

# (IN)SECURE

OPEN. INFORMATIVE. TO THE POINT.

Issue 30 - June 2011

## MICROSOFT'S ENHANCED MITIGATION EXPERIENCE TOOLKIT



IPv6



### TRANSACTION MONITORING

DON'T FEAR THE AUDITOR  
**CYBER SECURITY REVISITED**  
SECURE MOBILE PLATFORMS



# RSA® CONFERENCE EUROPE 2011

11-13 OCTOBER | HILTON LONDON METROPOLE | U.K.



## Could your organisation hit the headlines for all the wrong reasons?

With information security threats becoming more targeted and sophisticated, how can you and your organisation stay on top of the situation and out of the news?

Find out at RSA® Conference Europe 2011 - the place for Europe's smartest information security professionals who want to discover the latest trends, technologies and threats affecting the industry. Benefit from:

- 70 educational track sessions
- Keynotes from industry thought leaders
- Interactive programmes
- Demonstrations from leading vendors
- Time to meet and collaborate with peers

Dates: 11th – 13th October

Venue: Hilton London  
Metropole Hotel, U.K.

the adventures of

**Be educated. Be informed. Register now.**

[www.rsaconference.com/2011/europe](http://www.rsaconference.com/2011/europe)

bob  
&  
alice

# TABLE OF CONTENTS

Page 05 - **Security world**

Page 10 - Microsoft's Enhanced Mitigation Experience Toolkit

Page 14 - Transaction monitoring as an issuer fraud risk management technique in the banking card payment system

Page 21 - **Twitter security spotlight**

Page 23 - IPv6: Saviour and threat

Page 32 - The hard truth about mobile application security:  
Separating hype from reality

Page 36 - **Events around the world**

Page 37 - Don't fear the auditor

Page 41 - Book review: Kingpin

Page 43 - **Malware world**

Page 47 - Secure mobile platforms: CISOs faced with new strategies

Page 52 - Security needs to be unified, simplified and proactive

Page 55 - Whose computer is it anyway?

Page 58 - **Security software spotlight**

Page 60 - 10 golden rules of information security

Page 63 - The token is dead

Page 65 - **Security videos**

Page 68 - Book review: IPv6 for Enterprise Networks

Page 70 - Cyber security revisited: Change from the ground up?



## Welcome to (IN)SECURE 30 the digital security magazine

I'm proud to say that this issue marks six years since we started (IN)SECURE. I wanted to thank all the contributors for their hard work and readers for their constant feedback, keep it coming!

An information-packed summer is in front of us as we plan to head over to the heated Nevada desert to attend the Black Hat Briefings, DEFCON and Security B-Sides in August. I'm looking forward to meeting with many of you. I'm sure we'll bump into each other at the Qualys party, I hear it's going to be epic so make sure it's in your calendar. Have a safe summer!

Mirko Zorz  
Editor in Chief

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

### (IN)SECURE Magazine contacts

Feedback and contributions: Mirko Zorz, Editor in Chief - [mzorz@net-security.org](mailto:mzorz@net-security.org)

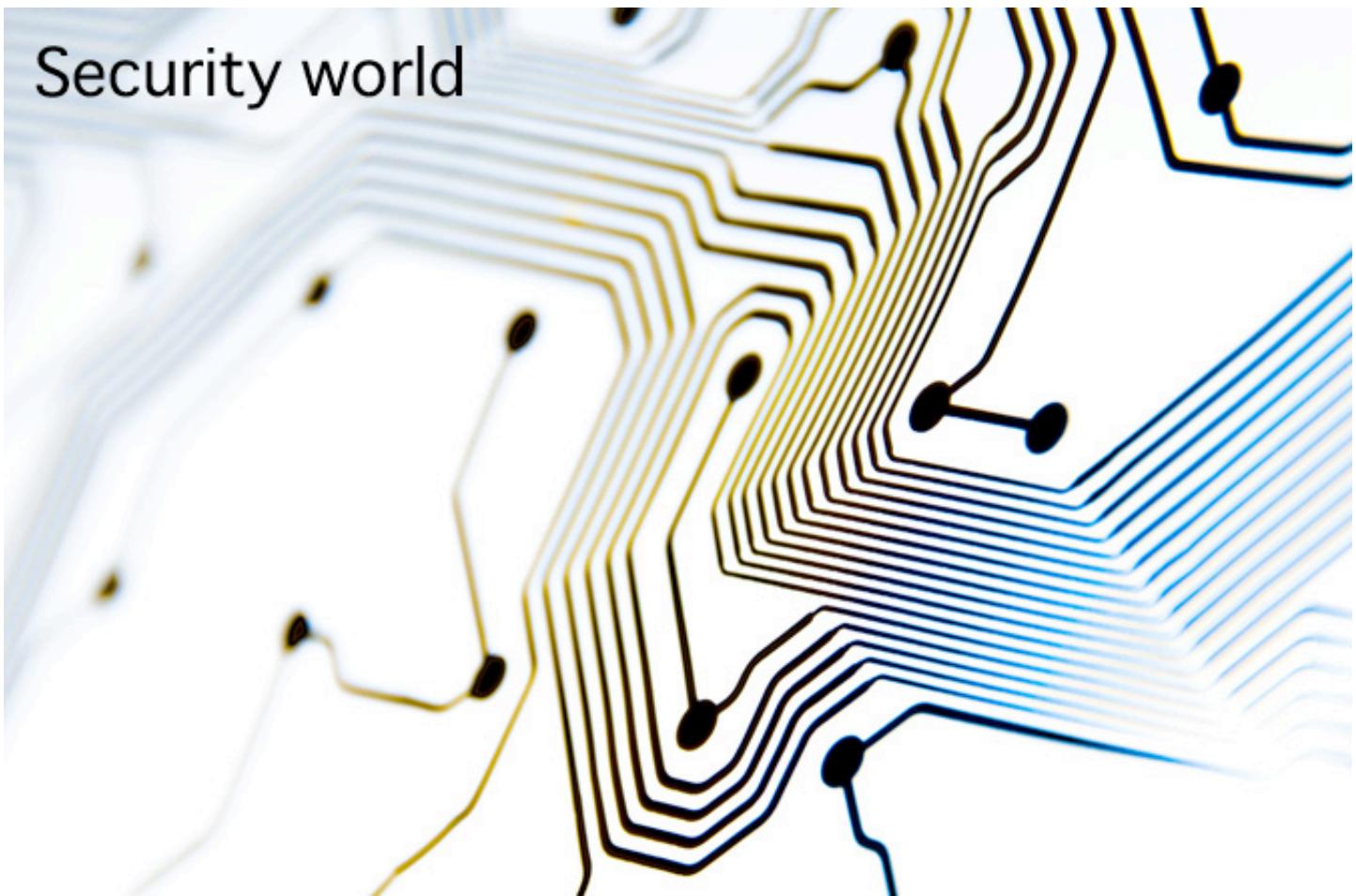
News: Zeljka Zorz, News Editor - [zzorz@net-security.org](mailto:zzorz@net-security.org)

Marketing: Berislav Kucan, Director of Marketing - [bkucan@net-security.org](mailto:bkucan@net-security.org)

### 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.

# Security world



## Poisoned Google image searches becoming a problem



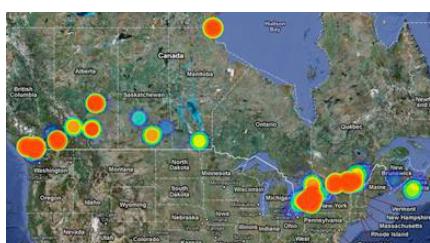
If you are a regular user of Google's search engine you might have noticed that poisoned search results have practically become a common occurrence. Google has, of course, noticed this and does its best to mark the offending links as such, but it still has trouble when it comes to cleaning up its image search results.  
[www.net-security.org/secworld.php?id=10989](http://www.net-security.org/secworld.php?id=10989)

## Files uploaded to file hosting services accessed by malicious individuals

File hosting services such as RapidShare, FileFactory, Easyshare and others have a number of flaws that make it possible for unauthorized people to access and download files hosted on them, says a group of European researchers. And what's more, they say that these vulnerabilities are being actively exploited in the wild.  
[www.net-security.org/secworld.php?id=10994](http://www.net-security.org/secworld.php?id=10994)



## Cyber criminals moving operations to Canada



Cyber criminals are on the move again and, this time, Canada is the prime target. IP addresses in China and Eastern Europe are highly scrutinized and undergoing intense evaluation so attackers are on a quest to move their networks to countries that have better cyber reputations, according to Websense.  
[www.net-security.org/secworld.php?id=10998](http://www.net-security.org/secworld.php?id=10998)

## Google Chrome sandbox apparently cracked

VUPEN's researchers have managed manufacture an exploit able to bypass Google Chrome's sandbox, ASLR and DEP. It is precisely the sandbox feature what made hackers eschew or fail in their attacks directed at Chrome at Pwn2Own time and time again - since, as researcher Charlie Miller pointed out, it has a "sandbox model that's hard to get out of". The feature is also what secured its reputation as the most secure browser around.

([www.net-security.org/secworld.php?id=11001](http://www.net-security.org/secworld.php?id=11001))



## Majority not prepared for IPv6 transition



88% of business networks were not fully ready for a change to IPv6, with two thirds (66.1%) saying their networks are only 0-20% ready, despite the fact that the last blocks of IPv4 addresses have already been allocated, according to Ipswitch.

([www.net-security.org/secworld.php?id=11007](http://www.net-security.org/secworld.php?id=11007))

## Obama administration reveals cybersecurity plan

The Obama administration has issued a new legislative proposal that contains a number of steps it thinks critical to improving cybersecurity for U.S. citizens, the nation's critical infrastructure and the Government's own networks and computers. ([www.net-security.org/secworld.php?id=11027](http://www.net-security.org/secworld.php?id=11027))



## Hackers steal, publish Fox employee passwords



A group of attackers managed to access Fox Broadcasting's server with hundreds of their employees' email usernames and passwords. They published the collected information on the Internet.

([www.net-security.org/secworld.php?id=11028](http://www.net-security.org/secworld.php?id=11028))

## VMware acquires Shavlik Technologies

VMware has entered into a definitive agreement to acquire Shavlik Technologies, which provides a portfolio of on-premise and SaaS-based management solutions that enable SMBs to manage, monitor and secure their IT environments while addressing their needs when moving to virtual and cloud computing IT deployments.

([www.net-security.org/secworld.php?id=11032](http://www.net-security.org/secworld.php?id=11032))



## Two teenage GhostMarket members sentenced



Brighton residents Zachary Woodham, 19, and Louis Tobenhouse, 18 were arrested in December 2010 after the investigation by the Metropolitan Police Service's Police Central e-Crime Unit showed that Woodham had hacked into the systems of web hosting company "Punkyhosing" and taunted its employees, who were unable to prevent the breach. ([www.net-security.org/secworld.php?id=11036](http://www.net-security.org/secworld.php?id=11036))

## New vulnerability reporting framework

The Industry Consortium for Advancement of Security on the Internet published of its Common Vulnerability Reporting Framework 1.0 - an XML-based framework that enables stakeholders across different organizations to share critical vulnerability-related information in an open and common machine-readable format.  
([www.net-security.org/secworld.php?id=11041](http://www.net-security.org/secworld.php?id=11041))



## HADOPI stops monitoring for copyright infringement due to breach



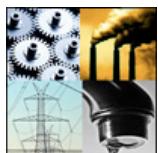
Trident Media Guard - the company tasked by the French High Authority for the Dissemination of Works and Protection of Rights on the Internet to monitor P2P networks and warn offenders about their breaking of the infamous HADOPI (three-strike) law - has apparently been breached. Eric Walter, the secretary-general of HADOPI, has issued a statement saying that the agency has temporarily suspended its interconnection with TMG.  
([www.net-security.org/secworld.php?id=11042](http://www.net-security.org/secworld.php?id=11042))

## Worrying trend in credit card data security

A BitDefender study has revealed some concerning statistics on the personal protection of credit card data. 97% of 2,210 respondents aged 18 to 65 said they purchased goods and services online. Of these, 57% declared that they had replied with sensitive information to potentially fraudulent requests for data, leaving themselves at risk of fraud and their account being compromised. ([www.net-security.org/secworld.php?id=11044](http://www.net-security.org/secworld.php?id=11044))



## SCADA flaws talk cancelled due to security fears



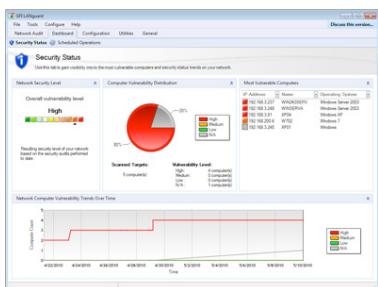
NSS Labs researcher Dillon Beresford was scheduled to demonstrate the vulnerabilities he found after researching various Siemens SCADA systems for only two and a half months, but changed his mind after talking to the DHS and Siemens.  
([www.net-security.org/secworld.php?id=11051](http://www.net-security.org/secworld.php?id=11051))

## 40% of IT staff could wreak havoc to your network

A survey showed that 40% of IT staff admit that they could hold their employers hostage - even after they've left for other employment - by making it difficult or impossible for their bosses to access vital data by withholding or hiding encryption keys. A third of the Venafi survey respondents said that their knowledge of and access to encryption keys and certificates, used for both system authentication and data protection, means they could bring the company to a grinding halt with minimal effort and little to stop them.  
([www.net-security.org/secworld.php?id=11062](http://www.net-security.org/secworld.php?id=11062))



## GFI LANguard 2011 released



GFI Software launched GFI LANguard 2011, the latest version of the network vulnerability scanning and patch management solution. It is the first network vulnerability and patch management solution to integrate with more than 1,500 security applications and to include keyword search functionality. The tool combines vulnerability scanning, patch management and network and software auditing into one solution. ([www.net-security.org/secworld.php?id=11063](http://www.net-security.org/secworld.php?id=11063))

## The rise of layered fraud prevention

By 2014, 15 percent of enterprises will adopt layered fraud prevention techniques for their internal systems to compensate for weaknesses inherent in using only authentication methods, according to Gartner. Gartner analysts said no single layer of fraud prevention or authentication is enough to keep determined fraudsters out of enterprise systems. Multiple layers must be employed to defend against today's attacks and those that have yet to appear. ([www.net-security.org/secworld.php?id=11067](http://www.net-security.org/secworld.php?id=11067))



## Spammers establish their own fake URL-shortening services



For the first time ever, spammers are establishing their own fake URL-shortening services to perform URL redirection, according to Symantec. Under this scheme, shortened links created on these fake URL-shortening sites are not included directly in spam messages. Instead, the spam emails contain shortened URLs created on legitimate URL-shortening sites.

([www.net-security.org/secworld.php?id=11071](http://www.net-security.org/secworld.php?id=11071))

## Apps with dangerous permissions pulled from Chrome Web Store

Do you trust Google to review and ban potentially malicious applications from its online stores? The Android Market has already been found offering "trojanized" apps, and now the Chrome Web Store has been spotted offering two popular game extensions that request potentially dangerous permissions of users that want to install them.

