If interested in installing and testing fe3d go to [projects.icapsid.net/fe3d](http://projects.icapsid.net/fe3d). There you will also find very well written installation and configuration instructions.

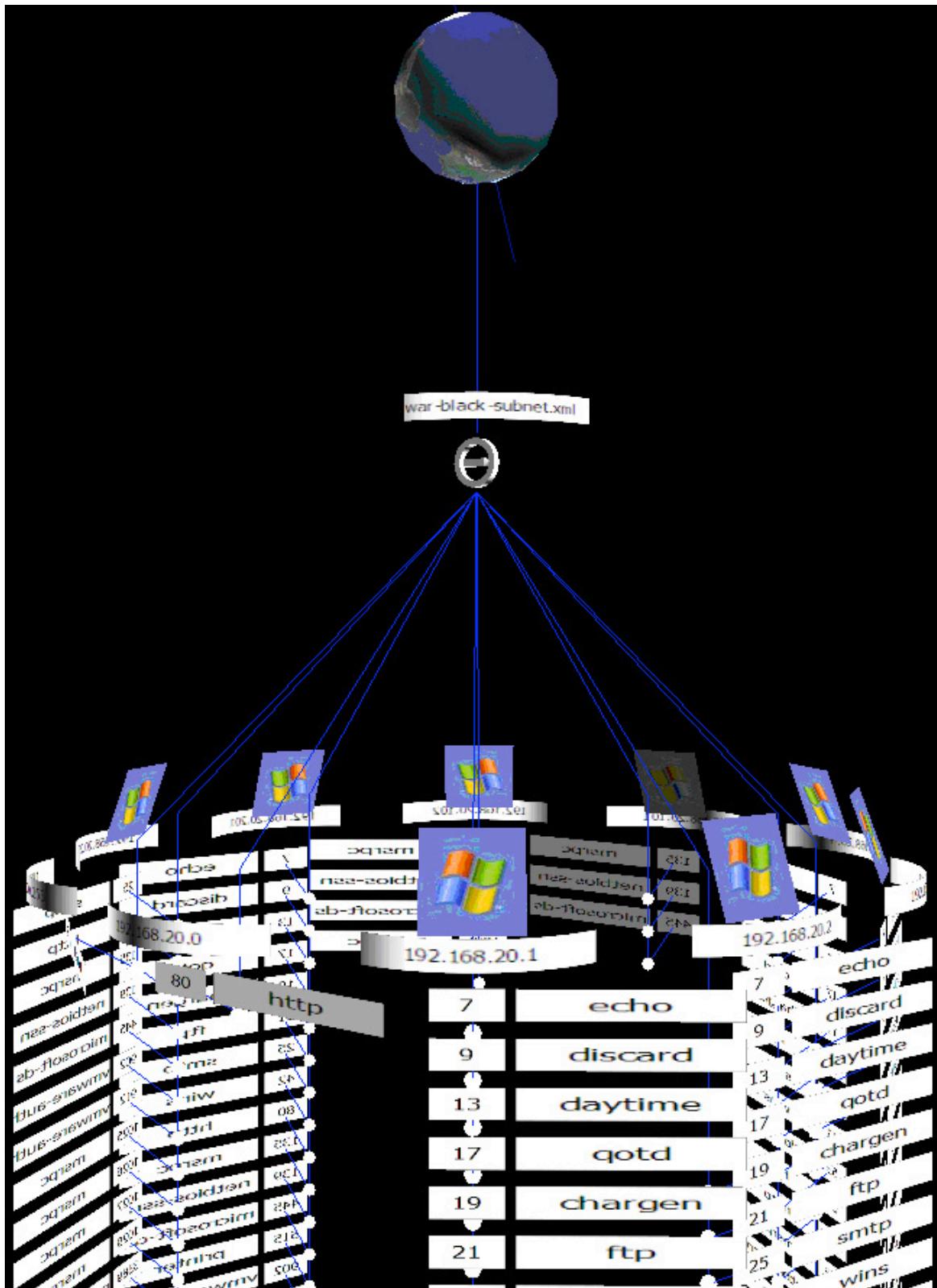


Figure 2: The fe3d visualization tool acts as a 3D front end for nmap scans.

## Network monitoring

There are a wide range of tools for network monitoring that give a graphical overview of activity on the network. One of the original tools on the market was WhatsUp Gold ([www.whatsupgold.com](http://www.whatsupgold.com)). WhatsUp Gold is a robust and scalable, but expensive monitoring system.

Although WhatsUp Gold is a quality product, we found that OpManager ([www.opmanager.com](http://www.opmanager.com)), see Figure 3, provides most of the same functionality in addition to being available as freeware for network administrators of less than 10 critical systems. Available for Windows and Linux platforms, OpManager installs a password protected webserver on the designated host, which is accessible from any client on the network. Some of the OpManager's functionality includes: WAN monitoring, services monitoring (Web, FTP, SMTP, LDAP, DNS, and more),

application monitoring (MySQL, Microsoft Exchange, among others), Windows Services monitoring (IIS, DHCP Server, Event Log), URL monitoring, server, and switch monitoring, among other functionality. The network status is clearly represented by numerous reports and customizable network displays. OpManager is fairly intuitive and easy to set up.

Another product to try is Nagios ([www.nagios.org](http://www.nagios.org)). Nagios is Linux-based and Firefox-friendly. However, Nagios can be difficult to setup initially, but if you are familiar with PHP include files (.inc), then subsequent networks can be easily configured. Nagios is also a web-based client/server package which gives near real time updates. Another software package that is worth checking out is OSSIM ([www.ossim.net](http://www.ossim.net)). OSSIM is a Linux-based solution which goes beyond simple monitoring by integrating software such as Snort and Nessus.



Figure 3: The free version of OpManager lets a network or system administrator monitor up to 10 hosts.

## Packet visualization

Wireshark ([www.wireshark.org](http://www.wireshark.org)) is the best of breed tool for protocol analysis and provides a powerful text-based GUI for analyzing network traffic captures.

RUMINT ([www.rumint.org](http://www.rumint.org)), a prototype graphical network sniffer, takes a different approach. It lets an analyst compare large numbers of packets, including both header fields and payloads, using seven different visualization windows.

Figure 4 shows a parallel coordinate plot (top left) that allows comparison of up to 19 packet header fields, a binary rainfall view (top right) which plots the raw bits from each packet and a text rainfall view (bottom left) which uses Unix strings-like functionality to display printable ASCII characters, one packet per horizontal row, as well as a detail view (bottom right) to see a single packet in hexadecimal and ASCII. Not shown are three additional visualizations, a scatter plot that plots any combination of packet header fields on a two-dimensional display, an animated visualization

of packets emanating from ports and IP addresses, and a byte frequency visualization that displays a scrolling graph of bytes contained within each packet. RUMINT uses a VCR metaphor, where an analyst loads a packet capture file and “plays” back the packets in the visual displays. Because it is a prototype, RUMINT lacks the robust filtering and protocol parsers included with tools like Wireshark and is limited to 30,000 packets. It runs on Windows XP and later systems, but has been used successfully on Linux using Wine.

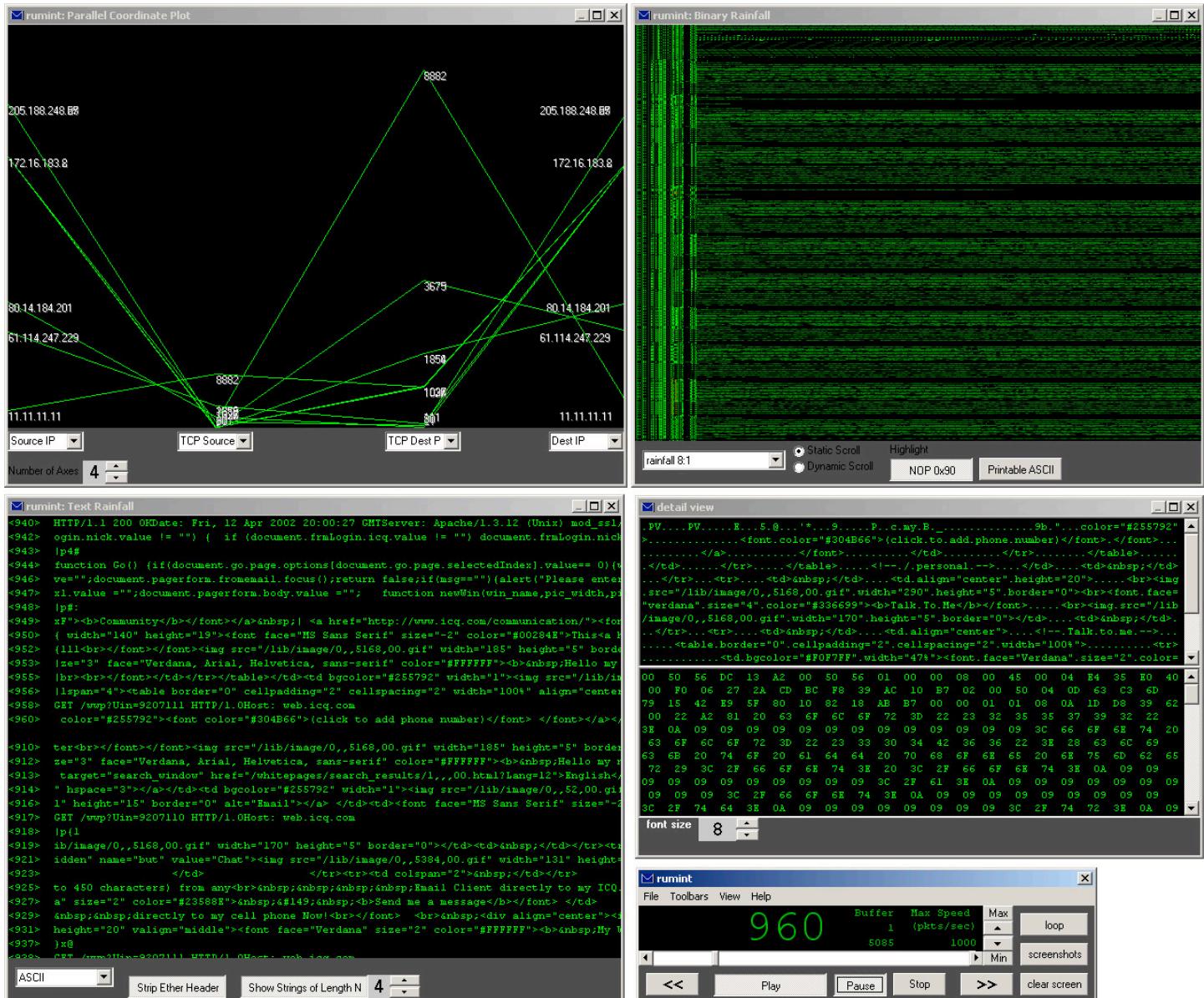


Figure 4: The RUMINT Visualization tool lets you capture and visualize network packets in real time.

## General purpose visualization

Many Eyes is a free service offered by IBM and is an efficient and simple web-based application that incorporates numerous visualiza-

tion techniques and facilitates collaborative analysis of security data. For example, after you collect network traffic from a tool such as Wireshark you can output the data to a comma separated value (CSV), upload it to

Many Eyes and view it using a number of interactive visualizations. (Note that a spreadsheet, such as Excel, can be very useful as an intermediate step to enhance or clean-up the dataset). A simple data table with named columns, each of the same length is required. Each column in the table supports two data types, text or numeric. You upload your data to Many Eyes via an HTML form by copying and pasting your data set.

Although Many Eyes has a dozen different types of visualization components, the network graph and treemap often provide the best insight into network traffic. Once a data

set is uploaded to the Many Eyes server, you simply select a desired visualization component, allowing for flexible exploration.

Figure 5, is a snapshot of a network data capture from a Defcon Capture the Flag competition shown using the graph visualization component. The data set presented in this visualization contains the source and destination IP address of each packet. The Java applet is interactive and allows you to pan or zoom the view of the visualization as desired. Selecting a node, shown in orange in the figure, highlights all adjacent nodes to facilitate analysis.

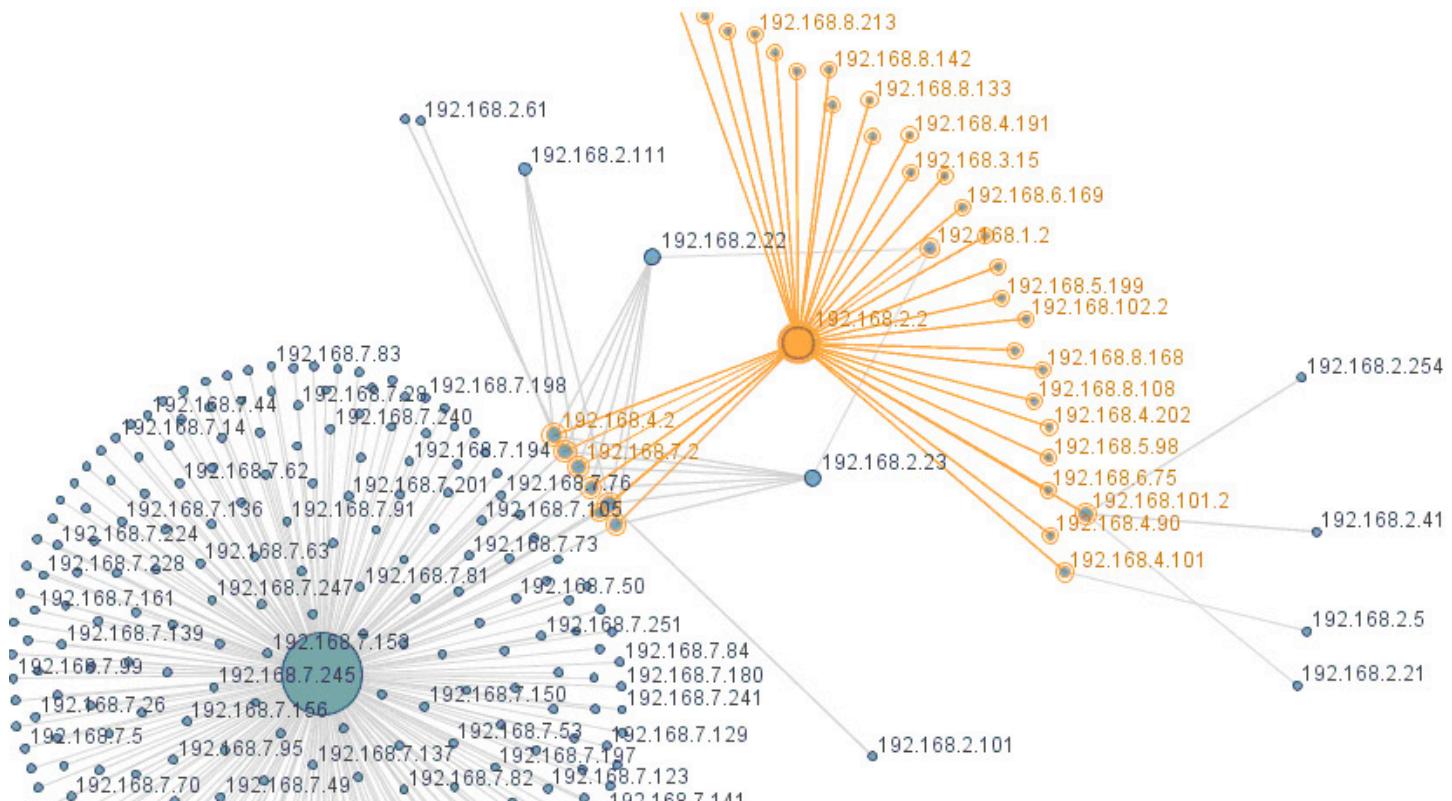


Figure 5: Using the Many Eye's visualization tool to graph a Defcon Capture the Flag Dataset.

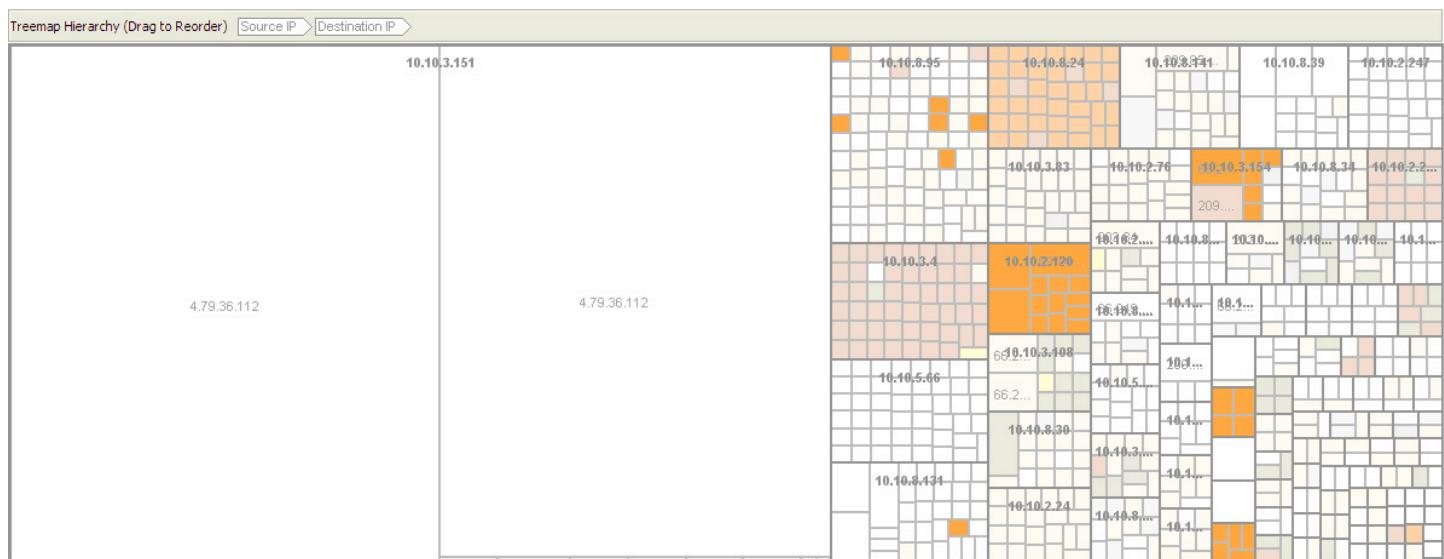
On the following page is a snapshot of a similar network data capture, but using a treemap visualization technique. Treemaps are useful for visualizing hierarchical data, such as network addresses, as nested rectangles.

In the case of Figure 6 on the following page, the rectangles contain destination IP address, where the size of each rectangle corresponds to the quantity of packets, and the color corresponds to the destination port, where white is used for lower port numbers and dark orange for higher values. This visualization provides

an alternative way to look at network data that can quickly identify patterns or anomalies, that a graph-based visualization cannot.

The benefit of Many Eyes is that it allows experimentation with a large number of visualization techniques and supports public collaborative analysis.

Registered users of Many Eyes (note that registration is free) can view, post comments and create additional visualizations based on a given dataset.



Unfortunately, at this time, there is no way to make a dataset or visualization private. Because of this issue, many network administrators may be reluctant to post data associated with their network. We leave it up to you to balance the risk of sharing your data against

the strength of ManyEyes' visualization techniques and collaborative analysis facility. If you like Many Eyes, you may wish to explore other similar offerings such as Swivel ([www.swivel.com](http://www.swivel.com)) and the Google Chart API ([code.google.com/apis/chart](http://code.google.com/apis/chart)).

Name	Notes	URL
Afterglow	Graph visualization	<a href="http://afterglow.sourceforge.net">afterglow.sourceforge.net</a>
Doomcube	3D IP address and port visualization	<a href="http://www.kismetwireless.net/doomcube">www.kismetwireless.net/doomcube</a>
Etherape	Network graph visualization	<a href="http://etherape.sourceforge.net">etherape.sourceforge.net</a>
fe3d	nmap visualization	<a href="http://projects.icapsid.net/fe3d">projects.icapsid.net/fe3d</a>
INAV	Visualization of network bandwidth, source and destination nodes	<a href="http://inav.scaparra.com">inav.scaparra.com</a>
FlowTag	Visualization of network flows	<a href="http://chrislee.dhs.org/pages/research/projects.html#flowtag">chrislee.dhs.org/pages/research/projects.html#flowtag</a>
Google Chart API	Allows creation of dynamically generated charts	<a href="http://code.google.com/apis/chart">code.google.com/apis/chart</a>
Many Eyes	General purpose visualization tool, accepts most CSV data	<a href="http://services.alphaworks.ibm.com/manyeles">services.alphaworks.ibm.com/manyeles</a>
Nagios	Network monitoring	<a href="http://www.nagios.org">www.nagios.org</a>
OpManager	Network monitoring	<a href="http://manageengine.adventnet.com">manageengine.adventnet.com</a>
OSSIM	Network and security data monitoring	<a href="http://www.ossim.net">www.ossim.net</a>
Packet Hustler	Network traffic visualization	<a href="http://shoki.sourceforge.net/hustler">shoki.sourceforge.net/hustler</a>
RUMINT	Packet-level sniffing and visualization	<a href="http://www.rumint.org">www.rumint.org</a>
Swivel	General purpose charting tool	<a href="http://www.swivel.com">www.swivel.com</a>
Wireshark	Best of breed protocol analysis tool.	<a href="http://www.wireshark.org">www.wireshark.org</a>

## Conclusion

Security data visualization is an active area of research. In the near future expect to see tools that not only present data in insightful ways, but also help bridge the gap between human analysts and machine processing.

Human time and attention are a precious resource

Researchers are currently developing tools that allow insights made by human analysts to be offloaded to machine processors.

A good example is a tool that facilitates analysis of a new malware variant and allows the analyst to immediately generate a Snort signature.

We encourage you to evaluate the tools listed here, see Table 1, but more are being developed frequently. Two places to monitor for the latest developments are [www.secviz.org](http://www.secviz.org) organized by Raffy Marty and [www.vizsec.org](http://www.vizsec.org) sponsored by SecureDecisions ([www.securedecisions.com](http://www.securedecisions.com)). For the latest security visualization research consider partici-

pating in the annual VizSEC Workshop ([vizsec.org/workshop2008](http://vizsec.org/workshop2008)). The next VizSEC will be held in Boston on September 15, 2008 in conjunction with the Recent Advances in Intrusion Detection (RAID) Symposium.

One final note, we are currently in the process of attempting to catalog all open source security visualization projects, current and historical, if you have a suggestion please feel free to send an email to [gregory-conti@usma.edu](mailto:gregory-conti@usma.edu). We will freely share the results of the survey with the security community.

Sam Abbott-McCune is currently an Instructor, teaching Information Technology, Network Systems Management and Theory and Practice of Military IT Systems, at the United States Military Academy at West Point. He received his Master's Degree in Computer Science from Virginia Commonwealth University.

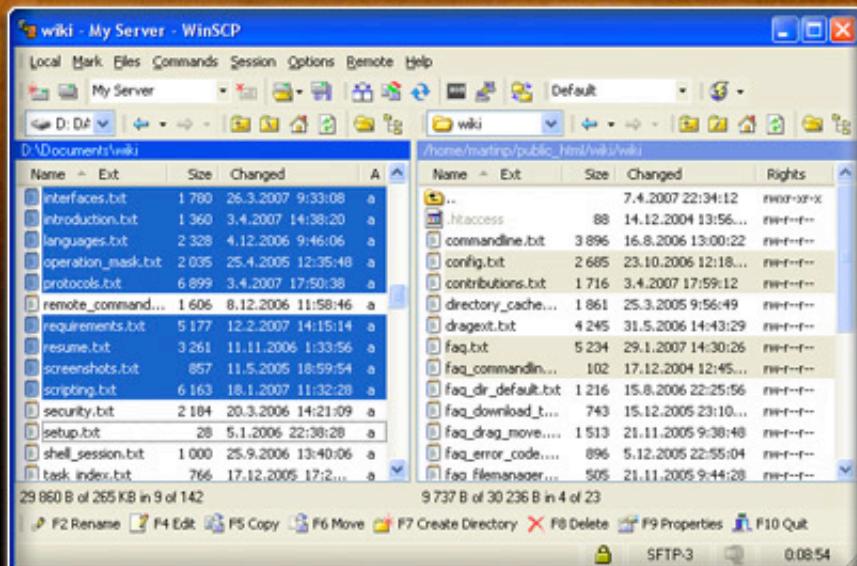
A.J. Newtonson is currently an Instructor, teaching Theory and Practice of Military Information Technology Systems, at the United States Military Academy at West Point. He received his Master's Degree in Information Technology Management from the Naval Postgraduate School.

Robert Ross is presently an Information Technology Instructor at the United States Military Academy at West Point. He received a Master's Degree in Computer Science from Monmouth University.

Ralph Ware is currently a Course Director and Instructor, teaching Information Technology, at the United States Military Academy at West Point. He received his Master's Degree in Computer Science from the Georgia Institute of Technology.

Gregory Conti, Director of the Information and Technology and Operations research center and Assistant Professor of Computer Science at the United States Military Academy, is the author of Security Data Visualization (No Starch Press) and the RUMINT visualization tool. His work can be found at [www.gregconti.com](http://www.gregconti.com).

**WinSCP is freeware SFTP, FTP client for Windows using SSH. Its main function is safe copying of files between a local and a remote computer.**



**Download it for free at [winscp.net](http://winscp.net)**

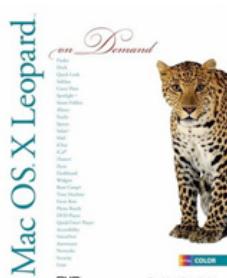


## Latest additions to our bookshelf

### Mac OS X Leopard On Demand

By Steve Johnson

Que, ISBN: 0789736543

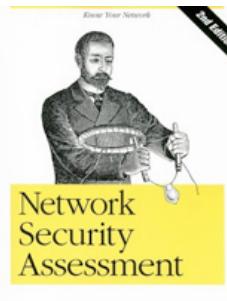


This book uses real world examples to give you a context in which to perform a task. Some of the topics covered include Master the Mac OS X Leopard user interface, file management, and applications, use Windows along with Leopard using Boot Camp, customize and fine-tune Mac OS X Leopard, set up multiple users and maintain security, keep your files up to date and backed up with Time Machine, and more. "Mac OS X Leopard On Demand" is written by people from Perspection, e-learning provider specializing in online IT training.

### Network Security Assessment: Know Your Network (2nd Edition)

By Chris McNab

O'Reilly, ISBN: 0596510306

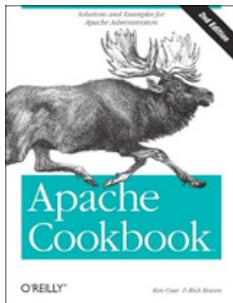


Network Security Assessment provides you with the tricks and tools professional security consultants use to identify and assess risks in Internet-based networks—the same penetration testing model they use to secure government, military, and commercial networks. This new edition is up-to-date on the latest hacking techniques, but rather than focus on individual issues, it looks at the bigger picture by grouping and analyzing threats at a high-level. By grouping threats in this way, you learn to create defensive strategies against entire attack categories, providing protection now and into the future.

## Apache Cookbook (2nd Edition)

By Rich Bowen, Ken Coar

O'Reilly, ISBN: 0596529945

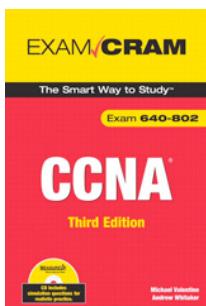


The new edition of the Apache Cookbook offers you updated solutions to the problems you're likely to encounter with the new versions of Apache. Written by members of the Apache Software Foundation, and thoroughly revised for Apache versions 2.0 and 2.2, recipes in this book range from simple tasks, such installing the server on Red Hat Linux or Windows, to more complex tasks, such as setting up name-based virtual hosts or securing and managing your proxy server.

## CCNA Exam Cram (3rd Edition)

By Michael Hayes Valentine and Andrew John Whitaker

Que, ISBN: 0789737124

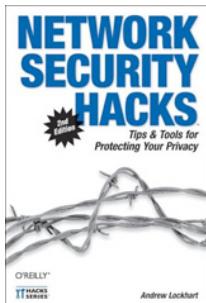


This book covers CCNA exam topics including: connecting Cisco equipment, make initial configurations, and connect to other devices to build a network, configuration of Cisco routers and the process of backing up and restoring your Cisco IOS software configurations, the configuration of PPP and Frame Relay for WAN connectivity, the mitigation of network security threats and secure network devices, the filtering of traffic from one network to another with access control lists, and much more.

## Network Security Hacks (2nd Edition)

By Andrew Lockhart

O'Reilly, ISBN: 0596527632

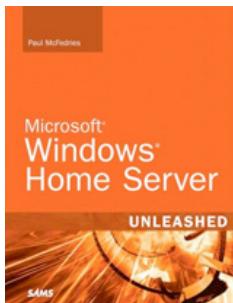


The second edition of Network Security Hacks offers 125 concise and practical hacks, including more information for Windows administrators, hacks for wireless networking (such as setting up a captive portal and securing against rogue hotspots), and techniques to ensure privacy and anonymity, including ways to evade network traffic analysis, encrypt email and files, and protect against phishing attacks.

## Microsoft Windows Home Server Unleashed

By Paul McFedries

SAMS, ISBN: 0672329638

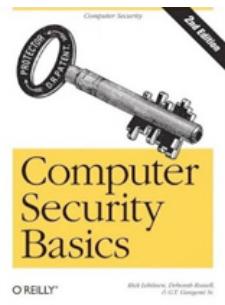


Microsoft Windows Home Server Unleashed takes a deep look at what makes this new server operating system tick. Inside you'll learn how the Windows Home Server storage system combines multiple hard disks into a single storage space that expands and contracts automatically as you add and remove hard disks, how to access your files from any PC in the network and provide secure access to the network via the Internet for your users, how to automate the backup of every computer on your network and more.

## Computer Security Basics (2nd Edition)

By Rick Lehtinen and G.T. Gangemi

O'Reilly, ISBN: 0596006691

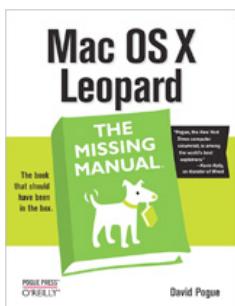


The new edition builds on the well-established principles developed in the original edition and thoroughly updates that core knowledge. For anyone involved with computer security, including security administrators, system administrators, developers, and IT managers, Computer Security Basics 2nd Edition offers a clear overview of the security concepts you need to know, including access controls, malicious software, security policy, cryptography, biometrics, as well as government regulations and standards.

## Mac OS X Leopard: The Missing Manual

By David Pogue

Pogue Press, ISBN: 059652952X



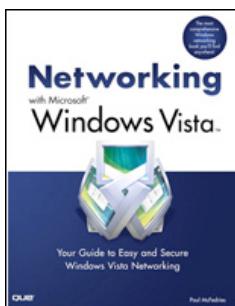
Mac OS X: The Missing Manual, Leopard Edition is the authoritative book for Mac users of all technical levels and experience. If you're new to the Mac, this book gives you a crystal-clear, jargon-free introduction to the Dock, the Mac OS X folder structure, and the Mail application.

There are also mini-manuals on iLife applications such as iMovie, iDVD, and iPhoto, and a tutorial for Safari, Mac's web browser.

## Networking with Microsoft Windows Vista

By Paul McFedries

Que, ISBN: 0789737779



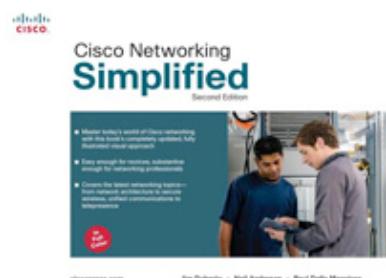
Your Guide to Easy and Secure Windows Vista Networking is a complete beginner's guide to creating, configuring, administering, and using a small network using Windows Vista computers. Inside you'll find comprehensive coverage of networking hardware, including ethernet (wired) hardware (from NICs to cables to switches to routers) and wireless hardware - from wireless NICs to access points to range extenders.

Read the review at HNS: [www.net-security.org/review.php?id=174](http://www.net-security.org/review.php?id=174)

## Cisco Networking Simplified (2nd Edition)

By Neil Anderson, Paul L. Della Maggiora, Jim Doherty

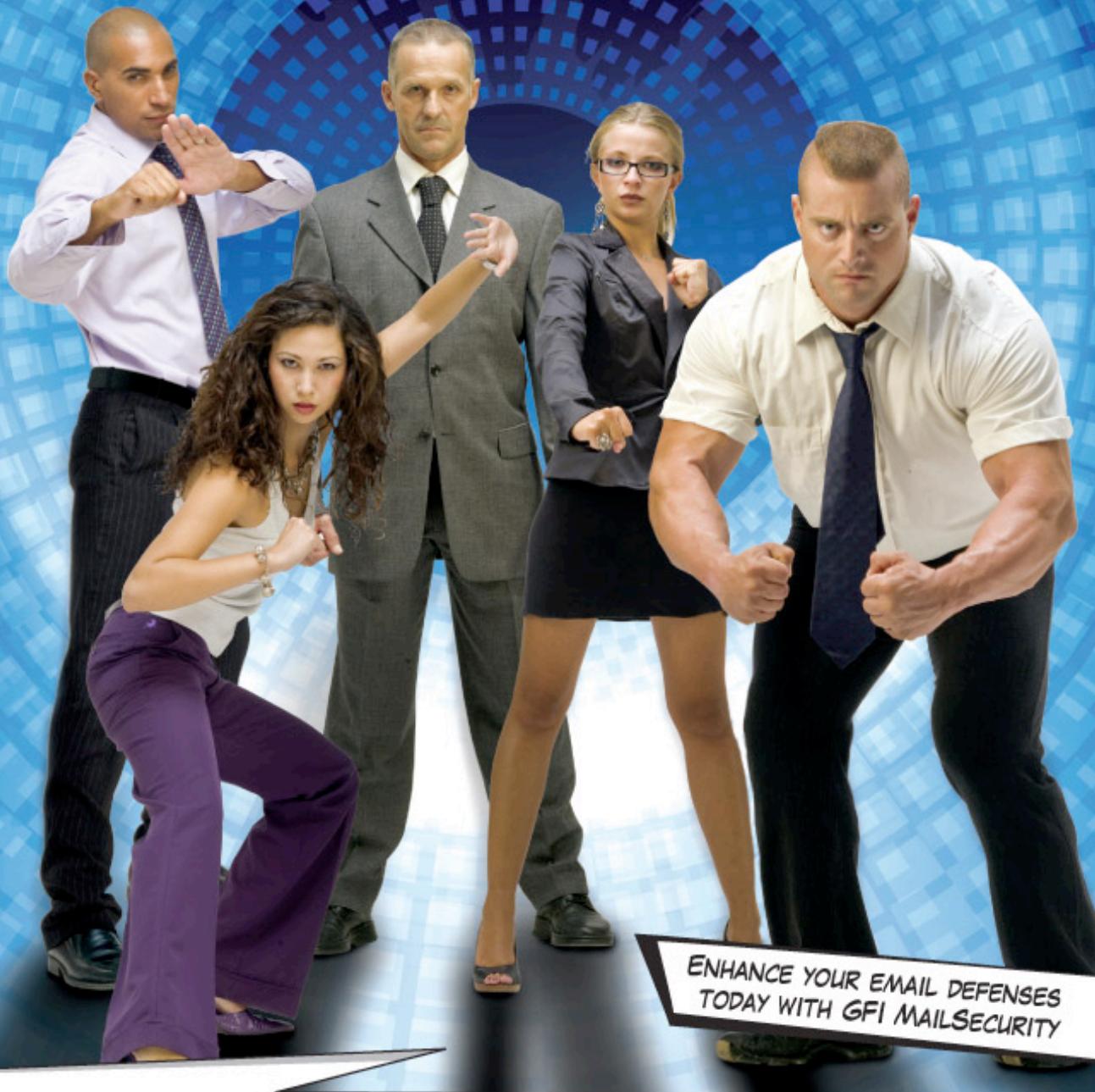
Cisco Press, ISBN: 1587201992



Even if you've never set up or managed a network, this book helps you quickly master the concepts you need to understand. Its full-color diagrams and clear explanations give you the big picture: how each important networking technology works, what it can do for you, and how they all fit together. The authors illuminate networking from the smallest LANs to the largest enterprise infrastructures.

Read the review at HNS: [www.net-security.org/review.php?id=174](http://www.net-security.org/review.php?id=174)

ONE PRODUCT. FIVE DEFENDERS.  
FIVE ANTI-VIRUS ENGINES. ONE CHOICE.



## GFI MailSecurity

Complete email security with up to five anti-virus engines for Exchange/SMTP/Lotus

**No single anti-virus vendor scanner is the BEST and can stop ALL viruses.** To obtain maximum security, you need GFI MailSecurity which uses not one, but up to five virus scanners to check all company email, with limited or no effect on network and server performance.

GFI MailSecurity is better priced than most single anti-virus engine solutions on the market. With multiple anti-virus engines you:

- React fastest to the latest virus threats by receiving the quickest virus signature updates
- Take advantage of all their strengths because no single anti-virus scanner is the BEST
- Virtually eliminate the chances of an infection.



**McAfee®**

**NORMAN®**



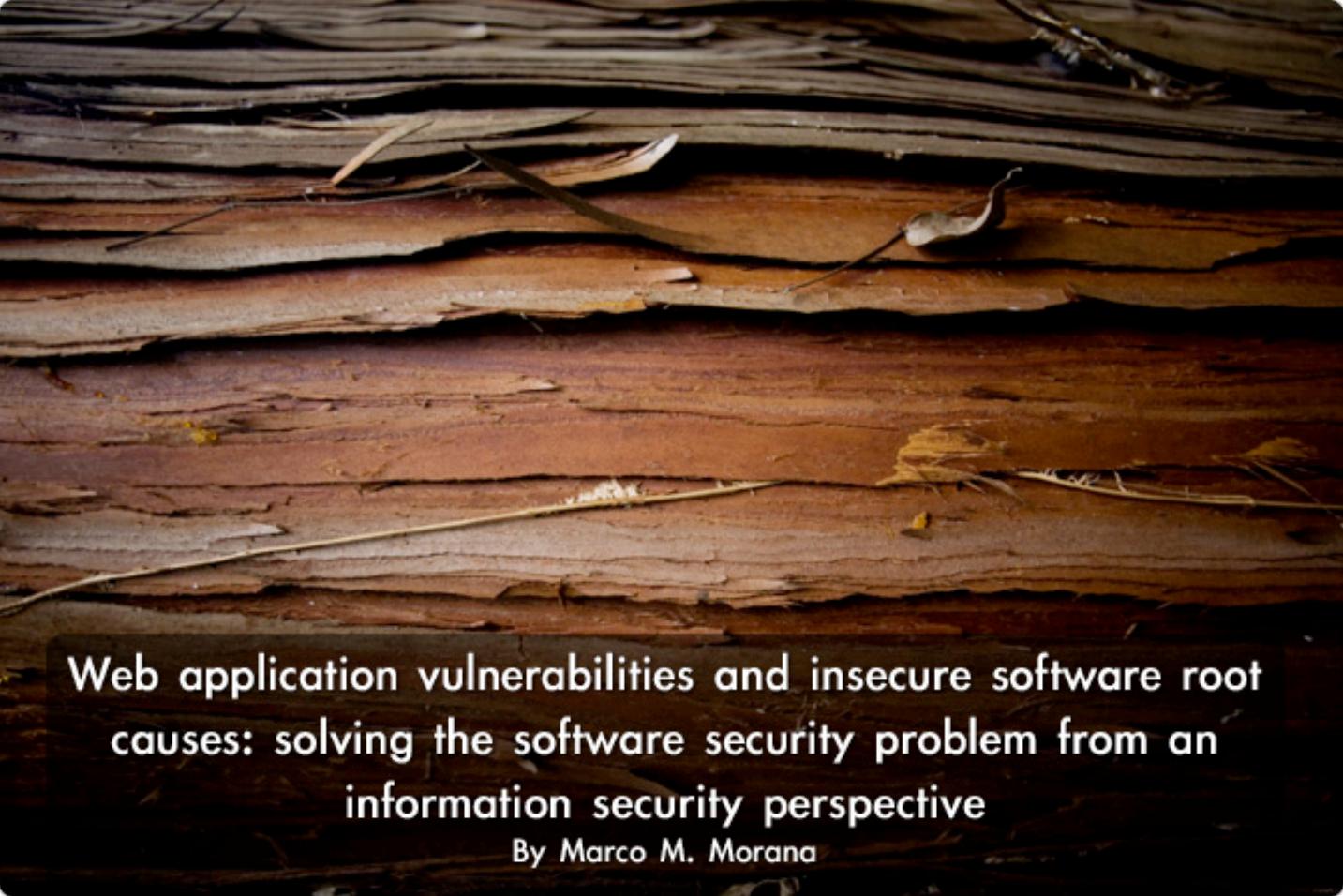
**AVG Anti-Virus**

Download your FREE trial version from [www.gfi.com/ehns/](http://www.gfi.com/ehns/)



**GFI**

NETWORK SECURITY  
CONTENT SECURITY  
MESSAGING



## **Web application vulnerabilities and insecure software root causes: solving the software security problem from an information security perspective**

By Marco M. Morana

**Before to diagnose the disease and provide the cure a doctor looks at the root causes of the patient sickness, the risk factors and the symptoms. In case of application security most of the root causes of the security issues are in insecure software: the risk factors can be found in how bad the application is designed, the software is coded and the application is tested.**

Typical symptoms of insecure software are the exposure to web application vulnerabilities as well as weaknesses in the application security controls. How critical such vulnerabilities are really depends on what the application is designed for: in case of on-line retailers, weaknesses in web application security controls might allow for a malicious user to manipulate the price of an item or the shipping address. The cause of these vulnerabilities, in most of the cases, is due of not validating on the server side data that can be manipulated via web pages on the client side.

Web applications that handle customer sensitive data such as credit card information might be exposed to the risk of identity theft as well as fraudulent transactions. In the case of banking on-line applications and web sites delivering financial services such as insurance, mortgages, brokerage for example, identity

theft is a growing threat and often times is facilitated by web application vulnerabilities such as lack of strong security controls for input validation, weak authentication and authorization, weak session management as well as data poor data protection in transit and storage.

Practically every business that has a web presence on-line has a inherent risks due to the exposure and the potential web application vulnerabilities. Such risks are more or less quantifiable. For example, if the web site has been just defaced the impact can be “reputation” and the loss is a matter or perception. In the case of losing credit card holder information the monetary loss is in terms of fines for non compliance with security standards such as PCI as well as law suits on behalf of the third parties suffering the loss (e.g. banks).

From the information security perspective you can learn how important PCI compliance and lawsuits are to retailers by looking at the TJ Maxx data breach and credit card fraud incident: [tinyurl.com/22zsm3](http://tinyurl.com/22zsm3).

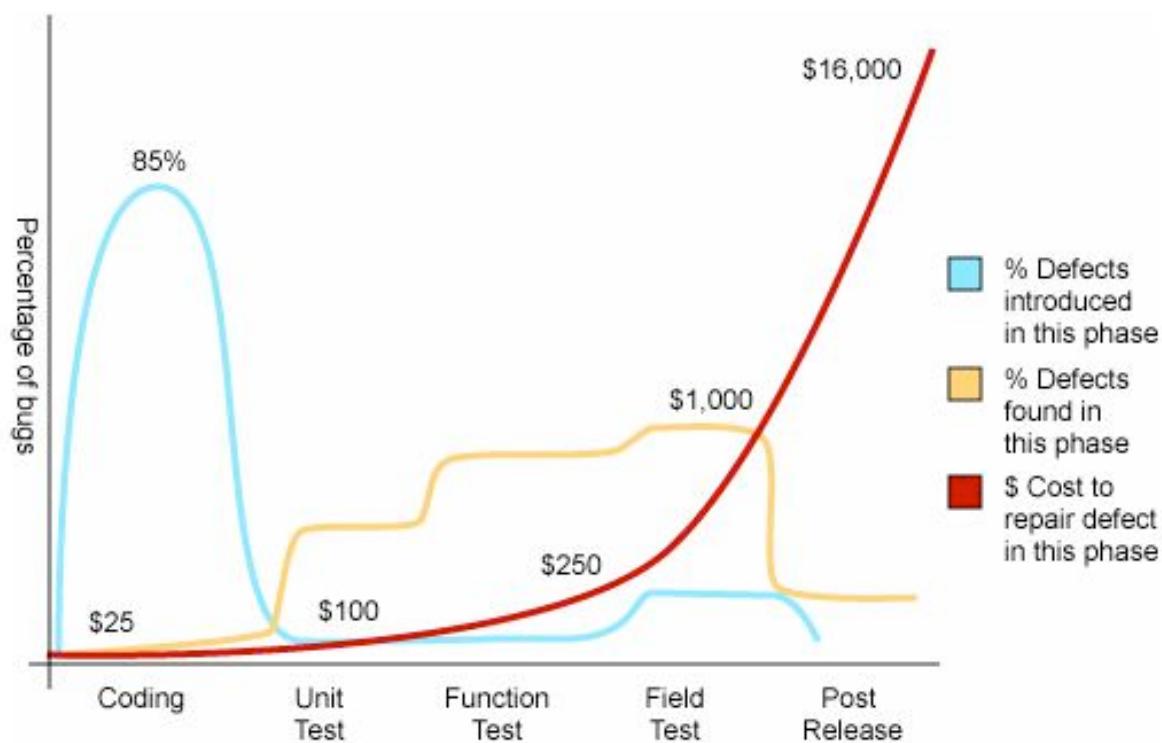
In case of financial institutions with on-line presence losses due to web application vulnerabilities can also be directly quantifiable in term of exposure of the site to potential fraudulent transactions. Common vulnerabilities might include weak authentication that allows unauthorized access, server buffer overflows causing a denial of service, loss of confidential information due of weak data protection controls (e.g. sensitive data not encrypted), weak session management (e.g. session tokens in clear, re-use of someone else user session) as well as server misconfigurations (SSL not enforced, admin web pages left on the production site, non essential services left running, application information disclosure via test web pages etc.)

Web application vulnerabilities represent a big cost to organizations that need to fix them: according to a NIST study in 2002 ([tinyurl.com/2fq8tr](http://tinyurl.com/2fq8tr)) the cost of fixing vulnerabilities in applications was estimated to be 59

billions USD. In a recent study David Rice, director of the Monterey Group who has just published a new book called "Geekonomics: The Real cost of Insecure Software" has estimated the 2007 dollar figure of the actual cost of insecure software to the U.S. to be at least \$180 billion per year.

Now the main question is, if insecure software has so big impact on our economy why we are not getting better on building secure web applications? Finding the real answer is not easy and probably the truth is in the details, so let's try to find it.

First of all is important to understand that software security awareness does not happen overnight. Fixing software for security is a more complex problem to deal with than most security practitioners might think of. It is complex because requires an holistic approach involving people with different skills such as developers that build secure applications and security officers that manage the security risks, processes with different disciplines such as software security engineering and threat analysis and least and not last new security technologies and security assessment tools.



Source: *Applied Software Measurement*, Capers Jones, 1996

Figure 1: The cost of fixing bugs in the SDLC.

Most of all, software security requires a different perspective in the way companies traditionally view the solution of insecure software. For most of development shops fixing insecure software that really means: *stop try to fix security bugs (security issues in code) when the software is already build and shipped to production*. According to a software defect metrics compiled by Capers Johns back in 1996 about 85 % of overall defects are introduced during coding. If you compile the same metrics today with your applications, depending on the maturity of your software security processes, you probably will find a number of 55% or higher: that proves the point!

Timing to address the security issues is also a critical factor, from the perspective of spending your \$\$ to fix the security issues in the software you build, the later you wait to address them the more expensive they will become. As shown in Figure 1 on the previous page, the cost of implementing a code change for fixing a security bug during coding will increase exponentially when addressed later in the SDLC during field test and post release.

In case of software products such as web applications the majority of security issues are due to coding errors no matter how you approach the problem of insecure software, from either the software security (build security into the SDLC) or application security perspective (catch and patch).

If indeed most of the vulnerabilities found are security issues due to insecure coding that's where the focus should be. If you are not sure, set up a target such as trying to eliminate at least 30% of vulnerabilities found during penetration tests (e.g. ethical hacks) that might have root causes in software. Set up a software security framework for software activities and a roadmap by looking at state of the art best practices in software security assurance: [tinyurl.com/3yk3cn](http://tinyurl.com/3yk3cn).

Most importantly, take into account the maturity of the software security practices within your organization so you can realistically assess the maturity level of the software security practices within organization and what realistically you can achieve in the short and in the long term.

If your software security practices are not yet mature yet you can start with a set of tactical activities such as secure coding standards and source code analysis. The next step could be validation with security testing at component level (unit tests) and security tests integrated with system tests.

From the information security perspective you can also look at enforcing software security throughout your organization as part of information security and risk management processes: for software security compliance you could also include regulatory guidance (e.g. FFIEC) as well as industrial standards (e.g. VISA PCI).

A set of software security requirements is the best place to start to address the root causes of web application vulnerabilities. Software security is a defensive game: that means empowering software developers with best practices that allow them to build strong security controls. It also means thinking like an attacker that is making sure the software developers know what the common threats to web applications are, how can be exploited and the resulting impact.

From the defensive perspective, if we look at common web application vulnerabilities as a result of weaknesses in software mitigation controls, it is possible to generalize the software security issues in basic category types using the Web Application Security Frame (WASF) [tinyurl.com/yrj44k](http://tinyurl.com/yrj44k):

- Access Control: Authentication and Authorization
- Configuration Management
- Data Protection In Transit and Storage
- Data Validation
- Error and Exception Handling
- Logging and auditing
- User and Session Management

By categorizing web application vulnerabilities as weakness in security controls it is easier to describe the root causes in terms of coding errors. For example the buffer overflow vulnerability is the direct cause of lack of input validation that can be addressed with software input validation requirements as well as other coding requirements such as use of safe string manipulation APIs.

To approach web application vulnerabilities that have root causes in software is important to describe them according to software security assessment criteria:

1. The security threat that the issue is exposed to
2. The software security root cause of the vulnerability
3. How to find the potential vulnerability
4. The countermeasure
5. The risk rating.

Describing what the security threat is helps to understand why the mitigation control is not effective. The software security root cause of the vulnerability is the code snippet (e.g. the offending source code) that need to be fixed. It is important also to provide guidance to the software developer on how to find the potential vulnerability. For example, by looking at the source code it is possible to spot the vulnerability. This can be done with a “white box testing technique: that consists on a security code review with the help of a source code analyzer (e.g. static parser) to point out the area of the code that could possibly present vulnerability. In most cases this vulnerabilities can also be spotted via a black box technique (penetration test) to validate the critical exposure of the vulnerability to the front end (e.g. client). The countermeasure in this case consists on a sample of secure code that does not present (aka mitigates) the vulnerability.

Finally the risk rating helps to prioritize the remediation effort. Typically, assigning a risk rating to the vulnerability involves a risk analy-

sis based upon factors such as impact and exposure. Most of organizations have established information risk analysis processes that can be used as a reference to assign severity to vulnerability. If your organization does not have one, you can refer to best practices such as the one referred in the OWASP Testing Guide - [tinyurl.com/ytf48z](http://tinyurl.com/ytf48z)

Some examples on how to document root causes for some basic web application vulnerabilities are included herein in tables 1 to 7.

Finally, if you document secure software requirements in a standard document is also important that your organization put in place a process to verify compliance with the standards, typically this means performing a source code review and source code analysis with the help of automated tools such as code scanners. If such is too restrictive and costly for your organization, you could deliver software security best practices as a guideline document.

Finally software security training is critical as well as the use of adequate tools for source code analysis, make sure that you effectively communicate software security best practices to software developers.

Secure software requires people, process and tools as any other information security initiative within your organization. Above all commitment from different levels of management within your organization is the key to deliver a successful software security initiative.

**Table 1: Weak Web Based Authentication**

<b>Vulnerability</b>	Weak Web Based Authentication
<b>Vulnerability type</b>	Access Control: Authentication
<b>Security issue</b>	Weak authentication used to verify a user outside the trust boundary of the web application.
<b>Security threat</b>	Basic authentication credentials (username and password) are passed in clear from the authentication component to the client and BASE64 encoded. A malicious user can capture and decode such credentials during transmission with the use of a web proxy.
<b>Software security root cause</b>	<p>The “web.config” file is potentially configured to use HTTP Basic authentication.</p> <pre>&lt;system.web&gt; &lt;authentication mode="Windows" /&gt; &lt;/system.web&gt;</pre>

<b>How to find the potential vulnerability</b>	Source code review the web configuration file “web.config” and verify that the authentication mode is not set to Windows. On the client, the user sees (on first request and in the default mode) a dialog requesting her credentials. By typing user name and password, the Base64 encoded version of these credentials is sent back to the server. In the authorization header, along with a token indicating that the offered authentication scheme -- Basic -- has been accepted by the client.  <code>Get / HTTP/1.1 Host: host Authorization: Basic dGVzdDp0ZXN0</code>
<b>Countermeasure</b>	Change web form authentication to use secure form authentication such as NTLM vs.2 or Kerberos. Enable SSL to protect the authenticated sessions.
<b>Risk rating</b>	High

**Table 2: Errors in RBAC Server Side Business Logic**

<b>Vulnerability</b>	Errors on RBAC Server Side Business Logic
<b>Vulnerability type</b>	Access Control: Authorization
<b>Security issue</b>	Weak mechanisms to enforce access controls on protected resources within the system
<b>Security threat</b>	A business logic error allow for default elevation of privileges of users logged into the application.
<b>Software security root cause</b>	Principle of least privilege is not enforced by the server side role based access controls. A source code analysis revealed a logical condition clause do not default to least privileges when user role normal user cannot be validated  <code>if user.equals("NormalUser") {     grantUser(Normal_User_Permissions); } else{ //user must be admin/super     grantUser ("Super_User_Permissions");}</code>
<b>How to find the potential vulnerability</b>	Review source code for potential coding errors in the Role Based Access Control (RBAC) business logic implemented on the server. Log on as normal user and either modify or delete the permission/ role parameters before sending them to the server. The server will grant the user admin/super privileges.
<b>Countermeasure</b>	Modify the error in the RBAC business logic as follows:  <code>if user.equals("NormalUser") {     grantUser(Normal_User_Permissions); } else if user.equals("SuperUser") {     grantUser ("Super_User_Permissions");}</code>
<b>Risk rating</b>	High

<b>Vulnerability</b>	Information disclosure via server error messages
<b>Vulnerability type</b>	Configuration management
<b>Security issue</b>	Application server not configured securely
<b>Security threat</b>	Stack traces in default error messages disclose application information that can be useful for a potential attacker
<b>Software security root cause</b>	Declarative setting in “web.config” file “customErrors” set to Off  <code>&lt;customErrors mode="Off"/&gt;</code>

<b>How to find the potential vulnerability</b>	Force the web server to errors. If errors server messages reveal important information such as SQL exception errors and stack traces, custom errors are not turned on. For example an SQL exception error disclose application information when custom errors are not turned on: <code>[SqlException (0x80131904) : An error has occurred while establishing a connection to the server. When connecting to SQL Server 2005, this failure may be caused by the fact that under the default settings SQL Server does not allow remote connections. (provider: SQL Network Interfaces, error: 26 - Error Locating Server/Instance Specified) ]</code>
<b>Countermeasure</b>	Use declarative programming setting in “web.config” file and set “customErrors” to On and “mode=RemoteOnly”. All the errors unless explicitly specified will be brought to defaultRedirect i.e. myerrorpagedefault.aspx. a statuscode 404 will be shown myerrorpagefor404.aspx. <code>&lt;customErrors defaultRedirect="myerrorpagedefault.aspx" mode="On Off RemoteOnly"&gt;&lt;error statusCode="404" redirect="myerrorpagefor404.aspx"/&gt;&lt;error statusCode="500" redirect="myerrorpagefor500.aspx"/&gt;&lt;/customErrors&gt;</code>
<b>Risk rating</b>	Low

**Table 3: Hard-coded Passwords**

<b>Vulnerability</b>	Hard-coded passwords
<b>Vulnerability type</b>	Data protection in transit and storage
<b>Security issue</b>	Lack of adequate protection for secrets and other sensitive data
<b>Security threat</b>	Hard-coded hashed passwords can be recovered from source code and used by a malicious user to gain access to the application or to brute force the password (i.e. computing the hash of all possible passwords or a dictionary attack).
<b>Software security root cause</b>	Password hash is hard-coded in VerifyPwd API <code>int VerifyPwd(String password) {     if (passwd.Equals("68af404b513073584c4b6f22b6c63e6b")) {         } return(0)     return(1);}</code>
<b>How to find the potential vulnerability</b>	Try to access source code (Java files) on the server side and verify if access controls (ACLs) are enforced to prevent access to the file. If source files are accessible the application is vulnerable.
<b>Countermeasure</b>	Use secure key storage such as CryptoAPI or Java Key Store for storing encryption keys and store password password's digests in a database.
<b>Risk rating</b>	High

**Table 4: Cross Site Scripting**

<b>Vulnerability</b>	Reflected Cross Site Scripting (XSS)
<b>Vulnerability type</b>	Data Validation
<b>Security issue</b>	Lack of input and output validation when data crosses system or trust boundaries.

<b>Security threat</b>	Invalidated input entered in the web application is not validated before being reflected back to the client and can be run on the client browser potentially exposing the user. This kind of attack can be delivered to the user via social engineering (e.g. phishing) by encouraging the user to select a link to the web application that carries the malicious XSS script as part of the URL parameters. The malicious script can be used for stealing cookies, session hijacking and any confidential data stored on the user's client browser.
<b>Software security root cause</b>	Data passed in the HttpServletRequest is placed into a "req" parameter from user input without being validated. The same data is returned back to the servlet response without output validation/encoding. <pre>import java.io.*; import javax.servlet.http.*; import javax.servlet.*; public class HelloServlet extends HttpServlet {     public void doGet (HttpServletRequest req, HttpServletResponse res) throws ServletException, IOException     {         String input = req.getHeader("USERINPUT");         PrintWriter out = res.getWriter();         out.println(input); // echo User input.         out.close();     } }</pre>
<b>How to find the potential vulnerability</b>	Verify whether an application or web server will respond to requests containing simple scripts with an HTTP response that are executed by the user's browser.  The attack vector can be a script to show sensitive information (e.g. cookie stored on the browser) in an alert. <code>http://server/cgi-bin/testcgi.exe?&lt;SCRIPT&gt;alert("Cookie"+document.cookie)&lt;/SCRIPT&gt;</code>
<b>Countermeasure</b>	Perform input data validation using white lists (e.g. default deny) of unsafe characters and output encoding. When using .NET make sure that request validation is enabled as well as HTML encoding for the content to be displayed.  <code>&lt;pages validateRequest="true" ... /&gt; Server.HtmlEncode(string)</code>  Enforce encoding in output to assure that the browser interprets any special characters as data and markup. HTML encoding usually means < becomes &lt;, > becomes &gt;, & becomes &amp;, and " becomes &quot;. So for example the text <script> would be displayed as <script> but on viewing the markup it would be represented by &lt;script&gt;;
<b>Risk rating</b>	Medium

**Table 5: Application Fails Insecurely**

<b>Vulnerability</b>	Application Fails Insecurely
<b>Vulnerability type</b>	Error Handling and Exception Management
<b>Security issue</b>	Failure to deal with exceptions effectively and in a secure manner, resulting unauthorized disclosure of information.
<b>Security threat</b>	The application fails leaving users in higher privilege state because of errors in the business logic that handles exception handling

<b>Software security root cause</b>	Exception thrown in the try block by “ReadSecretFile” will bypass “LowerPrivilege” call.  <pre>try{     ElevatePrivilege();     ReadSecretFile();     LowerPrivilege(); } catch(Exception e){ HandleError(e); }</pre>
<b>How to find the potential vulnerability</b>	Use automated code scan to identify incomplete exception error blocks (e.g. try-catch without finally). Manually review the exception handling business logic to identify unsafe exception handing.
<b>Countermeasure</b>	When catching exceptions with try-catch always use finally block to reset the original state of user permissions.  <pre>try{     ElevatePrivilege();     ReadSecretFile(); } catch(Exception e){ HandleError(e); Finally { LowerPrivilege(); } }</pre>
<b>Risk rating</b>	High

**Table 6: Application Information Disclosure**

<b>Vulnerability</b>	Application Information Disclosure
<b>Vulnerability type</b>	Logging and Auditing
<b>Security issue</b>	Failure to deal with exceptions effectively and in a secure manner, resulting unauthorized disclosure of information.
<b>Security threat</b>	The stack trace information displayed to the user as part of the exception message can be used by an attacker to stage the next attack to the application.
<b>Software security root cause</b>	The exception error is sent to standard output  <pre>try {     ... } catch (Exception e) { e.printStackTrace(); }</pre>
<b>How to find the potential vulnerability</b>	With white box testing, automatically scan source code for un-safe exception handling patterns.  With black box testing, verify that the web application handles errors by displaying general information to the end user. Displaying exception information such as stack trace and application information indicates un-secure exception handling. An example shown herein display sensitive information such as JSESSIONIDs and IP addresses  <pre>network: Connecting https://newtrade.sharekhan.com/rmmweb/applet/StreamingApplet/RTApplet.class with cookie "JSESSIONID=FG8c0kDgFywCcc9nZNZJTmHPhv4pG4y2F2nv6W nLFbJPDGSX114!-506720403" network: Connecting https://newtrade.sharekhan.com/rmmweb/applet/StreamingApplet/RTApplet/class.class with proxy=HTTP @ /192.168.40.7:8080 10:38:12:262:</pre>

<b>Countermeasure</b>	Made exception information only be used as debugging information that is not part of production release code. Use Log4jLogger to log exception error messages securely:  <pre>try{     //some code } catch(Exception ex){     logger.debug(exception.toString()); }</pre>
<b>Risk rating</b>	Low

**Table 7: Session IDs not marked secure**

<b>Vulnerability</b>	Session IDs not marked secure
<b>Vulnerability type</b>	User and Session Management
<b>Security issue</b>	Lack of mechanisms to maintain session independence between multiple logged-on users and insecure user provisioning and de-provisioning policies.
<b>Security threat</b>	Cookies without the secure flag set can be sent by through a non SSL session (transverse the network unencrypted).
<b>Software security root cause</b>	Session cookies used by the application do not have the secure flag set to true.  <pre>Cookie cookie = new Cookie("TEST", "TESTVALUE"); cookie.setDomain("abc.def.com"); cookie.setMaxAge(300); cookie.setPath("/"); cookie.setSecure(false); response.addCookie(cookie);</pre>
<b>How to find the potential vulnerability</b>	With white box testing, automatically scan source code for cookie settings.  With black box testing, verify that the cookie set by the server does not have the secure flag. <pre>Set-Cookie: name=newvalue; expires=date; path=/; domain=.example.org.</pre>
<b>Countermeasure</b>	Mark the cookies as secure so that they are transmitted only over secure (SSL) channel:  <pre>Cookie secure = secure; .NET cookie.setSecure(true); (Java)</pre>
<b>Risk rating</b>	Low

Marco serves as a leader of the OWASP (Open Web Application Security Project - owasp.org) where he contributed to write the OWASP Security Testing Guide. Marco and also works as Technology Information Security Officer for a large financial organization with key roles in defining the web application security roadmap and activities, document security standards and guidelines, perform security assessments for software security as well as training software developers and project managers on the software security and information security processes. In the past, Marco served as senior security consultant within a major security consulting company in USA where his responsibilities included providing software security services for several clients in the banking, telecommunication, computers and financial business sectors. Marco also had a career in the software industry in diverse professional roles such as contractor, senior software engineer and project manager with responsibility to design and to develop business critical security software products for several FORTUNE 500 companies as well for the US Government (i.e. NASA).

Marco is active in publishing on the topic of software security for several professional organizations (ISSA, OWASP) as well as on his blog: <http://securesoftware.blogspot.com>. Marco can be contacted at [marco.morana@owasp.org](mailto:marco.morana@owasp.org)



## Internet terrorist: does such a thing really exist?

By Rick Lawhorn

**Recently, I have experienced an increase in organizations questioning how real is the threat of Internet terrorism and what they can do to protect themselves. As a former CISO, this was one of the last concerns that crossed my mind, especially since it was a daily up-hill battle getting buy-in for the most basic security controls and services.**

The notion of worrying about the potential risk of terrorism against my organization seemed to be the lowest priority given the choices at hand. Ironically, terrorism today seems to be an emerging concern in the commercial world and many are actively pursuing methods and technology to help combat the problem. As a result, I began to research this trend to determine its drivers and potential implications to information security as we know it today.

I have been able to identify two main factors to date that play a part in the increased concern for businesses.

Governments all around the globe are spending vast amounts of money trying to track and contain internet terrorism.

As former government security professionals are landing executive roles as CSO and CISO in organizations, the awareness and education about terrorism is increasing and the company is driven to investigate the threat fur-

ther. Also, the news media is making Internet terrorism and the targeted attacks front-page news, which impacts a much larger audience. The combination of these factors propels companies and their leadership to ask the important questions in order to determine the risk it presents, especially in the critical industries like utilities and supply chains.

To better understand this threat and its impact on organizations today requires some background on how terrorism is defined. Once we have a definition laid out, we need to add the term “internet” to terrorism to gain an understanding of how this changes the overall meaning and its impact.

Each of us has a pre-conceived notion of what terrorism means. I am confident that your definition differs from mine since this is shaped by our personal environment and experiences.

I am also confident in saying that even though our definition of terrorism may differ, there are fundamental characteristics that we share in common. Today, there is no universally accepted definition of terrorism and countries define the term according to their own beliefs and to support their own national interests. In fact, it might be impossible to define because it is intangible and fluctuates according to historical and geographical contexts. Some forms of it are indistinguishable from crime, revolution, and war. Even the US government is struggling with a consistent definition by evidence of the following chart:

State Department definition, Title 22 of the U.S. Code, Chapter 38, Section 2656f(d):

premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents, usually intended to influence an audience.

FBI definition: the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

Defense Department definition: the calculated use, or threatened use, of force or violence against individuals or property to coerce or intimidate governments or societies, often to achieve political, religious, or ideological objectives.

**Today, there is no universally accepted definition of terrorism and countries define the term according to their own beliefs and to support their own national interests.**

United Nations definition: any act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act. Article 2(b) of International Convention for the Suppression of the Financing of Terrorism, May 5, 2004)

If we take all the three definitions and compare them, we can understand the governments' intent in defining the actions and the basic fundamental characteristics of terrorism. Realistically, the lack of a solid, universally accepted definition and having to rely on intent is the first major strike against understanding the threat.

The first rule in being able to track a threat is to understand what that threat is and the characteristics that make up the profile. If we do not have this understanding up front, it will spur a great amount of activity for the least possible value in targeting Internet terrorism. With so many different definitions, you can start to understand the reason behind failures in the identification and of course, tracking and monitoring.

In the interest of moving to the next phase in our discussion, let's assume that terrorism is defined as an unlawful use or threatened use of force or violence against people or property to coerce or intimidate businesses, governments or societies.

We can now tack on the term "Internet" to explore how the definition changes and the impact of those changes on information security. By building the term "Internet terrorism", we are saying that violence and physical harm can be conducted electronically. Now I don't believe that this is the intent, but in essence layering intent upon intent has now diluted our definition. This causes confusion and forces us to lean upon our beliefs, environment and current situations to form a definition. This does not provide us with any greater capability in tracking or monitoring and just seems to muddy the waters even further.

So how we identify the threat and what can we do to protect ourselves? Internet terrorism is really about two separate uses of the Internet. First, a terrorist can utilize the Internet as a vehicle to cause outages and denial of services with an overarching message to instill fear and to threaten physical harm.

From an information security point of view, we can readily understand this first point since we experience this noise today within our networks. The attacks are targeting our assets to cause electronic pain and fear with our Internet presence. But as we know, attacks that are conducted against our organizations can originate from many diverse groups with different reasons. Former employees, competitors, or fraudsters can have justifiable reasons in their mind to electronically cause you pain or reputation harm.

It becomes apparent that the campaign against Internet terrorism using the Internet in this fashion may stem from known terrorist in the real world who has conducted violent or harmful crimes to invoke fear.

The challenge is to know when these seemingly “innocent” attacks actually become terror.

Does the act require a certain number of members, a certain political/ideological principle, or a certain funding to be considered terrorism? Can one person be considered a terrorist?

These are great questions that need a clear definition to gain the appropriate buy-in and funding within an organization. Since the activity and characteristics are not well defined, the message today will be a hard sell for information security professionals and will get lost in the shuffle of shifting priorities.

Likewise, when the terrorist begin to electronically target organizations and prevent services from working, companies today would see the threat as noise since there is nothing that distinguishes them from the rest of the pack. The challenge is determining how to distinguish the noise that is normally experienced from an actual terrorist activity.

## The attacks are targeting our assets to cause electronic pain and fear with our Internet presence.

The second use of the internet by terrorist is their utilization of technologies to build and coordinate their activities such as recruitment, fundraising and data mining. The internet is the perfect tool to use for this activity since much of it is not regulated and there is anonymity that protects against identification. This helps terrorist build memberships and raise funding to further their cause and distribute their message to a wider audience.

But can this equate to electronic violence or transform into physical harm? Each one of us use the internet for the same purpose, minus the terrorist intent, so tracking and monitoring are quite difficult to nail down without spilling over into our civil liberties as a whole.

The perceived harm that can be identified is the ability to organize a group for the intent of personal or physical violence. In order for an organization to keep on top of this issue, it would require vast amounts of resources and capital to infiltrate each terrorist group and monitor their progress. This goes way beyond what any commercial organization would do, especially since many still require basic secu-

rity controls and services. This type of request would certainly invoke some strange looks.

Here is where the government steps in on the war on internet terror. The government has the funding and resources to concentrate on infiltrating the terrorist groups to provide the community greater insight into the problem.

We know that the government’s main concern is infrastructure and self-preservation so terrorist targeting one specific entity or business becomes secondary by default. Disclosure of the intelligence takes a considerable amount of time since the information has to be interpreted and correlated against other information before being released.

I have not experienced a mechanism or process that would release intelligence in a timely manner to a commercial business unless it was a matter of national security. Strike two is the inability, either by design or accident, to make the intelligence gathering and disclosure transparent and timely.

This seems to be the greatest gap in protecting our commercial industries from Internet terrorist today. The lack of communication, fear or retaliation coupled with the shear expense prevents organizations from becoming the watchdogs for their respective industries. The terrorist seem to capitalize on this short-fall and use it to their benefit.

There are many journals and white papers that clearly confirm that the internet terrorist community is becoming increasingly sophisticated and beginning to leverage technology to protect their interests. I find this is amazing considering the lack of a fundamental definition to understand what we are monitoring, but I digress.

Online session encryption and file encryption are being used to conceal information about activity and potential targets. They are building redundant systems that have the ability to withstand constant bombardment of noise by other terrorist groups or disgruntled citizens.

They are beginning to build highly dynamic services that can disappear, re-emerge to

change locations quickly and easily. The content on their sites is rich with multimedia such as movies or audio. They even implement security controls to track and prevent their version of threats to their presence.

As the use of technology sophistication continues to grow, the less insight our governments will have about their activities and potential targets. The small amount of information we could potentially access today is drying up fast. We really need to open our eyes to this problem and build better methods to keep up or offset this threat growing into something much larger. We need to convince our governments that our society can be radically impacted by the collapse of our commercial industries as well as our critical infrastructure.

Monitoring and active communication of emerging threats can further assist our industries to prepare or prevent the attacks, given the time to react. Sure, the down side is over-reacting, but given that the majority of our businesses are on-line, I would enjoy the ability and time to manage my reaction.

## **As the use of technology sophistication continues to grow, the less insight our governments will have about their activities and potential targets.**

As information security professionals, we are limited in what we can do to offer physical and logical protection. We always have to balance the security control with the convenience factor and no one wants to complicate any process that is suppose to generate revenue or get the revenue generators to their desks.

In the physical security space, we have a few more choices in protective services that push the terrorist out further into someone else's yard, but we are still very limited in coordinated information sharing within our respected industries. In the electronic world, we can continue to insist on the basic levels of security controls to detect and potentially prevent attacks, but it will always be perceived as Internet noise vs. terrorism until we accurately define the risk.

Let's return to how we identify the threat and what can we do to protect ourselves. We now know that there is no consistent method to define or track internet terrorism. We understand that the issue is extremely complex since the characteristics can change based on our environment and experience. We can now understand the government's role in being the watchdog for our critical national infrastructure and the government services, but this takes considerable resources and funding.

We also know that our communication in both our local community and our global industry vertical is limited since the intelligence is not readily available to share. The message we are left with is that there is very little we can do until we define with certainty the meaning and characteristics of Internet terrorism.

A great place to start would be to have the government develop a single definition that can be communicated to its agencies so that the right profile can be understood.

Another key development would be to rebuild certain structures that gather intelligence to facilitate a greater level of communication to impacted industries. With a clear definition and greater communication, we can then begin to monitor and track certain behaviors that could be potential threats with greater accuracy.

Accuracy equates to a reduction in cost and resources, which can then be reinvested into greater communication and intelligence gathering. Sounds simple but my guess is that it will take a great amount of time to achieve, if we even achieve it at all. In the meantime, we are left with vague definitions, variable characteristics and a method of attack that blends in with the normal noise we see on the internet daily.

It really does beg the question, does such as thing really exist?

Rick Lawhorn (CISSP, CISA, CHSS, CHP, TCNP) is the Director of Information Security & Compliance at PlanIT Technology Group. Rick was the Chief Information Security Officer (CISO) for GE Financial Assurance, Chief Information Security Officer (CISO) for Genworth Financial and served in information technology leadership roles within Hunton & Williams law firm and the National White Collar Crime Center. He has over 17 years of experience in information technology and extensive security industry experience. Rick has been published in numerous domestic and international security magazines such as Information Security, SC Magazine and (IN)SECURE Magazine. In addition, he is serving on several advisory boards for new, innovative security products and has created a working group focused on developing meaningful metrics for CISOs. He can be reached at rick.lawhorn@mac.com or find him on the LinkedIn network.

**Want to reach a large audience of  
security professionals by writing for (IN)SECURE?**



**Send your idea to editor@insecuremag.com**



## A dozen demons profiting at your (in)convenience

By George Moore and Anthony Arrott

### Organized web threat families pollute your PC for profit.

Just as personal computers and the Internet have become a regular part of our daily lives, so too have parasitic and malicious software. As the world has become more networked, vandal computer viruses of the early days have evolved into today's larcenous web threats.

Simply put, web threats are malicious software programs such as spyware, adware, trojan horse programs, bots, viruses, worms, etc. that are installed on a PC without the knowledge or permission of the owner. These programs utilize the internet to spread, hide, update themselves, and send stolen data back to perpetrators. They can be combined – for example, a trojan downloads spyware or a worm that is used to infect a PC with a bot.

Another way to consider web threats is as the software of individual malware and adware enterprises. At one end of a spectrum these enterprises are fully-incorporated publicly-disclosed corporations. These include enterprises such as Integrated Search Technologies and Zango.

The darker end of the spectrum gets much more complex. The economy in the darker end of the internet has multiple profitable layers. Resellers of sensitive data, the latest vulnerabilities and authors of toolkits are common new ways of making a buck in the digital black-market.

Until recently, malware variants generally have been treated as separate individual threats. This comes from the legacy of self-propagating viruses and worms where a single variant can spread its vandalism worldwide within hours.

In contrast, the economically-motivated web threats of today use different software as piece-parts of a singular web threat business model. This has led anti-malware threat researchers to group together individual web threats that serve the same malware enterprise – regardless of differences in technical characteristics – see the table on the following page.

How does it get there?	What does it do?	How does it do it?	How does it protect itself?
installed by:	money from:	operates by:	protected by:
<ul style="list-style-type: none"> <li>• exploit</li> <li>• unknowing consent</li> <li>• lack full disclosure</li> <li>• freeloader</li> <li>• trojan</li> <li>• worm</li> </ul>	<ul style="list-style-type: none"> <li>• adware</li> <li>• trackware</li> <li>• keylogger</li> <li>• browser hijacker</li> <li>• fraudulent changes</li> <li>• fraudulent royalty</li> </ul>	<ul style="list-style-type: none"> <li>• browser helper object (BHO)</li> <li>• browser toolbar</li> <li>• layered service provider (LSP)</li> <li>• application</li> <li>• cookie</li> <li>• dialer</li> </ul>	<ul style="list-style-type: none"> <li>• rootkit</li> <li>• watchdog program</li> <li>• mimicry</li> <li>• polymorphic variation</li> </ul>

Non-virus web threats on client PCs typically have four components that together characterize the web threat business model.

What emerges from these analyses is a much clearer view of the web threat economy. Web threat families are groupings of individual web threats and variants that serve the same malware enterprises. Web threat families can consist of multiple pieces of software on individual PCs – each piece serving the malware business model in its own specialized way.

Rather than counting up all the software pieces as individual infections or variants, it is more relevant just to consider whether a PC is infected by a web threat family or not. And unlike viruses, where the rate at which an outbreak spreads is so important, web threats are best measured by what fraction of PCs are infected and how long they stay there earning money for their malware enterprise. As a result, the relevant index of web threat families is the average proportion of PCs infected. For example, the Zango web threat family led all

others, infecting on average 9.7% of all PCs throughout 2007.

There is one small consolation in all this for defending PCs from the rising tide of economically-motivated web threats. While malware writers have almost infinite technical variations available to disguise and protect new malware, the web threat business model is far more constrained. Web threat behaviors associated with monetary gain are typically harder to disguise than the underlying technologies for implementing them.

This has helped threat researchers at Trend Micro identify the top perpetrators of web threat families that profit at the inconvenience and expense of PC owners and users. Trend Micro has designated the top twelve of these web threat families the “Dozen Demons”. Here they are:

1. Zango	9.7%
2. Hotbar	7.0%
3. Drivercleaner	6.7%
4. Winfixer	6.1%
5. Virtumundo	6.0%
6. WhenU	5.7%
7. IBIS	4.9%
8. Purity Scan	4.6%
9. Zlob	4.5%
10. New.net	4.1%
11. Softomate	3.4%
12. Starware / Comet	3.1%

The proportion of PCs infected with a web threat family is based on weekly averages from HouseCall scans of 2.4 million PCs worldwide measured throughout 2007. Infections from identified web threat families accounted for 67% of all infections.

## **1. Zango** - 2007 average proportion of PCs infected: **9.7%**

Zango software includes known adware and spyware typically required to access partner's games, DRM-protected videos and software. Zango's consumer website asserts that the company is "committed to creating a content economy built on a foundation of safe and ethical practices by protecting consumer privacy while offering a fulfilling and high-value content experience." Zango content includes sports, comedy, dance, erotic videos, online games, and screensavers. Warner Bros. and others have been known to provide content, although Warner Bros. has terminated its business relationship with Zango after an online outcry.

### **Zango Easy Messenger**

Undesirable behaviors associated with Zango Easy Messenger include:

- automatically runs on startup
- displays pop-up advertisements
- installs adware.

### **Zango Cash Toolbar**

• A number of user pages on the MySpace domain which have videos that look like they are from YouTube. The videos have an installer embedded within them for the Zango Cash Toolbar. When users click on the video, they are directed to a copy of the video, which is hosted on a site called Yootube.info.

Third parties are paid by Zango to install Zango software without the required user consent. Zango's past features a remarkable series of bad-actor distributors, from exploit-based installers to botnets to faked consent. Even today, some distributors continue to install Zango without providing the required notifications and consents.

### **Seekmo**

Seekmo is an adware program by Zango that claims to be a free tool to provide content such as mp3 files, screen savers and videos. Seekmo can pop-up advertisements even if you have a pop-up blocker on your computer, and will monitor your computer usage to gen-

erate ads that you are more likely to respond to.