([www.net-security.org/secworld.php?id=11085](http://www.net-security.org/secworld.php?id=11085))



## Google disrupts phishing attack against government officials, activists



An attack apparently coming from Jinan - the capital of China's Shandong province - against personal Gmail accounts belonging to hundreds of users has been spotted and disrupted by Google. Among the targeted individuals are a number of "senior U.S. government officials, Chinese political activists, officials in several Asian countries (predominantly South Korea), military personnel and journalists." ([www.net-security.org/secworld.php?id=11106](http://www.net-security.org/secworld.php?id=11106))

# 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.

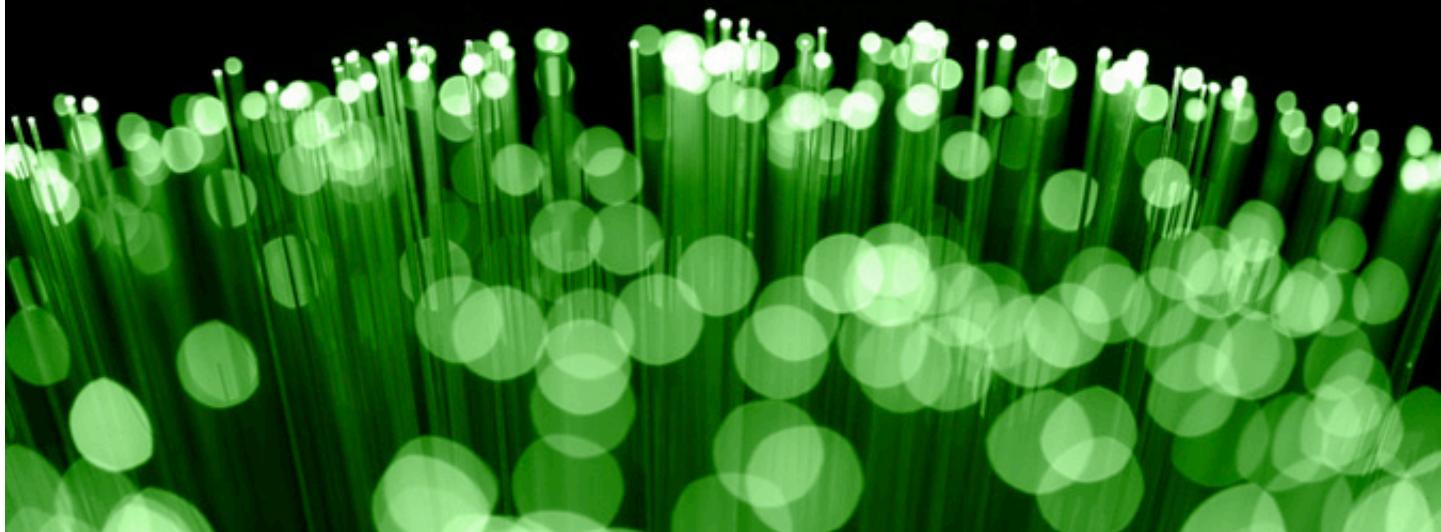
**For a free trial, go to a browser near you.**

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



# Microsoft's Enhanced Mitigation Experience Toolkit

by Didier Stevens



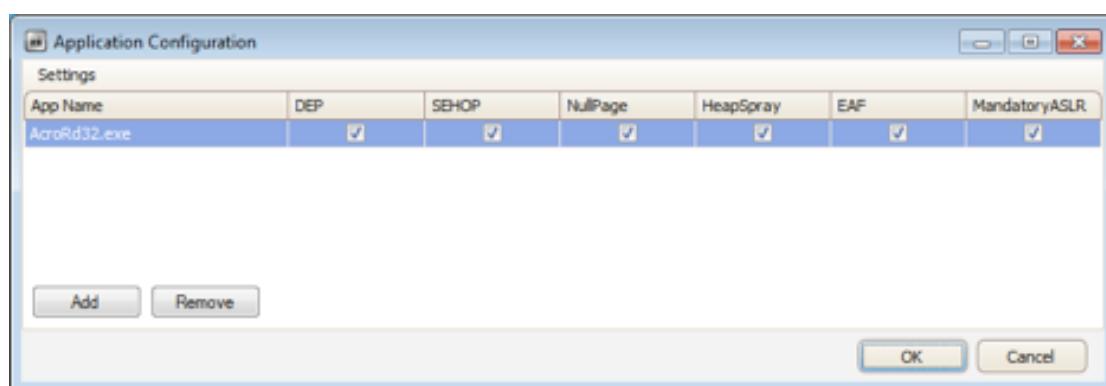
**Microsoft's Enhanced Mitigation Experience Toolkit (EMET) is a tool for enhancing the protection of (legacy) applications that do not support (relatively) new protection techniques like DEP or ASLR. If you use an application that does not use DEP or ASLR to mitigate vulnerabilities like buffer overflows for example, you can use EMET to force this application to enable DEP and ASLR.**

EMET v2.0 provides six mitigation techniques:

- DEP
- ASLR
- SEHOP
- Export Address Table Access Filtering

- NULL page Allocation
- Heap spray Allocation

You can enable these features for your applications by using the EMET configuration tool like this:



When you enable EMET for a particular application, the EMET mitigation DLL will be injected into each instance (process) of your application. EMET comes with a 32-bit (EMET.DLL) and 64-bit (EMET64.DLL) DLL.

When you install EMET, you might notice that it requires the Microsoft .NET Framework version 2.0. This is necessary for the EMET configuration tool, which is a .NET application, but not for the mitigation DLL itself, which is a

WIN32 executable.

The settings configured for EMET are stored under registry key HKLM\Software\Microsoft\EMET. This location (Hive Key Local Machine) implies that you need administrative access to configure EMET, which enables you as an administrator to force EMET on your users provided you have issued them Least-privilege User Accounts. When you configure EMET, your LUA users will not be able to disable your configuration.

Data Execution Prevention (DEP) is a security feature introduced with Windows XP SP2 to prevent code from executing from memory that is designated as data only. Windows applications can designate portions of memory (virtual memory pages) as data and/or code, but x86 microprocessors would indiscriminately execute code from data or code memory - until the introduction of DEP and microprocessors supporting it.

With DEP enabled, the Windows operating system prevents code to execute from data memory by generating an exception.

DEP mitigates a widely used type of attack where the attacker manages to write code (shellcode to be more precise) to data memory like the stack or the heap and gets it executed. But because DEP prevents execution from virtual memory pages marked as data, an exception is generated, which often results in process termination.

If your users have unsaved data when this occurs, they will experience data loss, unless the applications provides data recovery features like Microsoft Office applications do for example.

EMET enables DEP by calling SetProcessDEPPolicy from the process into which the EMET DLL was injected. SetProcessDEP-Policy is called to enable permanent DEP: permanent DEP can not be disabled for the calling process once it has been enabled.

Address Space Layout Randomization (ASLR) is an important feature to protect against remote and local exploits. With ASLR enabled (ASLR was introduced with Windows Vista), executable files (EXEs and DLLs) get loaded

at semi-random addresses in process memory.

Without ASLR, an executable file gets loaded into memory at the base address with which it was compiled.

If this address is not free (i.e. there is already memory allocated that includes the base address), the image loader will load the executable at another address. This address is different each time. But when an executable file is compiled with its ASLR flag set, the image loader will not try to load the executable at its base address, even if this address is not in use. Instead, it will load the executable at a semi-random address (the current implementation of ASLR supports 256 different possibilities). This semi-random address is the same each time for a given executable file, and changes only when Windows is rebooted.

ASLR is important to protect against remote exploits (for example when exploiting vulnerabilities in networked services) because the attacker's shellcode can not be hardcoded with the addresses of the WIN32 API functions it needs (their entry-point addresses are randomized because of ASLR).

ASLR is also important to protect against local exploits, because it prevents Return-Oriented Programming (ROP) code from working correctly. ROP is a technique used to bypass DEP: instead of writing shellcode to the stack (which is data and protected by DEP), ROP uses the addresses of small bits of code it finds in the running process' executable files. ROP code is built up of calls to ROP-gadgets - the small bits of code attackers consider suitable to build their own code.

Because ROP works by writing addresses of ROP-gadgets to the stack, code is not executed on the stack but it is executed in executable memory, thus DEP will allow this. But if attackers can not find ROP-gadgets, they can not use ROP to exploit vulnerabilities protected by DEP.

ASLR will prevent attackers from finding ROP-gadgets: when ASLR is in use, executable files get loaded at random addresses, and thus the attacker can not predict where his

ROP-gadgets are loaded in memory.

That is why it is important to supplement DEP with ASLR. If you use DEP without ASLR, ROP-techniques can be used to exploit vulnerabilities. There is a well-known exploit for an Adobe Reader vulnerability that uses ROP: Adobe Reader 9 and later uses DEP and ASLR to protect itself against attacks, but one of the third-party DLLs used by Adobe does not support ASLR. This DLL, icucnv36.dll, always gets loaded at the same address, and thus the attackers can use ROP-gadgets found inside this DLL, because they can predict the addresses of their ROP-gadgets.

When EMET is configured to force ASLR, it protects Adobe Reader against ROP attacks by forcing DLL icucnv36.dll to load at a random address. And this will prevent the ROP-attack from working. Strictly speaking, EMET does not use ASLR, but it will randomize the address at which a DLL is loaded by pre-allocating some memory at the base address of the DLL.

When a DLL is loaded that does not support ASLR, the EMET DLL will allocate some virtual memory at the base address of the DLL to be loaded. Afterwards, when the image loader loads the DLL, it will notice that the base address is in use, and load the DLL at another address. One could argue that EMET offers even better protection than standard ASLR, because the address is different for each process instance. EMET protects also against heap sprays by pre-allocating specific virtual memory pages. Attackers use heap sprays (often programmed in JavaScript or Flash) to fill the heap memory with the attack shellcode.

When the exploit executes and makes the program flow jump to a specific address inside the heap, the shellcode that has been sprayed in the heap at this specific address is executed. Address 0x41414141 is a popular example of such an address (it's the hex representation of AAAA, which is often found in buffer overflows).

EMET will prevent heap sprays from successfully inserting shellcode at specific addresses (like 0x41414141), by pre-allocating virtual memory pages at these specific addresses. This pre-allocation makes that this memory is

not available anymore to the heap, and thus that no shellcode can be written to it. The addresses protected by EMET can be found in registry value `heap_pages` and are currently 0x0a040a04;0x0a0a0a0a;0x0b0b0b0b;0x0c0c0c0c;0x0d0d0d0d;0x0e0e0e0e;0x04040404;0x05050505;0x06060606;0x07070707;0x08080808;0x09090909;0x14141414.

Another mitigation technique is NULL page allocation. Microsoft calls null-pointer dereference (i.e. using address 0x00000000) a theoretical attack, but nonetheless offers protection against it with EMET by pre-allocating memory at address zero, just like it does with pre-allocating often targeted addresses.

The only difference is that EMET needs to use a work-around to pre-allocate address 0x00000000, because WIN32 API function `VirtualAllocEx` does not accept address 0x00000000 as a valid argument. Instead, EMET will use `NtAllocateVirtualMemory` which can be used to allocate a virtual memory page that starts at 0x00000000.

Shellcode needs to call WIN32 API functions to perform its nefarious actions, and thus it needs to know the address of each function it uses (these are often functions found in `kernel32.dll` and `ntdll.dll`). Static shellcode uses hardcoded addresses: this means that this shellcode will only work on specific versions of Windows (not taking ASLR into account), because each version of Windows has different addresses for its WIN32 API functions.

Dynamic shellcode does not use hardcoded addresses, but it looks up the addresses of the WIN32 API functions it needs by enumerating the function tables found inside each process at a fixed address. Dynamic shellcode can operate on many different versions of Windows because it is not bound by hardcoded addresses.

EMET protects against the execution of dynamic shellcode by detecting function table enumeration (Export Address Table Access Filtering), and terminating the process when it detects enumeration. Technically, it does this by setting hardware breakpoints on a couple of addresses inside the function tables and

checking the origin of the enumeration when a breakpoint is hit. When data is read from these addresses (i.e. when shellcode is enumerating the tables), a breakpoint exception will be generated and EMET will prevent the shellcode from executing.

Structured Exception Handler Overwrite Protection (SEHOP) was introduced with Windows Vista SP1. SEHOP will prevent exploitation of Structured Exception Handlers (SEH) by checking the SEH chain for invalid pointers before the exception is dispatched to the handler. These invalid pointers are a side-effect of overwriting a SHE record. EMET provides SEHOP for pre-Vista SP1 versions of Windows.

Keep in mind that EMET will often, if not always, terminate the process it is protecting when it detects malicious actions. This stops the attack dead in its tracks, but it can also cause data loss. For example, if this occurs with Microsoft Office applications like Word, your users will lose any unsaved work, unless Word's data recovery features can recover most of the unsaved work via the autosave feature.

It is vital to thoroughly test your applications when you protect them with EMET, because not all legacy applications work correctly when they are forced to use features like DEP or ASLR. You should test these applications before making them available to your users, otherwise you could experience an increase in helpdesk calls. If your application malfunctions when protected by EMET, you will need to find out which EMET protection feature is the culprit by trial and error.

Since EMET is configured via the registry, you can define GPOs to set the right registry keys for all your domain users and thus save time by not having to configure each workstation individually.

EMET is a useful tool not only for protecting legacy applications, but also applications that fully support DEP and ASLR. Even software

applications that do support ASLR can become vulnerable to ROP attacks when they include DLLs that do not support ASLR – as is the case with some shell-extension DLLs. Shell-extensions provide extra functionality to Windows, for example in the right-click Windows Explorer context menu. When you install an application like WinZIP, for example, the setup program will also install a shell-extension that provides WinZIP integration with the right-click context menu in Windows Explorer, and all other applications that use the open and save common dialogs. Fortunately, WinZIP's shell-extension DLL supports ASLR, so it doesn't open up the hosting applications to ROP attacks. But not all software providers are as security-minded as WinZIP, you will also find software providers that install shell-extension DLLs that do not support ASLR. And these DLLs open up hosting applications up to ROP attacks - not only Windows Explorer, but also applications like Adobe Reader.

One drawback of EMET is that you get no notification when the application is terminated by EMET. The application just closes, you get no warning as to the reason, for example in the form of a message box. So you can expect an increase of helpdesk calls from users whose Adobe Reader crashes (for example). When they open a malicious PDF file, EMET can trigger on its suspicious actions and just terminate Adobe Reader. Your helpdesk needs to be aware that a crashing application protected by EMET can be a sign of a thwarted attack.

I recommend that you take a look at EMET to protect your applications, especially applications that are a usual target of malware authors, like Adobe Reader. Even if you use the latest version of Adobe Reader, EMET can help you to enforce ASLR on third-party DLLs that do not support ASLR. The icucnv36.dll DLL is a good example. And if your organization does not use the latest application versions (for whatever reason), it's certainly a good idea to introduce EMET to increase your users' protection.

Didier Stevens (Microsoft MVP Consumer Security, CISSP, GSSP-C, MCSD .NET, MCSE/Security, RHCT, CCNA, OSWP) 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 his open source security tools on his IT security related blog at [blog.DidierStevens.com](http://blog.DidierStevens.com).



## **Transaction monitoring as an issuer fraud risk management technique in the banking card payment system**

**by Maxim Kuzin**

**Banking cards are subjected to fraud due to the nature of the technology involved and because of existing vulnerabilities - as all IT systems are. But in the field, the risks can be evaluated and managed effectively by using transaction monitoring systems to detect fraud and decrease loss.**

When a payment effected with a card is not made by the cardholder himself or has not been verified by him - for example, when the cardholder purchased something at the given store, but the sum was different - we call it fraud, or fraudulent operation. According to international payment systems such as Visa International and MasterCard Worldwide, there are five types of payment card fraud:

- Lost and stolen card.
- Never-received-issue (for example, when a card is intercepted by a fraudster while getting delivered to the client via mail).
- Counterfeit card.
- Card not present (CNP) - card data is used in the Internet or in mail order/telephone order (MOTO) transactions.
- Card ID theft.

Payment card fraud leads to losses for the bank that issued the card. Many actions are

required by the bank following the discovery of a fraudulent transaction. The bank must:

- Contact the cardholder or get information about the case from him.
- Conduct an internal investigation.
- Initiate dispute work with the corresponding payment card system.
- Contact the insurance company.
- Get in touch with the police.
- Reissue the card.
- Return the money to the cardholder.

Banks must consider the various risks tied with fraudulent incidents. All of the aforementioned steps cost the bank considerable effort, time and money (operational risk), not to mention the danger to its reputation if an incident that involves many cards and cardholders is made public and is discussed extensively on the Internet and by the media (reputational risk).

In some cases, hacks and permanent violation of payment card brand security rules, procedures and instructions could bring the business to a halt, because the incident negatively influences the brand (business continuity risk).

Due to the nature of the technology behind payment cards, the underlying system is vulnerable to information security attacks. Any card payment system includes IT systems and technologies of issuers, acquirers, merchants, service providers, processors, payment brand net – and all of them have weaknesses that can be exploited by hackers and fraudsters.

If one cannot say that his personal computer is completely safe from attacks with a 100% certainty, is it any wonder that the same cannot be said for an entire payment system? To mention just a few examples of massive card data compromise that happened in the last few years: TJX, CardSystems, RBS Worldpay, Heartland Payment Systems. Millions of ac-

counts were compromised, and the technologies used have been proven to be insecure – and that's why we are talking about risks for the issuer.

In the case of counterfeit card fraud and CNP fraud, there are four steps that the fraudster needs to make in order to accomplish what he set out to do (Figure 1):

- Compromise the card data.
- Use it for the production of a counterfeit card or to perform a CNP transaction (primary account data, card expiration date, CVC2/CVV2).
- Attempt a fraudulent transaction at a store or - if the PIN is also compromised – at an ATM.
- Obtain the issuer authorization.

If all the steps are completed, the fraudster gets the money/goods/services, and the issuer is left with losses.

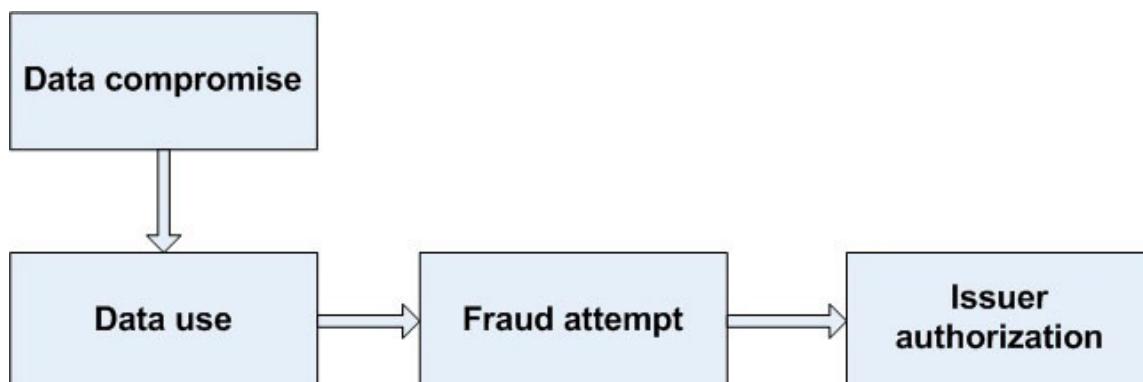


Figure 1. Payment card fraud steps.

How can the issuer reduce the risks he's facing? What technologies, policies, strategies should he implement to achieve this goal?

In general an issuer can do:

- Nothing when it comes to card data compromise, since cardholders use their cards anywhere they want, and hackers attack merchants, acquirers, processors and service providers.
- Nothing to prevent the use of compromised data – hackers sell compromised data and counterfeit cards or card requisites all over the world.
- Nothing to eliminate fraud attempts, but can do something to limit or transfer its liability by

issuing EMV cards and supporting 3D secure transactions for the cardholders.

- Something to detect fraudulent transactions during or after the authorization process.

Fraudulent transactions can be identified at the issuer's side using a transaction monitoring system (TMS). A TMS analyzes all transactions in the banking cards payment system (authorization and clearing) in order to detect suspicious ones so that the issuer can react appropriately.

It is a tool to manage risks in banking cards payment systems and should be an integral part of a complex information security approach.

A TMS can be categorized based on five characteristics: reaction speed, decision type, data used for analysis, mathematical tools and transaction type (see Figure 2).

**Reaction speed.** If a suspicious transaction can be detected and declined during the authorization process, it means that the reaction speed is real time, i.e. the TMS is online. When an analysis is conducted in parallel with the authorization process, we can say that the system is “pseudo online”, since the issuer can only take actions that will affect future transactions (for example, block the card account, set a withdrawal or POS limit, etc.) Offline reaction means that all actions take place after the current transaction is processed, and they can be scheduled to start after a predetermined period of time.

**Decision type.** After a transaction is assessed as suspicious or fraudulent, a decision must be made on how to handle it. It can be made automatically by the system or by trained staff using automated systems and services.

**Data used for analysis.** Suspicious transactions can be spotted by analyzing transaction data, data such as card/merchant transaction history, behavior patterns and models application.

**Mathematical tools** can include simple logical operations ( $>$ ,  $<$ ,  $=$ ,  $\neq$ ), statistical methods (descriptive statistics, correlation analysis, regression analysis), data mining (classification and forecasting, cluster analysis, association rules) and neural networks.

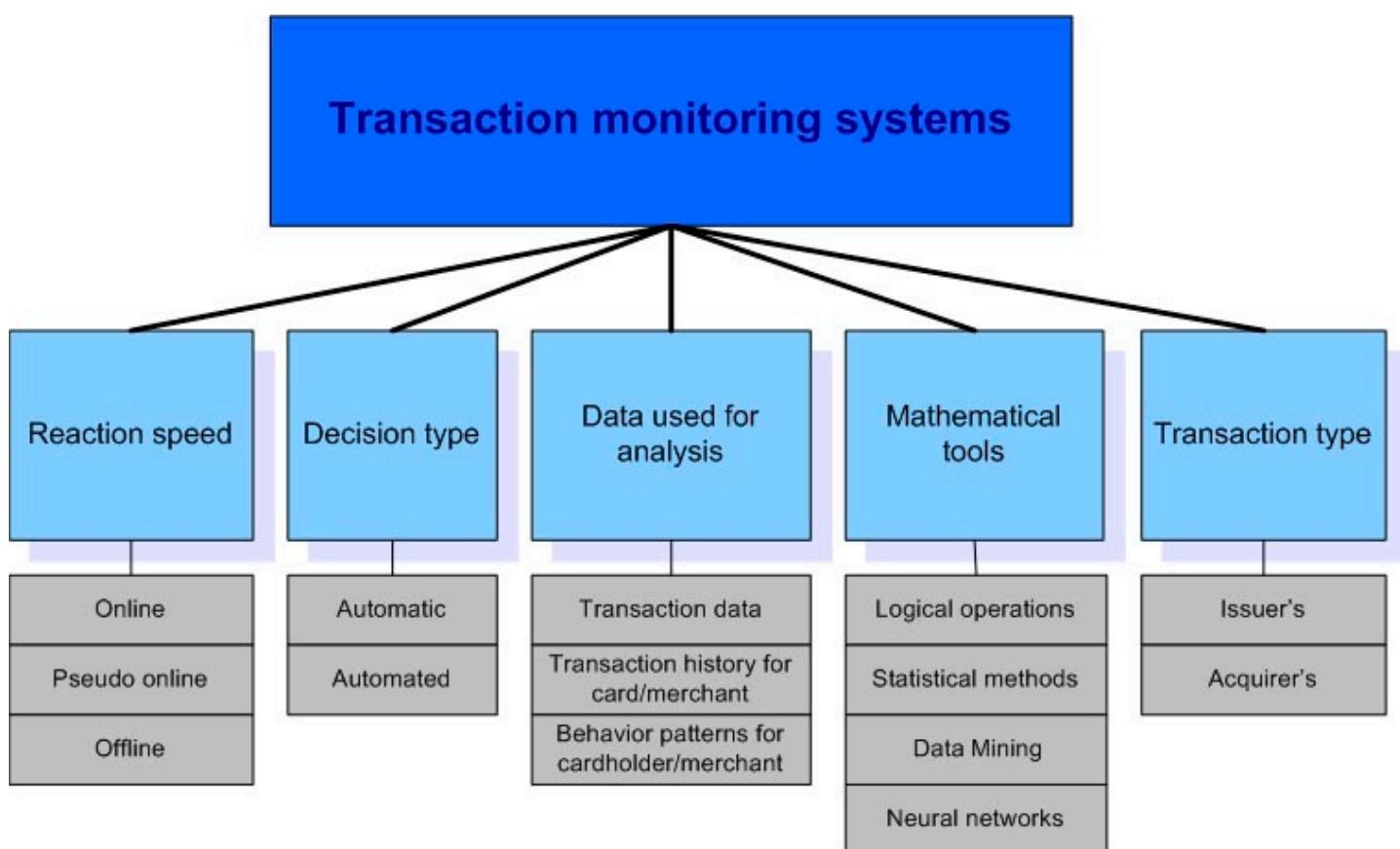


Figure 2. Transaction monitoring systems classification.

**Transaction type.** The transactions performed by the issuer and/or the acquirer could be entered into the TMS. The proposed TMS classification can help compare different systems and describe their functions and capabilities.

I've talked with practitioners in the field and sometimes found that the terms used for TMS are somewhat inaccurate and unclear, especially when reaction speed is discussed. Common and standardized definitions and terms are extremely important when utilizing a TMS in a payment cards system, when

developing a new one or when trying to choose between those proposed in the market.

Transaction data goes to the TMS and is analyzed with the use of additional statistics. If a transaction is flagged as fraudulent or simply suspicious, the final decision should be made

according to set criteria and fraud detection parameters. The parameters are tuned by the expert, the effectiveness of the system is assessed by the analyst, and the operators take part in analyzing and investigating all suspicious and fraudulent transactions. Cardholders are notified by email, SMS, Mobile bank and other auxiliary systems.

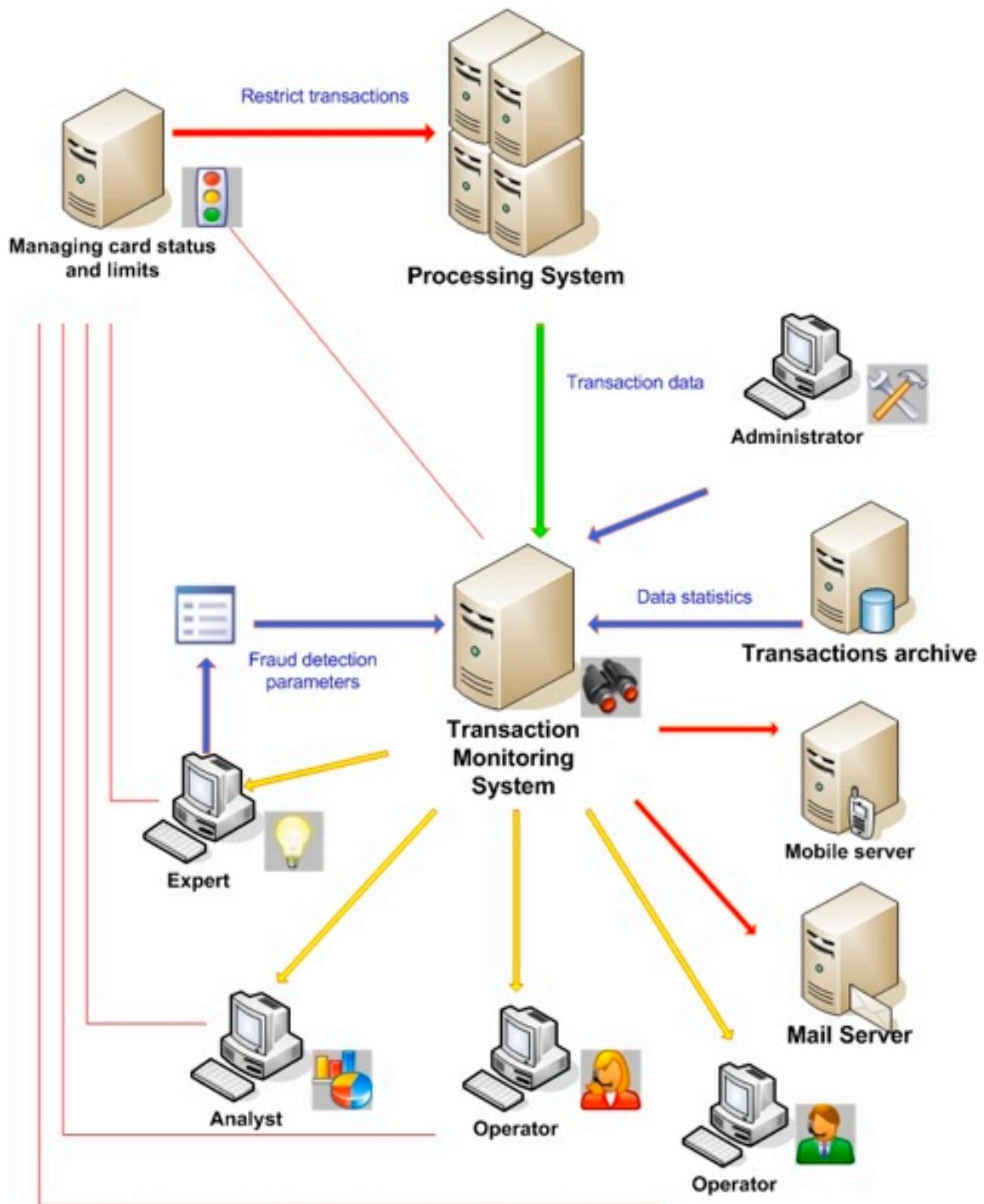


Figure 3 shows TMS concepts and its integration with the processing system.

Regardless of the TMS applied, a bank should implement mandatory criteria for fraud monitoring placed by the various payment systems – Visa International, MasterCard Worldwide, American Express, and others. The criteria include thresholds for sums and operation count set by the issuer or the acquirer, and if the threshold is exceeded, the operation/card should be treated as suspicious.

Practice shows that the threshold approach is not effective in a TMS because of a high false positive rate. For example, if a transaction sum at a merchant exceeds daily average by 150% (it concerns fraud monitoring at the acquirer's side) it should be treated as suspicious according to payment system monitoring best practices and rules, and TMS will produce a number of alerts.

The best practices and rules mentioned were developed primarily for regular reports and statistics, and not for real or near-real time analysis and response. That's why they are inadequate nowadays.

Moreover, payment systems don't offer techniques and criteria to assess fraud risks and adjust the TMS accordingly, though TMS are offered to be applied to reduce fraud risks. But how should it be done?

There is a well-known axiom that says "You can't manage what you can't or don't measure". So, how can you manage payment card fraud risks if you don't measure them?

We know that the quantitative evaluation of information security risks is an issue, since it is extremely hard to propose a methodology to measure it regardless of IT system, environment or business. Can you, for example, give the measured risk of an un-patched OS flaw on your notebook? Are all your firewall rules correct and up-to-date? Is your IT system free from vulnerabilities? The answers to these questions are not obvious.

But when it comes to payment card fraud, risks are easier to measure. If we know the account balance for a debit card and the exceed limit for a credit card, we can assume maximum losses will be limited by the value of the balance/exceed limit (of course, opera-

tional costs to conduct fraud investigation should be taken into account, too).