## **2. Hotbar** - 2007 average proportion of PCs infected: **7.0%**

Hotbar (also known as HbTools) is a plugin for Internet Explorer, Microsoft Office Outlook, and Outlook Express. Hotbar adds a toolbar and the option of extra skins to these programs. It also allows the user to add emoticons to emails created in Outlook or Outlook Express or check the weather report. Its major revenue comes from the excessive use of pop-ups which are displayed according to a user's behavior and current URL. The application can show over 15 pop-ups a day, depending on how much Internet browsing has occurred.

Undesirable behaviors associated with Hotbar include:

- bombards users with ads in pop-ups, web browser toolbars, Windows Explorer toolbars, auto-opening sidebars, and even desktop icons
- failing to affirmatively show a license agreement.

Originally independent, Hotbar has since been acquired by Zango.

## **3. Drivecleaner** - 2007 average proportion of PCs infected: **6.1%**

DriverCleaner is a program that is silently installed by using an exploit or social engineering. The program falsely claims the PC is infected and will not clean until you purchase the software. This threat is often installed along side the Vundo Trojan that holds position 5 on the dozen demons list.

## **4. Winfixer** - 2007 average proportion of PCs infected: **6.1%**

Winfixer is a program that is silently installed by using an exploit or social engineering. The program falsely claims the PC is infected and will not clean until you purchase the software. This threat is often installed along side the Vundo Trojan that holds position 5 on the dozen demons list.

## **5. Virtumundo** - 2007 average proportion of PCs infected: **6.0%**

Virtumundo is a trojan that typically uses social engineering tricks and silent install websites to get installed. Many have been observed to install fraudulent security software such as Winfixer or DriverCleaner.

Also known as VirtualMundo and VirtuMonde, Virtumundo facilitates the spread of adware and spyware that results in large amounts of unsolicited pop-up advertisements. The threat regularly contacts predetermined web sites to receive ads and additional instructions. VirtuMundo is also bundled with spyware and advertising-supported applications that automatically run on every Windows startup.

## **6. WhenU** - 2007 average proportion of PCs infected: **5.7%**

WhenU, a popular adware company make an array of products such as Save Now and WhenU search. These products are installed by themselves as well as bundled with 3rd party applications such as screen savers and shareware.

WhenU offers contextual advertising through their software. The software selects which advertisements and offers to show you based on several factors, including which web pages you visit, search terms you use while searching online, the content of the web pages you view, and your local zip code (if you have supplied it.)

### **WhenUSearch**

WhenUSearch is an adware application that creates a special desktop toolbar, monitors user Internet activity, collects details of performed web searches and serves marketing and advertising content. WhenUSearch can update itself via the Internet. The adware is bundled with ad-supported WhenU.com software. It can also be manually installed. WhenUSearch runs on every Windows startup.

### **SaveNow**

SaveNow is adware that delivers relevant offers, coupons, and advertisements to you based on your web browsing habits. SaveNow

may track which web pages you visit, the search terms you use while searching online, the content of the web pages you view, and your local zip code. This information may be used to base which advertisements and offers to show you.

## **7. IBIS** - 2007 average proportion of PCs infected: **4.9%**

IBIS are a company that distributed a toolbar that used several unique methods to make it difficult to be manually removed or cleaned with security software. This toolbar was discontinued by Ibis LLC last year but still remains installed on many users machines.

### **IBIS Toolbar**

IBIS Toolbar is a web browser toolbar that may redirect your search requests and display pop-up advertisements. IBIS Toolbar may monitor your Internet activity, including your search requests, websites you are visiting, products you are buying, and data you enter into forms. IBIS Toolbar may share this information with third party partners. IBIS Toolbar may also download and install adware without your knowledge or permission. IBIS Toolbar may prevent you from visiting various anti-spyware websites. IBIS Toolbar is typically distributed through pop-up advertisements and bundles with other spyware, such as CyberDoor.

## **8. Purity Scan** - 2007 average proportion of PCs infected: **4.6%**

Purity Scan is a program that is supposed to scan your PC for pornography. This program has been installed with the use of exploits and social engineering tricks. Purity Scan is owned by Clickspring and is also known to go by the alias VirtuScope.

PurityScan is a free tool that checks your computer for objectionable adult content. PurityScan scans your computer files and Internet history for keywords that may hint at pornographic material. When it locates questionable content, it displays the URL, word, or file name in a display table so you may delete it. After installation, when you connect to the Internet PurityScan may also launch advertisements, and automatically update itself.

PurityScan upgrades may include the automatic installation of third party applications.

#### **9. Zlob** - 2007 average proportion of PCs infected: **4.5%**

Zlob is commonly assigned to trojans that pose as video codecs on adult websites and have also been noted to spoof popular video services such as YouTube. These trojans have been noted in the wild to install fraudulent security applications as well as DNS hijackers.

Zlob is a backdoor designed to give the attacker remote control over a compromised PC. It changes essential computer settings and modifies certain files. Zlob starts automatically on every Windows startup and hides its activities by injecting code into explorere.exe. It waits for remote connections and allows the attacker to download and install additional software, execute certain commands and manage the entire computer. Zlob can be very dangerous. Use antivirus and malware removal tools in order to get rid of this spyware.

Zlob Trojan installs many popular rogue anti-spyware programs, among them are IEDefender, AntiVirGear, SpyShredder, WinAntiVirus Pro 2007, Ultimate Cleaner and SecurePCCleaner.

#### **10. New.net** - 2007 average proportion of PCs infected: **4.1%**

NewDotNet is a layered service provider to the TCP/IP stack that allows other domain suffixes besides .com such as .xxx and .shop. This application is commonly bundled with other software.

NewDotNet is an Internet Explorer plug-in that sends a web browser to sponsored web sites whenever the user enters a non-existent or mistaken site address into the address bar. The threat can track user browsing habits and may show commercial pop-up advertisements. It is able to silently update itself via the Internet. NewDotNet is bundled with a variety of advertising-supported products. It also can be manually installed. The threat runs on every Windows startup.

NDotNet is an adware program that associates non-existent domain names with sponsored content. When a user enters a keyword into a browser address bar or types a mistaken or non-existent URL, the adware redirects the user to a sponsored page.

#### **11. Softomate** - 2007 average proportion of PCs infected: **3.4%**

Softomate are a company that provides customizable toolbars. Some of the toolbars created are used in a malicious fashion and others are used for legitimate purposes.

Softomate toolbars may change your browser settings and redirect your search requests through a parent server. Softomate may also monitor your Internet activity and habits and launch pop-up advertisements accordingly.

#### **12. Starware / Comet Systems** - 2007 average proportion of PCs infected: **3.1%**

Starware is an Internet Explorer toolbar with specialized search functions and a pop-up blocker. Starware Toolbar may display advertisements and redirect your search requests through their parent server. Bug fixes and new features may be added to Starware Toolbar without your notice.

George Moore is a senior threat researcher at Trend Micro specializing in spyware and adware. He focuses on the methods by which Web threats surreptitiously install and protect themselves on user PCs as well as the organization and economics of malware publishers.

Anthony Arrott is a special assistant to the CTO at Trend Micro. He manages threat analytics operations and threat data sharing agreements with outside organizations.

Together in 2007, the authors led the project team for Trend Micro HijackThis v2.0 - enhancing the popular malware diagnostic tool originally developed by Merijn Bellekom.

# NEW THREATS. NEW SOLUTIONS.

The stakes are high for today's network defenders.

New security threats to governments and businesses emerge hourly, from sophisticated wireless attacks to remotely organized Bot armies.

Black Hat Europe brings together the best minds in computer and network security to define tomorrow's information security landscape.

**March 25-28**

Moevenpick Hotel  
Amsterdam City Centre  
The Netherlands

Black Hat returns to Europe with an expanded program with six full tracks, more trainings and more intense, comprehensive presentations on the hottest topics in information security. Please join us for the very best technical security conference on the European continent. It's security done right,



# BLACK HAT STYLE.

Diamond Sponsor

**Microsoft®**

Gold Sponsors

**CORE**  
SECURITY TECHNOLOGIES

**Google**

**IOActive**  
COMPREHENSIVE DIALECTIC SECURITY SERVICES

**QUALYS®**  
ON DEMAND SECURITY

# Weaknesses and protection of your wireless network

By Rob Faber



The ease of use of wireless networks and being able to be connected everywhere and at any time is a part of our lives. Unfortunately this also comes with some disadvantages. Properly protecting your WLAN, both at home and at the office, can be a challenging task. This time we dive a bit deeper into the known weaknesses, misconfiguration and protection of wireless networks.

WiFi, WLAN, Wireless, GPRS, EDGE, HSDPA, UMTS, Bluetooth, are all technologies that are used intensively in our world today, where information is available anywhere, at anytime. Wireless networks appear to be everywhere these days. You can find them on airports, in restaurants, at the office and of course at home. And the use of it will only increase in the coming years. However, the fact is that alongside all that freedom there are also several security issues that must be dealt with effectively.

It should be made clear that there are some implementations out there today that don't even begin to address the starting points of information security. Despite the many breaches, warnings and recent headlines in newspapers, WEP (Wired Equivalent Privacy) for example is still being widely used today. Not only in a home environment but also within company networks.

Security and hacking methods are continuously evolving and mean that there is a definite need to stay informed.

This time we'll take a look at sniffing and analyzing WLAN traffic - working with Wireshark and AirPCap, and also how to better protect a WLAN with for instance EAP/TLS.

## Sniffing and monitoring a wireless network

Sniffing, or catching packets on a wired ethernet network is relatively easy. Just plug in a network cable, install a packet sniffer on your laptop and start a capture while the network card is set to promiscuous mode. When it comes to wireless analysis however, the sniffing of traffic becomes more complicated. This is because wireless networks operate on multiple channels, using different frequencies and broadcast in the open air.

Most wireless network cards support different modes of operation. Normal behavior in many cases will be the user connecting with a wireless network card to an Access Point (AP). This is the so-called “managed mode”. Another option is to connect directly to another wireless device without using an Access Point, the so called “ad-hoc mode”. The third option is the “master mode”, where the wireless card can act as an Access Point to serve other wireless devices. This mode can be used for hacking purposes because the attacker is able to pretend to be a legitimate Access Point in your network, which - of course - it isn’t.

The final option is the “monitor mode”. In this mode the wireless network card will just listen on a specific channel and then stealthily capture packets. Naturally, the monitor station will not announce itself and will thus be completely undiscoverable.

Most Windows’ drivers for wireless cards unfortunately do not provide support for this monitor mode. So by using - for instance - the AirPCap adapter, it is possible to make use of this specific mode and listen to a channel while remaining “below the radar” and not interfering with other traffic.

If you want to analyze wireless traffic, the first step is to find the channel or frequency used by another Wireless station, or the Access Point. You will then be able to eavesdrop on the conversation. With this information, it is possible to configure your wireless card to use the same channel and start collecting packets. Normally, a wireless card can only fully operate on one frequency at a time. The Kismet and Cain tool both makes it possible to scan or “hop” around between different channels, just to check if communication is going on.

## WITH A NETWORK SNIFFER IT IS POSSIBLE TO ACTUALLY DISPLAY WHAT IS GOING ON IN THE AIR AROUND YOU

### Preparation: how to monitor WLAN traffic

With a network sniffer it is possible to actually display what is going on in the air around you and catch the wireless networks and in this way identify security vulnerabilities such as weak encryption or authentication problems. The tools used in this article for ethical hacking also uses a wireless adapter with the special features described earlier.

In this article we use the AirPcap adapter. In order to overcome the limitations of most wireless drivers for Windows systems as discussed earlier, CACE Technologies ([www.cacetech.com](http://www.cacetech.com)) introduced a commercial product called AirPcap. It is a combination of a USB IEEE 802.11 a/b/g adapter, supporting driver software, and a client configuration utility. AirPcap provides a mechanism for capturing wireless traffic in monitor mode on Windows workstations. The adapter is ideal for this purpose and personally I like it because the ease of use. Other wireless cards can be used also such as from Atheros. You’ll have to keep in mind that the wireless card (and driver) have to support monitor mode. See for yourself what you prefer.

### Sneaking into a wireless network

There are several tools that can be used to sneak into a wireless network. An extensive list is available today and includes EtterCap, Kismet, Cain&Abel, Netstumbler, THC-RUT, Hotspotter, ASLEAP, THC-LEAPCracker, AirSnort, Airodump, HostAP, WEPWedgie, WEPCrack, AirSnarf, SMAC, AirJack, DSSniff, IKECrack and Nessus. Please note that this list is by no means exhaustive. Next we will discuss a couple of the better known tools placed within a scenario. This can be representative case to gather information and discover vulnerabilities in wireless networks.

I’ll stress the fact that all I present to you only can be practised in a test environment or on your own network for ethical and legal reasons!

### Gather basic information using Kismet

Kismet is a common used tool for site surveys. It features a little functionality that NetStumbler is missing: displaying Wireless Networks that are not broadcasting their SSID.

Access Points broadcast this information most of the time and Kismet will also detect and display SSIDs that are not being broadcast in the open. The first thing that you have to do is to get a clue on the wireless networks that are out there. To get this information fire up Kismet.

I sniffed around a bit and the result you can find in the next screenshot. You can see now

that there are indeed networks active (and when I installed the external antenna of the AirPCap about 20 networks more showed up!). The next step then is to gather information about a specific network. Like this, it is possible to detect rogue APs easily in your business environment. Now you have to sort the networks presented on your screen (by pressing "s") so you'll be able to select one of them and get detailed information.

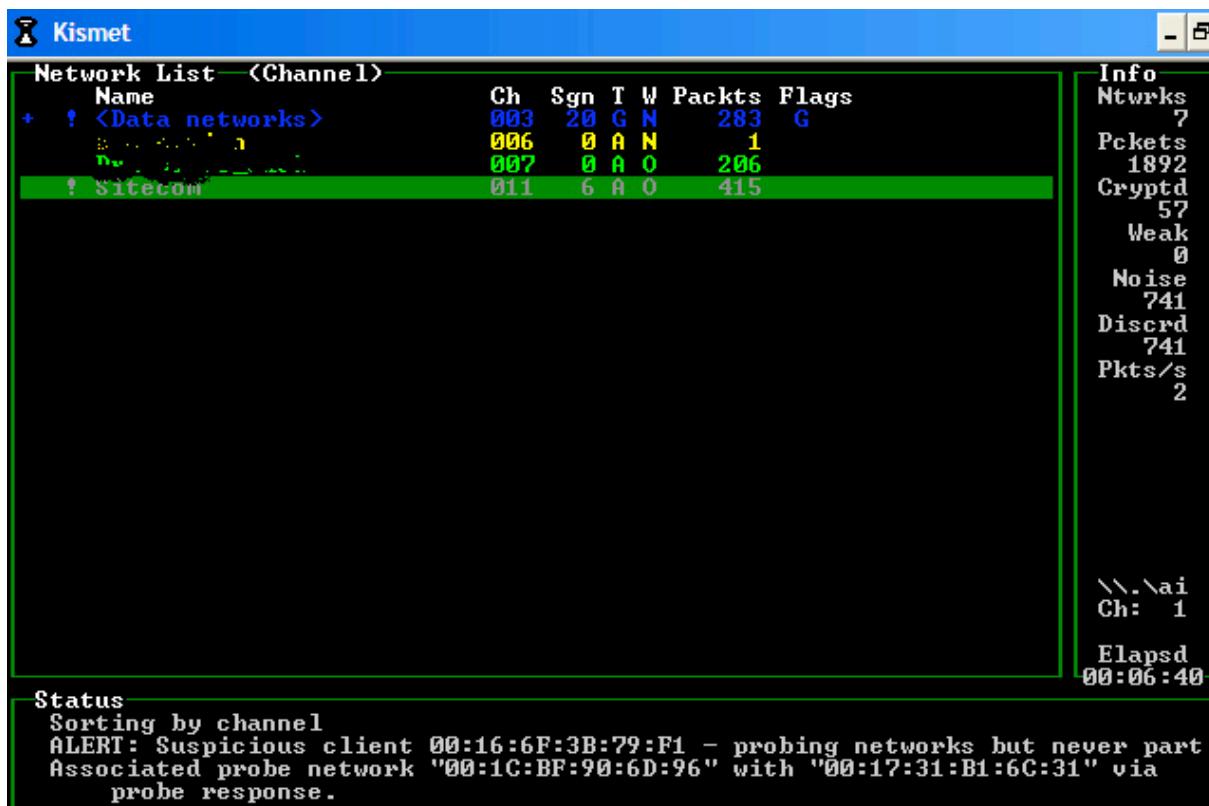


Figure 1. Kismet presenting wireless networks.

To have a better look now, select a (your!) network, highlight it and press "i". An example of the information that can be presented here you can find in the next screenshot. Presented are the SSID, the BSSID, the active channel and the encryption method currently used. If WEP or WPA PSK is used for encryption you'll know that because Kismet is presenting this information straight forward. Attackers will ultimately use this like you did to get some weak spots and to possibly gain access to a network.

### Collecting information using Kismet, Cain and Airodump-ng

The tool Cain & Abel from Oxid is a very sophisticated password recovery tool that allows

you to recover various kinds of passwords. On networks it works by collecting packets from the network and cracking encrypted passwords by either using a dictionary, brute-force, or cryptanalysis attacks. With this tool it is possible to collect packets and then later on recover WEP keys. AiroDump is a tool that is part of the AirCrack suite.

With AiroDump-ng the same basic features are presented that you can find in Cain only command prompt orientated. AirCrack-ng makes it possible to derive a WEP key. There are a couple of methods that can be used to crack WEP and WPA. Both are supported in the mentioned tools.

**Kismet**

**Network List <Channel>**

**Network Details**

- Name : Sitecom

**SSID : Sitecom**

**Server : localhost:2501**

**BSSID : 00:0C:F6:2D:C3:A6**

**Carrier : IEEE 802.11b**

**Manuf : Unknown**

**Max Rate: 11.0**

**BSS Time: ae131c4046**

**Max Seen: 1000 kbps**

**First : Fri Jan 18 13:32:45 2008**

**Latest : Fri Jan 18 13:41:13 2008**

**Clients : 0**

**Type : Access Point (infrastructure)**

**Info :**

**Channel : 11**

**Privacy : Yes**

**Encrypt : TKIP WPA PSK**

**Decryptd: No**

**Beacon : 25600 (26.214400 sec)**

**Packets : 565**

- Data : 0
- LLC : 565
- Crypt : 0
- Weak : 0
- Dupe IU : 0
- Data : 0B
- Signal :
- Power : 6 (best 29)
- Noise : -101 (best -104)
- IP Type : None detected
- Min Loc : N/A
- Max Loc : N/A
- Range : N/A

Figure 2. Detailed information from Kismet.

File View Configure Tools Help

Decoders Network Sniffer Cracker Traceroute CCDU Wireless

AirPcap USB wireless capture adapter nr. 00  
\\.\airpcap00 Stop

AirPcap  
Driver version: 3.1.0.965  
TX ch: 1,2,3,4,5,6,7,8,9,10,11,12,13  
Current channel: 3

Lock on channel: WPA-PSK Auths  
Hopping Send to Cracker

Capture WEP IV's to dump.ivs file

Analyze Delete Save As

Packet Injection TxRate (Mbps)  
ARP Requests 2

BSSID	Last seen	Vendor	Signal	SSID	Enc	Mode	Channel	Rates (Mbps)	Packets	Unique WEP IVs
00:0C:F6:2D:C3:A6	12/10/2007-14...	Siemens AG	-96 dBm	S	WEP?	Infrastructure	1 (2412000...)	9, 18, 48, 5...	16	0
00:0C:02:00:13	12/10/2007-14...	SONIC SYS...	-77 dBm	V	WEP?	Infrastructure	1 (2412000...)	6, 9, 12, 48...	57	0
00:0C:BA:0F:A4	12/10/2007-14...	3COM EUR...	-82 dBm	WPA	WPA	Infrastructure	8 (2447000...)	6, 9, 12, 18...	78	0
00:14:C9:41:3E	12/10/2007-14...	Netgear Inc.	-99 dBm	G	WEP?	Infrastructure	6 (2437000...)	6, 9, 12, 48...	6	0
00:14:FB:1C:FD	12/10/2007-14...	Cisco-Linksys...	-96 dBm	linksys	WEP?	Infrastructure	11 (246200...)	6, 9, 12, 48...	20	0
00:0C:51:0A:65	12/10/2007-14...	Sitecom Eur...	-98 dBm	J	WEP?	Infrastructure	11 (246200...)	6, 9, 12, 18...	5	0
00:0C:9FFE:E2	12/10/2007-14...	U.S. ROBO...	-97 dBm	WPA	WPA	Infrastructure	11 (246200...)	6, 9, 12, 48...	21	0
00:01:35:74:ED	12/10/2007-14...	Siemens AG	-94 dBm	F.....	WEP?	Infrastructure	11 (246200...)	9, 18, 48, 5...	9	0
00:01:3C:04:D4	12/10/2007-14...	Siemens AG	-98 dBm	WEP?	Infrastructure	11 (246200...)	9, 18, 48, 5...	16	0	
00:17:1B:1E:31	12/10/2007-14...	ASUSTek C...	-95 dBm	L	WEP?	Infrastructure	7 (2442000...)	6, 9, 12, 48...	5	0
00:6E:F5	12/10/2007-14...		-87 dBm	Z...	WPA	Peer	9 (2452000...)	6, 9, 12, 18...	16	0

MAC Address Last seen Vendor Signal Rate Packets ARP Requests

Figure 3. The interface of Cain & Abel.

Now that some basic information is available a hacker can set up an attack. It is possible to simply collect packets using Cain & Abel or Airodump-ng and use this information for offline analysis trying to uncover the WEP key being used or to capture a four way hand-shake in case of WPA-PSK and more actively start a hack. How? I'll show you.

## WEP vulnerabilities

WEP uses the RC4 stream cipher for encryption. RC4 is used for the confidentiality part and the CRC-32 checksum for integrity.

Stream ciphers like RC4 are vulnerable if the same key is used multiple times. This is called collision in cryptography. One way to get around this problem is to use an initialization vector (IV). This IV is an extra added value (random) in the encryption process. Combined with a secret master key the one-time key for the stream cipher is created. One of the many problems with WEP is that the IV is too short, 24 bits. In this case of WEP it is possible that the same IV would be used more than once if thousands of packets were sent with the same master key. So by capturing enough packets it is possible to break the encryption method.

The mainly used versions of WEP are the 64-bit with an IV of 24 and the 128-bit version with a 24 bit IV. WEP uses in the 64-bit variant a 40 bit key, together with a 24-bit initialization vector (IV). In case of 128-bit WEP the key is most of the times a string. Each character represents 4 bits of the key.  $4 \times 26 = 104$  bits.

Together with the 24-bit IV will make the 128-bit WEP key.

Cracking the WEP key requires interception of lots of transmitted packets and this will take quite some time. There are active attacks that stimulate the necessary traffic. In 2004 a new WEP statistical cryptanalysis attack method (KoreK) became available. The code and method is currently supported in Cain and AiroCrack-ng. This KoreK attacks changed everything. Before that a packet collection worked only well with lots of packets due to the fact that only certain "interesting" or "weak" IVs were vulnerable to attack.

Kismet tells you how many of these packets have been gathered. If you use Kismet for network discovery and sniffing, it breaks down the packet count for you, displaying the number of "encrypted" packets separately from the total number, as shown in my screen capture on the right.

It is now no longer necessary that millions of packets are required to crack a WEP key. In this attack method the critical ingredient is the total number of unique IVs captured, and a key can often be cracked with hundreds of thousands of packets, rather than millions.

The number of packets required for success varies. To present some figures here: a minimum of 200,000 for a 64-bit WEP key and around 500,000 for a 128-bit WEP key. Only encrypted packets with unique IVs counts in this situation.

```
C:\WINDOWS\System32\cmd.exe - aircrack-ng -a2 capture.cap -w password.lst
Aircrack-ng 1.0 beta1

[00:00:01] 230 keys tested (144.29 k/s)

KEY FOUND! [ . . . . ]

Master Key      : CD D7 9A 5A CF B0 70 C7 E9 D1 02 3B 87 02 85 D6
                  39 E4 30 B3 2F 31 AA 37 AC 82 5A 55 B5 55 24 EE

Transient Key  : 33 55 0B FC 4F 24 84 F4 9A 38 B3 D0 89 83 D2 49
                  73 F9 DE 89 67 A6 6D 2B 8E 46 2C 07 47 6A CE 08
                  AD FB 65 D6 13 A9 9F 2C 65 E4 A6 08 F2 5A 67 97
                  D9 6F 76 5B 8C D3 DF 13 2F BC DA 6A 6E D9 62 CD

EAPOL HMAC     : 52 27 B8 3F 73 7C 45 A0 05 97 69 5C 30 78 60 BD
```

Figure 4. AirCrack in action.

## The weak spots: attacks against WPA

WPA or Wi-Fi Protected Access is introduced to overcome some weaknesses of WEP. WPA ultimately provides every user with different keys or provides a dynamic generation of keys. In smaller offices or companies and at home the more complex and expensive 802.11x will leave the choice to WPA-PSK. PSK stands for Pre Shared Key.

The PSK provides an easily implemented alternative to generate a Master Key. This same principle is used in the more complex 802.1X where there is also a generated Master Key. Within PSK a 256-bit key is used directly as the Master Key. The Pre Shared Key (PSK) is most of the times a passphrase (also kept in the Access Point), the Master Key then is derived from this passphrase.

Currently the method used to break the WPA-PSK is a dictionary attack at the four way handshake.

## The four way handshake

When a wireless client tries to gain access to an access point (AP) there will be a little conversation between the client and access point (AP). This is the so called “4-way handshake”. The WPA handshake was designed to occur over insecure channels and in plain-text so the password is not actually sent across. There are some algorithms as described before that eventually in the background turn it into a primary master key, PMK.

The only step is to have a capture of a full authentication handshake from a wireless client and the AP. If you are lucky you will capture a full handshake and at that time you can start a dictionary attack. Again: it can take some time to catch a full handshake. So we can force this behavior of an authentication handshake by launching a de-authentication attack. If the wireless client is already connected we can force the connected client to authenticate itself again by sending de-auth packets.

The reaction of the OS of the wireless client will be to reconnect to the AP and thus performing the 4-way handshake! When we cap-

ture the re-connect and authentication, it saves time so we don't have to wait for the wireless client to do it themselves. Now that we have captured the 4-way handshake and saved it, we can start AirCrack-ng to work offline with a dictionary attack. Most pass-phrases are simple, short and easy predictable so in most cases there will be success!

I showed you the weaknesses of WEP and WPA. That concluded the hacking part and brings us to the countermeasures and tools you can use to close the gates.

## Analyze traffic with Wireshark

You can use the Wireshark protocol analyser to have a better look at the traffic and analyse it in an understandable way. Although there are other solutions on the market (for example Wildpackets with Omnipcap and Microsoft with Network Monitor and other commercial solutions) we chose to use this tool for this article because of the perfect cooperation with the AirPcap.

There is no doubt that Wireshark is a valuable tool. While this is open source software it can be downloaded instantly from their website ([www.wireshark.org](http://www.wireshark.org)). It is possible to scan ethernet data and it comes with some extensive filtering capabilities. Of course, it can also be used to capture 802.11 traffic.

For wireless traffic, Wireshark presents the “packet list pane” which will give you an overview of all the packets captured (find it in figure 5 under section 1). If you zoom in on a specific packet, you can find information about it in the “packet details pane” (section 2) and finally, you will find the raw bytes of the contents at the lowest part of the screen (section 3).

The IEEE 802.11 header can be found in figure 6. As you can see, this is fairly complex and wireless frames can have additional protocols appended to them. A lot of flags such as power management and encryption options can be set. By using specific filter options it becomes much easier to search for the specific data you are interested in and likewise exclude traffic that isn't of interest.

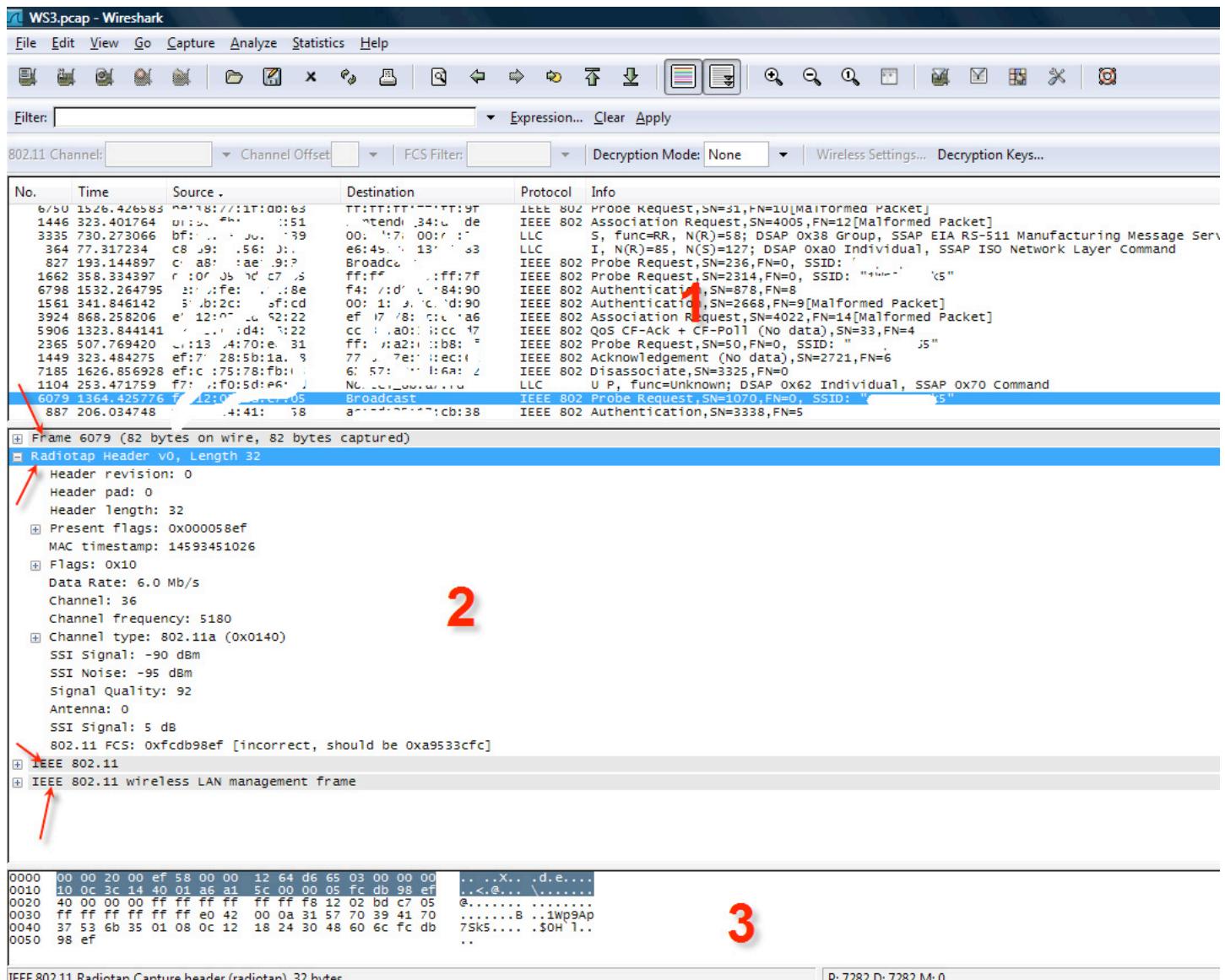


Figure 5. The Wireshark screen.

## Protecting your wireless network: 802.1X

The 802.1X standard provides the opportunity to carry out authentication and encryption based on certificates and that on mutual basis. Public Key cryptography (PKI) shows up here!

The 802.1X standard has been developed to block or restrict access on a port. The moment a computer initiates a connection with, for example an Access Point (AP) in your network, there must be successful authentication before there is a complete network connection. Until that point, protocols such as DHCP and HTTP are permitted. So all traffic will be blocked at the Data link layer of the OSI model. Actually, 802.11X is somewhat misleading due to the suggestion that it can be used purely for Wireless networks. This is

however a misunderstanding and this solution is even more widely used in wired networks.

## PKI and wireless networks

PKI or a Public Key Infrastructure can be used to centrally manage certificates. These certificates can be enrolled and in this way they can be used to control access to the wireless network. As well as the authentication, there is also the opportunity to encrypt the network traffic.

The protocol that we use in these cases is EAP-TLS. EAP-TLS works with X.509 digital certificates. EAP is the acronym for Extensible Authentication Protocol, where TLS is Transport Layer Security. EAP is the part of the protocol that simply fills in the authentication gap that 802.11 has.

```

+ Frame 887 (66 bytes on wire, 66 bytes captured)
+ Radiotap Header v0, Length 32
- IEEE 802.11
  Type/Subtype: Authentication (0x0b) ←
  - Frame Control: 0xD8B0 (Normal)
    Version: 0
    Type: Management frame (0)
    Subtype: 11
  - Flags: 0xD8
    DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
    .... 0... = More Fragments: This is the last fragment
    .... 1... = Retry: Frame is being retransmitted
    ...1 ..... = PWR MGT: STA will go to sleep
    ..0. .... = More Data: No data buffered
    .1... .... = Protected flag: Data is protected
    1.... .... = Order flag: Strictly ordered
  Duration: 61513
  Destination address: ae:a:b:c:d:e (ae:ad:b:c:d:e)
  Source address: fb:c:d:e:f:g (fb:c:d:e:f:g)
  BSS Id: 91:c9:1b:4f:17:16 (91:c9:1b:4f:17:16)
  Fragment number: 5
  Sequence number: 3338
- Frame check sequence: 0xdf35b8c7 [incorrect, should be 0x91d3159c]
  [Good: False]
  [Bad: True]
- WEP parameters ←
  Initialization Vector: 0x48303e
  Key Index: 2
Data (2 bytes)

```

Figure 6. The IEEE 802.11 headers.

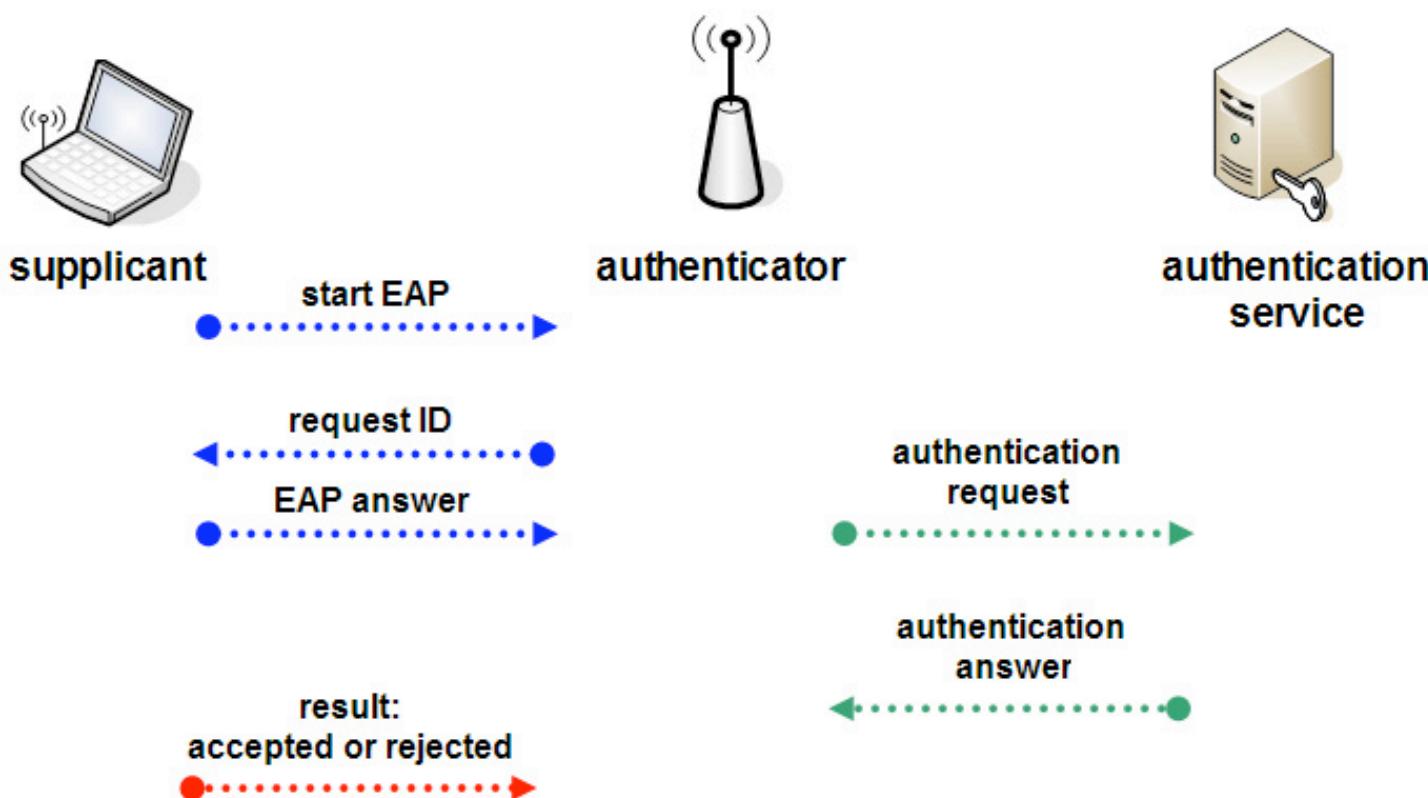


Figure 7. The EAP-TLS handshake.

## EAP-TLS

In the whole process, there are roughly three parties involved. The supplicant requests access onto the wireless network. This can be a laptop computer with a wireless card. The authenticator is the one receiving that request. Most of the time this will be an AP or Access Point. And third, there is the authenticating service. This will be the server or appliance that processes the request and then decides if access is granted. As you can see, there is strict separation between the entry point in the network (AP) and the party that accepts or rejects the request (authenticating services). If the authenticating service grants access, the supplicant can make a full connection to the network.

There is no other possible traffic in the first stage of access. It is just traffic that is necessary for the authentication process. The authenticator will perform an EAP-request and ask the supplicant to identify itself. The answer will be passed to the authenticating server. The authenticating server then checks if the request is acceptable and access can be granted. If access is granted, the port will be opened for other traffic. Otherwise, the request will be rejected and no access is possible to the wireless network. The authenticating

service will pass on to the authenticator the order to either open the network port or keep it closed.

Within the EAP-TLS handshake, the authentication service will exchange a digital certificate with the wireless device. This is called "mutual authentication". Thus it is not only the wireless device that hands over a certificate but also the authenticating service (server).

The steps in this process are almost the same as those found in setting up an SSL connection to a web server (more specifically: between a web browser and the web server). The server in this case also presents a certificate.

The SSL protocol is therefore the predecessor of TLS. If the procedure is successfully completed, the wireless device is connected and receives a certificate from the authenticating service (server or appliance in most cases). In the event that the wireless device accepts this certificate (and this is what you want of course for your certificates) both partners accept communication. EAP-TLS now provides the opportunity to exchange the keys that will be used to set up an encrypted tunnel for safe communications.