That's why criminals try to attack assets that can easily be converted into money or are money/e-money. According to Verizon Risk Team's 2011 Data Breach Investigations Report ([tinyurl.com/6aposxh](http://tinyurl.com/6aposxh)), payment cards data is still extremely attractive to hackers: 800 new confirmed data breach incidents were discovered in 2010 and among the 3.8 million records confirmed stolen, 96% were payment card numbers/data.

The result is not surprising – the year before, 93% of compromised records were related to financial services, payment card data/numbers were compromised in 54% of breaches and comprised 83% of all compromised records. It is obvious fraudsters evaluate their profits, so let's evaluate issuer risks!

Let SFR be fraud risk for a bank's payment card, then

$$SFR = P_{fraud} \times S_{sum}$$

where  $P_{fraud}$  - fraud probability for the card,  
 $S_{sum}$  - card account balance or exceed limit.

According to payment card fraud steps described earlier (Figure 1), fraud is successful for a criminal if and only if data is compromised, data is used, a fraud attempt was effected and the transaction was authorized by the issuer. Consequently,

$$P_{fraud} = P(cmp) \times P(use | cmp) \times P(att | cmp \times use) \times (1 - P(det))$$

where  $P(cmp)$  - data compromise probability

$P(use | cmp)$  - use of compromised data probability

$P(att | cmp \times use)$  - fraud attempt success probability

$P(det)$  - fraud transaction detection probability at the issuer's side.

Let's introduce some premises according to the issuer fraud risk management technique proposing:

- All fraud cases in the banking card payment system are recorded and stored in the Fraud Database (FDB).

- Transactions history (legal and fraudulent) is available for analysis and statistical processing from the Transactions Database (TDB).
- Data for each card is available: transactions history, account transfers history, card status and limits change history, additional features (for example, VIP client flag).
- We know nothing about the cardholder's diligence and knowledge on information security issues and secure card usage (so, we don't know if a client carries not only his card but also the PIN in his wallet).
- Each card transaction performed by the holder increases fraud risk due to card data or/and PIN compromise probability increasing.
- Fraud detection by the TMS depends only on fraud type, i.e. the same criteria is applied for all cards to discover counterfeit fraud, CNP fraud and so on.

Fraud admissible thresholds are set:

- $S_{ann}^{ctf}$  - annual counterfeit fraud total sum.
- $S_{ann}^{cnp}$  - annual CNP fraud total sum.
- $\tilde{N}_{ann}^{mon}$  - annual fraud monitoring cost.

Let A be an event of card data compromise in  $k$  operation made by the cardholder at any terminal, B – that data were compromised in  $r$  operation at any terminal,  $k < r$ . The events mentioned are independent, that is

$$P_{AB}(cmp) = P_A(cmp) \times P_B(cmp) = P_k(cmp) \times P_r(cmp), \quad k < r.$$

If card data has not been compromised in any transaction, the non-compromised probability is:

$$P(ncmp) = (1 - P_1(cmp)) \times (1 - P_2(cmp)) \times \dots \times (1 - P_n(cmp)) = \prod_{i=1}^n (1 - P_i(cmp))$$

Thus, data compromise in at least one transaction would be:

$$P(cmp) = 1 - \prod_{i=1}^n (1 - P_i(cmp))$$

where  $n$  – total transactions count performed by the cardholder

$P_i(cmp)$  - data compromise probability in  $i^{\text{th}}$  transaction.

The TMS can be relied upon to detect such fraud types as CNP and counterfeit cards

fraud because the corresponding risks are to be managed by the issuer. It is also possible to identify lost and stolen cards fraud, though the risks are often to be taken by the insurer or the cardholder. Never-received-issue card fraud could be eliminated by implementing secure card and PIN distribution technologies and applying other techniques unrelated to the TMS.

So, let's try to evaluate counterfeit cards fraud and CNP fraud.

Counterfeit card fraud risk for a card is to be computed as follows:

$$SFR^{ctf} = P^{ctf\_crd}(cmp) \times P^{ctf\_crd}(use | cmp) \times P^{ctf\_crd}(att | cmp \times use) \times (1 - P^{ctf\_crd}(det)) \times S_{sum}^{mch} + P^{ctf\_PIN}(cmp) \times P^{ctf\_PIN}(use | cmp) \times (1 - P^{ctf\_PIN}(det)) \times S_{sum}^{ATM}$$

where  $P^{ctf\_crd}(cmp)$  - card track compromise probability

$P^{ctf\_crd}(use | cmp)$  - counterfeit card use at a merchant (not including ATMs) probability

$P^{ctf\_crd}(att | cmp \times use)$  - counterfeit card acceptance for transaction probability

$P^{ctf\_crd}(det)$  - fraud detection by the issuer probability

$S_{sum}^{mch}$  - account's available funds for operations at merchants, not ATMs

$P^{ctf\_PIN}(cmp)$  - card track and PIN compromise probability

$P^{ctf\_PIN}(use | cmp)$  - counterfeit card use at ATM probability

$P^{ctf\_PIN}(det)$  - fraud detection by the issuer probability

$S_{sum}^{ATM}$  - account's available funds for operations at ATM.

CNP fraud for a card is evaluated as follows:

$$SFR^{CNP} = P^{CNP}(cmp) \times P^{CNP}(use | cmp) \times P^{CNP}(att | cmp \times use) \times (1 - P^{CNP}(det)) \times S_{sum}^{CNP}$$

where  $P^{CNP}(cmp)$  - card data compromise probability to commit CNP fraud (it's not track, it could be hpan, expiration date, CVC2/CVV2)

$P^{CNP}(use | cmp)$  - compromised data use probability for CNP transaction

$P^{CNP}(\text{att} \mid \text{cmp} \times \text{use})$  - compromised data acceptance probability for CNP transaction

$P^{CNP}(\text{det})$  - fraud detection by the issuer probability

$S_{\text{sum}}^{\text{CNP}}$  - account's available funds for CNP operations.

According to criteria set, reliable risk values are as follows:

$$SFR_{\text{ann}}^{\text{ctf}} \leq S_{\text{ann}}^{\text{ctf}}, \quad SFR_{\text{ann}}^{\text{CNP}} \leq S_{\text{ann}}^{\text{CNP}},$$

$$\tilde{N}_{\text{ann}}^{\text{TMS}} = \text{const}.$$

The probabilities in formulas could be computed by country and merchant category code (MCC) values. In such a way probability of magnetic card stripe compromise in  $i^{\text{th}}$  transaction in the country at given MCC for a year can be evaluated by counting transactions with the conditions specified and all transactions as follows:

$$P_{\text{ctr}_c, \text{mcc}_m}(\text{cmp})(i) = \frac{W_{\text{cmp}}(\text{ctr}_c, \text{mcc}_m)(i)}{W_{\text{trn}}(\text{ctr}_c, \text{mcc}_m)(i)}$$

where  $W_{\text{cmp}}(\text{ctr}_c, \text{mcc}_m)(i)$  - transactions count in which card data were compromised in the

$\text{ctr}_c$  country and merchant category code  $\text{mcc}_m$  for one year

$W_{\text{trn}}(\text{ctr}_c, \text{mcc}_m)(i)$  - all transactions count in the country and merchant category code for one year.

Counterfeit cards fraud risk is computed by summarizing all bank cards risks of the type. The same is true for CNP fraud. Assessing risks for counterfeit cards fraud and CNP fraud demands and explains TMS fraud detect criteria definitions -  $P^{\text{ctf\_crd}}(\text{det})$ ,  $P^{\text{ctf\_PIN}}(\text{det})$ ,  $P^{\text{CNP}}(\text{det})$ . Then the existing TMS should be adjusted to identify fraud more effectively according to the assessments made.

## Conclusion

In contrast to any IT system security risks in the field of payment cards can be evaluated for issuing bank quantitatively due to the nature of technology. A payment card is used (by the cardholder or a fraudster) to get access to the cardholder's banking account, so the asset has quantity and cost, thus fraud could be assessed. The technique proposed is rational and feasible and was implemented in practice to reduce issuer's fraud risks.

Maxim Kuzin, PhD, is a banking security expert, lecturer, Banking Systems Information Security National Research Nuclear University "MEPhI" ([www.mephi.ru/eng](http://www.mephi.ru/eng)), Russia.





Here are some of the Twitter feeds we follow closely and can recommend to anyone interested in learning more about security, as well as engaging in interesting conversations on the subject.

If you want to suggest an account to be added to this list, send a message to **@helpnetsecurity** on Twitter. Our favorites for this issue are:

#### **@CyberCrime101**

Joe Garcia hosts a podcast that covers everything from computer and Internet safety to information security and computer forensics.  
<http://twitter.com/CyberCrime101>

#### **@packetlife**

Jeremy Stretch - network guy.  
<http://twitter.com/packetlife>

#### **@InsiderThreats**

Insider threats and technologies that could potentially put your organization at risk.  
<http://twitter.com/SteveD3>



# Gartner Security & Risk Management Summit 2011

19 - 20 September • London, UK • [europe.gartner.com/security](http://europe.gartner.com/security)

## Business Beyond Boundaries: Managing Security and Compliance Risks in a World of Cloud and Mobile Computing

The must-attend event for Security leaders in 2011. Understand what you can do to protect your organization's information resources in the most efficient and effective ways and, by pro-actively managing risks, to enable new technology and business.

The Summit will provide a unique mix of **Gartner research presentations, guest keynote addresses, case studies, solution provider sessions and roundtable discussions** taking you from the high-level strategic view all the way to your specific issue.

### KEY TOPICS

- Cloud Computing and Security
- Mobile Device Management and Security
- Governance, Risk, Compliance and Regulation
- Web Filtering and Access, Internet Security
- Security Threats and Vulnerabilities
- Application and Data Security
- Security Metrics and KPIs
- User Authentication and Provisioning
- Privacy Legislation and Assurance
- Content Monitoring and Filtering



**Register Now**

[View the full agenda at: europe.gartner.com/security](http://europe.gartner.com/security)

[europe.gartner.com/security](http://europe.gartner.com/security) • +44 20 8879 2430 • [emea.registration@gartner.com](mailto:emea.registration@gartner.com)



**Early-bird savings** Register by 22 July 2011 and save €300

# IPv6: Saviour and threat

by Simon Heron



**As the number of devices requiring IP addresses increases, the number of addresses available under the Internet Protocol version 4 (IPv4) is dwindling. The Internet Assigned Number Authority (IANA) handed out the last batch of IPv4 addresses on January 31, 2011, and the Asia-Pacific Network Information Centre (APNIC) exhausted them on April 15, 2011. It appears that there will finally be no other option but to move on to IPv6, the successor to IPv4.**

Fortunately, there are still vast numbers of IPv4 addresses that have been allocated but never used and some ranges are getting freed. Just recently Microsoft paid \$7.5 millions for 666,624 IPv4 addresses from Nortel's liquidation sale, and other deals like this can be expected.

Some sources estimate that half of the IPv4 address ranges are not being used, another source says as little as 14% ([tinyurl.com/6kxwxp7](http://tinyurl.com/6kxwxp7)).

But, even if the most optimistic estimates are true, the demand for IP addresses will continue to grow and no matter how successful people are when it comes to recycling or conserving IP addresses, the IPv4 address range is going to run out.

## Advantages of IPv6

Table 1 provides a quick summary of the differences between IPv4 and IPv6. Apart from the huge increase in the address range there are other advantages to deploying IPv6, which will help in justifying the expense in moving when it comes necessary to do so.

## Simplified headers

From Table 2 and Table 3, it can be seen that IPv6 headers have a much simpler format, which will ease implementation. As complexity is the enemy of security, this may have the welcome side effect of improving security in the long run.

	IPv4	IPv6
First Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.168.3.1	Hexadecimal Notation: 1ABC:2DEF:3ABC:4DEF: 5ABC:6DEF:7ABC:8DEF
Prefix Notation	192.168.3.0/24	1ABC:2DEF:3ABC::/48
Number of Addresses	$2^{32} = \sim 4,294,967,296$	$2^{128} = \sim 340,282,366,920,938,463,$ $463,374,607,431,768,211,456$

Table 1: Differences between IPv4 and IPv6 (Credit: Number Resource Organization).

IPv4 Header						
8 bits		8 bits	8 bits	8 bits		
Version		Header Length	Type of Service	Total Length		
Identifier		Flags		Fragment Offset		
Time to Live		Protocol	Header Checksum			
Source Address						
Destination Address						
Options (if Header Length > 5)				Padding		

Table 2: IPv4 header format.

IPv6 Header						
8 bits		8 bits	8 bits	8 bits		
Version		Traffic Class	Flow Label			
Payload Length		Next Header		Hop Limit		
Source Address (128 bits)						
Destination Address (128 bits)						

Table 3: IPv6 header format.

## Stateless auto-configuration

As more devices become networked, this feature will be increasingly useful. With IPv4, IP address could be assigned using DHCP and this is also possible in IPv6 using DHCPv6. However, stateless auto-configuration allows the devices to configure their own IPv6 addresses by communicating with a neighboring router.

This will obviously help in most networks but where it becomes interesting is in networks that are mobile or used by devices with limited management capability.

In a sensor-based network that could include millions of devices that are accessible only via the network, auto-configuration will allow for the automatic installation and replacement of these devices without further infrastructure.

Overall, stateless auto-configuration should help companies lower their network administration costs and the resources required to maintain and move network devices. With IPv4, Automatic Private IP Addressing (APIPA) provided similar features and func-

tionality but had the following restrictions in comparison to stateless auto-configuration:

- APIPA allocates an address from a specific range of IPv4 address space (169.254.0.1–169.254.255.254) when a DHCP server is not available.
- Address Resolution Protocol (ARP) is used to verify that IP addresses are unique on the Local Area Network (LAN).
- Once a DHCP server is available, the IP addresses of the clients are updated automatically.
- APIPA addresses are only usable for the local subnet.
- Routing information is not provided to the host.
- APIPA addresses are not routed off the local subnet.

These limitations are removed with the implementation of IPv6.

# STATELESS AUTO-CONFIGURATION SHOULD HELP COMPANIES LOWER THEIR NETWORK ADMINISTRATION COSTS AND THE RESOURCES REQUIRED TO MAINTAIN AND MOVE NETWORK DEVICES

## Extension headers

The options field in the IPv4 header is used to convey additional information on the packet or on the way it should be processed.

Routers - unless instructed otherwise - must process the options in the IPv4 header. This inevitably involves a performance hit and increased complexity in the router.

The problem is that IPv4 Options perform a very important role and so must be replicated in some way with IPv6. The functionality of Options is removed from the main header and

implemented through a set of additional headers called "Extension Headers" (EHs).

The main header is defined as in Table 3 and is of a fixed size of 40 bytes, which means it is constant and deterministic. EHs are only added as needed and provide a tremendous flexibility to the protocol for future development.

These "extensions" to the protocol can determine behavioral characteristics at the infrastructure and routing level, or at the application level, providing dynamic, policy-based networking and user-defined end-to-end services.