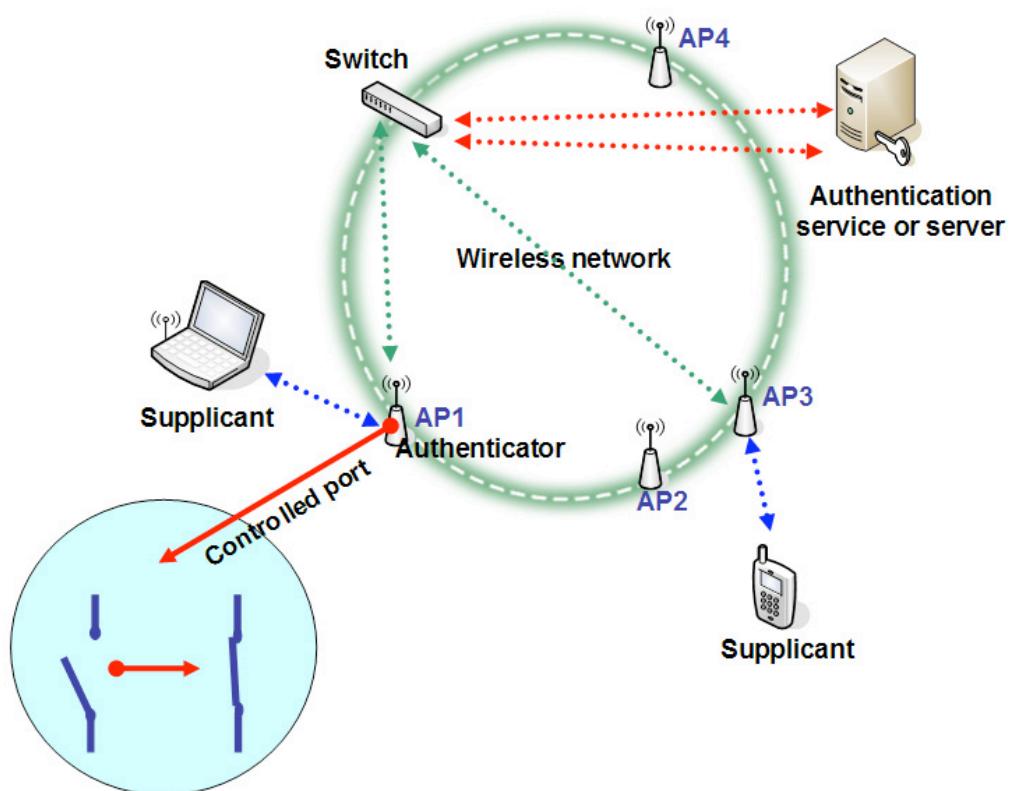


Figure 8. Wireless network and EAP-TLS.

## How to stay in control

In larger wireless networks with a lot of Access Points (AP's) and large numbers of workstations, the question arises as to how to manage all this effectively. Setting up all workstations with the proper configuration and rolling out the certificates can be a real disaster if it isn't automated correctly. In daily life, we want to be able to streamline this process as much as possible but still be sure that it is safe.

Although a number of manufacturers have implementations of RADIUS, or support for 802.11X, we set about looking for a solution in combination with a Microsoft infrastructure. In this case, we made use of Internet Authentication services (IAS) and the Microsoft Certificate services. The main reason for this restriction in this article is that many companies will have a network in place, which is mainly

based on Windows client computers. There are of course alternative solutions available such combinations or stand alone solutions from Cisco, Nortel or Blue Socket. It depends on the needs of the organization and architectural starting points.

Initially, Microsoft IAS was frequently used to serve both authentication and authorization in a centralized way for users who make connections into the network from outside the company. But IAS can be used satisfactorily as a central authentication server within Wireless networks. The IAS server in this case must be incorporated in the same Active Directory domain where the users and computers that want to make use of the wireless network can be found. IAS can then use data already present in the Active Directory database. This can be easy to do and yet less time consuming as most organizations will have set up an Active Directory.

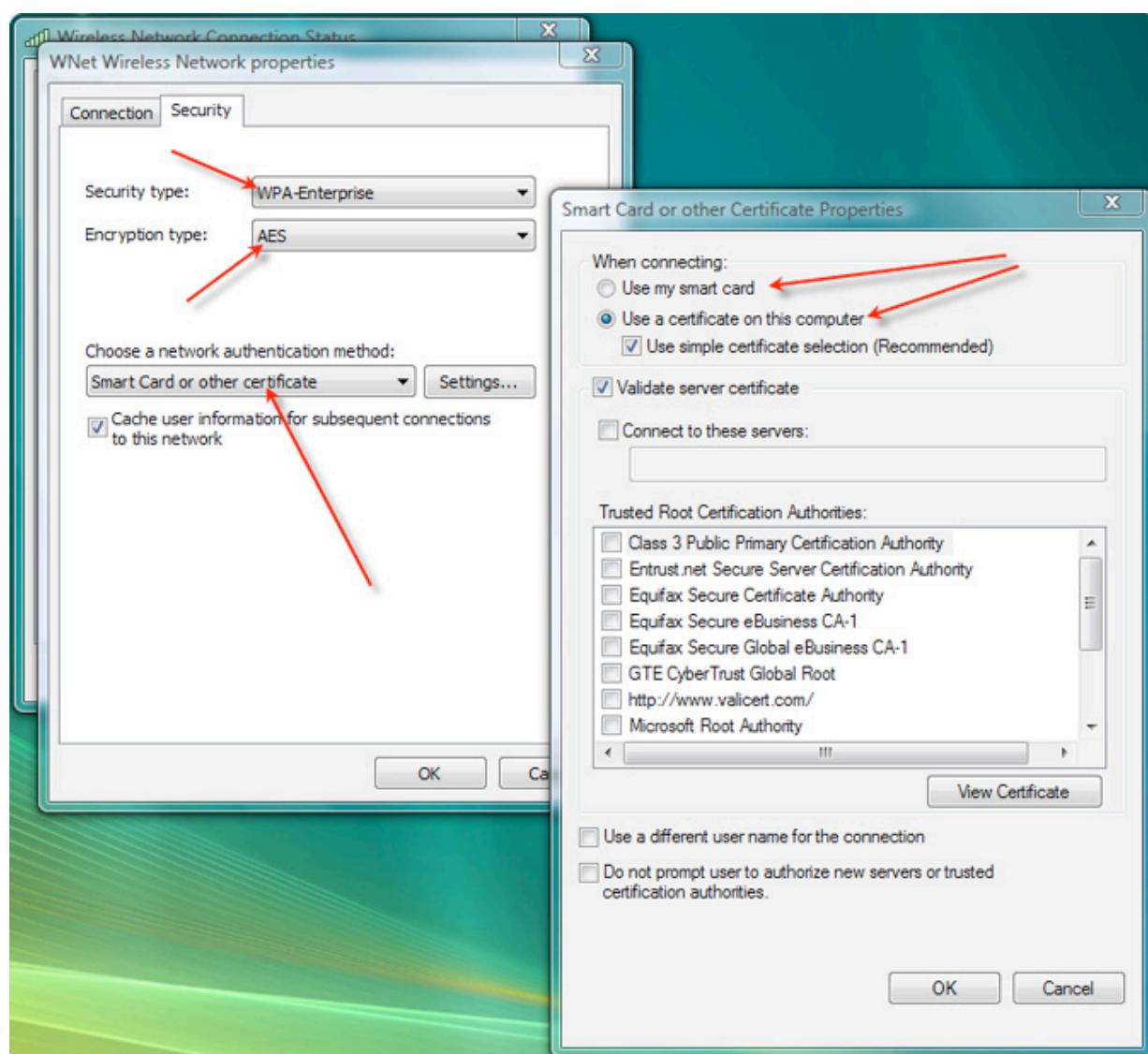


Figure 9. Set up the use of certificates in Windows Vista.

In addition to the IAS/RADIUS solution, you also have to set up a PKI infrastructure. For this purpose, the Microsoft certificate server can be used to issue the X.509 digital certificates needed for EAP-TLS. It is outside the scope of this article to discuss the installation / implementation of the PKI fully. Within the Microsoft solution it is possible to automate the roll out of certificates to both workstations and the IAS/RADIUS, by making use of the so-called "auto-enrollment". This is possible because the client computers and the IAS server are already members of the Windows domain and have therefore already established trust. It is possible to regulate a couple of settings on workstations by means of Group Policies. Windows XP and Windows Vista are out of the box supporting 802.1X.

Certificates themselves can be stored on the computer (but you have to protect the storage by, for example encrypting the hard drive). The fact that the TPM chip can also play a role in this as a Hardware Storage module (HSM) is new. Although the use of EAP-TLS is more complicated to initially configure and manage (although PKI is necessary and in itself does have some challenges to cope with), at this time, EAP-TLS is the safest method for protecting wireless networks.

### General recommendations securing your wireless network

Finally, here are some general recommendations and best practices on how to secure your wireless network against common attacks.

- Using WEP better than nothing at all but as a minimum 128-bit encryption. If your equipment supports it, just use WPA2 instead. WPA2 supports also AES encryption.
- Ensure your WLAN is protected by using advanced authentication and encryption. If possible use mutual authentication which is supported by the 802.1X standard (EAP/TLS). Relying on just MAC address filtering is certainly not enough!

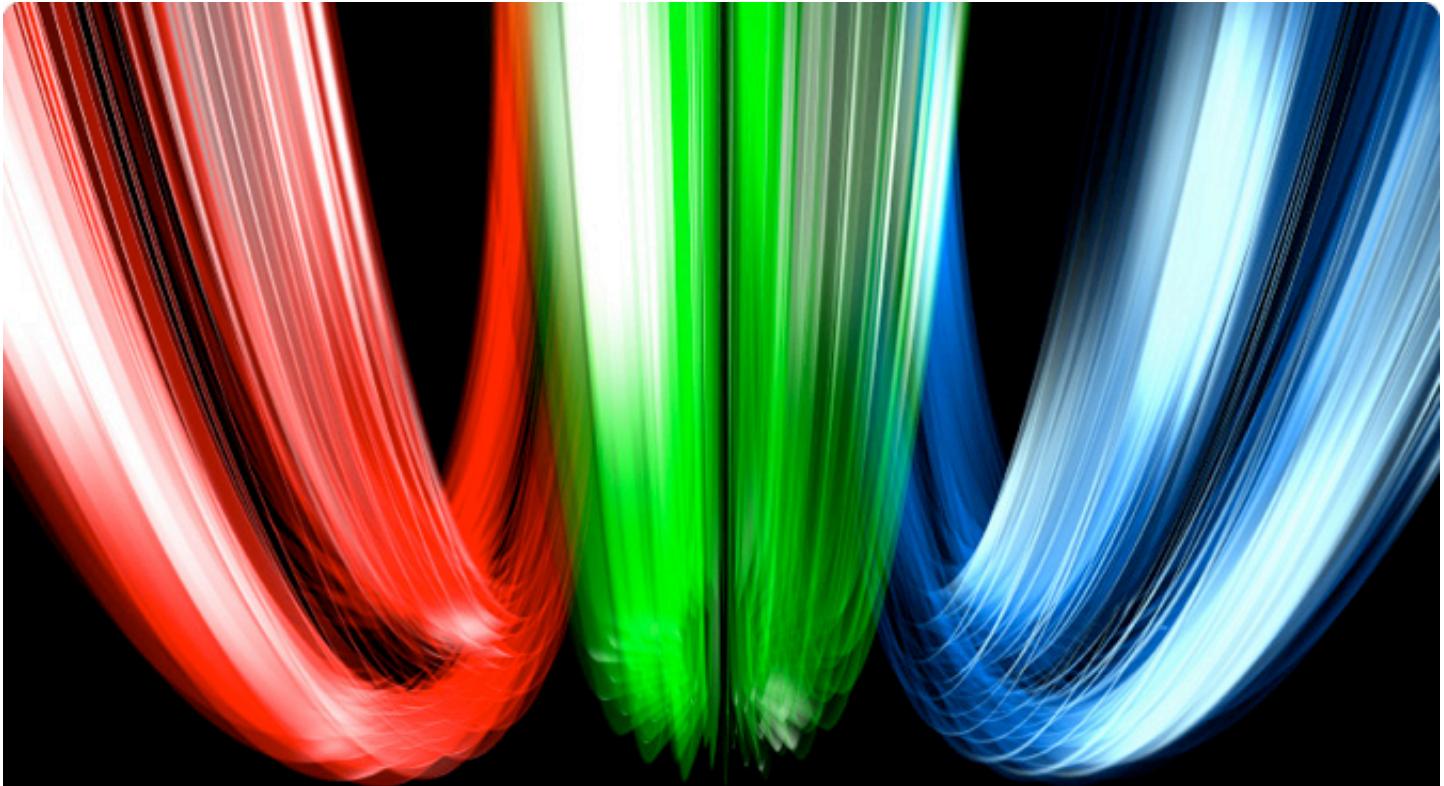
- Use encryption so that any conversations sniffed by an intruder would be very difficult to break. When using a wireless hotspot, use SSL like solutions or IPSec VPN without split-tunnelling. If not, a concept of the Man in the Middle attack (MITM) can be used.
- For smaller organizations. If you use WPA, get a very long and complex WPA pre-Shared Key. This type of key is much harder to crack by performing a dictionary attack. It would take much longer to do so.
- If possible, don't use WPA with a Pre-Shared Key at all. Use a non vulnerable EAP type to protect the authentication and limit the amount of incorrect guesses it would take before the account is locked out. If using certificate-like functionality, it could also validate the remote system that is trying to gain access to the WLAN and will not allow a rogue system to have access to the network. Be aware that the account lockout threshold is below the Windows lockout (or have another precaution taken), otherwise your whole enterprise can be knocked out by just trying all of the accounts a couple of times! So check your configuration thoroughly!
- Take the time to adopt the technology and to properly set up the infrastructure. Have the test lab review it before promoting it to production status.

### Conclusion

Due to the wide adoption of wireless networks and their complexity, it is recommended that you take the necessary measures to prevent the loss or disclosure of sensitive information to the public. Not only is this a concern for you and your company but it can also be part of local legislation!

Take this seriously because it is the main entrance point to the companies' infrastructure. Wireless LAN can be secured, but it takes time to make important decisions. It wouldn't hurt to have some kind of review undertaken, to check out what is going on in your network. This can be done by either making use of a tool like Wireshark, or by hiring an expert to perform an audit or ethical hack.

Rob P. Faber, CISSP, CEH, MCTS, MCSE, is an information security consultant. He currently works for a global company and international IT services provider in The Netherlands. His specialization and main areas of interest are Windows Platform Security, Ethical Hacking, Active Directory and Identity Management. He maintains a weblog at [www.icraniun.com](http://www.icraniun.com) and you can find him on LinkedIn network.



## Fraud mitigation and biometrics following Sarbanes-Oxley

By Paul Sheldon Foote and Reena Hora

### Your company might be compliant, but you are still exposed to fraud.

The old days of external auditors claiming that they are not responsible for detecting fraud and of managements depending upon management letters from external auditors for learning about weaknesses in their internal control systems have changed with the enactment of the Sarbanes-Oxley Act (SOX).

Following SOX, external auditors, corporate attorneys, directors, and managements of large companies have legal obligations to mitigate fraud. Just as it is smart to use seat belts in automobiles regardless of local legal requirements, it is smart to use biometrics to improve internal controls and to mitigate fraud regardless of whether companies are large enough to be subject to SOX or to other mandatory laws, regulations, standards, or to codes. Laws represent minimum standards. Companies may still suffer large losses from frauds even if their internal control systems meet minimum standards.

#### Accounting frauds and scandals

The numbers and sizes of major accounting frauds and scandals became so excessive

that Congress passed and President George W. Bush signed the Sarbanes-Oxley Act (SOX) of 2002. For general summaries of SOX, see [tinyurl.com/2b5t3j](http://tinyurl.com/2b5t3j).

#### Lawsuits and criminal cases

Investors and other third parties who have relied upon managements' representations and certified financial statements have sought to recover their losses in the courts. As experience with SOX and court cases develop, there will be a better understanding of who will be held responsible for accounting frauds, scandals, and internal control failures.

Lawsuits against external auditors, corporate attorneys, directors, and managements will provide evidence of what needs to be done to correct these failures. There can be several legal cases related to the same loss because parties may file cross complaints against each other.

However, there are steps corporations should be taking now to mitigate future frauds.

## Lawsuits against external auditors

Over time, court decisions have expanded the types of third party users of certified financial statements.

In *Ultramares v. Touche & Co.* (1931), the court held that auditors may be held liable for ordinary negligence to a third party - provided that the auditors were aware that their certified financial statements would be used for a particular purpose by known parties.

More recent cases have moved from the known user approach to a foreseen user approach. For example, in *Williams Controls v. Parente, Randolph, Orlando & Associates*, 39 F. Supp. 2d 517 (1999), the court held that

auditors could be liable to a purchaser of a client's business even if the auditor did not know at the start of the audit who the purchaser would be.

In New Jersey, in *Rosenblum v. Adler* (1983), the court extended the liability of auditors to any third parties the auditors could "reasonably foresee" as recipients of certified financial statements for routine business purposes. [Whittington, O. Ray, and Kurt Pany, *Principles of Auditing & Other Assurance Services*, Sixteenth Edition, McGraw-Hill Irwin, 2008]

Certified public accountants will not be able to continue to accept financial audit engagements unless corporate managements mitigate the possibilities of frauds.

**It is not realistic to expect that companies will be able to make no improvements in their internal control systems and to buy enough insurance to cover all possible losses in legal cases.**

## No insurance coverage

It is not realistic to expect that companies will be able to make no improvements in their internal control systems and to buy enough insurance to cover all possible losses in legal cases. For example, one international public accounting firm paid \$6 million to defend successfully a lawsuit involving a client with \$20,000 annual audit fees. At least one major insurance company has responded by refusing to insure accounting firms for legal liabilities. [Whittington, O. Ray, and Kurt Pany, *Principles of Auditing & Other Assurance Services*, Sixteenth Edition, McGraw-Hill Irwin, 2008]

Directors and officers have relied upon the availability of errors and omissions (professional liability) insurance.

## Sarbanes-Oxley act (SOX)

For a long time, external auditors attempted to defend themselves in fraud cases by claiming that the purpose of a financial audit (as opposed to a fraud audit) is not to detect fraud. Sections 302, 404 and 906 of the Sarbanes Oxley changed the responsibilities of corporate managements and of auditors with respect to fraud mitigation.

**Section 302** mandates corporate responsibility for financial reporting and internal controls. It requires the CEO and CFO to certify that they have reviewed the report for the periodic filing and that the financial statements and disclosures in all material aspects truly represent the operational results and financial conditions of the company. [Sarbanes-Oxley Act Section 302. Retrieved September 2007 from [tinyurl.com/2xgs7u](http://tinyurl.com/2xgs7u)]

**Section 404** requires management's assessment of internal controls. It requires each annual report filed with SEC to contain a report on its internal controls. This report should state management's responsibility to establish and maintain internal control procedures for financial reporting and also assess the effectiveness of these internal controls. A registered public accounting firm needs to evaluate management's assessment of their internal controls. [Sarbanes-Oxley Act Section 404. Retrieved September, 2007 from [tinyurl.com/2dauws](http://tinyurl.com/2dauws)]

**Section 906** increases corporate responsibility for financial reporting by requiring the chief executive officer and the chief financial officer to certify financial statements filed with SEC. These certifications must state compliance with Securities Exchange Act and also state

that all material aspects truly represent the operational results and financial conditions of the company. [The Sarbanes-Oxley Act of 2002. Retrieved September, 2007 from [tinyurl.com/2af3lx](http://tinyurl.com/2af3lx)]

#### CRIMINAL PENALTIES - Whoever -

"(1) certifies any statement as set forth in subsections (a) and (b) of this section knowing that the periodic report accompanying the statement does not comport with all the requirements set forth in this section shall be fined not more than \$1,000,000 or imprisoned not more than 10 years, or both; or

"(2) willfully certifies any statement as set forth in subsections (a) and (b) of this section know-

ing that the periodic report accompanying the statement does not comport with all the requirements set forth in this section shall be fined not more than \$5,000,000, or imprisoned not more than 20 years, or both."

To comply with the Sarbanes-Oxley Act, corporations need to improve documentation and internal controls for financial reporting. These internal controls need to be tested and monitored to make financial reporting transparent. Management is required to provide a report on its internal controls. An independent auditor has to evaluate management's assessment of its internal controls and provide a report. Thus, the external auditors now have added responsibility for fraud mitigation.

**To comply with the Sarbanes-Oxley Act, corporations need to improve documentation and internal controls for financial reporting.**

#### SOX compliance requirements for management

1. Assess risk and design controls
2. Segregate duties
3. Place internal controls for processes and system access
4. Monitor controls and follow up to check if controls are in place.
5. Document and test the controls
6. Management has to provide a report on its internal controls.
7. An independent auditor has to evaluate management's assessment of its internal controls and provide a report.

DuPont's 10-K report filed in 2005, 2006 & 2007 includes Management's Reports on Responsibility for Financial Statements and Internal Control over Financial Reporting.

These show DuPont's management reports on its internal controls for financial reporting for SOX compliance. The 10 K report also includes independent auditor PricewaterhouseCoopers LLP's report on their evaluation of management's assessment of their internal controls.

These certifications are examples of SOX compliance.

#### Public Company Accounting Oversight Board (PCAOB)

The Sarbanes Oxley Act of 2002 created the Public Company Accounting Oversight Board (PCAOB) for setting auditing standards for public companies. Smaller companies continue to use Statements on Auditing Standards from the American Institute of Certified Public Accountants (AICPA).

On July 25 2007, the SEC approved PCAOB's Accounting Standard No 5 "An Audit of Internal Control over Financial reporting That Is Integrated with an Audit of Financial Statements" ["PCAOB's New Audit Standard for Internal Control over Financial Reporting is approved by the SEC". Date: July 25, 2007. Retrieved September, 2007 from [tinyurl.com/2fl2gr](http://tinyurl.com/2fl2gr)]

All registered audit firms will be required to use this standard for their audits of internal controls.

#### Statements on Auditing Standards (SAS)

In November 2002, in the wake of the accounting scandals, the Auditing Standards Board issued SAS 99 "Consideration of Fraud in a Financial Statement Audit".

SAS 99 supersedes SAS 82. It gives the auditor more guidance to detect material misstatements due to fraud in financial statements. [CPAs' Perceptions of the Impact of SAS 99" Authors: Donald C. Marczewski and Michael D. Akers. Source: The CPA Journal. June 2005 issue. Pg 38. Retrieved September 2007 from [tinyurl.com/2ttzv6](http://tinyurl.com/2ttzv6)]

### Case study: DuPont fraud

In the DuPont fraud case, Gary Min, a former employee who worked as a research chemist at DuPont stole trade secrets from DuPont valued at \$400 million. He had accepted employment with rival firm Victrex in 2005. After accepting the employment, he continued to work with DuPont for a few months and down-

loaded 180 confidential papers and thousands of abstracts from the DuPont server and intended to use this confidential data in his new post. Most of this data was unrelated to his work.

When he resigned from DuPont, his unusually high usage of the server hosting DuPont's technical documentation was detected. Victrex cooperated with DuPont and seized Min's laptop and handed it over to the FBI for investigation. Min later admitted to misusing DuPont's trade secrets. ["DuPont chemist pleads guilty to IP theft." Computer Fraud & Security. Volume 2007 issue 3 March 2007, pg 3 Retrieved online from Science Direct database in September 2007 - [tinyurl.com/378gmr](http://tinyurl.com/378gmr)]

**In the DuPont fraud case, Gary Min, a former employee who worked as a research chemist at DuPont stole trade secrets from DuPont valued at \$400 million.**

### Sarbanes-Oxley compliant yet exposed to fraud

DuPont's 10-K report filed in 2005, 2006 & 2007 includes CEO & CFO's certifications of the financial statements filed with SEC stating compliance with Section 13 (a) of Securities Exchange Act of 1934 and also stating that the report fairly represents in all material aspects the financial condition and results of operations of the company. Their 10 k reports also include Management's Reports on Responsibility for Financial Statements and Internal Control over Financial Reporting.

These show DuPont's corporate responsibility for financial reporting and their internal controls. These were assessed and certified by public accounting firm PricewaterhouseCoopers LLC as seen in their 10-k report. Thus, DuPont complied with SOX. This compliance did not eliminate their exposure to fraud by internal security threats.

This fraud could have been mitigated if biometrics were used at DuPont for internal controls. The confidential data access should have been restricted to certain users by using biometric computer authentication instead of passwords for computer authentication. Min should have had access after biometric

authentication to only data related to his research. DuPont could have used various levels of biometrics authentication to grant access to users accessing the confidential data. As this was unrelated to Min's work, Min would not have access to this confidential data. This would prevent unauthorized users from accessing the trade secrets.

The report of who accessed or tried to access this server would have shown that Min tried to access this data and would have authorities at DuPont investigate Min's intentions. Biometrics authentication could have saved DuPont the risk of losing confidential data to rival firms and also have saved them the expense of going through a court case to protect their intellectual property.

### Biometrics: an identity management and fraud mitigation solution

Accounting frauds perpetrated by high-level managers of major companies prompted the passage of the Sarbanes-Oxley Act. These accounting frauds were possible because of weak internal control systems and of external auditors claiming that financial audits were not designed to detect frauds. The DuPont case shows that there are reasons beyond accounting frauds for strengthening internal control

systems. A single employee accessing trade secrets can cause hundreds of millions of dollars of losses for a company, lawsuits, and declines in the value of a company's stock.

According to a 2006 study by Association of Certified Fraud Examiners, 25% of internal frauds caused at least \$1 million in losses per incident. The first single incident median loss was \$159,000 and in over 9 cases the internal fraud cost the company over \$1 billion. [ACFE (Association of certified Fraud examiners) 2006 Report to the nation on Occupational Fraud. Retrieved September 2007 from [tinyurl.com/3bkzuy](http://tinyurl.com/3bkzuy)]

Frauds cannot be completely eliminated, but controls can be put in place to minimize frauds. A company has to have tighter controls over the user's system access rights, limit access to sensitive data based on user role, and monitor who tried to access sensitive data. Instead of using a weak password control system, companies need to be using a user access authentication system with these characteristics: unique identification of each user and controls extending to the transaction and field levels.

## Biometrics

Biometrics can provide this solution. Biometrics uses certain characteristics of a person such as fingerprints, retinal pattern, or even speech pattern to uniquely identify a person, grant access for an authorized user and clearly reject unauthorized users. Biometrics for computer authentication is different than biometrics for law enforcement. For law en-

forcement an "open system" is used where law enforcement authorities scan a finger with an optical sensor and store an entire image of the finger (mostly all fingers) in the national IDENT or AFIS database. This enables all law enforcement authorities to check fingerprints against those templates.

Biometrics for computer authentication can protect the privacy of users of the system while still identifying uniquely the users. A proprietary binary template (01110101010) consisting of a unique set of numbers is created, not an optical scan of the fingerprint.

While a few laptop computers had fingerprint sensors already in the late 1990's, every major laptop manufacturer offers now at least one model with a built-in fingerprint sensor. With the astonishing improvements in the sensor technology, manufacturers have switched from a larger touch sensor to a smaller and much more secure swipe sensor. They favor the proven swipe sensor from biometric leader UPEK. Built-in fingerprint sensors, together with hard drive encryption, were the top 2 requirements from corporate America for laptop manufacturers.

[Notebook with a built-in fingerprint sensor". Author: Jean Francois Manguet. Retrieved September 2007 from [tinyurl.com/25rczj](http://tinyurl.com/25rczj)]

A company does not need to wait until the next round of computer purchases to implement biometrics solutions. Inexpensive USB add-ons using UPEK sensors are available from UPEK and from The Cherry Corporation.





[www.cherrycorp.com](http://www.cherrycorp.com)

## Fraud mitigation in an SAP Environment using bioLock

### Security risks

A major reason for the popularity of SAP R/3 with corporations is the fact that SAP integrated most of the data of a company across most or all of the departments. While corporations need integrated data, individual users of computer systems should not be able to access data for which they lack authorizations. Internal control systems must have segregation of duties. The Sarbanes-Oxley Act formalized the legal requirements for corporations and for external auditors.

SAP is all about business processes and roles assigned to users for these processes. This ensures segregation of duties. SAP has a report-generating feature which generates reports of who performed which transaction when. So, this does seem like it is complying with SOX. Is this enough, however, to mitigate fraud?

1. The system gives access to users with passwords which match the approved user profile. Anyone having access to this password can basically log on to SAP and perform the desired transaction.

2. SOX requires segregation of duties. SAP provides that with allowing access to certain transactions to restricted users with predefined roles having their passwords. Is this

really secure? Anyone who has access to the username and password can easily perform the transaction. This defies segregation of duties.

Basically, a user can log on to the SAP system perform a transaction and use another password and username to perform another transaction. It is very easy for User A to get access to a username and password of User B and perform a Sales transaction and then to get User C's username and password and perform a financial transaction. The SAP report would show that User B and User C have performed the transaction when User A has performed the transaction. User B and User C are completely innocent.

Another scenario would be that User B logs on to SAP and leaves his desk to make a few photocopies. Meanwhile, User A goes to User B's desk and performs a financial transaction before User B returns. Poor User B has no idea what just happened, but the transaction report would report User B as having performed that transaction. It is impossible to track, which "actual" person accesses or changes critical information

3. Business partners and outsourced companies have access to SAP. Many processes and audits are being outsourced. This would give the users from an outsourced company or external consultant's access to company data. Sometimes, business partners and vendors also have access to the company SAP

system. This makes the system more vulnerable to security threats. With increasing globalization, many employees access critical information from different parts of the world.

All of the above shows that the SAP system, or any other ERP system using only passwords, does not provide adequate fraud mitigation or possibly even compliance with SOX sections 302 and 404.

The historically accepted flaws in security completely defy the internal controls and segregation of duties required by SOX. Everything has changed since the invention of computers including programming languages and platforms, but one thing which has not changed is the most critical factor: security. We still use the same old way of usernames and passwords for security. This is just an illusion of security.

There are many ways to discover passwords, ranging from casual coffee conversation to more sophisticated software which grabs passwords. If the password requirements get more complex, to increase security people usually write down this password someplace so that they do not forget the complex password. Whoever has access to this written password is a security threat.

[[www.fraudmitigation.com](http://www.fraudmitigation.com)]

Another easy way to access passwords is small cameras that now are built in cell

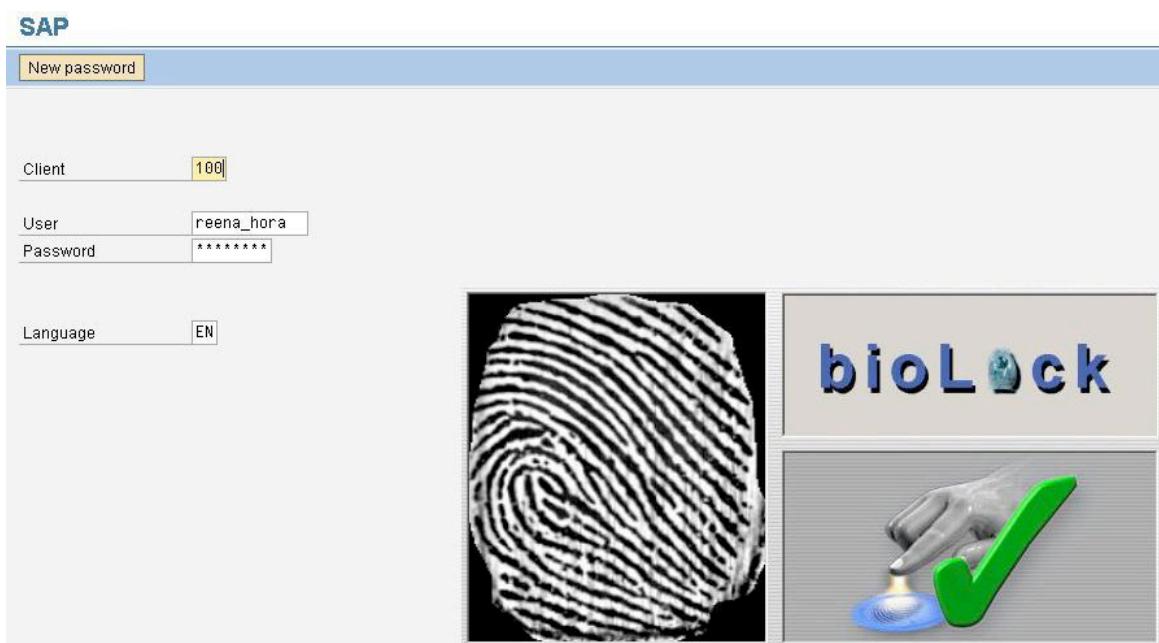
phones, pens, and buttons. Someone can record a password and play it back slowly to see what the password was. Even if you cannot play the password back, you can determine the password.

To view a demonstration of this, visit the following educational website [www.showpasswordsthefinger.com](http://www.showpasswordsthefinger.com) and see if you can figure out the password in the video. It is quite easy to determine what she is typing. The following link shows how truly dangerous it is to use only passwords for security: [tinyurl.com/3x6a5r](http://tinyurl.com/3x6a5r).

Realtime has used biometrics to create bioLock. The bioLock system is currently the only biometrics system certified by SAP for use with SAP's systems.

### **bio Lock provides 3 levels of security in an SAP environment**

1. Firstly, the user will have to provide finger-print identification to get access into the SAP system.
2. Secondly, bioLock controls can be installed at certain transaction levels requiring finger-print verification before allowing the transaction. For example: A company's balance sheet has sensitive data and the access to this can be restricted to authorized personnel. So, whoever tries to view the balance sheet will be asked for fingerprint authentication.



## Balance Sheet/P+L Statement

The screenshot shows the SAP Balance Sheet/P+L Statement configuration screen. It includes sections for G/L account selection, Selection using search help, Accounting transaction selection, Further selections, Special evaluations, Output control, and List output. The 'Further selections' section contains fields for Financial statement version (Language EN), Reporting year (2007), Reporting periods (1 to 16), Comparison year (2006), Comparison periods (1 to 16), and Plan version (ledger 00 only). The 'List output' section allows choosing between Classical list, ALV grid control, or ALV Tree Control, with Layout options for each. A note at the bottom indicates the identified user is PAUL\_FOOTE.

If someone who does not have access to this balance sheet tries to view this balance sheet, the system will kick them out and also log that they tried to access the system to view the balance sheet. Unlike the Enron case, this system can also provide evidence in court cases if the executive management had viewed the balance sheet in case of fraud.

3. Thirdly, the security can be further tightened by requiring fingerprint authentication at the individual field level. For example: Something as secure as a wire transfer can be set to require a fingerprint authentication if the amount to be transferred is more than \$10,000. If any amount more than \$10,000 is entered in the field, then the system would automatically require fingerprint authentication.

To add security, the wire transfers could be set to require dual fingerprint authentication which would require an additional designated person to approve the wire transfer.

bioLock can create a log of who accessed or tried to access the system and of who performed or tried to perform certain transactions within SAP. It even has a feature of 911 alerts wherein you can designate a finger as your 911 finger and use it if somebody forces you to perform a transaction. This will immediately alert security.

The report on the following page shows that using bioLock no one can logon as a different user. The report gives the following details.

When SAP user Paul (bioLock-User Column) tried to log on as Reena (SAP User / User Name Column to the left) the system identified him and denied access. When user Reena tried to logon as herself the system uniquely identified her and allowed system access to release a purchase order of \$40,000 car. When user Reena was away and another unidentified person who didn't even have a

biometric template tried to access the purchase order on user Reena's computer, the bioLock could not identify the stranger and rejected him. When user Paul tried to access the system as himself, the system uniquely identified him and granted access. When user Reena tried to create a Purchase order on this computer the system rejected her. The report shows next Thomas logged on as administra-

tor and accessed the bioLock transaction. The next line shows that Paul opened the balance sheet transaction. Next, Reena tried to view this balance sheet and as this was protected by bioLock the system identified her and denied access to the balance sheet. The last line shows Paul opened the balance sheet transaction again.

#### Call bioLock Protocol and System-Log



Current Date	Time	User Name	function	Text	Area	N	bioLock-User	Text	Transaction Code	Transaction text
07.09.2007	22:09:18	REENA_HORA	000	SAP Logon	Y4	3	PAUL_FOOTE	not authorized for this function	SESSION_MANAGER	Session Manager Menu Tree Display
07.09.2007	22:13:38	REENA_HORA	000	SAP Logon	Y4	1	REENA_HORA	was recognized	SESSION_MANAGER	Session Manager Menu Tree Display
07.09.2007	22:24:14	REENA_HORA	104	Display Purchase Order ME29N	Y4	1	REENA_HORA	was recognized	ME29N	Release purchase order
07.09.2007	22:24:42	REENA_HORA	104	Display Purchase Order ME29N	Y4	2		was rejected	ME29N	Release purchase order
07.09.2007	22:24:55	REENA_HORA	104	Display Purchase Order ME29N	Y4	1	REENA_HORA	was recognized	ME29N	Release purchase order
07.09.2007	22:25:32	PAUL_FOOTE	000	SAP Logon	Y4	1	PAUL_FOOTE	was recognized	SESSION_MANAGER	Session Manager Menu Tree Display
07.09.2007	22:25:53	PAUL_FOOTE	104	Display Purchase Order ME29N	Y4	3	REENA_HORA	not authorized for this function	ME29N	Release purchase order
07.09.2007	22:26:24	PAUL_FOOTE	001	bioLock	Y4	1	PAUL_FOOTE	was recognized	/REALTIME/BIOLOCK	bioLock - Administration
07.09.2007	22:26:46	SAPALL	000	SAP Logon	Y4	1	THOMAS	was recognized	SESSION_MANAGER	Session Manager Menu Tree Display
07.09.2007	22:26:57	SAPALL	001	bioLock	Y4	1	THOMAS	was recognized	/REALTIME/BIOLOCK	bioLock - Administration
07.09.2007	22:30:09	PAUL_FOOTE	006	Open Balance Sheet Transaction	Y4	1	PAUL_FOOTE	was recognized	S_ALR_87012284	Balance Sheet/P+L Statement
07.09.2007	22:32:01	PAUL_FOOTE	007	Display Balance Sheet	Y4	3	REENA_HORA	not authorized for this function	START_REPORT	Starts report
07.09.2007	22:32:18	PAUL_FOOTE	006	Open Balance Sheet Transaction	Y4	1	PAUL_FOOTE	was recognized	S_ALR_87012284	Balance Sheet/P+L Statement
07.09.2007	22:32:32	PAUL_FOOTE	007	Display Balance Sheet	Y4	1	PAUL_FOOTE	was recognized	START_REPORT	Starts report

A report like this gives details of who tried to access the system and performed or viewed which transaction. This can prove which officers and managers looked at certain financial

statements or documents. This report can be used as evidence in court cases of who accessed the financial and other documents and performed which tasks.

07.09.2007	23:06:13	PAUL_FOOTE	030	Financial Transaction on input Level	Y4	3	REENA_HORA	not authorized for this function	FB01	Post Document
07.09.2007	23:07:10	PAUL_FOOTE	030	Financial Transaction on input Level	Y4	1	PAUL_FOOTE	was recognized	FB01	Post Document
07.09.2007	23:11:28	SAPALL	001	bioLock	Y4	1	THOMAS	was recognized	/REALTIME/BIOLOCK	bioLock - Administration
07.09.2007	23:14:50	SAPALL	001	bioLock	Y4	5	APRIL	was confirmed	/REALTIME/BIOLOCK	bioLock - Administration
07.09.2007	23:16:06	PAUL_FOOTE	030	Financial Transaction on input Level	Y4	2		was rejected	FB01	Post Document
07.09.2007	23:17:32	PAUL_FOOTE	030	Financial Transaction on input Level	Y4	3	REENA_911	not authorized for this function	FB01	Post Document

The above report shows that Reena was identified but rejected as she tried to perform a wire transfer on computer which was logged on as SAP user Paul. Next the report shows that SAP user Paul tried to make a wire transfer above a certain amount which had an internal control requiring biometric confirmation. The report also shows that SAP user Thomas who was logged in as SAP ALL administrator tried to access the bioLock transaction. The next line shows that SAP user April confirmed Thomas's request for the bioLock transaction. For extremely critical task two different people and their biometric authentication can be required to perform a task. This ensures the 4-eye principle within the SAP system.

The next to the last line shows that an unauthorized user who was not their employee tried to make a wire transfer on Paul's computer which was logged onto SAP. AS the system did not recognize him, he was rejected. In a desperate attempt, the intruder forces Reena to execute the wire transfer for him on Paul's computer. Reena reacts calmly and uses her separately enrolled 911 finger for authentication. This system rejects the task visible for the intruder, but notes in the log file that a "911 finger" was used to alert authorities about a known security breach. An automated scanner could alert security when a 911 is posted in the log file.

This report demonstrates how a sensitive transaction, such as a wire transfer,



is protected by bioLock and will also provide evidence in a court case.

Using a technology like bioLock provides true segregation of duties and internal controls as the system uniquely identifies each user and only allows certain users access to sensitive data or transactions. All users in a company do not need to have a bioLock controlled access. Only certain users having access to sensitive data can be set to access the critical data using bioLock. Once the sensitive transactions are locked by access to restricted users by bioLock all other users are automatically filtered out and blocked from accessing the sensitive data. For the first time, the business can clearly define a simple "invitation only" list for certain transactions and users. bioLock will ensure that no other actual users will access the protected functions. bioLock packages are available with as low as 50 users and can be available for as many users as required. A complete installation package starts under \$100,000 and would go up depending on the number of users. This will provide evidence in case of a court case and also make it very transparent to auditors. This will truly make SAP compliant with SOX.