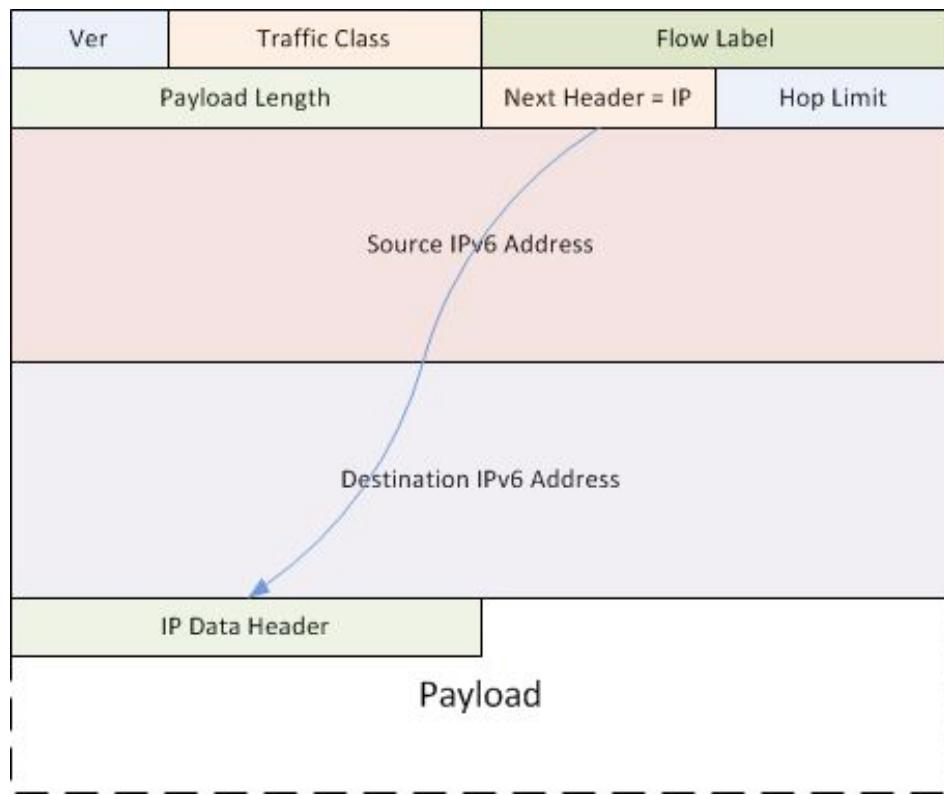


Figure 1: IPv6 packet without Extension Headers.

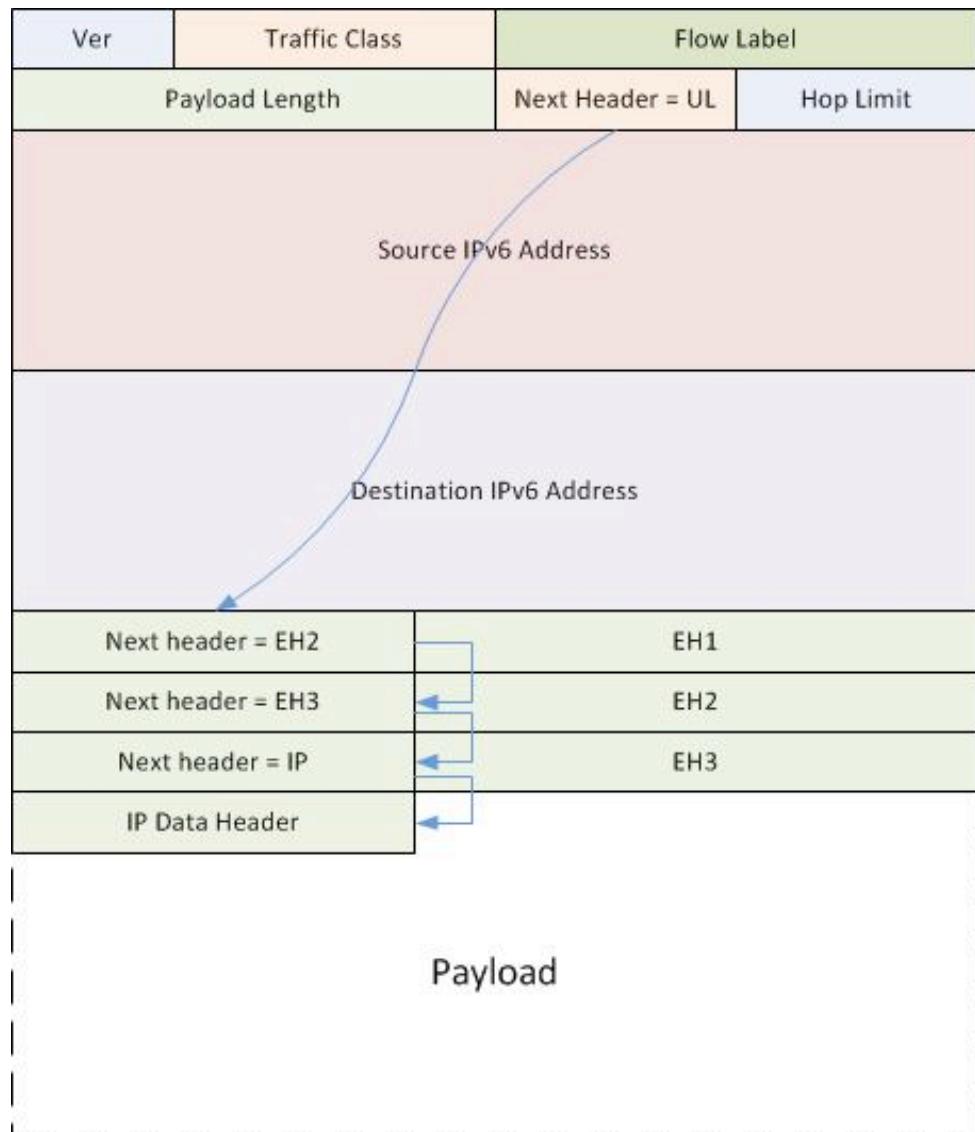


Figure 2: IPv6 packet with Extension Headers.

## Mandatory security

Internet Protocol Security (IPsec) is built into IPv6 and while it has been back-ported into IPv4, it has been an add-on. With IPv4, IPsec has been primarily used for tunneling, network encryption for remote access and site-to-site connectivity.

The problem has been that with IPv4, IPsec has been difficult to implement as NAT, firewall rules and the number of options make IPsec hard to deploy. With IPv6, IPsec is a mandatory part of the implementation. In theory, it will provide for a common network layer security infrastructure, which should allow organizations to extend their security policies down to the host level. In practice, the problems with NAT and firewall rules may remain.

Furthermore, with the increased use of SSL VPNs and the ease with which these VPNs can be set up and how easily they work with firewalls, it may be that companies will continue with this model, maintaining a much more enclave-based mentality than IPv6 had envisaged.

Although the size of local area networks can vary, there are 18,446,744,073,709,551,616 IPs per subnet. This is a vast address space to try to enumerate. For instance, a comprehensive ping sweep would take around 500 million years with the current technology. With a more intelligent approach and advances in technology, the time required would probably come down to months, but this is still an extensive window in which to operate as the reconnaissance might well be discovered by the victim during this time.

As a result, it is likely that hackers will move to new ways of operating. For instance, DNS servers will be holding more information and hence may be their first port of call.

## Security considerations

At the moment attacks on IPv6 are rare because the organizations that hackers want to attack are not yet on IPv6. As the number of deployments grows, IPv6 will provide a much more attractive target for attack and in the following section, various attack vectors are discussed.

## Little real-world experience

An important issue is that vendors do not have much experience with IPv6. IPv4 has been around for 30 years, so extensive experience has been obtained in its implementation.

However, with IPv6, there are a lot of bugs in the code that have not been found yet, protocol weaknesses are yet to be identified and poor implementation by vendors is inevitable as they learn the pitfalls of developing for IPv6.

For example, there are rules about extension headers (EHs) that stipulate how many times EHs should be used in a packet and where they should appear. If an attacker chooses to flaunt those rules by putting in multiple headers where there should only be one or change the order of the headers, how will IPv6 stacks handle this? Will it cause the packet to be dropped or the system to crash or, more worrying, for the packet to pass through a badly implemented stack?

So, as with “Slow Loris” Denial of Service (DoS) attacks where the browser is attacked as opposed to carrying out a brute force flooding attack against a network, IPv6 attacks could be targeted against a specific model of device.

Consequently, with a far wider range of devices being attached to networks, this will make cyber warfare a far more effective weapon. At the moment, malware like Stuxnet might be able to render a nuclear power station inoperable by targeting the Siemens Supervisory Control And Data Acquisition (SCADA) system but imagine the options that could be available by targeting different makes of IPv6 addressable devices and sensors.

The number of devices that might have flaws is increased by orders of magnitude, offering a hacker a much greater selection of attacks, multiplying the number of industrial systems vulnerable to abuse and increasing the effectiveness of any concerted cyber-attack against a country.

Finally, on a much more mundane level but still on this topic of moving from one

technology to another, a change from IPv4 to IPv6 requires all security infrastructure to be mirrored from one system to the other which is likely to introduce errors by system integrators. A great deal of care will be required to ensure that these changes do not open up organizations to attack.

### Rogue IPv6 traffic

Another attack vector is against organizations that have bought and deployed IPv6 enabled equipment or are running ‘dual stack’ systems. Dual stack systems are able to parse both IPv4 and IPv6 traffic and will be of increasing importance as organizations transition to IPv6.

Another way that IPv6 traffic gets on a network is that many operating systems, including Microsoft Vista, 7, Windows Server 2008, Mac OS X, Linux and Solaris, ship with IPv6 enabled. Joe Klein, director of IPv6 Security at Command Information estimated that in 2009 there were over 300 million systems that had IPv6 enabled by default ([tinyurl.com/ktatpw](http://tinyurl.com/ktatpw)).

If they are not using IPv6, network managers should consider disabling it on every device that they install on their networks – otherwise, these devices may be able to receive and send IPv6 traffic.

Attackers have engineered tools that let them establish IPv6 network communications on IPv4 networks using this IPv6 capability. This allows them to establish new covert channels for data extraction that current IPv4 networking monitoring devices have a hard time catching.

Common hacker practices are to use IPv6 to run Internet Relay Chat (IRC) channels over unsuspecting IT enterprises. Others use the channel created as the covert channel to control tools.

The lesson to be learnt here is that IPv6 enabled devices need to be investigated to ensure that they are not allowing IPv6 traffic to be passed unless actually required to do so and then be sure that only the required traffic is being passed. As always, do not rely on default settings to be safe.

### Rogue IPv6 devices

The auto-configuration capabilities that are built into IPv6 allow an attacker to define a rogue device that assigns IP addresses to all the other devices on the network. A hacker could set up a rogue device, like a router, to assign IPv6 addresses on a network and to act as an IPv6 router. Once in place, it can divert traffic through itself and carry out traffic analysis, modification or simply denial of service by dropping packets.

Another attack implants routes with ICMP6 redirects illustrated in Figure 3. In IPv6, if a User chooses the wrong router to send its traffic, the router will respond with a ‘redirect’ packet that will tell the User where to send the traffic to.

In IPv6, to prevent hackers from abusing the system, the redirect must be accompanied by the exact packet that the router received. The success of an exploit is dependent on knowing what the victim of the attack (User 1 in this example) will send to the router.

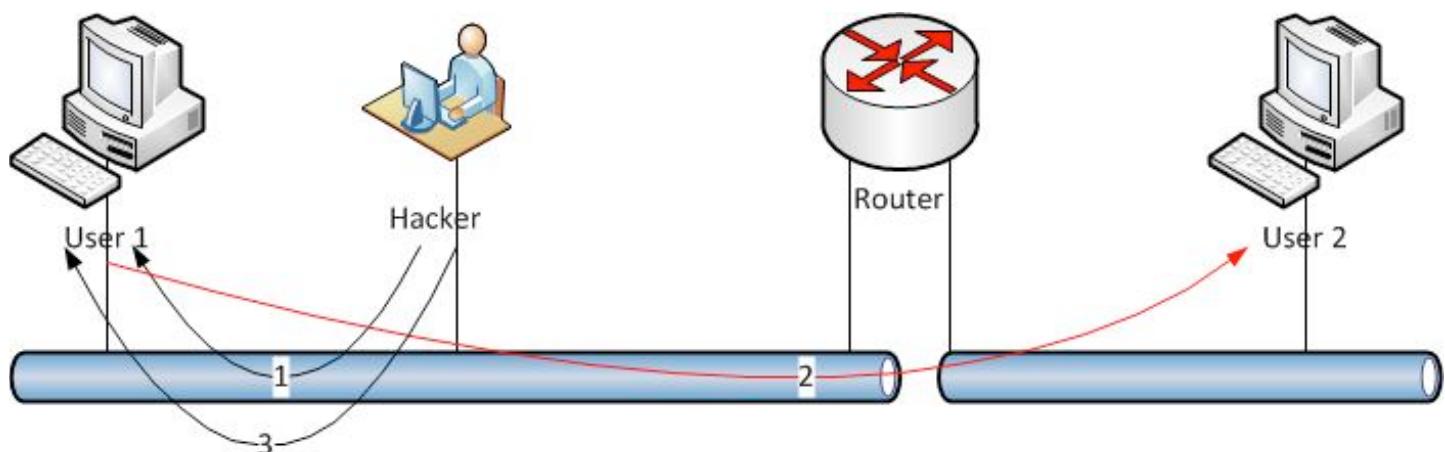


Figure 3: ICMP6 redirect attack.

The attacker, by using an Echo Request, knows that the Victim will respond with an Echo Reply and hence can spoof User 2. The attack unfolds as follows:

1. A attacker with access to the network sends an Echo Request with the source address as User 2 and the destination as the User 1.
2. The victim receives this echo request and sends an Echo Reply to User 2.
3. The attacker then creates a redirect packet with the Echo Reply attached. The packet is constructed with the source as the router and the destination as User 1 and in this packet tells User 1 to redirect all traffic for User 2 to the attacker. The Hacker then receives packets from User 1 and can spoof User 2.

### Type 0 routing header

The severity of this threat is such that it has resulted in the following routing feature being deprecated. I include it here because it is useful in demonstrating how a useful feature can be so dangerous to normal operation that it has to be withdrawn, and because - as described above - some systems have been installed and forgotten and will still retain this functionality.

The Internet Protocol Version 6 Specification (RFC2460) defines an IPv6 extension header called a "Routing Header". A routing header subtype is called "Type 0" and referred to as "RH0". This RH0 can contain multiple intermediate node addresses, as shown in Figure 4.