In the DuPont case, the company's management did not detect Min's unusually high activity on the server with the intellectual property until he resigned. The management did not have effective internal controls securing access to the server. They could have set controls which would flag the authorities if there was such unusual activity. They could have purchased a bioLock package of 1,000 seats protecting their top 1,000 users with access to their various departments including finance, human resources, research to name a few. This would have cost them a few hundred

thousand dollars, a small price to protect their intellectual property, image, stock price and hassles of a court case. This would have mitigated the risk of losing \$ 400 million of intellectual property. If DuPont had lost millions of dollars, there would have been shareholder lawsuits. Using bioLock, they could have restricted scientists such as Min's access to a small reasonable part of the system for research. Anything above normal could have been set to require dual fingerprint authentication and also raise a flag to be investigated if found unreasonable. bioLock could also have provided a report of who accessed and who tried to access the data. This evidence could have been used in the court case against Min. DuPont's internal controls were inadequate for this type of fraud. While DuPont's executives and external auditors (PricewaterhouseCoopers) certified the adequacy of internal control systems for accounting frauds, there are other types of frauds for which shareholders can sue companies and external auditors.

## Conclusions

Contrary to popular beliefs, corporate managements and external auditors have legal obligations to mitigate fraud. In addition to frauds perpetrated by persons not working for a company and accounting frauds perpetrated by employees, companies can be exposed to large risks of losses from the theft of intellectual property. Laws and regulations provide only minimum standards for corporate internal control systems. For corporate managers, directors, and external auditors who want to avoid lawsuits, they need to implement better security than the use of only passwords. Using only passwords is an invitation to fraudsters. Biometrics systems provide fraud mitigation.

Paul Sheldon Foote is a Professor of Accounting at California State University, Fullerton. Dr. Foote speaks and consults internationally on fraud. His courses provide students with hands-on opportunities using SAP R/3 and bioLock.

Reena Hora is currently pursuing her Masters in Information Technology from California State University, Fullerton.



(IN)SECURE Magazine is a proud media sponsor of the following events:

**Black Hat DC 2008**

18 February-21 February 2008  
<http://www.blackhat.com>

**InfoSec World Conference & Expo 2008**

10 March-12 March 2008  
<http://www.misti.com>

**Black Hat Europe 2008**

25 March-28 March 2008  
<http://www.blackhat.com>

**HITBSecConf2008**

14 April-17 April 2008  
<http://conference.hitb.org/hitbsecconf2008dubai/>

**Infosecurity 2008**

22 April-24 April 2008  
<http://www.infosec.co.uk/helpnetevents>

**Hacker Halted USA 2008**

28 May-4 June 2008  
<http://www.eccouncil.org/hhusa/index.html>

# INFORMATION SECURITY

it's all about trust.

insider threat

identity management

security awareness

wireless security

intrusion protection

remote access

**Are you sure that your  
information security  
is in safe hands?**

Threats to your business can come at anytime and from anyone; your customers, your suppliers or your employees.

**Find out how to protect your company's business information at Infosecurity Europe, Europe's No.1 information security event.**

Register FREE\* to attend now at:  
**[www.infosec.co.uk](http://www.infosec.co.uk)**



**22nd – 24th April 2008**

Grand Hall, Olympia, London, UK.



\*Visitors not registered by 5pm on Friday 18th April will be charged a £20 entrance fee.



## Interview with Andre Muscat, Director of Engineering at GFI Software

By Mirko Zorz

### What are some of the challenges you face in your current position?

I believe the major challenge is to continue building security software that is easy and lightweight to use. The vast majority of security software is built for enterprise customers that have significant IT departments. Thus the software tends to be labor intensive to install, set up and most importantly administer. These solutions are then pushed on to smaller companies that, frankly, do not have the capacity, expertise or inclination to use such a heavyweight and costly solution. At GFI we continually challenge ourselves to build security software that is effective whilst also being easy and lightweight to use.

### What new security trends and technologies do you find exciting?

It is the fact that security is not just about having a firewall and an anti-virus scanner any more. Malicious threats and computer misuse have moved on and we are now witnessing the transition to a full-scale eCrime industry.

This industry is now worth \$100M per year and driving ever more sophisticated attacks and scams. Companies are maturing their response slowly shifting from 'security' to a 'risk management' approach, whereby business decisions drive how and what a company uses in terms of security products or computer systems.

### Based on your experience, what is the biggest challenge in protecting sensitive information at the enterprise level?

Protecting sensitive information is a major challenge for companies irrespective of size, activity or location. The use of technology has greatly facilitated the way they do business – both in terms of volume and speed – yet it has also created security issues that need to be addressed.

Today most companies have an online presence, they do business over the internet, they transfer data from one office to another and their employees are mobile thanks to laptops and remote access.

Therefore, any data stored on a network can, unless properly secured, be accessed by malicious individuals for financial gain or for revenge.

There is no one 'big' issue, one major challenge, but rather a mix of problems and concerns that include network growth, the threat posed by company insiders and financial restrictions.

Undoubtedly, network growth is one the biggest challenges. As networks grow larger and more systems are connected, the more complex they become and the more difficult for a company to keep track and control what is happening on its network and what use is being made of it. Furthermore, as networks grow so do the risks of data loss and downtime – and obviously this comes at a cost. Each network and business running on that network is unique and only the businesses themselves can quantify in hard currency how much network downtime will actually cost them... but it never comes cheap.

The second security-related issue is the threat posed by employees and other insiders. This is a growing concern for companies and recent breaches are proof that it is a problem that cannot be ignored any longer. Disgruntled employees can abuse a position of trust to steal company data. Security naïve employees may open an executable which arrived in their email inbox to look at a joke without stopping to think that a virus may be embedded within that joke. Internal employees may be tricked into performing actions which they themselves would not know are insecure e.g. sticking username and passwords to their monitors, sending out sensitive information such as company credit card details in reply to an email claiming it comes from the user's bank. There are also cases when employees are unlucky e.g. when their laptops are stolen or a USB Stick is lost.

There are other weaknesses such as the use of default configurations, the uncontrolled use of consumer devices, such as USB sticks which are used extensively by employees, browsing of consumer-focused websites, web-based threats such as phishing sites and email scams which expose the company to high risk.

The third category of security issues revolves around finances and budgeting. Companies are typically run on tight budgets. This makes it more difficult for IT administrators to seek funds to purchase software to protect the network. The problem is exacerbated when a communication gap exists between the IT administrator and senior management and the two fail to speak the same language, resulting in companies being either unaware of the risk or operating at a high risk of a security breach.

Improving security requires a holistic approach that includes investing money in quality solutions, helping management to understand the risks and increasing awareness among employees about the importance of security.

**In your opinion, what is the most significant security threat at the moment? What do you see your customers most worried about?**

Personally, I would say that insider threats and the uncontrolled use of portable devices such as iPods, flash drives, USB sticks, Blackberrys, PDAs and laptops are a major concern for companies; or rather should be a major concern for companies and I'll explain why.

We are currently working on some research in the US and initial results indicate that the major concern for companies is still virus attacks. The threat posed by insiders using portable devices however is rather low, a single digit figure. There are two possible reasons for this; either companies already take the use of portable storage devices seriously and block all devices or, and in my opinion the most probable reason, companies are still unaware of the serious threat posed by insiders and these consumer devices. Why? That's a million dollar question but I think it boils down to education and greater awareness of the security threats facing companies. It is really easy for a trusted employee to plug in his lifestyle device such as an iPod and steal data in a matter of seconds. What is even worse is that iPods can be used to introduce malware, such as viruses and Trojans, pornography, part-time work material and more to the office.

What is unknown to the user is that malicious software (pre-installed on the USB stick) can run in the background and email out sensitive information such as usernames and passwords, office files and so on which are used by that user on that machine. These attacks are very real and very worrying because of the ease and speed of execution.

Unless network administrators take pre-emptive security measures to prevent these things

from happening through education and technology barriers which enforce company policy, the company will only be exposing itself to major security breaches and attacks.

Network administrators need to make better use of the tools that are available to them and senior management needs to start looking at security as an investment instead of an overhead.

## **Senior management needs to start looking at security as an investment instead of an overhead.**

### **What's your strategy when deciding on the implementation of new features for GFI software?**

“What do SMEs need or, more specifically, what do IT administrators in SMBs require?” is the question we always ask ourselves.

IT administrators in SMBs want best-of-breed solutions that offer quality and unbeatable price performance and that address the problems that they face every day. And this is what GFI has been doing successfully for many years now.

SMBs are faced with the problems resulting from expanding networks, an increase in attack vectors and little or no budget to improve and secure their network. GFI's focus has always been small and medium sized businesses. Unlike enterprise companies that have taken enterprise-level products and scaled them down for SMBs, GFI has designed its products from the ground up to meet the needs of SMBs but at the same time providing enterprise-level functionality at an affordable price.

We are constantly monitoring trends and new technologies that can impact negatively on our customers' networks. Our strategy to implement new features is based on a) research that our security teams carry out and b) the feedback that we receive from our technical support personnel and from our customers who provide us with feature requests. We are proud to say that we understand our customers much better because we listen to what

their needs are and accordingly develop and tweak our products on a regular basis.

### **What have been the most important software releases for GFI in 2007?**

Every product release is important for GFI because it reflects our commitment to providing our customers with quality and cost-effective solutions that address and solve the problems that IT administrators are facing. 2007 saw five important product launches. These were GFI LANguard Network Security Scanner (N.S.S.), GFI WebMonitor for ISA Server, GFI FAXmaker and GFI MailArchiver (November) and GFI EndPointSecurity (November/December).

GFI LANguard Network Security Scanner (N.S.S.), recently winner of the “Best of TechEd 2007” in the security category, is a solution that addresses the three pillars of vulnerability management: vulnerability scanning, patch management and network auditing. Apart from major updates to version 7, the new version shipped with state-of-the-art vulnerability check databases based on OVAL and SANS Top 20, providing over 15,000 vulnerability assessments when the network is scanned.

GFI WebMonitor for ISA Server allows companies to control employees' web browsing activities and to ensure that any files downloaded are free of viruses and other malware. The new version comes with WebGrade, a 100% human-reviewed site categorization database that gives administrators control over

what sites users can browse and block access to websites in particular categories, such as adult, online gaming, personal email, P2P, Facebook, Myspace, travel websites and more.

GFI FAXmaker is a fax server that makes sending and receiving faxes an efficient, simple and cheaper process. FAXmaker was GFI's first product and today is the leading fax server on the market. This version was released in October and supports Exchange 2007 and Cantata's Brooktrout SR140 FoIP technology.

The new version of GFI MailArchiver, an email management and archiving solution, comes with auditing functionality that ensures that all archived emails have not been tampered with and a PST migration tool which provides access to old PST files on client machines.

The final major release last year was GFI EndPointSecurity 5. This version comes with considerable improvements and new features that offer more granular control over portable device usage.

I believe that the challenges we face today will very much be the same in five years time. Companies will still be threatened by spam, by viruses, by malware.

#### **What challenges does GFI's product portfolio face in the next 5 years?**

Our products have developed very much in parallel with developments and trends in the security sphere and, most importantly, on the basis of feedback and feature requests from our customers.

I believe that the challenges we face today will very much be the same in five years' time. Companies will still be threatened by spam, by viruses, by malware. Networks will still be subjected to DoS attacks, hackers will still ply their trade making the most of vulnerabilities in systems. Employees will still be a concern because they have access to company information. Portable devices will still be misplaced or stolen.

The threats will not change but merely evolve to reflect improvements in technology and new trends and approaches to security.

The challenge for GFI is to remain one step ahead of these changes and to evolve with them. The challenge is to continue providing high quality products for the SMB market that meet the needs of IT administrators and suit the pocket of management.

All this will have to take place in a competitive market that is becoming more selective, more critical and more budget-conscious. That said we are confident that we have the expertise and the ability to face these challenges. So long as people use technology to communicate and networks are needed to do business, then companies will need our products for their security and peace of mind.

#### **What can customers expect from GFI in 2008?**

Our customers can expect GFI to continue providing quality solutions for IT administrators in SMBs at a price that is not only affordable but among the lowest they will find on the market – but without compromising on functionality.

Price performance has, and will always be our key differentiator. We insist on this in every product that we sell to our customers. We have a number of product launches planned for next year and these will ship with larger feature sets to reflect, in great part, the needs of our customers.



## QualysGuard visual walkthrough // sponsored article //

QualysGuard ([www.qualys.com](http://www.qualys.com)) is product used for conducting automated security audits without any need of software or hardware installation by its users.

The service is provided through a very fast and stable online application which does over 150 million IP audits per year.

The screenshot shows the QualysGuard Express dashboard. On the left, a vertical navigation menu includes: Dashboard, Map, Scan, Schedule, Report, Remediation, Asset Search, and Risk Analysis. The main area has a title bar with 'New', 'Search', 'View', 'Setup', 'Help', and user info 'Mark Woodstone (review\_mw) | Log Out'. Below is a 'Dashboard' section with three charts: 'Vulnerabilities by Severity Level' (bar chart with 17 Severity 5 and 10 Severity 4), 'Vulnerabilities by Status' (donut chart with 171 total, 0 New, 0 Re-Opened, 171 Active), and 'Open Tickets by Severity Level' (empty box with message 'There is no data available'). At the bottom are two tables: 'Top 10 Tickets' (empty) and 'Top 10 Vulnerabilities' (list of QIDs and titles).

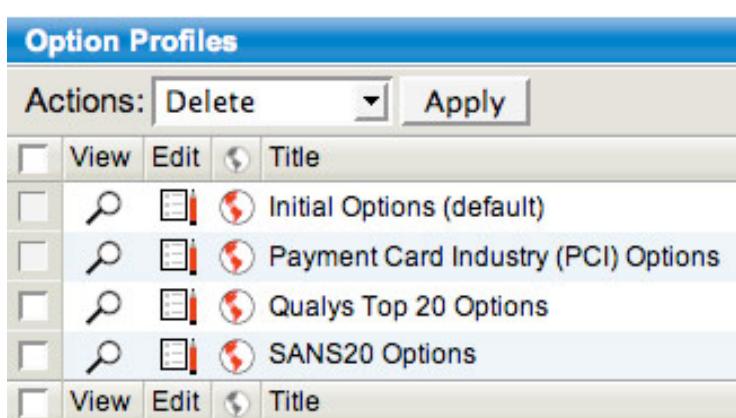
Ticket #	DNS Hostname	IP Address	Due Date	Owner
There was no data found matching your filters.				

QID	Title
15053	ISC BIND Remote Cache Poisoning Vulnerability
19217	MySQL Security Invoker Privilege Escalation Vulnerability
19223	Oracle October 2007 Security Update Multiple Vulnerabilities
27285	ProFTPD SReplace Remote Buffer Overflow Vulnerability
38577	Asterisk SIP Channel Driver Remote Denial of Service Vulnerability
42419	Multiple Cisco TCD/DV Vulnerabilities

From the QualysGuard dashboard you can start any of the actions provided in the Navigation menu located on the left of the screen.

<input type="checkbox"/>	10.20.30.100	vpn.qualys-test.com	10.20.20.1	Cisco VPN 3000 Concentrator	L	
<input type="checkbox"/>	<a href="#">64.41.134.59</a>	test1.qualys-test.com	192.168.110.1	Linux 2.4	S L	
<input type="checkbox"/>	<a href="#">64.41.134.60</a>	test2.qualys-test.com	W2KDEMO2	192.168.110.1	Windows 2000/2003/ME/XP	S L
<input type="checkbox"/>	64.41.134.61	test3.qualys-test.com		192.168.110.1	Solaris 2.8	S L
<input type="checkbox"/>	192.168.110.1	dmz.qualys-test.com			Cisco IOS 12	L
<input type="checkbox"/>	192.168.120.1	www.qualys-test.com	192.168.110.1	Linux		
<input type="checkbox"/>	192.168.120.2	www2.qualys-test.com	192.168.110.1	Linux		L
<input type="checkbox"/>	192.168.120.3		192.168.110.1			
<input type="checkbox"/>	192.168.120.4		192.168.110.1			
<input type="checkbox"/>	192.168.120.5	smtp.qualys-test.com	192.168.110.1	Linux		L
<input type="checkbox"/>	192.168.120.6	ftp.qualys-test.com	192.168.110.1	Linux		L

You can map a network by scanning IP addresses, domains or netblocks. This is a sample results of a mapping activity in a test environment.



After the mapping is done, you can start scanning. These are some of the default option profiles offered in QualysGuard.

#### Vulnerabilities (27)

	4	<a href="#">SSH Protocol Version 1 Supported</a>	port 22/tcp
	3	<a href="#">Discovery of Unix Account Names Vulnerability</a>	port 80/tcp
	3	<a href="#">Webalizer Web Usage Statistics Accessible</a>	port 80/tcp
	3	<a href="#">SSL Server Has SSLv2 Enabled Vulnerability</a>	port 443/tcp over SSL
	3	<a href="#">SSL Server Supports Weak Encryption Vulnerability</a>	port 443/tcp over SSL
	3	<a href="#">SSL Server May Be Forced to Use Weak Encryption Vulnerability</a>	port 443/tcp over SSL
	3	<a href="#">Discovery of Unix Account Names Vulnerability</a>	port 443/tcp
	3	<a href="#">Webalizer Web Usage Statistics Accessible</a>	port 443/tcp
	3	<a href="#">OpenSSH Key-Based Source IP Access Control Bypass Vulnerability</a>	port 22/tcp
	2	<a href="#">Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerability</a>	port 80/tcp
	2	<a href="#">SSL Certificate - Expired</a>	port 443/tcp over SSL
	2	<a href="#">SSL Certificate - Self-Signed Certificate</a>	port 443/tcp over SSL
	2	<a href="#">SSL Certificate - Subject Common Name Does Not Match Server FQDN</a>	port 443/tcp over SSL
	2	<a href="#">SSL Certificate - Improper Usage Vulnerability</a>	port 443/tcp over SSL
	2	<a href="#">SSL Certificate - Signature Verification Failed Vulnerability</a>	port 443/tcp over SSL
	2	<a href="#">Netscape/OpenSSL Cipher Forcing Bug</a>	port 443/tcp over SSL
	2	<a href="#">OpenSSL Insecure Protocol Negotiation Weakness</a>	port 443/tcp over SSL

When the scanning process is finished, you will be presented with the overview of the vulnerabilities detected on "target" hosts.

## New Rule

### Rule Title

Title: \*

Filter\_33

### Conditions

If all of the following conditions are met:

#### Hosts:

Asset Groups:

All, TechTeam

+ [Select](#)

IPs/Ranges:

+ [Select](#)

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

#### Vulnerability:

##### Severity Levels:

Confirmed Vulnerability:  1  2  3  4  5

Potential Vulnerability:  1  2  3  4  5

##### Qualys ID:

Select QID numbers that will trigger the creation of a ticket

[Configure...](#)

### Actions

Perform the following actions

##### Assign to:

User Running Scan (default) [View](#)

Set Deadline:

This ticket must be closed in 7 days (Range: 1-120)

##### Ignore:

Do not create a ticket for these conditions

**Within the application there is a dedicated ticketing service for prioritizing and fixing vulnerabilities by using recommended solutions. You can create your own policy for specific vulnerability types.**

## Report Templates

Actions: [Delete](#) [Apply](#)

1 - 12 of 12

	Title	Type	Source	User
<input type="checkbox"/>	Executive Remediation Report		Auto	System
<input type="checkbox"/>	Executive Report		Auto	Mark Woodstone
<input type="checkbox"/>	High Severity Report		Auto	Mark Woodstone
<input type="checkbox"/>	Payment Card Industry (PCI) Executive Report		Manual	System
<input type="checkbox"/>	Payment Card Industry (PCI) Technical Report		Manual	System
<input type="checkbox"/>	Qualys Top 20 Report		Auto	System
<input type="checkbox"/>	SANS Top 20 Report		Auto	System
<input type="checkbox"/>	Technical Report		Auto	Mark Woodstone
<input type="checkbox"/>	Tickets per Asset Group		Auto	System
<input type="checkbox"/>	Tickets per User		Auto	System

**QualysGuard has a powerful reporting capabilities, so besides the standard in-depth report, you can also chose one of the predefined reporting templates.**

#### Search Criteria

QID: 38304  
Asset Groups: TechTeam  
IPs/Ranges: -

#### Search for QID

▶ 4 SSH Protocol Version 1 Supported

#### Results (1)

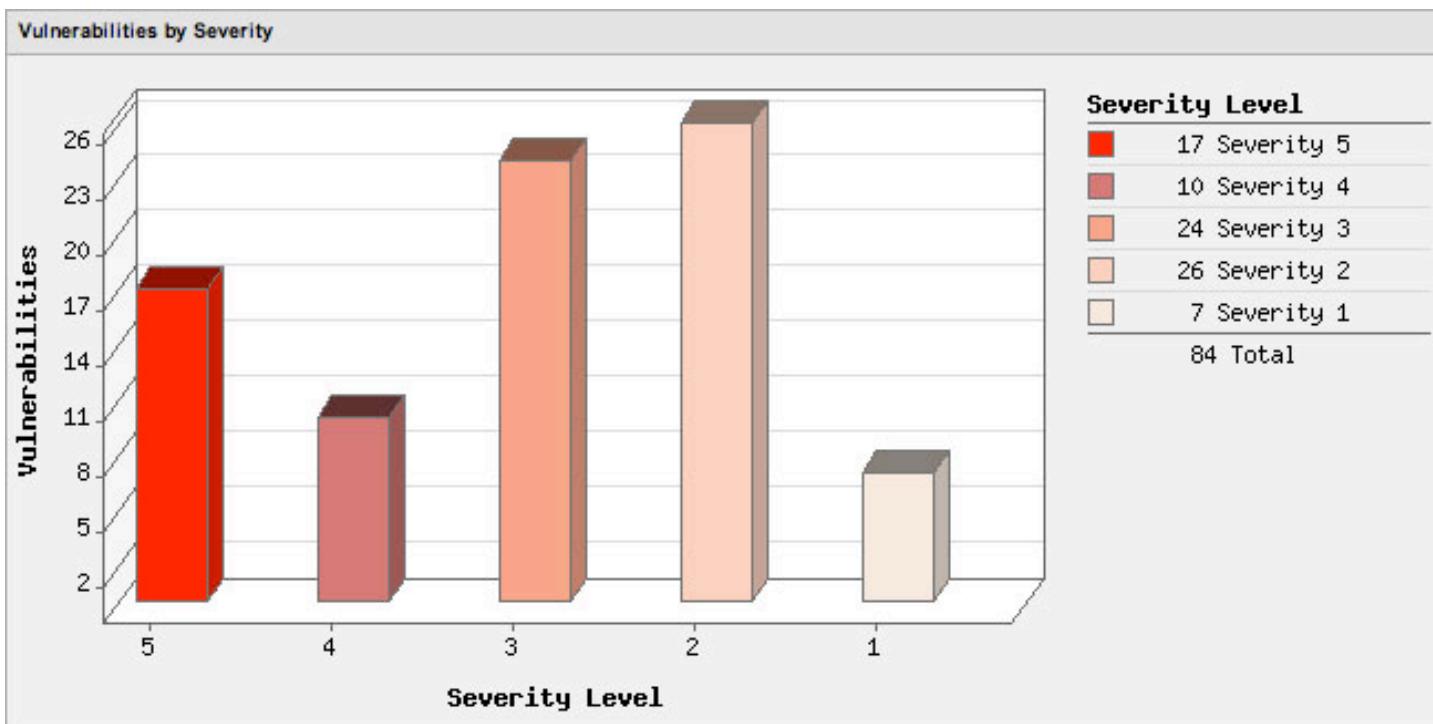
	IP Address	DNS Hostname	NetBIOS Hostname	Asset Groups	Impact	▼	QID	OS	Port	Service	Results
<input type="checkbox"/>	64.41.134.59	demo01.qualys.com		TechTeam	High		✓	✓	✓	✓	✓
<input type="checkbox"/>					Impact	▼	QID	OS	Port	Service	Results

## Results of a risk analysis test for a sample vulnerability.

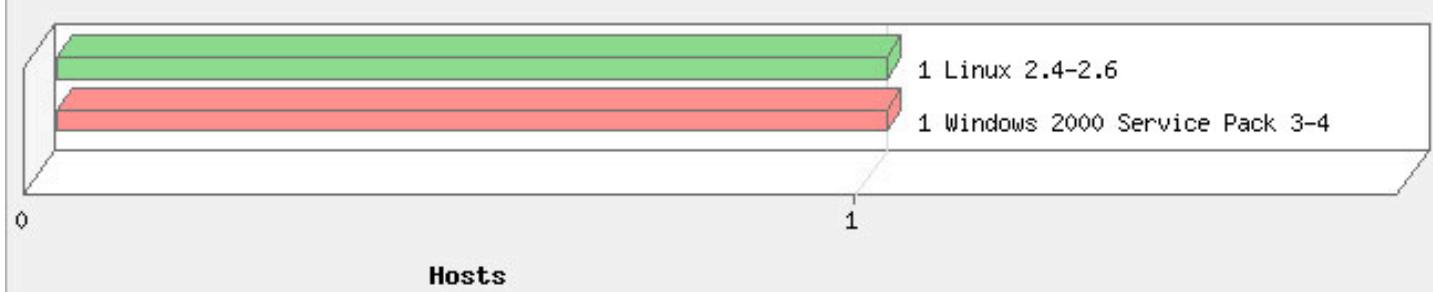
#### Tickets

	Actions:		Edit	▼	Apply							
	View	Edit	Ticket #	State	Due Date	▼	IP	DNS Hostname	NetBIOS Hostname	Severity	QID	Vulnerability Title
<input type="checkbox"/>			000001	Open	11/20/2007		64.41.134.59	demo01.qualys.com		3	38139	SSL Server Has SSLv2 Enabled Vulnerability
<input type="checkbox"/>	View	Edit	Ticket #	State	Due Date	▼	IP	DNS Hostname	NetBIOS Hostname	Severity	QID	Vulnerability Title

## Example of an active ticket related to SSL server security issue.



#### Operating Systems Detected



## Sample of a visual report detailing vulnerabilities by severity and operating systems.



## Application security matters: deploying enterprise software securely

By Ben Whaley

**One of the most interesting aspects of being an information security consultant is the exposure to an enormous variety of industries and organizations. From healthcare to governments, non-profits to small private companies and more, the consultant must be versed in dozens of technologies, regulations, and business practices in order to be effective. Today, any security consultant worth his salt recognizes at least one common security weakness across the board: vendor-developed applications, often industry specific, are the Pandora's Box of the information security program.**

Commercial off-the-shelf (COTS) software companies have developed applications in every conceivable nook and cranny to digitize and automate processes, storing the lifeblood of the organization in a database and making it accessible through a GUI front end. Increasingly, these types of applications are web-based, migrating IT back to the thin application environment of the 1980s. Because these applications are the window to the very information that keeps organizations alive, it is essential that they be protected with every tool in the infosec arsenal. Unfortunately, the monotonous “features now, security later” adage still rules.

Consider a new application deployment at ACME Corporation, a medium-sized, industry-generic company computerizing a key business process for reporting and efficiency purposes. ACME might take the following approach to the project:

- 1) ACME management initiates the project and issues a request for proposals (RFP) to select a vendor.
- 2) After choosing the vendor and signing a contract, ACME assembles the internal implementation resources to work with the vendor. The team consists of a system administrator, a database administrator, a network administrator, a project manager, and a business representative.
- 3) The project team engages the vendor to gather first steps and schedule an implementation date. A checklist of installation steps may be provided. Most often, a vendor-supplied service professional will be on-site for the installation.
- 4) During an installation phase, test and production servers are configured, the application is installed and configured for ACME’s unique business needs, and data is scanned from paper into the application’s database.

- 5) The application is tested and accepted by the business representative.
- 6) End users are trained, and the application is promoted to production.
- 7) The maintenance and support phase begins.

This familiar IT project life cycle leaves a security guru feeling unquestionably queasy. How could this seemingly straightforward installation increase risk to the organization?

Here are just a few vulnerabilities that were overlooked.

- Because the application was developed about a year ago, it was certified by the vendor against the operating system patches available at that time. Too busy developing the next version to certify new patches, the instal-

lation checklist explicitly disallows the more recent patches.

- After completing the database software installation, the widely accessible database administrator account password is left at the default - blank.
- Several application administrator accounts with simple passwords were created during the testing phase and are not removed prior to the production deployment.
- The application has auditing capabilities, but the required module was not purchased during the contracting phase and subsequently was not installed.
- The vendor supports only Telnet for remote support, and was given a generic account with a shared password for ongoing maintenance.
- The web front end is deployed without the use of SSL encryption.

## SECURITY SHOULD BE PART OF THE PROCESS FROM THE BEGINNING

This is an extremely common result of many application deployments at organizations such as ACME. Most vendors simply do not have the time, resources, or expertise to develop applications securely, and the customers may not see security as a key requirement of the project. What can be done to increase security when deploying new applications or migrating from old software?

First, security should be part of the process from the beginning. If all customers wrote security requirements into the RFP, for example, vendors would start to take it more seriously. At the very least, management would be aware of some of the risks inherent in selecting a particular vendor simply by reviewing responses to the requirements. Measures could be taken to mitigate any risks during the implementation, or the risk could be accepted and documented.

In step 2 of the project cycle, an important resource was not included in the team: the security team representative. This individual will watch out for, and hopefully mitigate, just the sort of weaknesses that were discovered after the fact. The security team should have a template (discussed below) for securing applications, but individually they will also be

thinking outside of the box to proactively resolve non-standard problems as well.

It's a rare organization that has documented security findings for each application in the environment. Adding a security sign-off in addition to the more common business acceptance procedure will show auditors that the company takes security seriously.

The security representative certainly has her work cut out for her. Convincing the vendor, management, and the rest of the project team that the security changes are implementation requirements is no simple task, and it takes creative technical thinking and attention to detail to resolve many of the technical issues.

To make the job more tangible, the security team should have a checklist of requirements for new application installations. Major version upgrades of existing software should follow a similar, or identical, procedure.

The checklist can be broken into categories such as authentication, logging and auditing, encryption, networking, and so on. It may also make sense to include items such as backups and monitoring that are not solely security related.

To simplify the process, a standard, universally accepted checklist can be used as the basis for the certification process. One such guide is the DISA Application Security Checklist, available at [iae.disa.mil/stigs](http://iae.disa.mil/stigs). It provides an excellent, if overly wordy, guide for application security requirements. Although the document is aimed primarily at U.S. Department of Defense entities, it is easily adapted to any organization.

Using the DISA document as a template, we can quickly formulate our own set of application security requirements. For convenience, we'll split them into logical sections, just as is done in the checklist.

## Identification and authentication

This covers how applications process and authenticate user identities. Several lengthy requirements are listed in the DISA checklist, but they boil down to the following requirements:

- The application must use valid, standards-based strong encryption for authentication. For most organizations, this means that the application uses a certificate signed by an approved certificate authority. The certificate must not be expired, revoked, or otherwise invalid.
- An adequate client authentication process must be supported. This might take shape in a variety of ways. An obvious example would be a simple login form, but a less common case could be a web server becoming a client when connecting to a database server on the back end. Authentication processes may include a password, a certificate or key, and/or a biometric. If passwords are used, the application must support a minimum set of complexity requirements (for example, at least 9 characters of mixed alphanumeric and special characters and a set expiration). An application that allows access with only a username, does not support password complexity, or does not properly enforce controls that it claims to support would fail this requirement.
- If applicable, the client should authenticate the server. For example, a web browser connecting to an SSL-enabled web server would validate the SSL certificate. In this case, it should validate that the certificate was signed

by a trust certificate authority, is not expired, and matches the URL of the page.

## User account management

The DISA guide only contains one requirement in this section, but there are potentially many more concerns. For example, how does the application manage user accounts? Are administrative accounts carefully protected?

A proper application certification thoroughly checks the user account protection mechanisms.

Requirements:

- User IDs should be unique. Duplicate user IDs can lead to overlooked privileges or weak passwords.
- The application must authenticate to a centralized authentication system. Most organizations have a centralized user account directory, such as Active Directory, OpenLDAP, or Red Hat Directory Server. To minimize the number of accounts and passwords that users must remember, the application should support at least LDAP authentication.
- Shared accounts must be prohibited. This is a central requirement of some regulations, such as HIPAA. Accounts should be tied to an individual – particularly administrative accounts.
- Access requests should follow a standard request procedure. This should be tracked and reported against on a regular basis.

## Data protection

Requirements in this area are common in regulations and standards such as the Payment Card Industry Data Security Standard.

Permissions and cryptography should be used to protect data when stored on disk and in transit.

- Sensitive data should be protected by file permissions at rest. On disk, files should only be accessible by administrators and by the processes that need access (for example, the operating system, database service, or application processes). If backups or duplicates of the data exist, they should also be examined.

- Authentication credentials should be encrypted at rest. Furthermore, non-privileged accounts should not have access to the keys that encrypt data.
- All sensitive data in transit should be encrypted with FIPS 140-2 validated cryptography. This can be accomplished in a variety of ways, such as by using technologies such as stunnel, SSL-enabled HTTP, or LDAPS.
- All cryptographic modules should be FIPS 140-2 validated. The check can be performed at [csrc.nist.gov/groups/STM](http://csrc.nist.gov/groups/STM). In particular, be especially wary of applications that use proprietary, in-house developed encryption.

## Audit

Auditing is certainly one of the least exciting yet most critical application security features. The application should log events and transactions in a meaningful manner.

- The application should adequately log security-related events. Such events might include startup/shutdown, user authentication, authorization changes, data transfer, configuration changes and more. Furthermore, the application should log specific information about the event, such as the user ID, success or failure, the date and time, the origin of the request, etc.
- The application should include a method to notify administrators when the logs are near full.
- The audit logs must not be vulnerable to unauthorized deletion, modification, or disclosure. Filesystem permissions should be reviewed, but the application interface might also be vulnerable. Integrity is perhaps the MOST important element of audit logs, particularly if they are to be used in court.
- Centralized logging should be supported. This can be done by syslog, by a manual database export and daily copy, or by sending logs to the system log utility (such as the Windows Event Viewer) and using a commercial tool. The benefits of centralized logging are widely known, and it should apply to applications as well as operating system logs.

## Application operation

Certain aspects of the application's operation have an impact on the overall security. This

section looks at a variety of operational concerns.

- The application must support role-based access control. Administrative accounts should be able to perform system maintenance, manage user accounts, and review audit logs. Regular user accounts should have significant restrictions.
- Actions should be authorized prior to execution. For example, an attempt to delete a user account by a non-privileged user should be denied.
- The application should run with only the necessary privileges for operation. A Windows application, for example, should not run with domain administrator privileges. Similarly, a Linux application should not run as the root account.
- Session limits should exist. User sessions should time out after a period of activity, and perhaps a specific number of simultaneous sessions should be allowed.
- Users should not be able to circumvent the user interface to access resources in the supporting infrastructure. A user may be limited by privileges in the application, for example, but could use SSH or NFS to access data directly.

## Enclave Impact

The most important consideration here is the logical separation of servers at the network level.

Application servers should be properly limited by firewall Access Control Lists. Externally accessible servers should be located in a DMZ. The section also recommends several methods for determining what ports are in use, but most of these don't make sense in the context of vendor-supplied applications. The vendor should be able and willing to supply information about what ports are needed for proper operation. If not, this can be easily determined by packet captures and network scans.

## Application configuration and authorization

A variety of client-facing requirements for applications are discussed in this section.

- A warning banner should be displayed at user logon. This can contain text about a user's consent to monitoring, no reasonable expectation of privacy, and other standard organizational user agreement text.
- Authentication credentials should not be stored on a client after the session terminates. Cookies are the most common method to store credentials for use in future sessions.
- Users should be able to explicitly terminate a session via a logout button or link. It should be easy to find and obvious to most users.

## Summary

This laundry list of security requirements is a lot to think about for every application deployment, but vigilance in this area can drastically improve an organization's security posture. The requirements can be put into a standardized template, and at the end of the process each requirement should have a mark for pass, fail, or perhaps not applicable.

Anything marked as a failure should be noted and can be escalated or accepted as a risk.

Ben Whaley is a senior engineer at Applied Trust Engineering ([www.atrust.com](http://www.atrust.com)) in Boulder, Colorado. Ben has a degree in Computer Science from the University of Colorado at Boulder, is Certified Information Systems Security Professional (CISSP) #109297, and is a Red Hat Certified Engineer under Red Hat Enterprise versions 3-5. Ben is also a contributing author to the *Linux Administration Handbook, 2nd edition*.

## HNS SECURITY SOFTWARE DATABASE

Get the largest selection of the best security software for Windows, Linux, Mac OS X and Windows Mobile platforms.

[www.net-security.org](http://www.net-security.org)





## Attend Hacker Halted 2008 Security Event in USA

**May 28th - June 4th 2008, Myrtle Beach**

Hacker Halted has been successfully held in Mexico City, Dubai, Singapore, Kuala Lumpur, China and now in the USA.

**Special Keynote Session  
Featuring Howard Schmidt**

For more information, please visit  
<http://www.hackerhalted.com>

Email: [info@hackerhalted.com](mailto:info@hackerhalted.com)



## Hiding inside a rainbow

By Didier Stevens

**Before I start explaining the techniques I developed to hide data inside a rainbow table, let's first cover some basics.**

Steganography is the art of hiding messages so that uninitiated wouldn't suspect the presence of a message. While cryptography makes the message unreadable, it doesn't conceal it. Steganography does the opposite: it conceals the message but the message stays readable. A very ancient example of steganography was to tattoo the message on the shaven head of the messenger, and send the messenger on his way once his hair had grown back. I trust you can work out the method to recover the message.

One could say that steganography is nothing more than security through obscurity.

Nowadays, you can find many steganography programs to hide data inside digital pictures. The principle is easy to understand: each pixel of the picture has a color. This color is coded with a given number of bits. Changing the bits changes the color. Changing the most important bits results in a dramatic change of color, but changing the least important bits results in a small color nuance, which is often imperceptible to the naked eye. To hide the message in

the picture, break it up into its individual bits and use them to set the least important bit of each pixel in the picture. When looking at both pictures (original and carrier), you won't see a difference. Send your picture to your recipient (via e-mail, a picture sharing service, or any other electronic means), and then she can recover the hidden message by extracting the bits and recomposing the message.

You'll understand that the size of the hidden message is severely restricted by the size of the carrier picture and the number of bits per pixel you use. Say that you can only use 1 out of 8 bits of a picture, then a 1 MB picture theoretically allows you to hide a 128 KB message. That's fine for text, but not enough for other media. My solution is to use much larger carriers than pictures.

A rainbow table is a huge binary file used for password cracking. We are talking about gigabytes, one table is often 1 GB large, and a set of rainbow tables comprises tens of tables. The rainbow tables I've used in my research are generated with software from Project

## RainbowCrack.

A rainbow table is just a sequence of records. Each record has 2 fields of 8 bytes each, this makes a record 16 bytes wide. Therefore the size of a rainbow table is a multiple of 16. A record represents a chain. The first field is the password that started the chain. Actually, the first field is an index into the keyspace of all

possible passwords for the given rainbow table set. It is a random number between 0 and the size of the keyspace - 1. The second field is the hash of the last password in the chain (actually, this is also an index and not the real hash). The rainbow table is sorted on the second field: the record with the lowest hash is first in the table and the one with the highest hash is last.