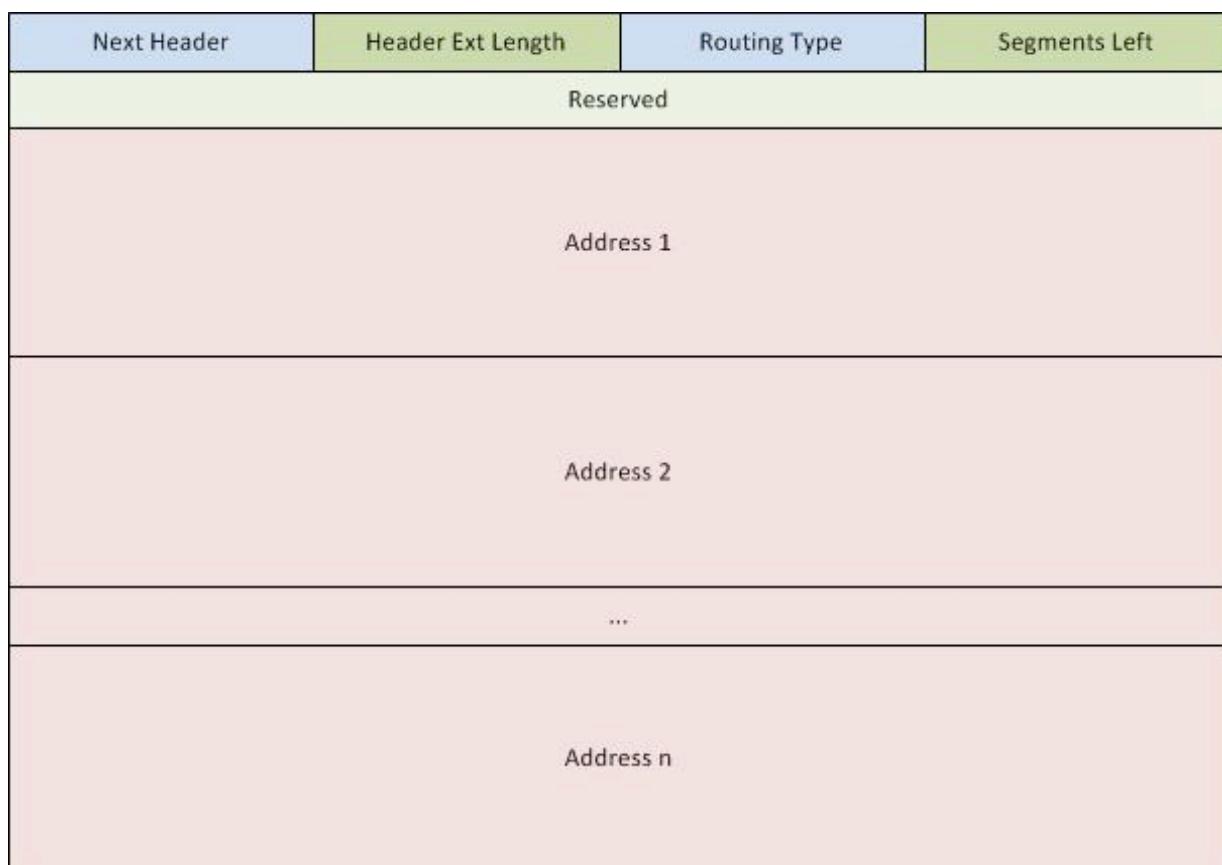


Figure 4: Routing Extension Header Type 0.

This then enables the attacker to build a packet that will bounce between two (or maybe more) remote routers creating unnecessary traffic in a denial of service attack. As reported on CanSecWest07 ([tinyurl.com/2oa95q](http://tinyurl.com/2oa95q)), a 88-fold amplification in the traffic can be achieved using this technique.

This attack is particularly serious in that it affects the entire path between the two exploited nodes, not only the nodes themselves or their local networks. While similar functionality is to be found in the IPv4 source route option, the opportunities for abuse of RH0 are greater due to the ability to specify many more intermediate node addresses in each packet.

## Built-in ICMP and multicast

IPv6 has built into it both Internet Control Message Protocol (ICMP) and multicast. These two types of network traffic are integral to how IPv6 works. With IPv4, network managers can block ICMP and multicast traffic to prevent attacks coming over these channels.

With IPv6, network managers will not have this luxury and ICMP and multicast will have to be let through from some sources and to some destinations.

One of the main uses of ICMP6 is neighborhood discovery. The Neighborhood Discovery Protocol (NDP) is used to discover other nodes on the network, to identify routers and a number of other tasks. But NDP - as defined in RFC2461 and RFC2462 - lacks a way of authenticating authorized neighbors and

hence has a number of vulnerabilities. For instance, neighborhood solicitation can be falsified with unreachability detection errors, or replay attacks carried out where previous neighbor or router discovery packets are replayed.

Issues like these were originally going to be solved by using IPsec but this is not practical with real world situations. A new protocol had to be developed. It was called Secure Neighbor Discovery (SEND) and was defined in RFC 3971. SEND secures the various functions in NDP, where a set of new Neighbor Discovery options is introduced and these options are used to protect NDP messages.

Organizations deploying IPv6, and especially those in environments where physical security on the link is not assured - for example, wireless - should consider the use of SEND.

# TRADITIONAL IPV4 ATTACKS CAN TAKE ADVANTAGE OF IPV6 TUNNELING TO ENTER NETWORKS WHERE TUNNELING TRAFFIC WAS USED

## IPv6 tunneling

There are three common types of IPv6 tunnels: Teredo, 6to4 and Intra-Site Automatic Tunnel Addressing Protocol (ISATAP). These allow IPv6 packets to be encapsulated inside IPv4 packets that can be sent through IPv4-enabled firewalls or network address translation devices. To a network manager, tunneled IPv6 packets look like normal IPv4 traffic.

Traditional IPv4 attacks can take advantage of IPv6 tunneling to enter networks where tunneling traffic was used.

To examine one tunneling technology in more detail, consider Teredo, which is a tunneling service built into Windows. Its intent was to allow anyone to have access to the IPv6 enabled Internet, free and simple without the need for infrastructure changes.

To use it an internal host asks a Teredo server for an IPv6 address. By default the Teredo

server is to be found at [teredo.ipv6.microsoft.com](http://teredo.ipv6.microsoft.com) and the data is carried over port 3544 (UDP).

When the tunnel is established, the host is given a 2001::/32 address. This address is a public IP and hence any Windows shares and any other listening services were publicly available, despite any NAT and firewall that might have been in place.

There is some unintentional protection provided by the fact that the chances of finding this address in the vast address space available are terribly small.

It should be added that obscurity is rarely a good security posture and it is possible that this backdoor might have been unearthed by error, perhaps in a posting or similar slip. As a result, such a security hole should be closed where detected.

It was not Microsoft's intent to provide a backdoor so this bug has been patched by denying all traffic from NAT transversals, which effectively blocks connections inwards via Teredo. But, this patch does allow systems to connect out. Obviously, it is essential that this patch is applied so that this protection is in place.

Again, if the system administrators are not aware of this feature then it is possible that this patch has not been applied.

There is a workaround the patch but it does require access to the host machine to enable and install IPv6 and activate Teredo. Although, if a hacker is trying to ensure backup access to a system he has already compromised, this is an option the can consider.

The attacker has to install Miredo on a Linux or Unix system to act as the Teredo server or relay but this can listen on any port meaning that blocking this traffic is not trivial.

### IPv6 creates problems in spam filtering

This migration towards IPv6 may make it harder to filter spam messages. With IPv6

having  $3.4 \times 10^{38}$  addresses compared to the trifling  $4.3 \times 10^9$  addresses offered by IPv4, this expansion allows far more devices to have a unique Internet address.

This creates a host of problems for security service providers, who have long used databases of known bad IP addresses to maintain blacklists of junk mail sources.

Systems that use IP reputation could become seriously overloaded trying to maintain accurate IP black lists of sources sending spam.

There are other security tasks that also track IP addresses for various purposes, for instance systems that block sources of denial of service attacks, click fraud and search engine manipulation.

Tracking IPv6's huge IP address space will require the querying of vastly increased databases which in turn requires more processing power to maintain throughput and in some cases this may just not be feasible. New approaches will be needed to protect against these forms of attack.

## IPV6 IS NOT INHERENTLY MORE SECURE THAN IPV4 BY HAVING IPSEC BUILT IN TO IT

### Conclusion

Needless to say, this article has not covered all of the issues that IT managers are going to face or are already facing. Attacks that reduce MTU size, deny access to new devices joining the network, neighbour solicitation requests with a lot of Cryptographically Generated Addresses (CGAs) that will overwhelm CPUs and other ploys are all possible in the new world that is almost upon us.

IPv6 will certainly have tremendous advantages but as with just about every new technological development - whether it is Web 2.0, Voice over IP or extending the address space

- there are security issues that need to be addressed.

IPv6 is not inherently more secure than IPv4 by having IPsec built in to it. In the short term it will probably be necessary for both IPv4 and IPv6 to be run concurrently. This will result in extra complexity and inevitably more confusion.

As a result, organizations will need to consider carefully how they make the transition from one protocol to the other as undoubtedly during this period they will be more vulnerable to exploitation.

Simon Heron is the CTO of Redscan ([www.redscan.com](http://www.redscan.com)).



## The hard truth about mobile application security: Separating hype from reality

by Rafal Los

This article addresses the market hype and misconceptions contributing to the mobile application security chaos.

Mobile applications are the new big thing. Mobile handsets, tablet devices and the various types of mobile computing platforms now have their own app stores or markets where mobile applications are appearing by the thousands.

While the explosion of purpose-built, inexpensive mobile applications is certainly no cause for alarm, there is a greater issue at stake, especially for enterprises that are taking their business onto mobile platforms.

With the inevitable discovery of security defects or vulnerabilities in a few important mobile applications, the floodgates of temperance have fallen to pieces and hysteria over mobile application security prevails.

### What is a mobile application?

Confusion still exists about what mobile applications are. The concept is still evolving and

has generated heated debates even among seasoned security professionals and application developers.

Mobile applications are applications that run on mobile devices such as your mobile phone handset, your tablet or some other widget that is considered a mobile device.

Mobile applications are not that different from regular applications, except for the fact that they run on somewhat exotic operating platforms like Apple's iOS, Google's Android, HP's WebOS, Microsoft's Window 7 Phone, or the BlackBerry OS platform – and that's just naming the most used.

With a wide variety of platforms, there comes a wide variety of language support and capabilities, and each with their own unique quirks and challenges.

For example, developing for the Android operating platform means writing code in Java for a Linux-based operating system that has a high level of modification by each mobile vendor. This presents a vast number of challenges if you're trying to write an application that utilizes the full potential of Android and that will be usable across all of the Android mobile platforms.

Writing code for Apple's iOS requires users to learn Objective-C, which is a reflective, object-oriented derivative of the C programming language, adding SmallTalk-style messaging. Each platform is distinct. The development styles also differ, as well as features such as sandboxing. All of this creates significant challenges when it comes to securing these applications.

While none of these languages are perfect when it comes to security, there is no reason to suspect that any one of these platforms is somehow inherently more prone to defective code than the others. Developing applications

for each of these mobile platforms should involve learning the localized operating platform, the development language and the ability of writing quality code. This is no different from writing good web applications, or using python or Cobol for that matter - it's all code.

The confusion over the various platforms and inherent vulnerability breaks down to a simple and easily understandable point: these are all end-point devices. Just like a laptop, these devices can be compromised by an outsider - either when one lands on a web site or when someone gains access to one's mobile device via other attack channels.

It is also important to remember that applications are not the only way to compromise and infect a mobile device.

Once there is agreement that mobile devices that run applications are just as susceptible to being over-run with malicious code as any other platform, we can start to see how mobile applications play into the picture.

## APPLICATIONS ARE NOT THE ONLY WAY TO COMPROMISE AND INFECT A MOBILE DEVICE

### Market hype and misconceptions

The hype surrounding mobile application security has reached a fever pitch, and the market has certainly done its part in perpetuating it. While the focus is currently turned towards the application installed on each mobile device, a bigger problem is being neglected.

That bigger problem is the back-end system that powers mobile applications. After all, mobile applications are just pieces of code that communicate with a back-end web server using HTTP or HTTPS requests. The endpoint mobile application may do some processing but most attacks happen when the application server listens for HTTP/HTTPS requests from that mobile application.

The marketing hype around mobile applications has blinded us to the fact that under the covers these are all just lightweight client/server applications that mainly talk HTTP/

HTTPS to a back-end system, which is where the real dangers lie.

Mobile applications should be treated like Adobe Flash or other similar browser applications. If your browser is compromised, then the application can (and will be) reverse engineered. The proper procedure in this example is to assess and strongly protect the back-end system, including the application server that stores the data.

The application server is where the emphasis should be made in the mobile application space – and not because mobile applications are not a risk, but because the application server back-ends pose a significantly greater risk.

If the operating platforms had sound security controls such as proper sandboxing, process isolation, and followed the least-privilege principles, the security of each individual mobile application would be of much greater concern.

Mobile applications absolutely must protect private information and data. However, if your application is leveraging a poorly protected operating platform, it just makes the security controls considerably less meaningful.

### **Addressing the real threats**

Security experts consider mobile applications as one of the severest up-and-coming threats to security. This is a misconception. The real risk is in the back-end application servers and systems which house the data, as well as the operating platform on which the mobile applications are built.

Activities aimed at manipulating or stealing data aren't new. Only the venue and 'packaging' have changed.

While it may be important to analyze a mobile application for outright security defects, the more critical component is the supporting

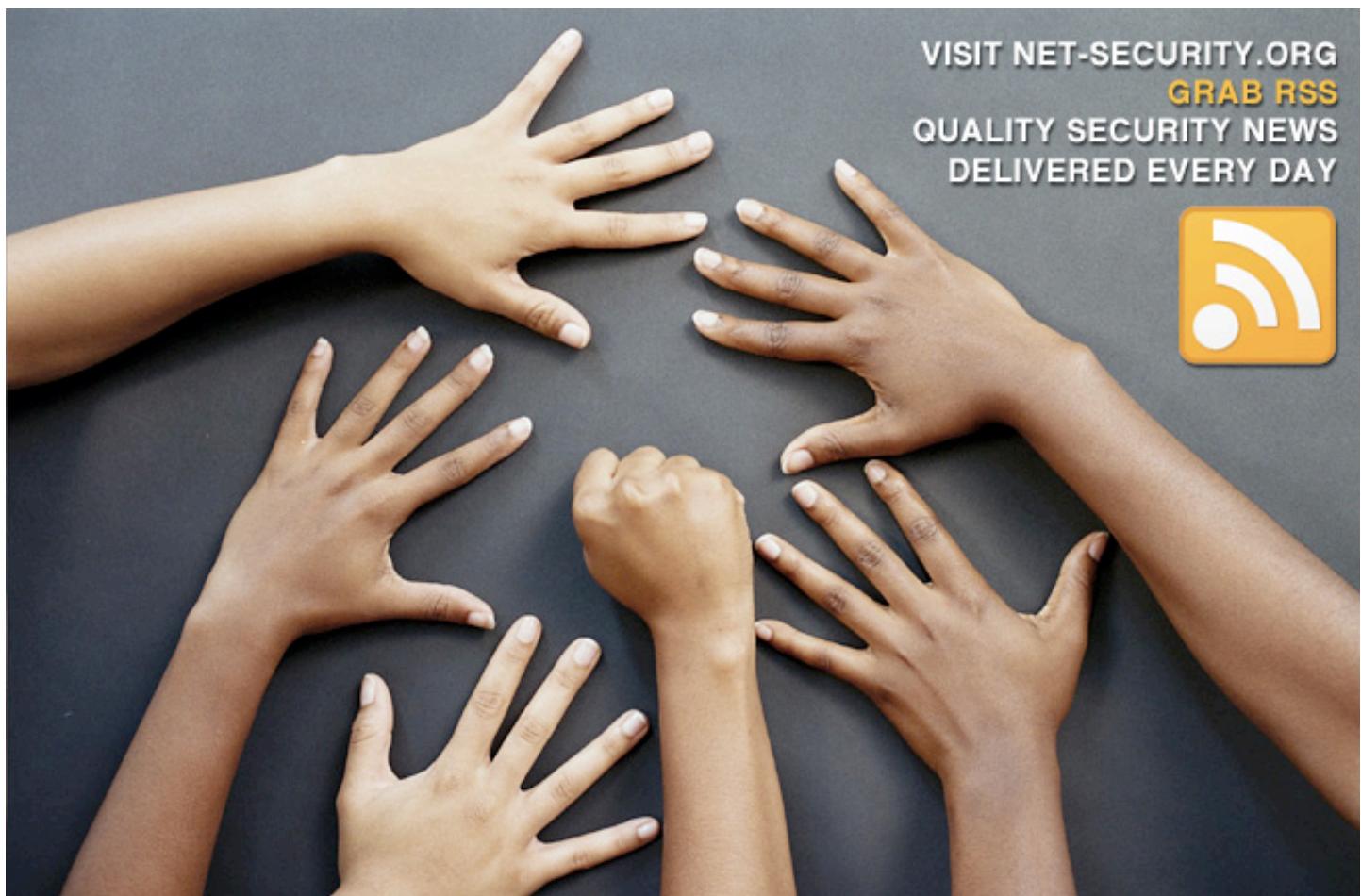
back-end system being attacked over HTTP/HTTPS. Many organizations are still housing critically sensitive information on a mobile device inside an application built upon a poorly secured operating platform.

And users should by no means avoid testing the security and integrity controls of mobile applications. In fact, it is absolutely necessary in some cases. Mobile platforms offer such low security hurdles for attackers to overcome in order to compromise the operating platform that the mobile applications themselves in many cases should be considered compromised.

This once again leaves the critically sensitive data residing on the back-end application logic and storage system. This is where the concentration of security testing in the mobile space should take place. The good news is that the industry is pretty good at testing web-based or web-services based applications.

---

Rafal Los is the Application Security Evangelist with HP Software. You can read his blog at [www.hp.com/go/white-rabbit](http://www.hp.com/go/white-rabbit).



VISIT [NET-SECURITY.ORG](http://NET-SECURITY.ORG)  
GRAB RSS  
QUALITY SECURITY NEWS  
DELIVERED EVERY DAY



# Reduce the **window of opportunity**

Why are end-points increasingly vulnerable to attacks?

**Access the Secunia Yearly Report 2010 to:**

- Understand the state of the security ecosystem
- View vulnerability data and trends
- Plot your optimal defence against vulnerabilities

**Stay updated, stay secure.**

Download Report:  
[http://secunia.com/company/yearly\\_report](http://secunia.com/company/yearly_report)



Secunia.com

# Events around the world



## RSA Conference Europe 2011

[www.rsaconference.com/2011/europe/](http://www.rsaconference.com/2011/europe/) - London. 11-13 October 2011.

## VB2011 - 21st Virus Bulletin International Conference

[www.virusbtn.com/conference/vb2011](http://www.virusbtn.com/conference/vb2011) - Barcelona. 5-7 October 2011.

## Gartner Security & Risk Management Summit 2011

[europe.gartner.com/security](http://europe.gartner.com/security) - London. 19-20 September 2011.

## SecurityByte 2011

[www.securitybyte.org](http://www.securitybyte.org) - Bangalore. 6-9 September 2011.



## Don't fear the auditor

by Brian Honan

The Blue Oyster Cult song “Don’t Fear the Reaper” from the 1970's is often misinterpreted to refer to people's fear of death, while in reality song is about eternal love. Similarly, in information security we often mistakenly focus our fears and energies into the wrong areas, such as the common fear of many information security professionals of the dreaded auditor rather than the attackers actively looking to breach our systems.

Being more afraid of the auditor rather than the attacker is understandable as it is more likely the former will look at our systems, while we hope the latter never do. As someone who works with clients to help them succeed in audits I am often puzzled by this reaction. After all, who would you rather find a security hole in your systems, an auditor or an attacker?

I argue that an auditor is one of the best tools in your armory to help you defend your systems. Of course, this depends on how good your auditor is and what the purpose of the audit is. So, how can you use an auditor to your advantage? Well, let's start with identifying the main types of auditors:

**The internal auditor** is an auditor employed by the same organization that you work for and is tasked with ensuring that you are implementing and managing the information security program for the organization as agreed.

**The external auditor** is an auditor hired by a client as part of their due diligence, to check if your organization is a desirable business partner and if you can be a trusted with their data.

**The audit body auditor** is an auditor from a certification body who is tasked with ensuring your information security management system meets the requirements of the standard they represent.

While each of the above auditors has the same objective - to ensure your information security program is operating as it should - the approach each of them takes can be quite different. However, the approach you should take to each audit should be the same regardless of the type of auditor you are working with. Your goal should be to use the output of the audit to better enhance the security of your systems.

An auditor can provide you with a fresh and unbiased pair of eyes to identify potential weaknesses in your security.

### **Be prepared**

The Boy Scout motto of "Be prepared" is especially appropriate when dealing with information security audits. Proper preparation for an audit is the key to passing an audit and for you to maximize the benefits from it.

Let's be clear - when I say preparation for an audit I do not mean writing your policies and documentation the week or indeed (as I have seen on some occasions) the night before the audit is due to happen.

An auditor will examine your policies to make sure they have been developed with your organization's business requirements in mind. This means ensuring you have proper senior management support and that the controls outlined in the policy are suitable for your organization.

Remember that your organization has unique business drivers and goals that may not be the same in another organization. You may also have to comply with certain laws applicable to the jurisdiction or regulatory environment that your organization operates in.

## **AN AUDITOR CAN PROVIDE YOU WITH A FRESH AND UNBIASED PAIR OF EYES TO IDENTIFY POTENTIAL WEAKNESSES IN YOUR SECURITY**

A prime example of this is the European Union's Directive on Data Protection which stipulates specific measures organizations in the EU member states must take to secure the personal data of their clients. Too often I see policies that someone has downloaded as a template from the Internet and simply replaced the name of the original organization with that of their own.

In some cases I have come across organizations based in Europe who have downloaded and implemented policies from the Internet which in fact contradict their legal obligations under the Data Protection Directive.

The other important elements of the information security policy are the security controls outlined in it. If your policy states that your organization will implement certain security controls then you should make sure that those controls can be implemented and are not simply aspirations. For example, if you password

policy states that all password must be of a certain length, complexity and longevity then you should make sure that this is implemented across all systems, applications and services.

To ensure that your information security program is operating as it should, the auditor will look for evidence to support your security goals. This can be in the form of logs, audit trails, interviewing users to ensure they are aware of the policies and records of training.

Having the evidence in place and working will, therefore, help you pass the audit as the auditor can verify everything is working as it should, or the auditor can identify gaps that you need to address before an attacker does. So, make sure that all systems have the appropriate logging and audit trails turned on and that you have documentary evidence to support any operational activities, such as change requests or training records for security awareness.

Some auditors will also test your security by means of a vulnerability assessment, a penetration test or a social engineering test.

This will, of course, depend on the technical skills of the auditor to not only to conduct the actual tests, but also to analyze and prioritize the findings in the context of your organization's business. This can provide a useful view of your defenses as it should replicate in some way how an attacker would examine your security.

### Making the auditor your friend

To get the most benefit out of any audits you should develop a strategy to engage with the auditor in a positive manner.

A critical element in this process is ensuring the auditor is properly qualified to conduct the audit. If it is an internal auditor, try to engage with him regularly to ensure he has the proper skills and background needed to conduct the audit.

If he lacks some of the needed skills, you should highlight this fact in a constructive manner before the audit begins so that it can be addressed.

You should at all times be open and honest with the auditor and encourage your team members to be the same.

A good auditor will be able to identify when he is being fooled, and if this should happen, it can then lead to an adversarial type of engagement which no-one enjoys. Being honest does not mean that you should blurt out all your secrets - it simply means when asked a question by the auditor be truthful in answering it.

You can also use the auditor to your advantage to help you get some initiatives approved by management. Very often management will take action based on the findings in an auditor's report, despite the fact that you may already have been recommending the same actions.

Getting your issues into the auditor's report can help get management to pay attention and allocate the necessary resources to address them.

Some may argue that the above approach may seem counter-intuitive. If your goal is to simply pass an audit and have a lot of ticks in a checkbox, then, yes, the above approach will not work especially well if your security program is not effective.

However, if your goal is to ensure the security of the systems and data under your responsibility then wouldn't you rather an auditor highlighted the weaknesses than read about them in the newspaper after you suffered a breach?

Brian Honan is the founder and head of Ireland's first Computer Emergency Response Team (CERT) team as well as owner of BH Consulting ([www.bhconsulting.ie](http://www.bhconsulting.ie)).



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

Send your idea to:  
[editor@insecuremag.com](mailto:editor@insecuremag.com)



# Are Hackers Finding a Way Into Your Network?

## GFI LANguard

Award-winning vulnerability management software

To lower the security risk you need GFI LANguard, a solution that provides network vulnerability scanning, patch management and auditing in one integrated package. This award-winning solution allows you to scan, detect, assess and rectify vulnerabilities on your network faster and more effectively.



WEB & MAIL SECURITY  
ARCHIVING & FAX  
NETWORKING & SECURITY

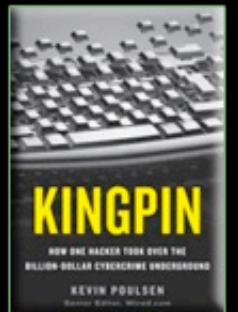
*Download your FREE trial version from [www.gfi.com/lannetscan/](http://www.gfi.com/lannetscan/)*

tel: +1 (888) 243-4329 | fax: +1 (919) 379-3402 | email: [ussales@gfi.com](mailto:ussales@gfi.com) | url: [www.gfi.com/lannetscan/](http://www.gfi.com/lannetscan/)



## Book review - Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground

by Zeljka Zorz



If you followed our site over the years, you had the opportunity to read a little about some of the protagonists of this book: Max Vision the creator of CardersMarket, Albert Gonzales - the TJX hacker, FBI agent Keith Mularski (a.k.a. MasterSplyntr) who was behind the DarkMarket shutdown, and others. This book will immerse you in their wheelings and dealings spanning a period of a number of years, and show you how their stories ended the way they did.

### About the author

In a previous life, Poulsen served five years in prison for hacking. He is now a senior editor at Wired.com and a contributor to Wired magazine. He oversees cybercrime, privacy, and political coverage for Wired.com and edits the Threat Level blog, which he founded in 2005.

### Inside the book

This is not your typical book about a heist that keeps you in suspense until the very end. You know how this book ends, so there are no surprises about that. But what preceded the

prison sentences? How did those hackers - Max Vision and Albert Gonzales in particular - manage to make such a great impact on our everyday lives and on how we view the state of (in)security of our financial information?

The story starts with Max Vision's background, childhood and teenage years, and shows us how his thirst for knowledge and amazing capability of solving problems made him what he is, but also how circumstances made him capable of compartmentalizing parts of his life.

This allowed him to reconcile the two parts of his personality - the ingenious white hat

hacker that wanted to help the authorities, and the resourceful black hat who time and time again sidestepped the white hat and his ethical ideas in order to make easy money and show his peers that he was above all of them.

Poulsen collected all the information for the book mostly from the actors themselves, in endless hours of interviews and email exchanges. Seemingly everyone who ever influenced Vision was given the opportunity to share their unique perspective on how he acted and their speculations about why he acted that way.

The book is written as a third-party account, focusing mostly on Vision and Mularski. I spent the first third of the book wishing that the story was told in first-person by Vision himself, but later realized that Poulsen had made the right choice. I particularly wanted to know the inner workings of Vision's mind as he saw it, but realized that an unbiased onlooker would manage to make more sense of it.

I believe that the author wanted to make Max Vision a sympathetic character, but I think that whether he comes across as such depends a lot on the reader. But, even if he doesn't, the book remains an enjoyable account. For those who prefer to root for the "good guys", there's always Agent Mularski's part of the story.

### Final thoughts

The writer would have been forgiven for a less skillful narrative given that the subject matter in itself is extremely engrossing - but, eschewing complicated explanations of the technology involved and covering the lives of some two dozen main "players", Poulsen entralls the user by depicting clearly their interpersonal dealings.

I would recommend the book to anyone and everyone, but especially to those people who know practically nothing about hacking and carding, since Kingpin offers a fascinating and detailed peek into a world whose existence most people aren't even aware of.

Zeljka Zorz is the News Editor at Help Net Security and (IN)SECURE Magazine.

## FRESH SECURITY NEWS

[www.twitter.com/helpnetsecurity](http://www.twitter.com/helpnetsecurity)





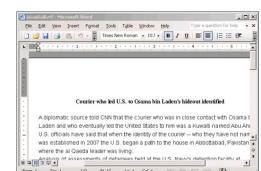
## Fake AV for mobile platform detected



Fake antivirus software for Windows crop up daily, but it seems that mobile users will also have to start being on the lookout for such scams. CA researchers have spotted a rogue AV solution misusing the well-known Kaspersky Lab name in order to trick Russian speaking users into paying up for bogus mobile protection.  
[\(www.net-security.org/malware\\_news.php?id=1706\)](http://www.net-security.org/malware_news.php?id=1706)

## RTF exploit hiding in bin Laden death-themed email

The email urges the recipient to download and open the attached Laden's Death.doc file. The file is, of course, crafted in such a way as to attempt to take advantage of a RTF Stack Buffer Overflow Vulnerability. If it succeeds, it exploits shellcode and drops a file named server.exe and executes it.  
[\(www.net-security.org/malware\\_news.php?id=1713\)](http://www.net-security.org/malware_news.php?id=1713)



## Multiplatform Java botnet spotted in the wild



Cross-platform malware is still a rare occurrence, so when it's detected, it usually attracts more attention than the malware engineered to affect only one particular platform. A recent one, detected by McAfee attacks both Windows and Mac OS users.  
[\(www.net-security.org/malware\\_news.php?id=1714\)](http://www.net-security.org/malware_news.php?id=1714)

## Fake AV spreading via Yahoo! Answers

From poisoned Google image search results to poisoned answers to legitimate questions on Q&A sites like Yahoo! Answers and public forums, malware peddlers are determined to use every possible way to spread their malicious payloads. Bkis researchers have recently spotted some new fake AV variants being distributed in the latter way, and have decided to investigate the matter. What they discovered is a number of questions answered with a variant of "Anyway, I think this will help you [LINK]". ([www.net-security.org/malware\\_news.php?id=1716](http://www.net-security.org/malware_news.php?id=1716))



## 400% increase in Android malware



Enterprise and consumer mobile devices are exposed to a record number of security threats, including a 400 percent increase in Android malware, as well as highly targeted Wi-Fi attacks, according to a report by Juniper Networks. With smartphones set to eclipse PCs as the preferred method of both personal and professional computing, cyber criminals have turned their attention to mobile devices. ([www.net-security.org/malware\\_news.php?id=1718](http://www.net-security.org/malware_news.php?id=1718))

## Explosive financial malware targets Windows

Trusteer identified Sunspot, a little known Windows malware platform that has been in circulation for some time, but was never previously recognized for its financial fraud capabilities. It is currently targeting North American financial institutions and has already achieved SpyEye and Zeus-like infection rates in some regions. ([www.net-security.org/malware\\_news.php?id=1719](http://www.net-security.org/malware_news.php?id=1719))



## Trojan paves way for rogue defragmenter



You might have heard about rogue AV solutions and scareware, but not many people have experienced a rogue defragmenter that hides files and (indirectly) asks money to return it. Symantec researchers warn about Fakefrag - a Trojan that moves all the files in the "All Users" folder to a temporary location and hides files in the "Current User" folder, hides icons and makes it look like they have been deleted, disables the Task Manager, and shows error messages that indicate that the hard disk might be failing. ([www.net-security.org/malware\\_news.php?id=1724](http://www.net-security.org/malware_news.php?id=1724))

## New Alureon variant improves on old evasion techniques

As time passed, the Alureon family of Trojans has been modified and managed to acquire rootkit capabilities and used a number of techniques to remain hidden from the user and AV solutions. This time, Microsoft researchers have spotted a variant that uses brute-force attacks against its encryption key to decrypt its components, making it even more difficult to spot and analyze, and for researchers to break down and understand. ([www.net-security.org/malware\\_news.php?id=1725](http://www.net-security.org/malware_news.php?id=1725))



## SpyEye Trojan attacks Verizon's online payment page



Trusteer discovered a configuration of the SpyEye Trojan targeting Verizon's online payment page and attempting to steal payment card information. Amit Klein, Trusteer's CTO explained that, "SpyEye uses a technique called HTML injection to modify the pages presented in the victim's browser, in this particular case the injected HTML is used to capture the following credit card related data." ([www.net-security.org/malware\\_news.php?id=1726](http://www.net-security.org/malware_news.php?id=1726))

## iPhone 5 spam run leads to malware

The date of the release of iPhone 5 is still unknown, but that doesn't stop malware peddlers from using it to lure in Apple fanatics. After all, didn't a recent research discover that "Apple was actually stimulating the same parts of the brain as religious imagery does in people of faith?" ([www.net-security.org/malware\\_news.php?id=1729](http://www.net-security.org/malware_news.php?id=1729))



## The progress of IT threats in 2010



Cyber criminals have capitalized on the recent growth in popularity of the Android mobile platform. Based on the number of new mobile malware signatures detected during this period, Kaspersky Lab's experts believe that the total volume of mobile malware in 2011 will be at least double that of 2010. That growth will be driven by the emergence of new methods of infecting users' computers.