000000000h:	6F AF B2 DD 24 00 00 00	32 24 00 00 00 00 00 00	o-^Ý\$...2\$.....
00000010h:	75 96 48 46 5E 00 00 00	F4 45 00 00 00 00 00 00	u-HF^...6E.....
00000020h:	89 A5 A4 31 66 00 00 00	97 A4 00 00 00 00 00 00	%Ý#1f...-x.....
00000030h:	5E C8 02 7F 1C 00 00 00	A7 C4 00 00 00 00 00 00	^È.Ø....SÄ.....
00000040h:	74 B6 B4 1A 2D 00 00 00	A7 C4 00 00 00 00 00 00	t¶'...-...SÄ.....
00000050h:	37 08 CE 19 57 00 00 00	11 0C 01 00 00 00 00 00	7.Í.W.....
00000060h:	82 C0 1C 3A 5E 00 00 00	0F 36 01 00 00 00 00 00	,À.:^...6.....
00000070h:	F2 41 2F BD 94 00 00 00	5D 60 01 00 00 00 00 00	ðA/Ý...]`.....
00000080h:	47 C5 6D 61 65 00 00 00	5D 60 01 00 00 00 00 00	Gímae...]`.....
00000090h:	D0 0E 56 13 85 00 00 00	B9 24 02 00 00 00 00 00	Ð.V.....`\$.....
000000a0h:	6B E8 97 D0 7F 00 00 00	56 8E 02 00 00 00 00 00	kè-ÐØ...VŽ.....
000000b0h:	42 8C B4 75 90 00 00 00	0E 19 03 00 00 00 00 00	BQE'u].....
000000c0h:	1A DE A7 9C 9C 00 00 00	25 34 04 00 00 00 00 00	.P\$œœ...%4.....
000000d0h:	F6 F4 54 F1 6C 00 00 00	C7 77 04 00 00 00 00 00	öôTñ1...Çw.....
000000e0h:	6E 34 EF E5 9A 00 00 00	B2 7F 04 00 00 00 00 00	n4iåš...^.....
000000f0h:	BB 97 87 9F 5E 00 00 00	3D A2 04 00 00 00 00 00	>-#Ý^...=ç.....

This is the hex dump of a rainbow table (the first 16 chains). The left box highlights the random data, notice that the 3 most significant bytes are 0. The right box highlights the hash, notice that this column is sorted.

## Rainbow-steganography method 0

The first method to hide data with a rainbow table is really trivial, just rename the file you want to hide to the name of a rainbow table, like this one:

Im\_alpha-numeric-symbol14-space#1-7\_0\_54  
00x67108864\_0.rt

But this method will not withstand a superficial inspection of the file. A forensic analyst will see through your subterfuge, by looking at the content of this file she will recognize the format of the media file you've renamed and realize that it's not a rainbow table.

## Rainbow-steganography method 1

Because the first field of a rainbow table record is just a random number, we can replace it with our own data from the file we want to

hide. We cannot use all the bytes in this field, because the size of the keyspace is usually smaller than 8 bytes wide. The most-significant-bits of the password field are set to zero. Setting them to one would give our secret away. We must limit our usage of the password field to the least-significant-bytes.

Changing these bytes will not change the structure of the rainbow table, so it will still appear as a valid rainbow table. The only consequence of our change is that the chain cannot be used anymore to crack a password. But if we leave a certain percentage of chains in the rainbow table unchanged, the rainbow table can still be used to crack some passwords.

To illustrate the technique, we insert 32 bytes (the sequence from 0x00 through 0x1F) in the rainbow table on the following page.

000000000h:	6F AF B2 DD	24 00 00 00 32 24 00 00 00 00 00 00 00 00 00 00	o^-^Y\$...2\$.....
00000010h:	75 96 48 46	5E 00 00 00 F4 45 00 00 00 00 00 00 00 00 00 00	u-HF^...6E.....
00000020h:	89 A5 A4 31	66 00 00 00 97 A4 00 00 00 00 00 00 00 00 00 00	%Yx1f...-x.....
00000030h:	5E C8 02 7F	1C 00 00 00 A7 C4 00 00 00 00 00 00 00 00 00 00 00	^È.Ø...SÄ.....
00000040h:	74 B6 B4 1A	2D 00 00 00 A7 C4 00 00 00 00 00 00 00 00 00 00 00	t¶'...-...SÄ.....
00000050h:	37 08 CE 19	57 00 00 00 11 OC 01 00 00 00 00 00 00 00 00 00 00	7.Î.W.....
00000060h:	82 C0 1C 3A	5E 00 00 00 OF 36 01 00 00 00 00 00 00 00 00 00	,À.:^...6.....
00000070h:	F2 41 2F BD	94 00 00 00 5D 60 01 00 00 00 00 00 00 00 00 00	ðA/Y"...]`.....
00000080h:	47 C5 6D 61	65 00 00 00 5D 60 01 00 00 00 00 00 00 00 00 00	Gimae...]`.....
00000090h:	D0 OE 56 13	85 00 00 00 B9 24 02 00 00 00 00 00 00 00 00	Đ.V.....^\$.....
000000a0h:	6B E8 97 D0	7F 00 00 00 56 8E 02 00 00 00 00 00 00 00 00	kè-ĐØ...VŽ.....
000000b0h:	42 8C B4 75	90 00 00 00 0E 19 03 00 00 00 00 00 00 00 00	BŒ'u].....
000000c0h:	1A DE A7 9C	9C 00 00 00 25 34 04 00 00 00 00 00 00 00	.P\$œœ...%4.....
000000d0h:	F6 F4 54 F1	6C 00 00 00 C7 77 04 00 00 00 00 00 00 00	öôTñl...Çw.....
000000e0h:	6E 34 EF E5	9A 00 00 00 B2 7F 04 00 00 00 00 00 00	n4iåš...^.....
000000f0h:	BB 97 87 9F	5E 00 00 00 3D A2 04 00 00 00 00 00 00	>-#Ý^...=ç.....

We will replace the random bytes in the red box. The keyspace of this rainbow table is less than 5 bytes (0xFFFFFFFF), that's

why I decide to change only the 4 least significant bytes of the start of a chain. This is the result:

000000000h:	00 01 02 03	24 00 00 00 32 24 00 00 00 00 00 00 00 00 00 00	....\$...2\$.....
00000010h:	04 05 06 07	5E 00 00 00 F4 45 00 00 00 00 00 00 00 00 00	....^...6E.....
00000020h:	08 09 0A 0B	66 00 00 00 97 A4 00 00 00 00 00 00 00 00	....f...-x.....
00000030h:	0C 0D 0E 0F	1C 00 00 00 A7 C4 00 00 00 00 00 00 00	.....SÄ.....
00000040h:	10 11 12 13	2D 00 00 00 A7 C4 00 00 00 00 00 00 00	....-...SÄ.....
00000050h:	14 15 16 17	57 00 00 00 11 OC 01 00 00 00 00 00 00	....W.....
00000060h:	18 19 1A 1B	5E 00 00 00 OF 36 01 00 00 00 00 00 00	....^...6.....
00000070h:	1C 1D 1E 1F	94 00 00 00 5D 60 01 00 00 00 00 00 00	...."..."`.....
00000080h:	47 C5 6D 61	65 00 00 00 5D 60 01 00 00 00 00 00 00	Gimae...]`.....
00000090h:	D0 OE 56 13	85 00 00 00 B9 24 02 00 00 00 00 00	Đ.V.....^\$.....
000000a0h:	6B E8 97 D0	7F 00 00 00 56 8E 02 00 00 00 00 00	kè-ĐØ...VŽ.....
000000b0h:	42 8C B4 75	90 00 00 00 0E 19 03 00 00 00 00 00	BŒ'u].....
000000c0h:	1A DE A7 9C	9C 00 00 00 25 34 04 00 00 00 00	.P\$œœ...%4.....
000000d0h:	F6 F4 54 F1	6C 00 00 00 C7 77 04 00 00 00 00	öôTñl...Çw.....
000000e0h:	6E 34 EF E5	9A 00 00 00 B2 7F 04 00 00 00 00	n4iåš...^.....
000000f0h:	BB 97 87 9F	5E 00 00 00 3D A2 04 00 00 00 00	>-#Ý^...=ç.....

It is clear that this modification is very obvious when you look at it, because the start entries are not random anymore. But if you use data that looks random (using compression or encryption), it will not stand out from the other random bytes. You can even use this modified rainbow table to crack passwords.

The first 8 chains will not crack passwords anymore, because the start of the chain has

been changed. But this does not cause an error and all the other chains are still usable. The only way to detect the hidden bytes (other than statistical analysis), is to recalculate the chain and compare the calculated hash with the stored hash. If they differ, the start has been tampered with.

You can do this with the rtdump command, like this:

```
rtdump lm_alpha-numeric-symbol14-space#1-7_0_5400x67108864_0.rt 0
```

If the chain has been modified, the message will be:

```
#5379 0000007892d3684e 2U-Z&_!32552d5a26255f f ae1f4032a13deb4
#5380 0000001cd18650f8 GA!!X^!_!47412121585e21 4f3b9b48a4f8bce9
#5381 00000012fdbd1b46a D50 L$ _!44354f204c2420 9087630c3c23978e
#5382 0000003974f7e304 NALI%T$ _!4e414c49255424 e949964227f9ff42
#5383 00000061198df1e W89+EB!_!5738392b454221 dde259f97179d81f
#5384 0000009cf37aafc @PLTBST !40504c54425354 5f4205884bb62199
#5385 000000218cfce0b0 H16C-zJ_!484936432d254a cb0c63789c153785
#5386 0000004b4b8a94bd RSN+RNN !52534e2b524e4e c4a3bb176cee0d99
#5387 00000070f855ff04 02NRC$^_!30324e5228245e 70ba56e3b7c5b4de
#5388 00000052a3cb0932 TH9&C++_!54483926402b2h 42220c7d53fce405
#5389 0000007b2cf16ade 3CPU_EW_!334350565f4557 6ea74d05e312265d
#5390 000000b59a9385cd *P6=WE_!2a50364f3d5745 223d5bf9c9053fdf
#5391 0000008e3fa0f8f7 79eHNK_!373940484e4b28 64621847c722d35a
#5392 0000000dh6b59025 CQ90!U_!4351394f21565f 78811308fc8e1de6
#5393 000000712fe1c581 04=FG^+_!30343d46475e2b b81b3fded1e7db2c
#5394 0000006f57e0cc98 0IA2^QN_!304941325e514e d823a3e10cbc642e
#5395 0000004bfccdd4d5 R0>9%AE_!52302939254145 b2ae5baf3099da79
#5396 0000002505d15ff0 IA*0-YZ_!49412a4f2d595a 7ff206f9e94f2d07
#5397 0000009de4f2d1f4 00ZC0=J_!40305a43303d4a abe8023b755e4466
#5398 000000059623c55c AR05*UU_!415230352a5655 9c6e1abd1889c564
#5399 000000b6a41b59a3
```

warning: rainbow chain integrity check fail!

D:\MyDirs\Hack\RTHide>

The problem with this test is that it is very time consuming, checking a complete rainbow table takes about as much time as calculating the rainbow table, because you're in fact recalculating all the chains. FYI, each 1 GB table from my set took about 1 week to generate.

## Rainbow-steganography method 2

The disadvantage of method 1 is that there is a way, albeit costly, to detect the hidden data. This is because we replace the random bytes, that makeup the start of the chain, by the data we want to hide, thereby breaking the chain. A broken chain can be detected by recalculating the chain and comparing the recalculated hash with the stored hash. If they differ, the chain is broken.

But if we know that we are breaking chains, why don't we fix them? We can proceed as follows:

- replace the start of the chain (random bytes) with the data we want to hide
- recalculate the chain
- replace the hash of the chain with the new hash we calculated.

This way, there are no more broken chains that give away our hidden secret. But now there is another telltale sign that the rainbow table has been modified to hide data: the hashes aren't sorted anymore. Remember

that a rainbow table has to be sorted (the sort key is the index of the hash) to be useful. It is very unlikely that our new hash is greater (or equal) than its predecessor and smaller (or equal) than its successor. Detecting an unsorted rainbow table is much easier than finding broken chains.

OK, so if the new rainbow table is unsorted, why don't we just sort it again? Well, if we resort the rainbow table, we destroy the order in which we stored our hidden data, so we loose the hidden data itself.

You could keep the original order of the hidden data by creating an index, this is another file that indexes the chains with hidden data. For example, you could make a list of all the hashes with hidden data. This list will then allow you to retrieve all chains with hidden data in the correct order. And the fact that you have such a list of chains isn't necessarily suspicious, it's just a list of hashes you want to crack.

But there is a simple way out of the unsorted rainbow table problem. Rainbow tables generated with the rtgen program are unsorted. In fact, you have to sort them with the rtsort command after generating them, before they can be used by the rtcrack program. The solution is to adapt the rtgen program to generate a rainbow table with hidden data, and keep this unsorted rainbow table.

Our modified rtgen program allows us to generate an unsorted rainbow table with hidden data. The only way to detect this hidden data is with statistical analysis, provided that the hidden data doesn't appear random. There are no broken chains that indicate hidden data, unlike with the previous method.

The disadvantage of this method is that you'll have to generate a new rainbow table to hide your data, which is a time consuming process.

### Rainbow-steganography method 3

My last steganographic technique is based on the fact that a rainbow table contains chains with the same hash index but with a different start index.

Take the rainbow table I've used in my tests. It's 1 GB large and has 67.108.864 chains. It contains 9.513.435 pairs of chains with the same hash index but with a different start in-

dex. For 4.756.561 of these pairs, the first chain has a higher start index than the second chain. And for 4.756.874 of these pairs, the opposite is true: the first chain has a lower start index than the second chain. This even distribution should be no surprise, as the rainbow table is only sorted on the hash index and not on the start index.

We can change the order of these pairs without breaking the chain and without disrupting the order of the rainbow table. This will allow us to encode 1 bit per chain. I define the following encoding convention:

- a pair of chains with the same hash index and with the start index of the first chain smaller than the second chain represents a bit equal to zero
- a pair of chains with the same hash index and with the start index of the first chain greater than the second chain represents a bit equal to one.

000000000h: 6F AF B2 DD 24 00 00 00 32 24 00 00 00 00 00 00 00 00	o-^Ý\$...2\$.....
00000010h: 75 96 48 46 5E 00 00 00 F4 45 00 00 00 00 00 00 00 00	u-HF^...6E.....
00000020h: 89 A5 A4 31 66 00 00 00 97 A4 00 00 00 00 00 00 00 00	%Ýx1f...-x.....
00000030h: 5E C8 02 7F 1C 00 00 00 A7 C4 00 00 00 00 00 00 00 00	^È.Ø...SÄ.....
00000040h: 74 B6 B4 1A 2D 00 00 00 A7 C4 00 00 00 00 00 00 00 00	tq'...-...SÄ.....
00000050h: 37 08 CE 19 57 00 00 00 11 0C 01 00 00 00 00 00 00 00	7.Î.W.....
00000060h: 82 C0 1C 3A 5E 00 00 00 OF 36 01 00 00 00 00 00 00 00	,À.:^...6.....
00000070h: F2 41 2F BD 94 00 00 00 5D 60 01 00 00 00 00 00 00 00	òA/H"...]`.....
00000080h: 47 C5 6D 61 65 00 00 00 5D 60 01 00 00 00 00 00 00 00	Gimae...]`.....
00000090h: D0 OE 56 13 85 00 00 00 B9 24 02 00 00 00 00 00 00 00	D.V.....*\$.....
000000a0h: 6B E8 97 D0 7F 00 00 00 56 8E 02 00 00 00 00 00 00 00	kè-DØ...VŽ.....
000000b0h: 42 8C B4 75 90 00 00 00 0E 19 03 00 00 00 00 00 00 00	BCE'uU.....
000000c0h: 1A DE A7 9C 9C 00 00 00 25 34 04 00 00 00 00 00 00 00	.PŠœœ...%4.....
000000d0h: F6 F4 54 F1 6C 00 00 00 C7 77 04 00 00 00 00 00 00 00	ööTñl...Çw.....
000000e0h: 6E 34 EF E5 9A 00 00 00 B2 7F 04 00 00 00 00 00 00 00	n4iåš...*.....
000000f0h: BB 97 87 9F 5E 00 00 00 3D A2 04 00 00 00 00 00 00 00	>-#Ý^...=ç.....

In our test table, the pair in the first box represents a 0 (0x1C7F02C85E < 0x2D1AB4B674) and the pair in the second box represents a 1 (0x94BD2F41F2 > 0x65616DC547).

Use this algorithm to hide a file in a sorted rainbow table:

- start a sequential search of chain pairs with equal hash indexes and different start indexes
- for each bit of the file to hide

    o if the bit is 0 and the chain pair has a first start index higher than the second, swap the order of the chains

    o if the bit is 1 and the chain pair has a first start index lower than the second, swap the order of the chains.

To extract the hidden file, use this algorithm:

- start a sequential search of chain pairs with equal hash indexes and different start indexes
- if a chain pair has a first start index lower than the second, write a bit equal to 0
- if a chain pair has a first start index higher than the second, write a bit equal to 1.

Use rthide2 to hide data in a rainbow table, it takes 3 arguments:

- the rainbow table (remains unchanged)
- the file to hide (remains unchanged)
- the new rainbow table

To hide a file data.zip inside a rainbow table called

lm\_alpha-numeric-symbol14-space#1-7\_0\_54  
00x67108864\_0.rt, use this command:

```
rthide2  
lm_alpha-numeric-symbol14-space#1-7_0_54  
00x67108864_0.rt data.zip  
lm_alpha-numeric-symbol14-space#1-7_0_54  
00x67108864_0.rt.stego
```

This will create a new rainbow table called  
lm\_alpha-numeric-symbol14-space#1-7\_0\_54  
00x67108864\_0.rt.stego

Use rtreveal2 to extract data from a rainbow table, it takes 3 arguments:

- the rainbow table
- the file to create
- the size of the hidden file

To extract the data, issue this command (you have to know the length of the hidden file, my PoC program doesn't store this).

rtreveal2

```
lm_alpha-numeric-symbol14-space#1-7_0_54  
00x67108864_0.rt.stego data.zip 1620
```

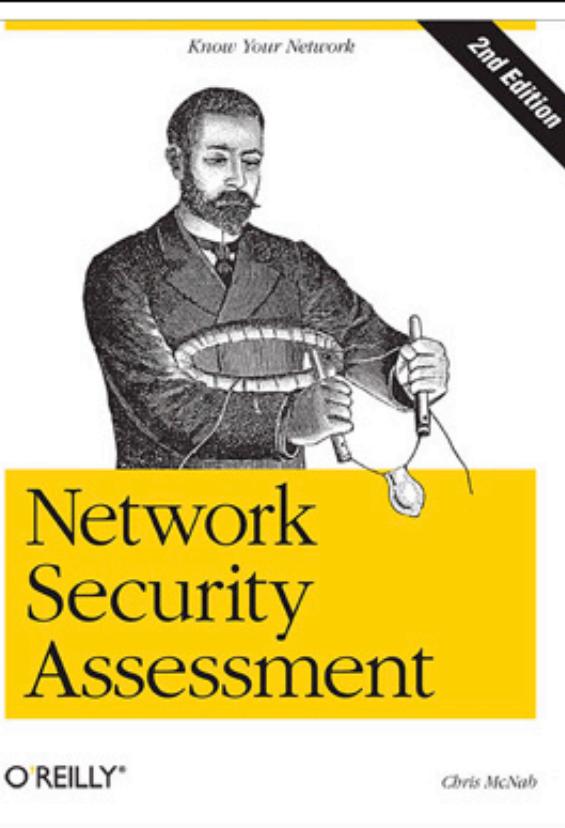
1620 is the length of file data.zip

The advantages of this technique over the previous techniques I developed is that it creates sorted rainbow tables without broken links, and that it is fast. The disadvantage is that it stores much less hidden data. In my example, a maximum of about 1 MB (9.513.435 bits) can be hidden in a rainbow table of 1 GB. Statistical analysis is the only way to detect the hidden data, but you can foil this by making your data appear random, for example with strong encryption.

### Source code

PoC code to store and retrieve data in rainbow tables using these technique can be found on my web site.

Didier Stevens (CISSP, MCSD .NET, MCSE/Security) is an IT Security Consultant currently working at a large Belgian financial corporation. He is employed by Contraste Europe NV, an IT Consulting Services company ([www.contraste.com](http://www.contraste.com)). You can find the rainbow table PoC code and other open source security tools on his IT security related blog at [DidierStevens.com](http://DidierStevens.com).



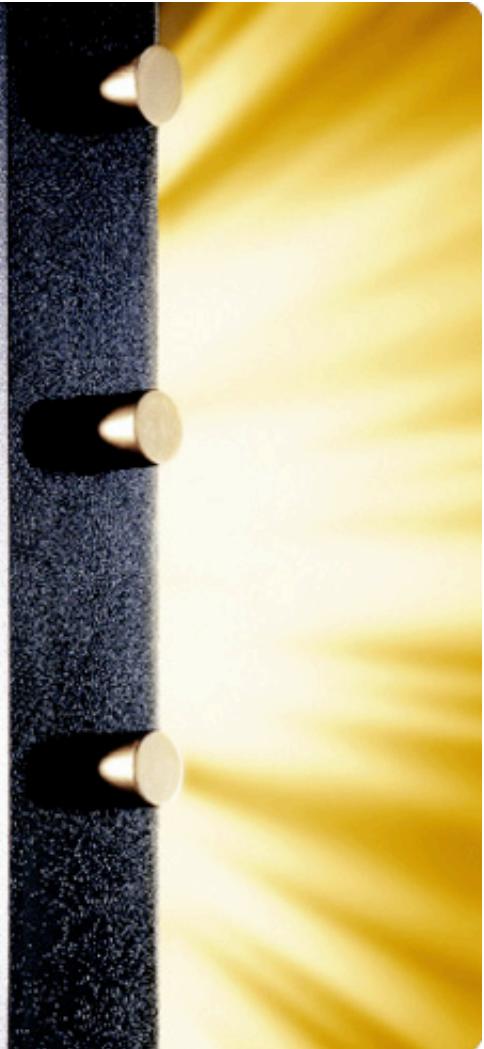
**Network Security Assessment** provides you with the tricks and tools professional security consultants use to identify and assess risks in Internet-based networks—the same penetration testing model they use to secure government, military, and commercial networks.

With this book, you can adopt, refine, and reuse this testing model to design and deploy networks that are hardened and immune from attack.

[www.oreilly.com](http://www.oreilly.com)

# The insider threat: hype vs. reality

By Dan Sarel



Nowadays, the term “insider threat” is banded about as the proverbial boogieman that is out to get us. There is confusion, vendor hype and statistics surrounding this topic and consequently some dismiss it as the latest in a wave of security scares with little substance behind it. The term “insider threat” may be misused but nonetheless the threat is real and poses significant risks to both enterprises and government.

The truth is that the insider threat is probably going to increase and worsen before it gets better and not just because we are paying more attention to it. This is due to a constellation of factors including rising organized cybercrime, increased use of outsourcing and the ubiquity of data. However, before we delve into the threat and the means we might employ in order to deal with it, we need to define what falls within the scope of “insider threat”.

## Defining the insider threat

The distinction between accidental damage from insiders and intentional, malicious damage is often forgotten, intentionally or not, and it is time to put it back in its place. While both types of damage can be significant, there is a

big difference between the two. Accidental damage has always been a concern and there is no particular reason to believe that it is on the rise – certainly, it is possible that more employees have access to more sensitive data, or that enterprises tend to retain more sensitive data than before, but this in itself does not increase the probability of a data leak.

The definition of “breach” is also tightly linked to the issue of data loss or leakage. There is a big difference, in risk terms, between the accidental loss of a laptop or disk with sensitive information, to intentional data theft. In the former, there is a concern that sensitive data might fall into the wrong hands, whereas in the latter, it is certain to fall into the wrong

hands.

It is akin to the difference between losing your house keys, worrying a burglar might find them and use them, versus having your house broken into and your money stolen. In other words, just because someone accidentally sent an email with sensitive documents outside the company by mistake, it is far from certain that the data would be misused. Similarly, even if someone who is not a model citizen finds a lost laptop, he will most likely wipe the hard disk clean and sell the laptop, not hack the login and password to retrieve the data.

Accidental “breaches” therefore pose significantly less risk than intentional ones. While accidental data loss is impossible to prevent completely, it is possible to prevent or mitigate much of it, which is what DLP solutions do. There is a reason why DLP stands for Data Leakage Prevention (or Data Loss Prevention by some accounts), and not for Data Theft Prevention. Most DLP vendors do not claim to be able to stop intentional data theft. An employee stealing data from the company is not likely to send it to her buyers via email or be foolish enough to download files to removable media if access to those is controlled.

**Technically, risk is the product of the probability of something happening and the damage it could cause if successful.**

Accidental data leakage by insiders is also not a localized phenomenon within the corporate IT infrastructure. It could happen in a variety of ways and using a variety of systems, which is why DLP solutions often span the network, desktops and end-point devices.

Intentional data theft by insiders, on the other hand, and especially the kind that could cause serious damage, is highly localized to those areas where valuable information is stored, and in large quantities – i.e., databases. While databases are usually at the bottom of the IT stack, feeding tiered layers of applications above them, they are accessible directly by privileged users such as DBAs, sys admins, developers, consultants and outside contractors. In large enterprises, this group of users with privileged access can span hundreds of people.

Whereas with accidental data leakage one can hope that employees largely try to follow procedures and may only falter occasionally, in the case of malicious data theft, the insider perpetrators intentionally flout policies and procedures, so much stronger enforcement is required.

### **Assessing the risk of malicious insider breaches**

Technically, risk is the product of the probability of something happening and the damage it could cause if successful. On that merit alone,

the risk posed by insiders is significant because the potential damage is huge. Highly skilled insiders with access privileges can do infinitely more damage than very talented hackers on the outside, and if they are really good, they are also more likely to cover their tracks successfully.

Earlier this year, in a highly publicized breach a DBA from Certegy, a credit card processing subsidiary of Fidelity National Information Services, sold 8.5 million records (at last count) containing customer credit card and bank account data. This is the poster child malicious insider attack, the nightmare scenario – and no doubt a very serious breach on a massive scale. In a similar incident, an insider working for a credit card processing company was caught by the Secret Service in a sting operation after he had tried to sell customer data belonging to Johnson & Johnson and the Disney Video Club. One could surmise that such large-scale breaches are unlikely to become frequent, and though their impact is noticeable, the overall scale and likelihood means that they are rare and far apart.

However, there are numerous, smaller incidents that are a lot more frequent. Most of them do not get reported, and it is likely that an even larger percentage go undetected. There may be minor infractions of policy, such as peeking into a colleague’s salary data in advance of salary negotiations.

Such things happen all the time. Moving up the ladder, we would encounter misdemeanors such as selling individual customer records to interested parties – for example, an employee of a phone company selling call records on demand to private investigators, or a student bribing an IT employee at a university to change his grades in the database.

All of those smaller acts of intentional data theft, unlawful data alteration and abuse of privileged access to information for personal gain add up to cause significant damage, but they are completely below the radar most of the time. So the overall risk is comprised of many smaller infractions that individually cause minor damage, along with fewer but increasingly grave breaches that can individually cause major damage affecting a company's bottom line.

### **Understanding motivation**

When looking into the more serious incidents, there are many reasons why a trusted employee would knowingly and purposefully cause damage or steal from his employer. The “disgruntled employee” is cited most often as

the malicious insider, though this is an oversimplification. Certainly, disgruntled employees are more likely to betray the trust of their employer than happy employees, given the opportunity to do so, but few are disgruntled enough to plan and execute such acts without some external motivation.

Understanding the insider threat is therefore inextricably tied to understanding the threat landscape in general. The motivation of hackers worldwide has shifted over the past few years from vanity and opportunity-driven acts to criminally motivated acts. Cybercrime is organized crime, with hierarchies, a complicated value chain of tools and methods, trading platforms for stolen credit card and personally identifiable information, and crime bosses who manage the operations.

Enterprises and ISPs now have server rooms full of firewalls, IDS/IPS, appliances that filter spam, malware and viruses, making the perimeter an almost impregnable wall. It is difficult to penetrate this wall and extract valuable data from inside the corporate IT stack, passing through layers of security.

### **Criminals always look for the easy way in.**

Criminals always look for the easy way in. Once their previous modus operandi become difficult, they start looking for other ways of getting the data they need – and this is where insiders become very valuable to them, and dangerous to the enterprise.

Imagine that you are a DBA with a large retailer. One day you get a phone call to your cell phone, and a stranger offers you \$5,000 if you pass them the details of 30,000 customers. You hesitate and the offer is sweetened to \$7,000. Some would succumb at this point, especially if their skills and level of access allow them to do so undetected. You still hesitate, though, at which point the stranger asks you how your daughter Emily is doing.

A farfetched scenario? Unfortunately, it is not, and in most cases that were made public, the implicated insider was motivated by money, not by threats.

### **Mitigation and remediation**

What about preventing this from happening in the first place? In the last season of *The Sopranos*, a couple of Tony Soprano’s goons go to the old neighborhood to shake down the manager of a newly opened coffee shop for “insurance”. The young manager explains that the coffee shop is a branch in a national chain and that headquarters count every coffee bean and dime – he simply cannot give them money off the books and if they force him, headquarters would simply send someone else to replace him. The goons leave empty handed, bemoaning the fate of the old neighborhood.

The same is true of data theft: Where there is no access, there is no crime. If privileged, trusted users knew that their actions could not go undetected and if this were made clear to criminals as well, such a course of action would become increasingly difficult.

The phone call described in the previous section would not achieve its purpose. We are still far from reaching this objective but it will eventually happen.

Before prevention, there are many other ways of mitigating the risk. Awareness of the issue at hand is a first and necessary step, which should lead to stricter policies and more granular access levels for privileged users. In a surprising number of enterprises, you would find shared logins and passwords, for example, or that privileges, once granted, are seldom revoked. Lack of awareness and prioritization is why this is still happening.

Frequent auditing, preferably by an external 3rd party, is the next logical step. It may not stop insider breaches, but it may discover them while they are ongoing and prevent them from continuing.

Ultimately, however, we must find a way of looking at what users are doing and ensuring it complies with policy, regardless of who those users are. After all, an outside hacker who is able to commit a privilege escalation attack would have insider privileges. He becomes the insider. This is where sophisticated tools for real-time monitoring, alerting and prevention can help.

In order to know which actions are legitimate and which are not, it is not enough to have

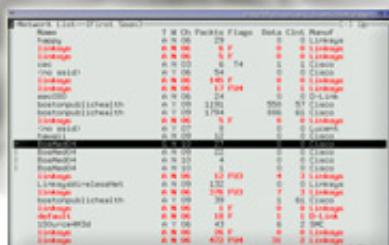
policies. We need to understand the context in which these actions are taken, be able to act in real-time, and do so without hindering daily operations. Given that databases hold the largest concentration of critical data, and that they are highly complex applications, they require a specific set of tools and technologies to perform this task, collectively known as database activity monitoring (DAM) or database intrusion/extrusion prevention.

Much of the risk posed by malicious insiders can be mitigated through intelligent use of these tools, providing that they can detect all forms of direct access to the database and the use of sophisticated attack vectors – after all, the users who have privileged access to databases are among the most sophisticated and skilled users within IT. Contrast this with DLP solutions that target the average user whose skills would normally not suffice to outsmart the system.

When separating the wheat from the chaff, the insider threat emerges as a threat that needs to be addressed, using the right tools and procedures for the right kind of insider threat. Unintentional data loss can be widespread but its effects are usually not severe. Intentional, malicious data theft or abuse by privileged insiders can deal very painful blows to the enterprise, but requires a different approach and focus on databases, where the attractive data assets are located.

Dan Sarel is responsible for directing Sentrigo's product definition and design, and brings over a decade of security software and hardware experience. Dan joined Sentrigo ([www.sentrigo.com](http://www.sentrigo.com)) after serving as Check Point Software Technologies' Director of Product Management. At Check Point Dan led the VPN product line and went on to manage an international team that leads all of Check Point's enterprise product lines. Dan led several new product launches and served as a member of the product council, which determines the company's product strategy. Prior to Check Point Dan held a number of product management, marketing and consulting positions in the hardware and software security product market.

**Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system.**  
[www.kismetwireless.net](http://www.kismetwireless.net)





# Software spotlight

## WaterRoof

<http://www.net-security.org/software.php?id=689>

WaterRoof is an IPFW firewall frontend for Mac OS X with a easy interface and many options. Features include dynamic rules, bandwidth management, NAT configuration and port redirection, pre-defined rule sets and a wizard for easy configuration. You can also watch logs and graphic statistics. Rules configurations and network options can be saved and optionally activated at boot time.

## Botan

<http://www.net-security.org/software.php?id=94>

Botan aims to be a portable, easy to use, and efficient C++ crypto library.

## ModSecurity

<http://www.net-security.org/software.php?id=518>

ModSecurity is an open source intrusion detection and prevention engine for web applications. It operates embedded into the web server, acting as a powerful umbrella - shielding applications from attacks. ModSecurity supports Apache (both branches) today, with support for Java-based servers coming soon.

## Jsch

<http://www.net-security.org/software.php?id=417>

JSch is a pure Java implementation of SSH2. JSch allows you to connect to an sshd server and use port forwarding, X11 forwarding, file transfer, etc. You can integrate its functionality into your own Java programs.



## How B2B gateways affect corporate information security

By David Walling

**B2B gateways were introduced in 2003, marking the first time IT professionals could deploy best-of-breed managed file transfer tools without sacrificing their larger investment in enterprise business applications. Today, that value proposition has an added advantage: gateways have become building blocks for a secure information strategy.**

The intent of this article is to provide even-handed criteria for evaluating B2B gateways within the context of overall information security. "Information security" refers to all activities—physical, electronic, social—related to corporate information protection. This includes, but is not limited to, physically securing the premises, encrypting and backing up data, and developing, publishing and promoting an enterprise-wide security policy.

### Data transfer over public networks: risks and rewards

The appeal of a B2B gateway is based, in no small measure, on cryptographic attributes that allow data to be transmitted securely over public networks rather than proprietary VANs. Although the cost savings are attractive, any enterprise choosing to transport data across a public network assumes responsibility for protecting its infrastructure against risks posed by

the public network itself. The basic factors to consider are network reliability, load capacity, in-transit data protection, and shielding the enterprise from viruses, worms, and other malware.

As Gartner points out, centralization is one of the explicit virtues of the B2B gateway. A single, secure data portal is advantageous for many reasons, particularly for firms that must demonstrate robust data security for compliance audits. This consolidated port of entry defines the "edge" of the corporate domain and clarifies accountability for data moving into and out of the enterprise.

### Security-related gateway evaluation factors

Gateway technology is specifically designed to address the data security risks described above.

But gateways entail risks of their own that must be factored into any system evaluation. These risks can be divided into two categories: absolute (functionality-driven) and relative (cost/value-driven).

### Absolute risks

- **Capability:** How effectively will the gateway handle the functions most important to your operation? How well will it conform to your enterprise's published performance standards?
- **Platform support:** How efficient will the technology be within your hardware/operating system environment? Is it certified to meet your corporate production requirements?
- **Compliance:** If you must comply with corporate or industry regulations—HIPAA, GLB, Sarbanes-Oxley, and PCI, for example—does the system meet those standards and support timely, efficient compliance reporting?

### Relative risks

Relative risk factors relate to the cost of acquiring, installing, operating and maintaining the system. The right gateway choice for your company is the one that delivers the most value per dollar compared to 1.) other options in the marketplace; and 2.) the importance of the following factors within your operation:

- **Performance:** Better-performing systems consume less CPU, disk and memory resources. They are typically a better long-term buy for two more reasons: corporate traffic almost always increases rather than decreases, and a robust gateway can reduce (or redistribute) overall loads so your existing infrastructure can accommodate more traffic.
- **Reliability:** By definition, gateways are expected to be highly available. How well will the system scale in large, clustered implementations? How quickly can it recover from exceptional conditions, including component failure?
- **Ease of implementation:** The more quickly the gateway can be installed and put into production, the better the odds for rapid adoption and support by the enterprise.
- **Ease of use:** The most vocal proponents (or critics) of any system are usually the people responsible for its day-to-day operation. Usability promotes user adoption and delivers tangible benefits such as fewer input errors and faster, more effective reporting. From an

operations standpoint, a system that can be readily modified and reconfigured requires shorter maintenance windows.

### Typical stages of corporate information security

The fundamentals of securing corporate data don't change. At the most basic level, they boil down to restricting access, applying safety measures to the data itself, and making duplicates in case the original is lost or corrupted.

The operational context for these fundamentals, however, is constantly evolving. Most enterprises go through four stages of integrating information security into their core business processes.

#### Stage #1: The Fortress

At this stage, the enterprise protects data by building a wall around it. Information within this fortress is not encrypted, and the data transfer mechanisms aren't necessarily secure. Protection consists of restricting physical access to campuses and data centers and requiring passwords for log-in. Database passwords are often left at default values or are widely known and rarely changed, since all the data is "internal" anyway. In this scenario, the safety of all data is essentially equivalent and completely dependent on physical safeguards. Security is not intrinsic to either the data or business process.

#### Stage #2: The Private Line

At this stage, the company embraces the "private line" or "secure tunnel" for inter-enterprise data exchange. This link is secure, but no assumptions are made about protection beyond the link, and a breach in the link will expose all in-transit data. Business processes at either end of the link expect data in its native format. Security is not intrinsic to either the data or business processes.

#### Stage #3: Security Off the Wire

The third evolutionary stage infuses protection higher in the protocol stack. The application-layer software encrypts data using features within a broader software suite, or through a separate security product integrated into the overall business information process. Data transformation for the sake of security is only applied when necessary.

This stage takes security "off the wire" and allows the use of non-dedicated (but intrinsically less secure) networks like the Internet. Data protection may be oriented toward the document itself, treating each discrete document as an independently secured message, or toward the session layer (SSL and TLS). In the latter case, security parameters are established between two end-points and applied to one or more discrete documents passing over the session.

At this stage, data protection is disengaged from the lower, physical or data-link layers. This takes the safety burden off the network's shoulders. But engaging security at the application layer makes information safety beholden to the prerogatives of the business process. Disparate applications may provide different, and possibly wholly incompatible, data security schemes.

These differences make secure data transfer between heterogeneous systems across a

public network a formidable integration challenge.

#### Stage #4: The B2B Gateway

At this stage the corporation recognizes the value of a single subsystem for reliable, interoperable, secure data transfer over relatively low-cost public networks. Within the centralized architecture, all applications conform to the corporate security policy. Adaptive gateway interfaces make application integration relatively simple. Ongoing gateway operations can be easily monitored and exceptional conditions reported immediately.

B2B gateways that understand multiple application-layer transfer protocols—HTTPS, S/FTP, and so forth—can be configured to adapt to changes in the way the enterprise arranges its communications with others. By disengaging the secure communications aspect from the business process infrastructure, the company can tune components without tearing down and starting over.

## ANY ENTERPRISE PREPARING TO EXPAND INTER- OR INTRA-COMPANY DATA EXCHANGE MUST HAVE AN UPDATED, WRITTEN CORPORATE INFORMATION SECURITY POLICY

### Choose technology to support your security policy—not vice versa

Any enterprise preparing to expand inter- or intra-company data exchange must have an updated, written corporate information security policy. (The SANS Institute provides useful guidelines and templates at [www.sans.org/resources/policies](http://www.sans.org/resources/policies).) Well-crafted policies are clear about the company's standards and procedures in the following areas.

**Asset protection:** Reducing or preventing data loss with measures such as eliminating single points of failure in critical data processing paths. Other examples: appropriate data backup, in-place redundant systems, and ongoing hardware maintenance.

**Access control:** Installing authentication controls at both human and external system access points; requiring and enforcing the use of security credentials.

**Vulnerability detection:** Establishing mechanisms to detect compromised and/or vulnerable systems. For example, a digital certificate approaching its expiry date represents a definite vulnerability. A user account that hasn't been accessed for a long period represents a potential vulnerability.

**Monitoring and reporting:** Creating procedures to record and report access to sensitive information. Reports showing usual-and-customary access patterns are helpful for operators on the alert for unusual, and potentially harmful, activity.

**PAIN:** the elements of secure data transfer Secure electronic data transfer has four attributes: Privacy, Authentication, Integrity, and Non-repudiation. Prudent business practices—and increasingly, government and industry mandates—require these attributes in electronic data exchange of all types, including gateways.

*Privacy:* Encrypted data is intelligible only to those with the proper security credentials. Typically a public-key encryption scheme is used to ensure that only the intended recipient of the data can decipher the message.

*Authentication:* Secure credentials identify the originator or sender of the information. This is typically accomplished by attaching a digital signature to the message. The signature, encrypted with security credentials held only by the sender, can be authenticated by any recipient in possession of the sender's public key.

*Integrity:* A relatively short sequence of bits, known as a message digest, is produced using an algorithm with a very high probability of generating a different digest should any single bit in a message be altered. By sending an encrypted digest along with the message, a recipient can compare a locally computed digest to verify that the message was not altered in transit.

*Non-repudiation:* To prove non-repudiation (a receipt which the receiver cannot effectively deny), the data recipient digitally signs and returns an acknowledgment to the sender that includes the matching digest of the message, thereby providing both a certain identification of the recipient and proof that the message was successfully decrypted and received intact.

### A B2B gateway evaluation matrix

In summary, B2B gateways represent the consolidation of secure communication services accessible to various internal systems through adaptive interfaces. Endpoint configuration is relationship (trading partner) oriented, given the underlying assumption that endpoint management requires handling protocols or connections that vary by endpoint. Gateway activity is driven through interfaces to a business process management (BPM) system and integrated with information gathered throughout the enterprise.

David Walling is Chief Technology Officer for nuBridges. He can be reached at dwalling@nubridges.com.



**The world's most widely-used e-mail security and anti-spam system  
that protects over 1 billion e-mails every day.**

**Over 1 million downloads!  
Get your FREE copy today:  
[www.mailscanner.info](http://www.mailscanner.info)**





## Reputation attacks, a little known Internet threat

By Inaki Urzay

**A less known threat is consolidating which exploits the Internet as a mass-communication channel: reputation attacks. These attacks target both individuals and companies, and their goal is to ruin the victim's reputation. While attack techniques are varied, the consequences are often the same: a damaged reputation resulting in many cases in financial loss.**

### Ways to attack a reputation

Attackers can use several methods to ruin a company's reputation. Until now, most common attacks have been based on distributed denial of service (DDoS). The objective of these attack is to flood corporate online services by means of millions of non legitimate requests from botnets.

In this way, business performance is affected, causing direct financial losses and the corresponding damage to corporate image and reputation.

Corporate websites are also the target of 'defacement' attacks. They consist of trying to exploit a server or Web application vulnerability to modify pages or introduce other content in the pages that shows the corporate web server. When users and potential customers visit a corporate web page and find it has been modified by a third-party, their confidence in the company is seriously affected.

Another method used by hackers that has proven successful is publishing false information on forums and blogs. Seemingly genuine news items, quotes included (false, of course) strategically distributed on several online sites can spread like wildfire, and achieve their goal: to convince a large number of users that the information is true.

Many urban legends that are still popular today were originally created in a similar way, and have managed to affect highly prestigious multinational companies.

In a similar vein, there have also been false rumors aimed at manipulating stock market prices. Firstly, attackers send true stock market information as spam, to potentially interested parties. After several messages and once attackers consider they have sufficiently gained people's trust, they send false information to manipulate stock prices.

## Google: a reference point on the Web

Google's strategic position on the Internet has seen it become a reference when searching for information, but also has a key role in establishing corporate reputations, good or bad. Consequently, Google is also used to attack the reputation of third-parties.

The best known method is 'Google bombing' which allows specific websites to appear at the top of search results. Attackers study the way in which Google indexes and orders web pages during searches, and try to introduce critical content regarding a specific brand or company in the first places of the results list. When users search for a specific brand in Google, the first links displayed include pages aimed at damaging their reputation. Although Google has improved its algorithm to avoid these attacks, they are still common practice.

PageRank is another Google-based method aimed at ruining corporate reputations. It consists of algorithms developed by Google to measure quantitatively the relevance or importance of web pages on a scale of 0 to 10. A company's PageRank usually represents its popularity. If the value is high, it is usually considered to be a reliable source accessed by many important sites.

Google is currently penalizing companies who exchange links and artificially try to increase PageRank. Attackers are exploiting this to insert penalized links on legitimate web pages. This way, they get the site to be penalized, its PageRank to decrease, and thereby damage its reputation.

### Other ways of attacking a reputation

CastleCops ([www.castlecops.com](http://www.castlecops.com)) is a volunteer security community focused on making the Internet a safer place. Its free services include malware and rootkit cleanup, malware and phishing research.

CastleCops accepts donations via PayPal. Attackers took advantage of this to begin a campaign aimed at discrediting CastleCops. They stole PayPal users' passwords using

Trojans and phishing techniques, and made several donations to CastleCops.

When users realized someone had sent their money to CastleCops, they blamed CastleCops for the fraud. Consequently, CastleCops was forced to return all the money, and invest in resources to manage all the complaints and requests. CastleCops' reputation was undoubtedly damaged.

### Malware-based attacks

Most of the methods described above are essentially malware-based. For example, botnets are used to carry out distributed DoS attacks and to launch spam that contains false information to ruin companies' images. Most defacements also use automated attack tools. In the case of Google, malware is also used to automate the insertion of links and spam on 2.0 websites that allow users to add content. In the case of CastleCops, Trojans were used to steal PayPal users' credentials.

There are numerous scenarios in which viruses, Trojans and other malware-types can damage a company's reputation. In 2004, even Google was affected by the MyDoom worm which disabled many of its servers for several hours. Worse still, the search engine underwent the attack hours before being floated on the stock market. Other search engines such as Altavista, Yahoo! and Lycos were also affected by the worm. Phishing techniques, which are still as popular as ever, can also damage companies. These attacks are critical for banks, since they cause financial losses and strike fear in users. In the same way, specially-crafted Trojans (mainly banker Trojans) have become one of the worst Internet threats. The main danger lies in the fact they are designed to specifically affect certain entities, and in many cases, operate totally invisibly and when users access their online bank, their access credentials are sent to hackers.

In 2006, Trojans accounted for 53 percent of all new malware created, and 20 percent of these were banker Trojans. During 2007, there have already been over 40 percent more attacks than in the whole of 2006.

# **o3: magazine**

**Open Source / Enterprise  
Free DIGITAL magazine**

**<http://www.o3magazine.com>**

**INSIDE: Open Source Web Acceleration with Varnish Cache**

**o3:** The Open Source Enterprise Magazine

Issue 6  
August 2007  
<http://www.o3magazine.com>

**Deploying Globally Distributed Web Applications with Ruby on Rails**

Production Rails Apps with Mongrel  
Deploying PostgreSQL  
Simple Appliance Stacks with LFS  
Secure Global Networks with OpenVPN  
Enterprise WiFi -- Thin Access Points



This issue is sponsored by:  
**OTHELLO**  
<http://www.othellotech.net>

**INSIDE: Building Secure Postfix SMTP Appliances with LFS**

**o3:** The Open Source Enterprise Magazine

Issue 8  
September 2007  
<http://www.o3magazine.com>

**Designing Scalable Enterprise SMTP Networks for Email**

Using Dovecot for imaps / pop3d  
Encrypting Mail Protocols  
Using DSPAM to reduce storage requirements  
Web based email with Roundcube



This issue is sponsored by:  
**ARUBA**  
networks  
<http://www.arubanetworks.com>

# Italian bank's XSS opportunity seized by fraudsters

By Paul Mutton



**An extremely convincing phishing attack is using a cross-site scripting vulnerability on an Italian Bank's own website to attempt to steal customers' bank account details. Fraudsters are currently sending phishing mails which use a specially-crafted URL to inject a modified login form onto the bank's login page.**

The vulnerable page is served over SSL with a bona fide SSL certificate issued to Banca Fideuram S.p.A. in Italy. Nonetheless, the fraudsters have been able to inject an IFRAME onto the login page which loads a modified login form from a web server hosted in Taiwan.

This attack highlights the seriousness of cross-site scripting vulnerabilities on banking websites. It shows that security cannot be guaranteed just by the presence of "https" at the start of a URL, or checking that the browser address bar contains the correct domain name.

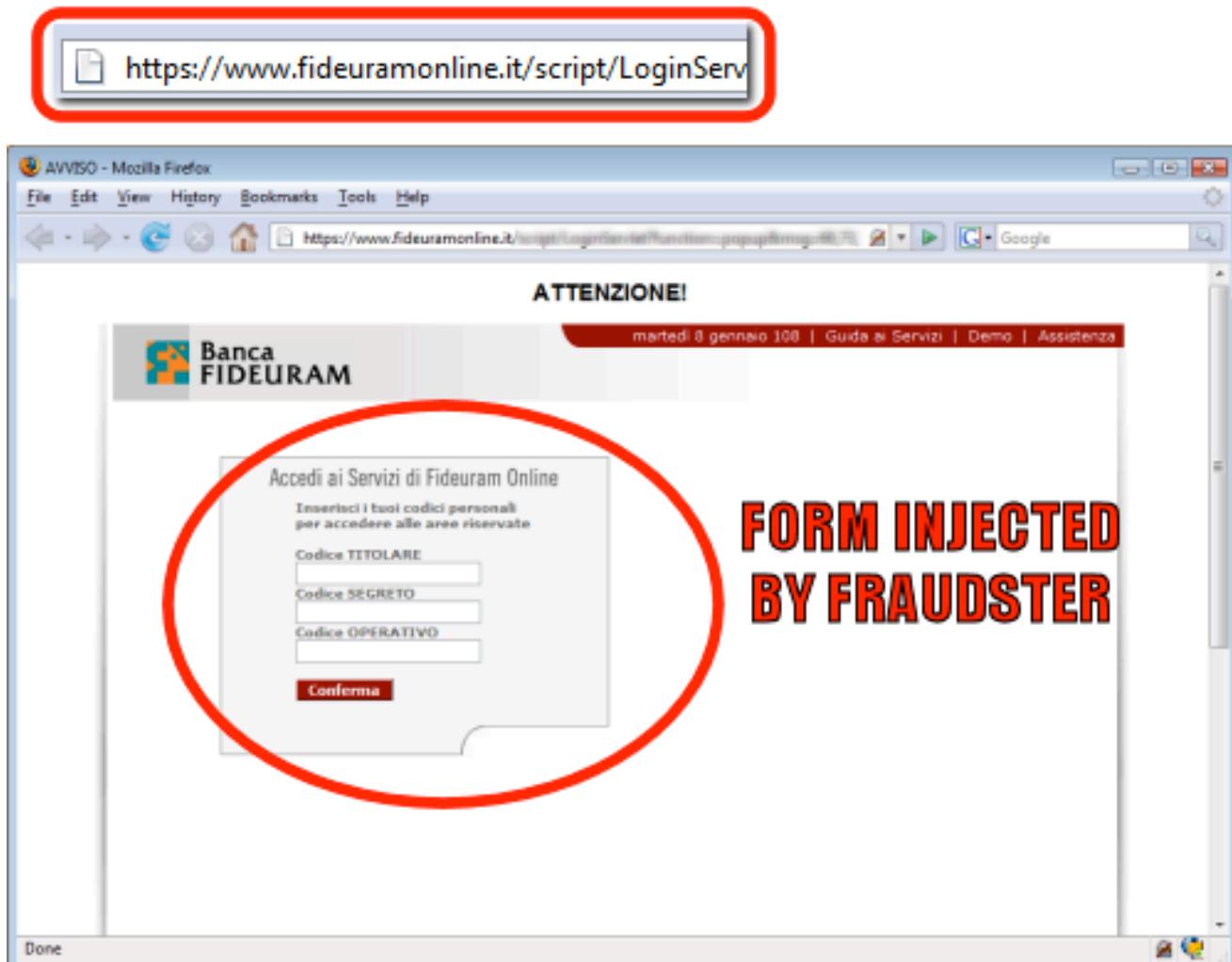
Cross-site scripting vulnerabilities on SSL sites also undermine the purpose of SSL certificates - while the attack detailed here injects external content via an IFRAME, it is important to note that a malicious payload could

also be delivered solely via the vulnerable GET parameter.

In the latter case, any SSL certificate associated with the site - included Extended Validation certificates - would display a padlock icon and apparently assure the user that the injected login form is genuine.

This particular attack is made all the more convincing by the vector used by the fraudsters: the URL employed by the attack injects a series of numbers directly into a JavaScript function call that already exists on the bank's LoginServlet page. This makes it difficult even for an experienced user to identify this as a cross-site scripting attack, as the URL does not look readily suspicious, with the injected content consisting only of numbers and commas.

## HTTPS URL



The fraudsters' login form presented inside the bank's SSL page.

The vulnerable page, decoding arbitrary GET parameters.

In a possible attempt to bypass automated security filters, the injected content from Taiwan also contains encoded JavaScript which is used to display the text "Inserisci i tuoi codici personali" ("Insert your personal codes") and "per accedere alle aree riservate" ("To access all reserved areas").

When the modified form is submitted, the contents are transmitted to the Taiwanese server

before the user is redirected to the bank's genuine, unaltered homepage. Netcraft has contacted the bank affected by this attack and blocked the phishing site for all users of the Netcraft Toolbar ([toolbar.netcraft.com](http://toolbar.netcraft.com)), and propagated the block to the companies which licence the Netcraft PhishFeed ([news.netcraft.com/phishing-site-feed](http://news.netcraft.com/phishing-site-feed)).

# The good, the bad and the ugly of protecting data in a retail environment

By Ulf Mattsson



The overall purpose of information security is to control risk by managing the impact of threats to information assets in the most cost-effective manner. This article takes a look at a typical Point-Of-Sale (POS) solution, identifying common architectural weaknesses that can lead to data compromise. Specifically, key business priorities are assessed against the POS architecture to vet the solution for potential security shortcomings that could prevent it from carrying out its business mission.

In many retail organizations, the principal business objectives are to achieve compliance to the Payment Card Industry Data Security Standard (PCI) to avoid fines and maintain proper standing in the industry, while protecting the brand name by avoiding breaches of customer credit card data. Many retail solutions have been carefully designed from both security and business goal perspectives. They may use hardening features such as PKI-driven strong mutual authentication of all system components, rigorous encryption of data in transit and at rest, secure unlock and update processes, etc. to be able to safely and reliably operate in the most hostile of networking environments. A computer containing sen-

sitive data that is physically stolen from a retail site can represent a significant risk.

Careful balance between business goals and security reduce the risk of a compromise that can threaten the retail organization's brand reputation and business operations. Compliance to PCI is not enough to safeguard information in a retail environment. This article will also assist in guiding security efforts in a POS environment. For example, weaknesses discussed here can prove to be effective at prioritizing testing attention and effort. In other words, the testing, design review, code review, penetration testing processes should be prioritized in order to make the most effective

use of the available development resources.

Some mature security solutions are also environmentally friendly and addresses “the green security challenge” by delivering software solutions that operate on existing computing infrastructure, typically on the same server as the application or database being secured. The appropriate level of encryption key pro-

tection can be achieved by using a well balanced combination of software cryptography and selective use of small footprint standard commodity type Hardware Security Modules. This environmentally friendly approach can provide the needed balance of protection, cost, operational needs and avoid installation of a large number of appliances.

## **ALL CREDIT CARD PROCESSING SYSTEMS REQUIRE LOGGING OF ALL ACCESS TO CREDIT CARD DATA, IN ADDITION TO QUARTERLY SCANS AND ANNUAL PENETRATION TESTS.**

### **The Payment Card Industry Data Security Standard**

The Payment Card Industry (PCI) Data Security Standard was created by major credit card companies to safeguard customer information. Visa, MasterCard, American Express, and other credit card associations mandate that merchants and service providers meet certain minimum standards of security when storing, processing and transmitting cardholder data. Merchants, service providers, and banks are required to perform an annual assessment for Level 1 (large) merchants, annual penetration testing and application testing Level 1 and 2 service providers. All credit card processing systems require logging of all access to credit card data, in addition to quarterly scans and annual penetration tests.

Credit card transmission networks, processing and storage systems require host and/or network intrusion detection or prevention. Firewalls providing access to credit card processing and storage systems require an appropriately configured and managed firewall. Remote access to credit card processing environments require two-factor authentication.

Databases, Web servers and applications that store or process credit card data require 128-bit SSL encryption and effective management of crypto key transmission and storage. Although currently not a PCI requirement, Visa and MasterCard encourage application development companies to certify their payment applications in accordance with the PCI Payment Application Best Practices program. Applications that meet these standards can be

listed on the Visa Web site as PCI-approved payment applications. For more information for merchants, including the current transaction volumes/categories for each level, please see [tinyurl.com/ypp9j4](http://tinyurl.com/ypp9j4). For the full text of the Data Security Standard, please see [tinyurl.com/ysdr77](http://tinyurl.com/ysdr77). To review the standards for the PCI Payment Application Best Practices program, please see [tinyurl.com/2lmgfp](http://tinyurl.com/2lmgfp).

### **How to review the state of security**

Data flows through a retail system, into and out of numerous applications and data stores. This flow, in its entirety, is the focus of a holistic approach to data security. A critical first step in any data-driven security review is to identify all the points and places where sensitive data is processed, transmitted and stored. The plan should address such issues as data retention and disposal, user access, encryption and auditing. One must take into consideration that business needs will often trump security requirement, and an effective security plan must take all of the stake-holders needs into account or it will fail.

People will always find a way to thwart security measures they don't understand or have a negative impact on their productivity. For each specific POS system significant amount of data should be collected, synthesized, and analyzed in order to draw specific conclusions beyond those presented in this article.

The process should begin with the collection of all available design and architectural artifacts – diagrams, architecture documentation, etc. Next, the POS team should facilitate an

architecture review meeting. During this meeting, a typical POS architecture should be described in detail, including various user stories that explain how the POS system is operated under different circumstances.

The next phase should analyze the artifacts and meeting notes in order to synthesize the information and gain a thorough understanding of how the deployed POS will function. This should include a thorough reading of the design and architecture artifacts. Next, the actual risk analysis should be performed, consisting of one or more of the risk analysis touch-point methodology sub-processes: 1) Attack resistance, 2) Ambiguity analysis, and 3) Weakness analysis.

For attack resistance analysis, the primary application components – and third party infrastructure components – must be analyzed for known and published vulnerabilities, patches, etc. Ambiguity analysis should consist of comparing the POS design documentation against discussions from a review kick-off meeting. Lastly, and most significantly, the architecture itself should be analyzed for potential weak points and weak operational modes.

## Typical threats

Any substantive analysis and discussion about an application's risks must include a discussion of the likely threats the application will face during its anticipated deployed life. In the analysis of the POS, the most likely threats that the system may face, for reasons we will describe below, are 1) malicious insiders and 2) technically knowledgeable outsiders motivated by profit. A brief discussion of each, along with the respective rationale, follows below.

## Basic assumptions

Due to the rigorous security design that usually went into a typical POS architecture, the bar is set quite high with regards to the difficulty that an attacker should have in order to compromise the system. Even an opportunistic attacker who manages to break one of the system's infrastructure components should still need to go to great lengths to compromise any of the system's true "crown jewels"—e.g., a Local Security Service unlock key, the actual

POS keystore, or (untokenized) valid credit card data. As a result, it is assumed that a successful adversary should need to possess a significant level of technology expertise.

As a goal any attacker should need to be more than just proficient at numerous technologies that for example could include C, Java, UNIX/Linux, TCP/IP networking, etc. Additionally, the attacker should need to attain a significant understanding of the functional and design aspects of the POS itself. This could be achieved through reverse engineering or analyzing the source code, design documentation, etc.

A reasonable target for this analysis of a five-year life-span of the POS and the difficulties associated with keeping secrets for that long of a time period, it must be assumed that a sufficiently motivated attacker will be able to acquire (or hire) the technology expertise as well as the application-specific knowledge in order to attempt an attack.

Phishing attacks on the Internet are increasing at an unprecedented rate, clearly indicating a dedicated and highly resourced profit-motivated adversary exists. It would be naïve to think that such an attacker should not, at some point, turn his attention to retailers with a significant brand "footprint" around the world.

## Common insider threats

There are likely to be one primary category of insider threat to the POS: retail employees. They may either be enlisted by an outsider(s) or may enlist the help of an outsider in order to attack the POS. Their motivations are likely to be either profit or to cause harm to the retailer by way of a direct denial of revenue and/or tarnishing the retailer's brand with bad publicity that would almost inevitably be the result of a successful compromise.

In any of the above scenarios, the insider has learned how the POS system functions to a level significant enough to attempt an attack. Traditionally, insider threats are the most difficult to prevent and detect. Further, it is likely that no technology solution will be adequate to safeguard against every possible attack scenario.

However, other industries (notably the financial services industry) have handled insider threats for centuries. In situations where known technology weaknesses are recognized, the financial services industry typically compensates by instituting procedural “checks and balances” to greatly reduce the likelihood of successful attacks.

In most cases, these checks and balances come in the form of separation of duties and

multiple points of possible failure, resulting in no single employee, with the ability to easily compromise the entire system. Instead, a conspiracy would need to exist, which is deemed to be much less likely. That same methodology of separation of duties is leveraged significantly in the recommendations made in this article in circumstances where weak points exist in a typical POS architecture out of necessity.

## IN SITUATIONS WHERE KNOWN TECHNOLOGY WEAKNESSES ARE RECOGNIZED, THE FINANCIAL SERVICES INDUSTRY TYPICALLY COMPENSATES BY INSTITUTING PROCEDURAL “CHECKS AND BALANCES” TO GREATLY REDUCE THE LIKELIHOOD OF SUCCESSFUL ATTACKS.

### Common outsider threats

A second category of threat that must not be neglected is outsiders. Although their motivation is far more likely to be profit rather than to harm the retailer's reputation, it is important to consider them in the analysis. At least two feasible scenarios exist that could provide an outsider with a vector for launching an attack on the POS. Both scenarios involve poorly configured retail store site networks. In the first scenario, a retail site network is misconfigured such that it is directly accessible to the external Internet at large. In this scenario, an opportunistic attacker may accidentally (or otherwise) find the retail network and begin an attack.

The second scenario would involve a misconfigured site network that inadvertently allows any ‘guest’ data traffic to traverse the same network that the business systems, including the Local Security Service itself, resides on. In both cases, a successful attack on the POS itself should need to include a significant additional effort to explore, analyze, and learn the operation of the POS. Such an attack may well take months or more, but considering the five-year lifespan of the POS, it should be wise to treat it as possible, however unlikely.

### Other threat considerations

Although we consider the above threats to be the most likely, they are in no way the only

ones that exist. Similarly, other motivations for attacking the POS may also exist. The Internet has seen an enormous amount of “joy riding” attacks over the years that seem to be motivated by little more than intellectual curiosity and bravado. The largest risk of successful attacks by these miscreants is denial of service and other forms of general havoc. Certainly, not something to be ignored, but the business impact to retail is not likely to be anywhere as significant as in either of the above scenarios.

### A retail system architecture

This article is using illustrating examples based on a retail system with a Local Security Service performing encryption of credit card data at the retail store level. The encrypted data is decrypted by a Central Security Service. Security administration and key management is performed by a Central Administration Service.

In the case where a store and forward approach is used between the store locations and the central system, a few of the potential scenarios that are reviewed below can be avoided. These include a major WAN outage.

In a typical Local Security Service deployment, other (non-Local Security Service) components are housed on the same equipment that the Local Security Service resides on.

This may also include an archive of credit card (tokens if used) in the POS environment. Although data is encrypted and believed to be quite safe from inadvertent disclosure, other system failures (e.g., disclosure of the encryption key) could expose the archived data to an attacker. The potential business impact to the retail organization in such a compromise should be regarded as high.

The most effective means of minimizing this risk is to separate the Encryption Key Service from the other components residing on the same computer hardware, minimize the volume of sensitive data, stored locally and if possible provide significant physical protection of hardware containing highly sensitive data. Many other industries commonly collect their most sensitive data and in data centers with substantial physical security.

## How to render data unreadable

There are three radically different ways to render data unreadable: 1) two-way cryptography with associated key management processes, 2) one-way transformations including truncation and one-way cryptographic hash functions and lastly 3) index tokens and pads. Two-way encryption of sensitive data is one of the most effective means of preventing information disclosure and the resulting potential for fraud. Cryptographic technology is mature and well proven, and there is simply no excuse for not encrypting sensitive data.

The choice of encryption scheme and topology of the encryption solution is critical in deploying a secure, effective and reasonable control. The single largest failure in deploying encryption is attempting to create an ad-hoc cryptographic implementation. Hash algorithms are one-way functions that turn a message into a fingerprint, usually several dozen bytes long binary string to avoid collisions.

Truncation will discard part of the field. These approaches can be used to securing data fields in situations where you do not need the data to do business and you never need the original data back again, but unfortunately a hash will be non-transparent to applications and database schemas since it will require several dozen bytes long binary data type string (longer than the 20 bytes for the broken

SHA-1 or two-way symmetric encryption). An attacker can easily build a (rainbow) table to expose the relation between hash values and real credit card numbers if the solution is not based on HMAC and a rigorous key management system. Salting can also be used if data is not needed for analytics.

An HMAC, is a type of message authentication code (MAC) calculated using a specific algorithm involving a cryptographic hash function in combination with a secret key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. Any iterative cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA-1 accordingly. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, on the size and quality of the key and the size of the hash output length in bits.

An attractive solution to this problem can be tokenization that is the act of replacing the original data field with reference or pointer to the actual data field. Tokenization enables you to store a reference pointer anywhere within your network or database systems and can be used to reduce the cost of securing data fields but will require a central service to assign permanent (persistent) token values. Tokenization by a local service can be used to assign a non-permanent token value at multiple end points early in the data flow. A tokenization system must always be supported by a rigorous encryption system based on separation of duties, secure audit, random key generation and protection of keys and credentials.

## How to choose cryptographic algorithms

The encryption algorithms used in the POS architecture should be chosen carefully and be widely accepted, subjected to extensive peer analysis and scrutiny. Such analysis is considered the norm in the cryptographic community. A weakness in the cryptographic algorithm could result in a complete compromise of the POS system. Thus, the potential business impact to retail would be extreme, and could result in failure of both of the POS's primary business objectives.

Cryptographic failure would have such a significant impact, that it is strongly recommended that a rigorous review of the selected algorithms in use be conducted. It is generally considered a best business practice to use a published cryptographic algorithm for protecting sensitive information. Accepted algorithms typically include those specified by the National Institute of Standards and Technology (NIST) as being Federal Information Processing Standards (FIPS).

## Protection of cryptographic keys

It is essential that each Local Security Service (as well as Central Security Services) retain a copy of the encryption key while in an operational (unlocked) state. This is a necessity of its business mission. At the same time, however, this “crown jewel” presents a security exposure of the POS system. An attacker with access to a Local Security Service could potentially peruse the system’s processes and memory to acquire the key and decrypt data. The likelihood of this sort of attack succeeding is quite low, but must be it to be successful,

the impact could be very high. Take every reasonable precaution to protect the key while the Local Security Service is operational.

## Combine software cryptography and specialized cryptographic chipsets

Encryption keys should be protected when stored in memory or in databases, and during transport between systems and system processes. This can be achieved by using a well balanced combination of software cryptography and specialized cryptographic chipsets (known as Hardware Security Module) can provide a selective added level of protection, and help to balance security, cost, and performance needs. Certain encryption keys and fields in a database require a stronger level of encryption, and a higher level of protection for associated encryption keys. Encryption keys and security metadata should continuously be encrypted and, have their integrity validated, even when communicated between processes, stored or cached in memory. Security data should remain ciphered until needed for use by crypto-services routines.

## ENCRYPTION KEYS AND SECURITY METADATA SHOULD CONTINUOUSLY BE ENCRYPTED AND, HAVE THEIR INTEGRITY VALIDATED, EVEN WHEN COMMUNICATED BETWEEN PROCESSES, STORED OR CACHED IN MEMORY.

### Some keys must be available in memory

Different types of keys need to be available in memory. With software based crypto the data encryption keys must be available in memory and with HSM based encryption the access keys to the HSM must be available in memory. It may not be feasible to use a primary and a secondary HSM in each store location. A solution based on distributed software and an optional HSM is a feasible approach in many environments since each POS must also be able to operate even if the connection to the HSM in the store is down.

Memory attacks may be theoretical, but cryptographic keys, unlike most other data in a computer memory, are random. Looking through memory structures for random data is very likely to reveal key material. Well made encryption solutions go to great efforts to protect keys even in memory. Protection meas-

ures to consider should include memory compartmentalization. Generate a separate ID that does the actual encryption/decryption, and ensure that no other process or system ID can access its memory.

Ensure that the encryption/decryption process and its memory does not get swapped out to a virtual memory swap/page file, which could leave behind persistent residue that could include the encryption key. Whenever the key is no longer needed, ensure that the memory location/variable where it was stored is thoroughly wiped, so that no memory residue is left behind for an attacker to discover. Consider a centrally monitored host-based intrusion detection system on every Local Security Service to vigilantly watch for attacks on the host itself. The above list of recommendations for encryption key handling is commonly practiced throughout various industries where sensitive data is encrypted.

## Some keys are more sensitive

Key-encryption keys are used to encrypt the key while in memory and the encrypted key is then split into several parts and spread throughout the memory space. Decoy structures may also be created that look like valid key material. Memory holding the key is quickly zeroed as soon as the cryptographic operation is finished. These techniques reduce the risk of memory attacks. Separate encryption can also be used for different data.

These encryption keys can be automatically rotated based on the sensitivity of the protected data. Since web servers, application servers, and databases have no place on a dedicated cryptographic engine, these common attack points are not a threat. A severely constrained attack surface makes it much more difficult to gain the access needed to launch a memory attack. To maintain a high level of security backups contain the encrypted data and only securely encrypted lower level keys. Additional details about implementation of key management will be discussed in a separate article.

## PCI DSS REQUIRES YOU TO USE DUAL CONTROL AND SPLIT KNOWLEDGE AND PROPER KEY MANAGEMENT PRACTICES TO MANAGE YOUR KEYS.

### Dual control, split knowledge and PCI

PCI DSS requires you to use dual control and split knowledge and proper key management practices to manage your keys. Dual control and split knowledge can be expressed as - no one person should have access to any information, device, or function, that allows them to determine the key that is being protected more quickly than through the best attack known for that algorithm. Ideally, this means a brute force search of the entire key space.

The determination of any part of the key must require the collusion between at least two trusted individuals. This requirement can be a challenge in the POS environment and solution approaches will be discussed in a section about the Local Security Service below.

Any feasible method to violate this axiom means that the principles of dual control and split knowledge are not being upheld. This principle is enforced by requiring both dual control, and split knowledge. In other words, at least two people are required to 'reconstruct' the key, and they must each have a physical thing (thereby providing dual control), and some information that is required (thereby providing split knowledge). It is not enough to split a 128 bit key 'in half' with each half, containing the plaintext bits of the original key, one of the two custodians can determine the key by exhausting the other half - which requires only  $2^{64}$  operations, instead of the

$2^{128}$  which is required for the entire key space.

Storing key components on two media and not requiring any further authentication by the users to use these components will not provide the required split knowledge. Storing a key enciphered under another key that can be reconstructed with one or more passphrases, provides split knowledge, but not dual control.

Storing a key on a single media that requires one or more passphrases to access does not meet the requirements of dual control. The dual control and split knowledge is only required to access the plaintext key. The use of a key to encipher or decipher data, or access to a key that is enciphered under another key does not require such control.

### Central help-desk access to keys

At various times during normal POS operations, Central Help-desk support staff and site system administration staff are likely to have access to unlock-keys and encryption-keys. Despite the fact that key management has been carefully thought through to minimize these exposures, opportunities do exist for this support staff to compromise customer data. Further, detecting this sort of insider attack can be extremely difficult, but the impact of a successful attack on the POS could be quite severe.

Best practices in similar data environments generally include most or all of the following measures. Checks of all personnel involved in sensitive operations such as key management. Ideally, support staff that has access to encryption keys should not have access to any sensitive, encrypted data and vice versa. This, however, can be a difficult measure to implement. To the extent feasible, functional duties should be separate within the data center. For example, Central Help-desk personnel who handle Local Security Service unlocking should not also be involved with encryption key management.

The above recommendations are entirely consistent with practices found in numerous other industries where similar access to sensitive customer data is required. The financial services industry, in particular, makes regular use of similar operational practices.

## PKI considerations

A tight integration of PKI and the POS system is possible in advanced POS environments. Rigorous mutual authentication, data encryption, etc., that a PKI enables are considered to be best practice solutions across numerous industries today. Consequently, a failure of the PKI would without a doubt have a devastating effect on the POS. A PKI 'situation', such as the retail organization's CA certificate appearing on a CRL could halt the entire PKI in its tracks. Since the PKI is literally infrastructure of the POS, a PKI failure could have a commensurate affect on the POS, resulting in considerable business impact to the retail organization.

Although the deployment and operation of the retail organization's PKI is outside of the direct scope of the POS project, great care must be taken to ensure that the PKI is operated in compliance with all relevant PKI industry best practices and procedures.

## SSL keys in plaintext

During a POS review, it is common to find SSL private keys left in plaintext on some servers. This could indirectly help an attacker get one step closer to successfully attacking the POS. In particular, the plaintext SSL key could enable an attacker to masquerade as

authorized server in a Security Service conversation. The likelihood of such an attack succeeding is quite low, but could enable an attacker to do anything that the local service is able to do. Consider password protecting the SSL key for the service. Although this can be unfeasible in some operational scenarios, if it doesn't present an undue burden for the retail organization, it should be done.

Password protecting SSL keys is commonly done on production servers throughout various industries. On the other hand, doing so is often not feasible, and thus, it is not uncommon to find plaintext SSL keys in production data centers. It is less common to find plaintext keys on field-deployed servers, however.

## Protecting the Security Services

A computer may sometimes be outside the physical control of its intended users. For example, a server, USB-drive or disk may be stolen rather easily. Therefore, it is prudent to restrict access to the computer's functions, for instance by requiring the entry of a password. It is also prudent to protect the files on the computer by encrypting them, for example under an encryption key derived from the password. The password itself should not be kept in the clear on the computer.

In this way, only parties that know the password can use the computer and read the files, even if they have direct access to the computer's storage devices. The password should be strong enough that an attacker cannot obtain it by guessing, and then decrypt the files. Assume that the user and computer a some secure means of communicating, perhaps because the user has direct, physical access, or can establish a secure network connection. The user may type a password into the server at log-in time and in addition to we add a password supplement that may be 40 bits chosen randomly.

Both will be replaced every time the user picks a new password, and when the computer is re-started, and can establish a secure network connection with the central key management computer. A challenge-response process may be added to avoid replay attacks if a cloned end-point server is attacked by using the manually entered password.

## **Unlocking the Local Security Services**

Each Local Security Service should be locked upon start-up. While locked, all sensitive data is encrypted and presumably safely stored. During the Local Security Service start-up procedure the application is unlocked so that it can get on with its business processing functions. Unlocking can occur through an automated or manual process – the latter is invoked in situations where the retail WAN connectivity is unavailable for some reason.

The security of this process depends on the secrecy of the unlock keys, which are unique to each retail site and should only be used once. Under the automatic unlocking process, the unlock key is discarded after use (and presumably wiped from memory) and then a new unlock key is automatically rotated in via the Security Administration Service, thereby greatly reducing the exposure of the unlock key. The manual unlock process, on the other hand, exposes a valid unlock key to at least two people – a central help-desk support person and a system administrator at the respective retail site (or similar).

Although the key is rotated after use, a maliciously cloned Local Security Service environment could still be unlocked using that unlock key if the cloned system remains off-line. This could enable an attacker to invoke and unlock a cloned Local Security Service in a safe environment and potentially use the data and processes on the Local Security Service to decrypt cached/archived credit card data. The impact of a successful breach of this process could be extreme. Customer data for several years could be compromised, resulting in customer identity theft, retail reputation tarnishing, etc.

This situation is acknowledged in a typical POS architecture and can be addressed by asymmetric keys or compartmentalization of symmetric encryption keys to limit the amount of data that is accessible by each encryption key. Additional details about implementation of solutions based on asymmetric keys and compartmentalization of symmetric crypto will be discussed in a separate article. If this is not implemented, it would be possible for an attacker, through social engineering, to get the

unlock secret from Central Help-desk, and then use this to attack the system.

## **Authentication cannot be done by the POS itself**

Note that this authentication cannot be done by POS itself - it must be an out-of-band mechanism. It is vital that a robust business process complete with adequate checks and balances, be instituted at every retail site that will run a Local Security Service. Additional technologies could be deployed to further protect this vital aspect of the Local Security Service's operation, such as smart cards. A smartcard based identification, authentication, and authorization mechanism should be a significant improvement in protecting the startup and unlock process for each Local Security Service. It is understood, however, that such measures in many cases would not be feasible to deploy at each retail location. As such, a process as mentioned above is even more important to address carefully. In numerous industries, mission critical applications commonly leverage technologies such as smart cards, one time passwords, and others for protecting such vital operating states as unlocking the Local Security Service.

The unlock keys are available in different formats in automatic mode and in response to a request to the Central Helpdesk. The same key is not used in both cases. The whole path in the automatic case must be protected. Since the key may be requested from the Helpdesk, the Helpdesk should not have complete knowledge of a single key for one store and the keys should be different across different stores. Additional details about the implementation of dual control in the automatic unlocking process will be discussed in a separate article.

## **Protecting Web-facing applications**

PCI DSS Requirement 6.5 requires that Web-facing applications be developed in accordance with secure coding guidelines to guard against such attacks. A successful SQL injection attack can have serious consequences. SQL injection attacks can result in the crippling of the payment application or an entire e-commerce site.

Through this avenue of attack, an attacker can break out of the Web server and database realms, gaining complete control over the underlying system. Another serious consequence can be the compromise and theft of data that resides within the payment application infrastructure. SQL injection is a technique used to exploit Web-based applications by using client-supplied data in SQL queries. SQL injection attacks are caused primarily by applications that lack input validation checks. Recently, commercial shopping cart products have been the focus of attack by hackers who seek account information. Automated tools are available in the marketplace to protect applications for susceptibility to an SQL injection attack and should be utilized.

### Logging server

Event logging, for PCI compliancy, forensics, and other purposes, is handled by a syslog server located in the Central Site. Syslog-NG will be used as an example since it is a syslog replacement supporting IPv6 and capable of transferring log messages reliably using TCP. Although Syslog-NG offers numerous operational and availability benefits beyond its predecessor (Syslog), it does little to protect any sensitive data that gets logged. Further, the Syslog-NG server is not integrated into the typical PKI that some POS components may

use. Thus, it represents a potential weak point where an attacker may be able to obtain sensitive POS data, in particular credit card data. One avenue of attack could involve an attacker setting up a rogue syslog-NG server and tricking the Local Security Service into sending its log events to include data.

The impact of a successful Syslog-NG-based attack should be similar to any attack that involves compromising data – quite high. Although this attack is quite unlikely, several steps should be taken to further minimize its likelihood. These should include integrating the Syslog-NG server into the PKI so that the Local Security Service and other components can strongly (mutually) authenticate with it, ensure rigorous host-hardening is done during the configuration of the Syslog-NG server. Also consider encrypting the actual data volume on the Syslog-NG server via an encrypting file system and minimize access to the Syslog-NG data to those staff who have an operational requirement to access it. Sensitive data logging in other industries, such as the financial services industry, is commonly strongly protected using methods such as those described above. Data centers containing such information are also commonly deployed with extensive physical security controls, rigorous access controls, compartmentalization of data, and so forth.

## COMMERCIAL SHOPPING CART PRODUCTS HAVE BEEN ATTACKED BY MALICIOUS HACKERS WHO SEEK ACCOUNT INFORMATION.

### Additional operational issues

In analyzing a typical POS architecture and operation, in the case a store and forward topology is not used, a few potential denial of service scenarios must be theorized. These include a major WAN outage that forces sites to use the Central Help-desk helpdesk for unlocking their Local Security Services and a long-term WAN outage and subsequent reconnection that results in a cache flood of the Central Site (including Syslog-NG, Central Security Services, and Security Administration Server systems). The common factor in most of the theorized scenarios may include widespread Local Security Service connections

into the Central Site that result in overwhelming the systems within the Central Site. The direct impact of such an attack would be to halt POS operations at the Central Site. It is possible that the sites continue running in a disconnected mode, but whenever they try to reconnect to the Central Site, another denial of service is the result. Such DoS reverberations could even recur if the dynamics of the entire system are not carefully designed. Ensure that the various POS components can safely adapt to a wide range of LAN/WAN connectivity states. Make sure the Central Site components themselves are able to throttle incoming connections after long term outage situations so that they do not become overwhelmed.

## Degraded WAN operation

During analysis of the POS system as a whole, the team theorized some modes of operation that may result in problems. For example, if a WAN or Central Site outage requires the secondary (Security Administration Server recovery) system to go into production, and the network connectivity to/from the secondary site is not as robust as that for the Central Site itself, there could well be situations where Local Security Service to Security Administration Server communications are substantially degraded. This may in turn result in a long-term caching of data and such, as

well as a subsequent “data storm” in the Central Site when normal communications resume.

The impact of this sort of situation could vary, but is not likely to be severe. A likely worst case scenario would include denial of service disruptions at the Central Site upon resuming normal business operations. Consider and plan for a wide range of LAN/WAN connectivity for the deployed Local Security Service servers such that they are least likely to flood the Central Site after prolonged outages or significantly degraded communications periods.

## THE IMPACT OF ANY PARTICULAR COMPONENT VULNERABILITY DEPENDS ON THE NATURE OF EACH VULNERABILITY, BUT IN THE AGGREGATE, THE POTENTIAL IMPACT TO THE RETAIL ORGANIZATION SHOULD BE PRESUMED TO BE HIGH.

### Infrastructure operational environment

The POS may include numerous off the shelf components and technologies (e.g., WebSphere, Struts, any (Java) package and library for managing projects and dependencies, Linux, UNIX). Since a system is only as secure as its weakest link, weaknesses in any of these components could provide an attacker with a vector to launch an attack on the POS itself. During this type of review, a cursory review of known and published vulnerabilities should be performed on several of the above components.

The actual impact of any particular component vulnerability depends on the nature of each vulnerability, but in the aggregate, the potential impact to the retail organization should be presumed to be high. Robust operational processes and procedures should be instituted across all POS components, including every Local Security Service operating at retail sites. These should include a suite of best practices in the areas of protection, detection, and response. Specific attention should be paid to network and operating system/platform configuration management.

### Protecting administrative functions

A typical POS architecture may include a (read-only) monitor in the form of a simple

web app interface for site system administrators to be able to see the operational status of their Local Security Services. This function may be intended to be used by local site personnel only.

Although (presumably) no sensitive data should be available to an outsider through this interface, it is a good idea to protect it from outside access as described below. The impact of an outsider accessing the POS monitor GUI should not be quite low, but could result in embarrassment to the retail organization should it be publicly disclosed. Minimize the likelihood and impact of this weakness by enable the monitor GUI on only the “localhost” (loopback) network interface; alternatively, if it is required to be accessed from a central helpdesk site LAN, enable access only via a single (or small set of) approved IP address(es) and use a username/password for accessing the monitor GUI.

### Administration and recovery

Although the POS may itself be essentially stateless, at a micro level, it must contain state data such as encryption keys, unlock keys for each retail site, update configuration data, and so forth. As such, the BC/DR systems must be current with the operational state of the primary production servers or else a state skew could occur.

Although the impact of such a failure could be quite high, its likelihood of occurring may be considered to be low. Ensure that all BC/DR planning and processes include state updating of the production POS servers on an on-going basis. Further, these systems should go through periodic live testing to help keep them in as reliable an operational state as possible. Mission critical systems throughout numerous other industries are regularly expected to have robust and mature business continuity including secondary data centers and such.

### Updating the Local Security Service

Another Local Security Service mode of operation during which it potentially exposes a weakness is during the update process. This process, can be orchestrated via a third party components, involves checking versions of all system components (e.g., jar files) and, if necessary, retrieving updates from the Central Security Services. Although all such components are digitally signed to aid in detecting any tampering, spoofing, etc., the security of the entire update process depends on Any (Java) package and library for managing projects and dependencies.

This (sometimes XML) formatted file contains all of the pointers to the respective system components, and is stored locally on the Local Security Service during start-up. One mode of attack could be to maliciously alter the .xml file such that it loads maliciously extended Java class files instead of the legitimate POS files. As with the Local Security Service unlock functionality, a compromise of the update function could result in a complete compromise of the Local Security Service and all its sensitive data. Thus, the overall business impact to the retail organization could be extreme. Both unlock and update functions are necessary features for such a widely distributed system, thus omitting these features is not be a feasible solution.

Omitting the update function would result in enormous configuration management overhead to the retail organization. The result should without a doubt be an untenable operational posture. Thus, the risks that these functions present should be accepted as a cost of doing business. In addition similarly to

the unlock function, the update function should include business processes that maximize separation of duties, checks and balances, etc. Although no single mechanism can achieve perfection, some security mechanisms around the update function should include rigorous access control including object files, environment variables, IDS signatures that specifically look for attempts (successful or otherwise) to tamper with files and a fail-safe process if compromise attempts are detected.

### Passwords issues

Passwords are the most common form of user authentication in computer systems, but they represent a weak link of a protection system. An administrative or master password should be particularly complex. Below is one easy way to solve the general password protection issue by using an encryption solution that can be application transparent and resistant to 'multiple attack vectors' protecting the access to API, to databases and to SSL communication sessions.

An encryption server box should be hardened and the session should be authenticated (with a password or multi-factor authentication) and encrypted (SSL or similar). Lock down the application storage of the passwords to the log-ins for the database, communication and the encryption server. A mature transparent file system encryption product on the application server platform can lock down the storage of the password and may also delegate a transparent authorization to the application.

### Increase the security of passwords

Password strengthening is a compatible extension of traditional password mechanisms. It increases the security of passwords, without requiring users to memorize or write down long strings. Password strengthening does not assume any extra hardware, and does not introduce any of the vulnerabilities that come with extra hardware. These characteristics makes password strengthening easy to adopt, and appealing in practical applications. The method does not require users to memorize or to write down long passwords, and does not rely on smart-cards or other auxiliary hardware.

The main cost of this method is lengthening the process of checking a password. Each password hash is associated to a small, usually random value called salt. The salt does not need to be kept secret, and it is used together with the password to generate the password hash. While the use of salted pass-

words does not increase the task for recovering a particular password, a salt of sufficient length should preclude pre-computed, offline dictionary attacks, as it becomes impractical to compute a large table of hashes corresponding to possible passwords and salt values in advance.

## ONE OF THE WEAKEST ASPECTS OF PASSWORD BASED AUTHENTICATION IS THE LOW ENTROPY OF COMMONLY CHOSEN PASSWORDS.

### Issues with weak passwords

One of the weakest aspects of password based authentication is the low entropy of commonly chosen passwords.

The main attacks for recovering clear text passwords from hash values consist of computation of all possible passwords up to a certain number of characters (exhaustive search attack), or perhaps a list of typically chosen passwords (dictionary attack). The computation is usually performed offline and the attacker simply compares the values on the password table with the pre-computed list.

Systems should therefore enforce password complexity rules, such as minimum length, requiring letters to be chosen from different sets of characters (e.g. lower-case, upper-case, digits, and special characters), etc.

An appropriate password length depends on the amount of resources available to the attacker that an organization wishes to defend against. Assuming an attacker has access to optimized DES-cracking hardware an organization may need to enforce 12-character passwords and a password expiration duration of 60 days to mitigate a brute-force attack against the password hash. A password generator is able to generate a strong password policy of a random sequence of numbers, lower-case letters, and upper-case letters.

These passwords are random and therefore very difficult for a hacker to guess. A password generator thwarts any key-logging attempts by automatically copying the generated password into the password field. Since your password is never typed and never copied to the clip-

board, a key getLogger has no chance to capture your information.

### Slowing down an attacker

A slow one-way algorithm will not noticeably increase the cost of one operation (e.g. for the legitimate user when logging in), but it substantially increases the task of mounting an exhaustive search attack. A common approach is to iterate the original one-way function many times. Some systems one-way function encrypts a known string 25 times with DES using a key derived from the user's password (another feature is that the salt value actually modifies the DES algorithm itself, making it harder for an attacker to use dedicated DES hardware to mount an attack. Given the current computer resources available, a minimum of 5000 iterations for constructing the hash algorithm, is recommended.

### Other Controls

Compensating controls may be considered when an organization cannot meet a technical specification of a requirement, but has sufficiently mitigated the associated risk. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Organizations should be aware that a particular compensating control will not be effective in all environments. Each compensating control must be thoroughly evaluated after implementation to ensure effectiveness. For organizations unable to render sensitive data unreadable (for example, by encryption) due to technical constraints or business limitations, compensating controls may be considered.

The basic conclusion from this analysis is that a combination of application firewalls, in addition to the use of data access monitoring and logging may, if effectively applied, provide reasonable equivalency for the use of data encryption across the enterprise. Such a combination of controls has weak spots however, mainly when it comes to preventing damage from careless behavior of employees or weak procedures in development and separation of duties.

Only organizations that have undertaken a risk analysis and have legitimate technological or documented business constraints should consider the use of compensating controls to achieve protection. Organizations that consider compensating controls for rendering sensitive data unreadable must understand

the risk to the data posed by maintaining readable data.

Generally, the controls must provide additional protection to mitigate any additional risk posed by maintaining readable data. Compensating controls should consist of a comprehensive set of controls covering additional segmentation/abstraction (for example, at the network-layer), providing ability to restrict access to data or databases based on IP address/Mac address, application/service, user accounts/groups, data type (packet filtering), restrict logical access to the database, control logical access to the database (providing separation of duties) and prevent/detect common application or database attacks (for example, SQL injection).

## A COMBINATION OF APPLICATION FIREWALLS, IN ADDITION TO THE USE OF DATA ACCESS MONITORING AND LOGGING MAY, IF EFFECTIVELY APPLIED, PROVIDE REASONABLE EQUIVALENCY FOR THE USE OF DATA ENCRYPTION ACROSS THE ENTERPRISE.

### Multiple network segments

Multiple network segments based in different geographic locations may require costly administration. The environment can be difficult to administer and sometimes people have to break "other" rules to administer effectively.

Many security/auditing tasks have to be duplicated for every environment where database resides. Database only network segment(s) have advantages including centralized entry point to manage and monitor all activity, administrative tools can effectively manage security/auditing tasks, database environments are brought together, in a reduced number of environments, in "back office", and separate database from application further reducing access to environments.

Adequate network segmentation, which isolates systems that store, process, or transmit sensitive data from those that do not, may reduce the vulnerability of the data environment. Network components include firewalls, switches, routers, wireless access points, network appliances, and other security appliances.

Server types include but web, database, authentication, mail, proxy, and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (Internet) applications.

### Data usage control

An advanced POS architecture may include a "Data Usage Controller" module that acts as a sort of intrusion detection system. Its purpose is to protect the data by looking for statistical anomalies in how a particular site accesses the data, and reporting any significant events to the Security Administration Server.

Until the statistical anomaly detection algorithm has proven itself in this way, it is likely to generate a significant number of both false positives and false negatives. This is largely unavoidable.

The direct security impact of excessive false positives from the Data Usage Controller should be small.

Indeed, a worst case scenario would be if an attacker realizes that the Data Usage Controller is prone to false positives, in which case he attempts to flood the Data Usage Controller monitoring facility with false positives in order to “smoke screen” a real attack elsewhere.

This attack is not very likely, but should not be ignored. If possible the Data Usage Controller algorithm should be tested thoroughly during the early deployment phases of the POS system.

Deliberately flooding it across numerous Local Security Services and observing the behavior at the Central Site, for example, should be part of the deployment process. As with any IDS-like system, its thresholds will inevitably require close attention whenever a new Local Security Service is deployed.

## Conclusion

Common architectural weaknesses that can lead to data compromise were identified and approaches beyond PCI to safeguard information in a retail environment were discussed. Careful balance between business goals and security reduce the risk of a compromise that can threaten the retail organization’s brand reputation and business operations.

Weaknesses discussed here can prove to be effective at prioritizing testing attention and effort. In other words, the testing, design review, code review, penetration testing, and other processes should be prioritized in order to make the most effective use of the available development resources.

Hash algorithms or truncation can be used to secure data fields in situations where the data is not needed to do business and the original value is not required, but unfortunately a secure hash will be non-transparent to applications and database schemas since it will require a longer binary data type string than symmetric encryption require. An attacker can easily build a table to expose the relation between hash values and real credit card numbers if the solution is not based on a rigorous key management system or scattered by using salting.

An attractive solution to this transparency problem can be tokenization supported by a rigorous encryption system based on separation of duties, secure audit, random key generation and protection of keys and credentials.

The environmental footprint is part of the decision process and elements such as power utilization, heat generation, physical rack-space, and upgrade and disposal strategies are all part of the green equation.

Mature security solutions address the green security challenge by delivering software solutions that operate on existing computing infrastructure, typically on the same server as the application or database being secured. The appropriate level of encryption key protection can be achieved by using a well-balanced combination of software cryptography and selective use of small footprint standard commodity type Hardware Security Modules.

This approach can provide the needed level of protection while balancing security, cost, and operational needs.

Ulf T. Mattsson is the CTO of Protegrity. Ulf created the initial architecture of Protegrity’s database security technology, for which the company owns several key patents. His extensive IT and security industry experience includes 20 years with IBM as a manager of software development and a consulting resource to IBM’s Research and Development organization, in the areas of IT Architecture and IT Security. Ulf holds a degree in electrical engineering from Polhem University, a degree in Finance from University of Stockholm and a master’s degree in physics from Chalmers University of Technology.

[www.net-security.org](http://www.net-security.org)

Get up-to-date security information now.



## Interview with Mikko H. Hypponen, Chief Research Officer for F-Secure

By Mirko Zorz

**Mikko Hypponen is the Chief Research Officer for F-Secure. He led the team that took down the world-wide network used by the Sobig.F worm in 2003, was the first to warn the world about the Sasser outbreak in 2004 and the first to stop the Zotob worm in 2005. Mr. Hypponen has addressed the most important security-related conferences worldwide. He is also an inventor for several patents, including US patent 6,577,920 "Computer virus screening". He was selected among the 50 most important people on the web in March 2007 by the PC World magazine.**

### What was the most dangerous piece of malware in 2007? Why?

It was Storm.

On Friday, January 19th 2007, e-mail messages with subject lines based on actual news began to circulate. The subject line of "230 dead as storm batters Europe" coined the name Storm. There were in fact dozens of real deaths related to European storms during that time.

Using sensationalized versions of real headlines as a template proved to be a very clever bit of social engineering and was initially very successful. However, during H1 the headline technique's success declined as it was repeated too often. So the gang behind Storm adjusted their procedures. During the second half of 2007 (H2), they have continuously up-

dated their social engineering tactics. Targeting the U.S. — they have used holidays such as Labor Day and seasonal events such as the beginning of the National Football League (NFL) season. Targeting others — the gang keeps up-to-date with popular trends and sites. One of their tricks was the promise of seeing "yourself" in a supposed YouTube video in a message pointing to a fake YouTube site.

The gang has also altered Storm's infection vector as detection of Storm increased and e-mail attachments were blocked. Instead of attaching the malware to the e-mail messages as before, they spammed messages with links to malicious Web pages. When the detection of the Web pages increased, they cleaned up the pages and instead linked to the malware from the page.

So the vector evolution moved from e-mail attachments to Web pages pushing files to Web pages linking to files. (And those files are modified on the fly...) The evolution continues and adjusts as needed.

It is interesting to note that we have seen IFrames (inline frames) used by some Storm sites offering 16 versions of Storm to U.S. based IP addresses rather than the 9 that were offered to IP addresses outside the United States. Storm is produced in Europe but the social engineering has a definite U.S. agenda. They appear to have agents on both sides of the Atlantic.

The computers responsible for sending Storm spam and for the hosting of Storm's Web pages are they themselves part of the Storm botnet. And that botnet is rather unique as it utilizes peer-to-peer (P2P) protocols. Traditional botnets use a centralized approach. If the server is located and taken out of service, then the botnet's head is decapitated. Storm is a collective with no central point to shut down. There's no central command-and-control point to kill.

September's Malicious Software Removal Tool, part of Microsoft's monthly updates, made a dent in the size of the Storm botnet — the tool removed a good number of Storm's bots during the update process — but the botnet remains and the dent hasn't muted its overall strength.

Another special feature of the Storm botnet is that it protects itself. Repeat requests from a single source of one particular machine will result in many members of the botnet retaliating with a Distributed Denial of Service (DDoS) attack. Researchers must use caution during investigations or the botnet gets aggressive.

October brought evidence of Storm variations using unique security keys. The unique keys will allow the botnet to be segmented allowing "space for rent". It looks as if the Storm gang is preparing to sell access to their botnet - and this finally started to happen for real in January 2008 when we saw first phishing run done with sites hosted in Storm botnet.

## **The organized enemy is already affecting the antivirus industry. I know analysts who have been threatened.**

**What has been the economic impact of malware for organizations during the past year? Is the overall situation improving?**

I'd love to see the situation getting better... but I'm afraid it's getting worse.

The actual amount of money being made by criminal online gangs seems to be impossible to measure. But in any case we're talking about hundreds of millions of Euros annually.

**Will the rising skill level of malicious uses and their grouping into criminal organizations ultimately have an impact on the anti-malware industry?**

The organized enemy is already affecting the antivirus industry. I know analysts who have been threatened. People are laying low. Using unlisted addresses and so on.

**Microsoft claims that Windows Vista is the most secure OS they've produced so far. How does it stack up in the real world to the assault of assorted malware varieties?**

This is incorrect. Operating system of XBOX is certainly more secure than Vista.

Vista is faring pretty well so far. Majority of the attacks are still targeting XP as it has a much larger user-base and apparently it's generating enough revenue for the attackers. Vista attacks will intensify as XP starts to slowly fade away.

**5) With Linux and Mac OS X gaining market share among end users, many are speculating that this will lead to an increased influx of malware for those operating systems. What's your take on that?**

The year 2007 was a banner one for Apple —

their hardware is more popular than ever. More Apple hardware equals a greater installed base of Apple software.

DNSChanger trojans have started targeting Mac OSX. Social engineering is used to persuade users to enter their admin password for the install — not a big problem for clever social engineering. Getting a Mac user to type his password for an easily installed "video codec" isn't a significant challenge to overcome, at least it hasn't been a challenge for password protected Windows malware. And we're seeing a growing number of Mac DNSChanger variants. The previous lack of Mac OSX malware could be a distinct disadvantage for its users. Social engineering can short-circuit a false sense of security.

Apple Mac's market share is now significant enough for the Zlob parasites to target, as malware gangs don't make an effort to develop something without the promise of a profitable return.

Apple's Safari browser for Windows likely contributed to this development. Released in mid-June, researchers seized upon the Safari for Windows Beta and many security flaws were

discovered. Many of those flaws were mirrored in the Mac version of Safari.

Web sites pushing DNSChangers determine the OS and the browser version being used by the visitor. The appropriate version of the malware is dynamically provided — visit with a Mac and you'll get Mac malware.

Also, the Apple iPhone is out there. It uses a version of Mac OSX, which is in turn based on Unix. If you understand Unix security, then you can relatively easily "port" your knowledge and understanding to the iPhone.

The iPhone also comes installed with the Safari browser and provides full rights to it. With the portability of understanding and the known Safari flaws mentioned above, coupled with the excellent hardware design, focus greatly intensified on the iPhone. Including the fact that the iPhone is a "locked" device and you have a perfect combination of factors leading to iPhone exploit research.

Exploits for the iPhone are sought as a means to unlock the device. But in revealing those exploits there's a security consequence. The first iPhone Trojan was found in January 2008.

## **Drive-by-downloads from malicious web pages are going to become a larger problem than traditional e-mail malware.**

**Is there a universal solution for fending off blended threats? What kind of assaults should we be on the lookout for?**

Targeted attacks are only going to get worse.

Drive-by-downloads from malicious web pages are going to become a larger problem than traditional e-mail malware.

**There's a variety of anti-malware tools on the market and everyone claims they are the very best. In your opinion, what should the end user base his purchasing decision on? What are the most important features that define such a critical piece of software?**

Look for a tool that works silently in the background and gets automatic updates several

times a day. Also make sure the products has HIPS-like features to protect you against unknown malware without relying on signatures or heuristics. A good rootkit detector would be an important feature as well.

**Although there have been many predictions about malicious code attacking mobile devices in the past, it hasn't happened yet on a large scale. Is there a real possibility that we will see an outbreak of malware on platforms such as Symbian and Windows Mobile in the near future?**

We've been working extensively with mobile phone vendors and operators to prevent such attacks - so far so good. Right now the biggest problem seems to be mobile spyware that can be used to monitor your activities and to eavesdrop your discussions.



## Interview with Richard Jacobs, Technical Director of Sophos

By Mirko Zorz



**Richard Jacobs is a board member and Technical Director of Sophos since 2000. He has 15 years' commercial experience in software development and has contributed to the success of Sophos since 1989. Before joining the board in 2000, Richard was president of Sophos's American subsidiary for four years. Richard received a degree in Electronic Engineering from Birmingham University.**

### **What was the most dangerous piece of malware in 2007? Why?**

The Storm worm, also known as Dref or Dorf, was 2007's most disruptive threat - this malware family had countless reiterations, a few of which are listed below.

The people behind the Storm attack have used a tried-and-tested formula of social engineering to get people to open their widely spammed-out emails and click on malicious links. By using topical news stories, or the lure of an electronic greeting card, videos and fear tactics, the cybercriminals seem to find a never-ending stream of unsuspecting users prepared to click without thinking twice.

The campaign started with a Happy New Year message first seen on 30 December 2006. It hit email systems hard in the last two days of 2006, posing as an electronic greeting celebrating the new year. With subject lines such as "Happy New Year!", "Fun Filled New Year!"

and "Happy 2007!", the worm spread via email with a malicious executable attachment.

Late in January 2007, the Storm worm turned to love in a major new attack. Attached to the emails were files called postcard.exe or greetingcard.exe, taking advantage of the upcoming Valentine's holiday.

Throughout 2007 Storm was aggressive about taking advantage of public holidays. For example, a campaign that posed as a 4th July greeting card, was heavily spammed out. Clicking on the link took surfers to a compromised zombie computer hosting the Troj/JSEcard-A Trojan horse.

In August of last year, Storm used a wave of malicious emails which posed as links to YouTube videos. The emails encouraged recipients to click on a link to download an online movie. Another August variant of Storm used the promise of music videos of popstars to get recipients to visit a hacked web page.

The infected page contained a malicious script and a Trojan horse designed to turn the user's PC into a compromised zombie.

Late last year saw cybercriminals change tactics, as they started to use fear to get people to click on an attachment. The emails claimed that the sender was a private detective listening to the recipient's phone calls. The 'detective' claimed that he would reveal who had paid for the surveillance at a later date, but for the meantime the user should listen to what it purported was an attached recording of a recent phone call. This attachment was in fact a

malicious executable program, designed to install malware, along with a piece of scareware to trick people into buying bogus security software for their computer.

But at the very end of the year, the authors of the Storm worm returned to their old favorite – taking advantage of the seasonal spirit. First, in early December, new versions of the Storm worm were spammed out, using the lure of Santa Claus's wife doing a striptease. These were followed at the end of the month with a return to Happy New Year e-cards which contained links to websites hosting malware.

## THE MALWARE THREAT HAS EVOLVED OVER THE LAST 20 YEARS, AND WILL CONTINUE TO DO SO

### **What has been the economic impact of malware for organizations during the past year? Is the overall situation improving?**

Organizations are worried about being infected and the cost of recovery. The overall numbers and range of types of threats continues to increase. A major change in 2007 has been the increasing concern about data loss.

Countless news stories, from TJ Maxx losing details of around 90 million customers over a two year period, and the November debacle of HMRC losing sensitive data of 25 million families in Britain, goes to show that even large organizations are at risk.

In a Sophos poll, 70 percent of people were worried about losing sensitive data via email. In another poll, more than 60 percent were worried that their employees are a concern when it comes to data theft.

### **Will the rising skill level of malicious uses and their grouping into criminal organizations ultimately have an impact on the anti-malware industry?**

The malware threat has evolved over the last 20 years, and will continue to do so. The same is true of threat protection – over the last few years there has been a fragmented approach to a fragmented threat.

Sophos recognized early that the various threats that we see today are all elements of the same overall threat.

The industry's solution has been to follow a comprehensive integration route, involving integrating analysis and protection against viruses, worms, spam and Trojans, deploying the appropriate combination of techniques in the appropriate mixture to contain threats without impeding productivity. However, it is inevitable that those with malicious intent will evolve their techniques as well.

### **Microsoft claims that Windows Vista is the most secure OS they've produced so far. How does it stack up in the real world to the assault of assorted malware varieties?**

Microsoft talked a lot about security when Vista was released. New features such as Patchguard and User Account Control help to improve security and Internet Explorer 7 similarly contains enhanced capabilities.

However, Microsoft's problem remains that it is the biggest target, and attackers will continue to find and exploit vulnerabilities.

Many of those vulnerabilities are not in the OS, but in the users. Most malware has always relied on social engineering to get the user to let it run - Vista doesn't change that. Any general purpose OS will always be vulnerable, particularly if users are allowed to install and run any application they choose.

**With Linux and Mac OS X gaining market share among end users, many are speculating that this will lead to an increased influx of malware for those operating systems. What's your take on that?**

Linux and Mac OS X are not fundamentally less vulnerable to malware than Windows, and it is right to suggest that they haven't been targeted as much because of their lower market share. So, as that share increases, their exposure increases and I anticipate that the threat will increase. In practice this is likely to be marginal, as Windows will continue to dominate the market for the foreseeable future.

However, it is still necessary to protect non-Windows PCs in an enterprise environment, to ensure that Windows malware does not get left on those machines, re-infecting at will. In addition, we may also see an increased targeting of these platforms as Windows security continues to improve - attackers will always go for the easiest target.

An additional trend is likely to be for OS-independent threats. Script/HTML based threats will run on any platform, and the vulnerability remains the same... the user!

**The CSO is becoming increasingly aware of the dangers posed by careless users that introduce malware into the network by using portable storage devices. What can be done in order to mitigate this kind of risk?**

The user is a critical vulnerability on a number of fronts, however portable storage devices shouldn't be a problem for malware introduction. The key here is that perimeter-based protection is not a viable solution. As our networks become ever more open and consumer technologies (iTunes, cameras, PDAs, smartphones, USB storage, IM etc) are increasingly used at work, it is critical that malware protection is tackled on the PC itself. Centrally managed endpoint security will handle threats, whether they're coming from email, web downloads, CDs, or USB keys. In many organisations it may not be possible to mandate exactly which security software is in place, particularly for contractors and partners connecting to the network, but it's still possible to mandate and verify that a security product must be installed and up-to-date.

The threat around portable storage devices relates to disclosure of the data stored on them. That's where we should be focussed, when discussing USB keys and iPhones.

## LINUX AND MAC OS X ARE NOT FUNDAMENTALLY LESS VULNERABLE TO MALWARE THAN WINDOWS

**Is there a universal solution for fending off blended threats? What kind of assaults should we be on the lookout for?**

The key is to recognize that we're not facing a set of distinct threats, but an ever increasing range of variations. We all started with anti-virus, and when the spyware problem emerged, a set of new products appeared. That was never going to deliver effective protection.

Users shouldn't have to be experts at choosing anti-virus, anti-spyware, anti-spam, HIPS and personal firewalls. These are all part of the same problem, and it is our job to be security experts, determining which technology to use at which times.

Integrated endpoint security solutions must be the way forward. Not suites, but integrated solutions that can blend the techniques and technologies they use as the threat varies in real-time.

**There's a variety of anti-malware tools on the market and everyone claims they are the very best. In your opinion, what should the end user base his purchasing decision on? What are the most important features that define such a critical piece of software?**

End users and administrators should not be getting into the details of individual technologies. They need to have a clear view of the problem that they're really trying to solve and

be asking for a comprehensive security solution. It's always been difficult for users to test the effectiveness of the products they buy and it's getting more difficult. I haven't seen any independent tests that match real-world protection recently, and the lab-based statistics we see are increasingly meaningless.

Most people therefore focus on service, reputation and manageability. That's where you should be. You're not buying a set of products, or buzzwords, but a service. Make sure that your vendor is looking at the whole problem and has the visibility into the whole range of threats - malware, email, web.

Security is evolving all the time, in response to both threat changes and IT use changes. Today's products can not only protect against malware, but manage the use of unauthorized software and enforce a range of user policies.

**Although there have been many predictions about malicious code attacking mobile devices in the past, it hasn't happened yet on a large scale. Is there a real possibility that we will see an outbreak of malware on platforms such as Symbian and Windows Mobile in the near future?**

The predictions about an imminent mobile device threat have always been hype. That remains the case today. The devices are certainly not invulnerable - there are a few hundred examples of mobile device malware, but they're not spreading for two main reasons.

Firstly, the mobile device OS market is fragmented. Malware aimed at PCs is almost certain to hit a Windows PC, which will be compatible with all the others. Malware aimed at mobile phones has to pick out not only the phones from other devices, but then the small percentage of smartphones, which is further subdivided into Symbian, Microsoft and Blackberry. In other words, the homogeneous environment that facilitates malware spread in the PC world doesn't exist for mobile devices, even if the absolute numbers seem large.

Secondly, many of the mobile device operating systems have better security than Windows, using techniques like application signing to restrict unknown applications. The key here is that while these systems may be general-

purpose computing platforms, they're not used in that way. Most devices are used to perform a narrow set of functions, with surprisingly little device to device communication, beyond voice and SMS.

As the market continues to evolve, we need to keep monitoring it and thinking about security. The situation could change, but not with the current generation of devices. As I said earlier, the real threat is about disclosure, accidental or deliberate, of confidential data stored on these devices. That exposure primarily comes through the loss of the device itself.

**What kind of evolution do you expect in the near future when it comes to malware in general? Do you expect increased occurrences of ransomware? What will probably be the next big threat?**

Today's typical hacker has been caught by greed disease. Not only can they steal information for the purposes of identity theft, they can also use the infected machines as part of a botnet or zombie army, allowing them to accept payment for hitting websites and bringing their servers down, or even to send out spam messages.

Behind many of today's attacks, there are huge cyber gangs that pay hackers to carry out this kind of work. Rather than write new pieces of malware – why reinvent the wheel? They use existing malware and try to obfuscate it through encryption and packing techniques. The other advantage is that they can send out tons of malware - Sophos sees about 10,000 pieces of malware each week, all designed to fool security filters and bypass them without being detected.

Today's main threat is not the geeky teenager, but a member of a large criminal gang intent on stealing cash and sensitive information. What is going to happen tomorrow? Who will the hackers be? We can't see them leaving the money trail any time soon. After all, how many infected with greed do you see throwing in the towel to be free and happy once again.

That's right - it's only in the movies.



## Interview with Raimund Genes, CTO of Anti-Malware at Trend Micro

By Mirko Zorz

**Raimund Genes, CTO Anti-Malware, has been with Trend Micro since 1996. Genes has worked in the computer industry since 1978. As a well-known IT expert, Genes has published many articles in security-related magazines.**

### What was the most dangerous piece of malware in 2007? Why?

There is no single piece of malware which could be named as the most dangerous one. Malware is tricky and silent these days and every day thousands of new variants are released. AVtest.org, independent testing organization for Anti-Virus Software added 225,000 new samples in June 2007 to their database ([tinyurl.com/32vnlr](http://tinyurl.com/32vnlr)).

At the end of 2007 we saw around 400,000 new malware per month. In terms of cleverness engineering of malware, I would claim that in 2007 the best written malware family was NUWAR.

### What has been the economic impact of malware for organizations during the past year? Is the overall situation improving?

Global outbreaks are over; this is why little is written about financial impacts due to malware. But 2007 was a record year in terms of malware spreading, and in terms of data theft.

Organizations might believe that thanks to their investments in security, the situation is improving. But that's wishful thinking! Malware attacks are affecting every organization, no matter what size. Nevertheless, malware writers don't have any interest that their attacks are discovered. They don't want any public attention so a report of an outbreak by the media is bad for cybercriminals.

### Will the rising skill level of malicious users and their grouping into criminal organizations ultimately have an impact on the anti-malware industry?

It already has an impact. Anti-malware companies have to invest a lot to cope with the amount of new malware. They have to work on new technologies to provide adequate protection for their customer base.

### Microsoft claims that Windows Vista is the most secure OS they've produced so far. How does it stack up in the real world to the assault of assorted malware varieties?

Microsoft Vista of course is the most secure

OS they have produced so far. But what does this say about their former operating systems like XP, which are still used everywhere. Vista indeed could be configured/used in a way, where it protects against most of nowadays malware, but the users will be confronted all the time with system warnings. And in a corporate environment, a system warning means a call to the helpdesk. That's why a lot of companies can't use UAC (User Access Control).

End-users are annoyed after a few days and click always on yes or disable UAC as well. And let's face it. If a user wants to download dancing skeletons for Halloween (a recent malware trick), the user will ignore all the warning messages, cause he wants to execute the application. The weakest link is always the human being, and with clever social engineering the cybercriminals are able to fool the average user, no matter what operating system is used.

**With Linux and Mac OS X gaining market share among end users, many are speculating that this will lead to an increased influx of malware for those operating systems. What's your take on that?**

Thanks to the uptake of alternative operating systems, especially Mac OS X, we already see malware which has been ported from Windows to Mac OS X. Mac OS X by design is more difficult to infect, but as mentioned above, with clever social engineering you could lure a Mac user to download a VIDEO CODEC, which is malware.

Linux is not on the radar for the malware industry yet, because it is seldom used as a desktop operating system. Linux users normally know a lot about computers and software (so they spot malware more easily than the average user). Most importantly, Linux has a lot of different builds/kernels/recompiled versions so there isn't a monoculture which is easy to attack.

In the past, the monoculture and low security have been the reasons why Microsoft is the number one target. With increased popularity of Mac OS X, this platform could be a high profile target as well. And while under Windows, malware is written for financial gains, under Mac OS X, it could be written just to

show off – that's what the virus writers did in the past (David L Smith with Melissa, Onel de Guzman with ILOVEYOU, Sven Jaschan with Sasser – they did it to show off, not for financial gains). So what about a malware which unlocks your iPhone... and at the same time converts the iPhone into a bot!

**The CSO is becoming increasingly aware of the dangers posed by careless users that introduce malware into the network by using portable storage devices. What can be done in order to mitigate this kind of risk?**

Strict policies and policy enforcement can mitigate risk. It is possible to block USB ports by changing the HW settings and by software which only allows registered USB HW. But the CSO should not be concerned too much about portable storage devices. He should be concerned about notebooks. Most of his users might be mobile within his organization, they might work from home or from a hotel. So what if their notebook is stolen, hacked, infected while the user is on the road? The best way to protect the users and the intellectual property of a company is to monitor and restrict the flow of information. It is about defining who could do what with certain data. Most CSO's think about implementing Data Leak Prevention technologies (DLP). But DLP at the gateway or within the Intranet is not good enough. That's why DLP solutions need to be installed on every notebook/computer as well, to ensure DLP for mobile users.

**Is there a universal solution for fending off blended threats? What kind of assaults should we be on the lookout for?**

Unfortunately there is no universal solution against blended threats. A combination of security solutions is needed to block these threats, firewalls, anti-malware, strict user policies, anti-spam, Web reputation/URL filtering just to name a few.

What worries me is that more and more employees are participating in social networks, and they reveal too much about their private and business life. Based on this it is very easy to craft a spear phishing attack against one or a few employees of a company, and this then leads to a successful infiltration of a company network.

**There's a variety of anti-malware tools on the market and everyone claims they are the very best. In your opinion, what should the end user base his purchasing decision on? What are the most important features that define such a critical piece of software?**

There's no best for everyone. It really depends on what the user cares about. There are some AV solutions out there scoring well against millions of malwares in tests by using multiple scan engines. But they are almost not usable because they slow down the system too much and they create tons of false positives. There are other solutions that provide good protection – but in case an infection occurs (and no AV vendor could protect against all threats), there's no vendor helpdesk, or the helpdesk is not able to do remote diagnostics/removal of malware.

The criteria's for me are:

- Detection rate above 90% - Avtest.org and others are conducting these detection rate tests on a regular basis.
- Low system impact in terms of system performance.
- Additional technologies besides pattern matching based on signature updates. URL filtering/Web reputation/firewalling/behavior analysis are a must have for a security suite.
- Malware knowledge – An established player with a long history in the security industry and with the financial muscles to compete with the malware industry.
- New protection and update methods like in-the-cloud reputation check/ community collaboration systems.

**Although there have been many predictions about malicious code attacking mobile devices in the past, it hasn't happened yet on a large scale. Is there a real possibility that we will see an outbreak of malware on platforms such as Symbian and Windows Mobile in the near future?**

The malware writers are making money with malware nowadays. A typical PC system is Windows based (monoculture) and is using DSL Flatrate to communicate with the Internet. It is an easy pray, and the average user will not recognize for months/years that his

machine is infected with a keylogger/spambot or something else sinister, as long as the malware author is not too greedy. That's totally different to smartphones. Smartphones are heterogeneous devices, relying on different operating systems (Symbian, Windows Mobile, Linux, Mac OS). These operating systems are tuned to specific phones, so one malware might infect only one series of Symbian smartphones. And this is not attractive for the malware industry. So the probability of a wide spreading malware for mobile devices is low. Actually Trend Micro has interviewed several companies, why they are buying mobile security solutions.

And the priority has been:

1. Encryption (risk of lost and stolen devices with confidential information on it)
2. Firewall (WIFI enabled smartphones could be hacked easily – again, loss of confidential information is the driver)
3. Antivirus

Naturally companies want a combination of these three functionalities in one package, to avoid the installation of multiple security agents.

**What kind of evolution do you expect in the near future when it comes to malware in general? Do you expect increased occurrences of ransomware? What will probably be the next big threat?**

It is really a malware evolution, no malware revolution. The malware industry has figured out how to make money with malware the last two years, so why should they completely change their business model? The malware industry has realized that it is not beneficial if an infection is detected too early (Monster.com attack, The Italian Job), so I expect more silent killers, malware which is unique and has a delay before it starts malicious activities.

Ransomware creates too much media attention, and by following the money it is relatively easy to figure out who is behind it. A threat for all of us is the fact that by combining hundred thousands of computers with a Botnet, a large scale attack on the infrastructure of a country is possible nowadays.



WELCOME ADDRESS



**HE Mohammed Nasser Al-Ghanim**  
Director General of the Telecommunications Regulatory Authority of the UAE (TRA)

KEYNOTE 1



**Bruce Schneier**  
Founder and CTO of BT Counterpane and the foremost authority on effective mitigation of emerging IT threats.

KEYNOTE 2



**Jeremiah Grossman**  
Founder and chief technology officer of Whitehat Security and former CTO of Yahoo!

## DEEP KNOWLEDGE SECURITY CONFERENCE

# HITBSecConf2008 - DUBAI

Dual Track Security Conference featuring the worlds leading network security specialists

5 Tracks of Deep Knowledge Hands on Technical Training Sessions

Capture The Flag 'Live Hacking' Competition

HITB/Zone-H Web Hacking Challenge

Technology Showcase & Exhibition



14th & 15th April 2008

Hands on Technical Training Sessions

16th & 17th April 2008

Dual Track Security Conference

16th & 17th April 2008

Capture The Flag

Technology Showcase & Exhibition

HITB/Zone-H Web Hacking Challenge

### Papers & Presentations By:

Marc Weber Tobias (Investigative Attorney and Security Specialist)

Dino Covotsos (Managing Director, Telspace Systems)

Alexander Kornbrust (Founder, Red Database Security GmbH)

Jamie Butler (Co-Author of Rootkits: Subverting the Windows Kernel)

Andrea Barisani (Chief Security Engineer, Inverse Path Ltd)

Daniele Bianco (Hardware Hacker, Inverse Path Ltd)

Domingo Montanaro (Information Security Specialist and Computer Forensics Expert)

Rodrigo Rubira Branco (Software Engineer, IBM)

Raoul Chiesa (Board of Directors Member @Mediaservice.net, ISECOM Group & TSTF)

Shreeraj Shah (Director, Bluelnfy)

Ralf Kaiser aka Skyper - Ex-Editor in Chief of Phrack Magazine

and many more!

Organized By



<http://conference.hitb.org/hitbseccconf2008dubai/>