([www.net-security.org/malware\\_news.php?id=1728](http://www.net-security.org/malware_news.php?id=1728))

## Apple acknowledges Mac Defender existence, gives removal instructions

Only days after the revelation of internal Apple documents that instructed AppleCare and Apple store employees not to acknowledge the existence of Mac Defender and not to offer help in removing it from infected computers when asked by the users, the company has posted a support document that explains the situation and offers advice on how to avoid installing this malware and how to remove it. ([www.net-security.org/malware\\_news.php?id=1731](http://www.net-security.org/malware_news.php?id=1731))



## The resurrection of the Mariposa botnet



When the news that the Spanish police arrested the three individuals suspected of running the Mariposa botnet was made public back in March 2010, it was generally thought that it might be the end of the line for one of the largest botnets ever reported on record. But, as we have learned from past experiences, a botnet is not completely destroyed until the last of its C&Cs is taken offline, and Mariposa's wasn't.

([www.net-security.org/malware\\_news.php?id=1733](http://www.net-security.org/malware_news.php?id=1733))

## Facebook users targeted with OS aware fake AV attack

Fake AV peddlers have begun using Facebook to drive traffic to the malicious site that tries to trick users into believing their computer is infected. With subject lines like "IMF boss Dominique Strauss-Kahn Exclusive Rape Video - Black lady under attack!" and "oh shit, one more really freaky video O\_O", they trick users into clicking on the link which does not take them to the desired destination but to a subdomain on newtubes.in, hosted on a Lithuanian server. ([www.net-security.org/malware\\_news.php?id=1736](http://www.net-security.org/malware_news.php?id=1736))



## The most active first quarter in malware history



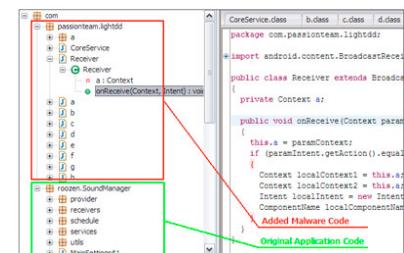
With six million unique samples of recorded malware, Q1 2011 was the most active first quarter in malware history, according to McAfee. The report revealed many of the trends that had a significant impact on the threat landscape, such as the takedown of the Rustock botnet, which resulted in spam remaining at its lowest levels since 2007, and confirmed that mobile malware is the new frontier of cybercrime.

([www.net-security.org/malware\\_news.php?id=1737](http://www.net-security.org/malware_news.php?id=1737))

## 26 trojanized apps pulled from Android Market

26 applications containing a variation of the DroidDream Trojan have been found on the official Android Market and are believed to have been downloaded by at least 30,000 users. Lookout researchers believe that they were created and uploaded by the same developers who were behind the original DroidDream onslaught back in March.

([www.net-security.org/malware\\_news.php?id=1738](http://www.net-security.org/malware_news.php?id=1738))



## Auto-dialing Trojans migrate to Android devices



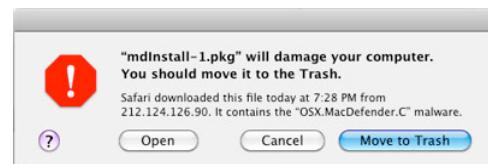
Auto-dialing malware has migrated from Symbian devices to Android ones, warns NetQin Mobile researchers. The Trojan has been spotted embedded in over 20 Android applications offered for download on various online forums, including Donkey Jump, Jungle Monkey, Gold Miner, Voice SMS, Drag Racing and others.

([www.net-security.org/malware\\_news.php?id=1739](http://www.net-security.org/malware_news.php?id=1739))

## Apple security update bypassed after 8 hours

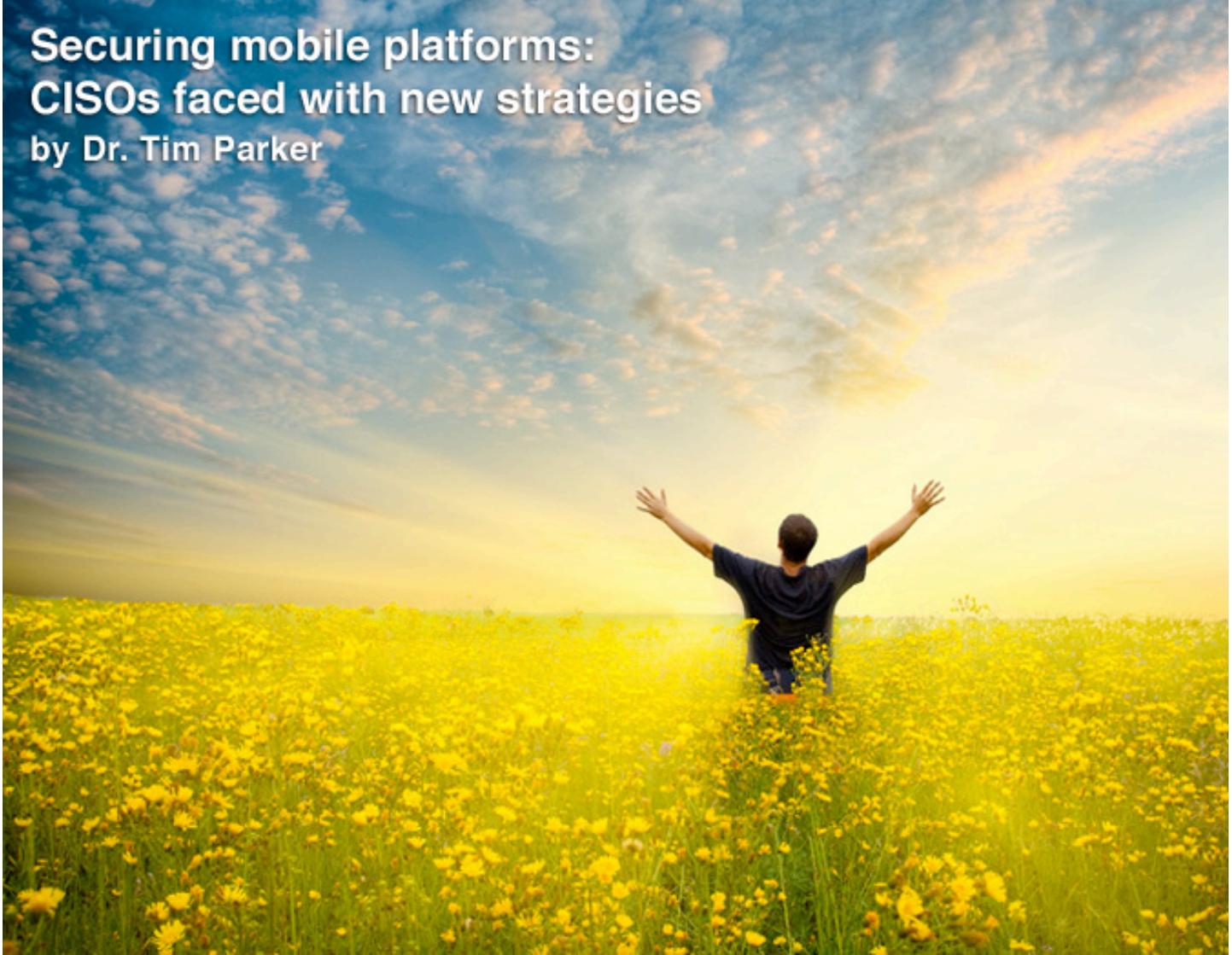
It took only eight hours for the malware developers behind the MacDefender and its variants to come up with a way to bypass the security update pushed out by Apple. According to Chester Wisniewski, a new variant of the malware has sprung up and it manages to infect the updated systems without asking for the administrative password. How does it manage to bypass the protection Apple put in place?

([www.net-security.org/malware\\_news.php?id=1740](http://www.net-security.org/malware_news.php?id=1740))



# Securing mobile platforms: CISOs faced with new strategies

by Dr. Tim Parker



**Five years ago, securing data on mobile devices - mainly laptops - came down to a few simple practices, today's mobile world is considerably different.**

Five years ago, securing data on mobile devices - mainly laptops - came down to a few simple practices: employing encryption on the computing platform to prevent unauthorized access in case of theft or loss; preventing data leakage through plug-in mass storage devices by using end-point security policies; and educating users about the importance of protecting the information on their devices through good security practices.

Corporate security practices protected the traditional employee laptop through the right balance of usability and security, policies to prevent misuse of sensitive data, and enforcement of mobile device best practices such as using VPNs.

Today's mobile world is considerably different. Not only has the generic corporate laptop given way to a mix of standard computing de-

vices used by employees, but the rise of smartphones, netbooks, and tablet devices have made it difficult for corporate policies to keep pace. When the executive layer is the trend-setter, sporting the latest version of the iPhone or iPad, mandating IT to keep up with these devices, limiting mobile device options to a select few approved devices is practically impossible.

The amount of data regularly accessed on smartphones and tablets exceeds that of the traditional laptop of five years ago by a wide margin, and many of these devices do not have built-in security mechanisms to prevent data from the device being transferred elsewhere. And since most of these mobile devices don't have strong passwords - if any! - protecting the data on the mobile device against access when lost or stolen can be difficult.

What's a corporate IT department, CISO, or security manager to do? Though one option is to ban certain devices, in my experience this can be very difficult to control and companies are often challenged to enforce these rules.

Keeping up with the leaps in technology we see every year, the best we can typically do is to manage the infrastructure, enforce some corporate security policies, and educate the end users about the issues. Fortunately, things are not entirely bleak: there are options available to help secure data on these mobile devices.

### Using VPNs

Almost all organizations have implemented VPNs to allow secure, authenticated access to corporate data repositories from remote devices. VPNs are designed to perform a simple task, and that is to authenticate the two endpoints and encrypt the data passing between the two. Where VPNs are useless is in protecting the data after it has been accessed.

Almost all mobile devices available today provide a VPN client capability of one form or another. So, someone using a mobile device and accessing their email and files on their corporate network can be sure the data between the server and agent is secure, but once it reaches the mobile device there is no standard protection mechanism available.

Typically, the agent converts the encrypted data stream to clear text when it is passed from the VPN agent to the mobile device's

application, such as an email client, file viewer, or software application.

These software packages do not enforce encryption. Worse, even if the application can be set to employ encryption there often remains a text version of the contents in the device's memory, accessible if the device can be queried quickly enough.

VPNs provide the first level of security for any corporate policy as they enforce authentication of the user. Accessing any data remotely should always be done with authentication, and a VPN is a convenient way to both enforce authentication and encrypt the data flow, but also allows the logging of sessions so that audit trails are available if needed.

For all the major mobile device operating systems available today, there is a VPN client offering from one or more of the VPN vendors.

What's more, some VPN servers allow the administrator to control the data that is conveyed through the VPN. While blocking email would be impractical, it is possible to create DMZs in the corporate network, which will not be available to remote devices.

The VPN can also be set to examine all incoming requests for data, and react accordingly. A stolen mobile device - used quickly and cleverly - can be used to crack open entire corporate networks through a VPN. Security administrators restrict access at the user level as a matter of course, so extending that practice to device-level is not a great leap in effort and can mitigate risks.

## SOME VPN SERVERS ALLOW THE ADMINISTRATOR TO CONTROL THE DATA THAT IS CONVEYED THROUGH THE VPN

### Encryption

While we are used to recommending the enforcing of encryption technologies on laptops - whether full-disk encryption solutions that embed in the device's Master Boot Record, or as a file/folder or volume encryption solution that encrypts only parts of the hard drive - there are very few organizations that mandate

encryption solutions for smartphones and tablets. Considering the fact that some of these smaller mobile devices are almost as powerful as a laptop, and that these devices are used more frequently for ad-hoc access to email and files, it is surprising how few mobile devices have any encryption policy enforced on them.

Availability of encryption is dependent on the actual device and intended usage.

Despite their popularity with corporate employees, Apple's iPhones and iPads do not have the same level of security available to them as the more corporate-oriented products like the BlackBerry. This is simply a reflection of the intended target market: Apple aims squarely at the consumer and not the corporate user, while BlackBerry has the opposite demographic.

Simply put, there is no universally accepted encryption product for the Apple devices that passively protects all data stored on the device. A password can be applied to the iPad or iPhone on the whole, and there are apps that provide encrypted folders, but full disk encryp-

tion for these products is still an immature market. BlackBerry, Android, and S60 (Symbian) devices all have more robust encryption solutions available and can be managed if a mobile device management solution is deployed in the organization. For all three platforms, there are a number of products, ranging in capabilities and pricing, that allow for security of information on these mobile devices.

When an encryption solution for mobile devices is available, it should be mandated and corporately managed to ensure it is used to protect information. Encryption coupled with VPNs allow for end-to-end data protection, at least while the data is on the mobile device. There's still the possibility of data leakage through emails or copying files.

## A NO-BRAINER SOLUTION FOR MANAGING MOBILE DEVICES IS THE ABILITY TO REACH OUT IMMEDIATELY AND UNOBTRUSIVELY TO A LOST OR STOLEN DEVICE IN ORDER TO DELETE FILES OR LOCK THE DEVICE

### Remote data deletion

A no-brainer solution for managing mobile devices is the ability to reach out immediately and unobtrusively to a lost or stolen device in order to delete files or lock the device. There are a wide number of solutions on the market, all with different features and capabilities, as well as differing device support, to allow a corporate security manager to specify a particular device and issue a command that wipes some or all of the device, or locks the device from further use.

And, because most of the mobile devices on the market today provide support for SMS access, these commands can take effect immediately.

Some mobile device management software applications add even more features, such as the ability to surreptitiously access the remote device and perform forensics on it, recover files remotely, or activate tracking capabilities such as GPS reporting or using the built-in camera.

These additional capabilities not only allow corporations to manage the data, but also track and recover the actual device. Audit logs recovered from lost or stolen mobile devices can immediately give a sense of the gravity of a data loss scenario, something critical to proper reactions to the loss.

The downside to these corporate management applications is that each phone needs to be registered with the application.

While it is practically impossible to dictate what devices an employee will use these days, you can enforce a policy that all devices that access corporate email or network resources must be registered with the management software. Most users will see the reason for this registration and cooperate.

### Bring your own device: Control software

While "approved" corporate software loads were common with laptops, they are hard to enforce with personal mobile devices as well as those supplied by the corporation. Having a set of policies that states "no games"

on iPhones and iPads is a surefire way of having those policies broken immediately. Instead, educating the end user about the applications available to them on any platform which can be considered security risks can help mitigate - but not eliminate - the risks of malware loads.

Curiously, one of the most often missed security breaches via mobile devices comes not from theft, but from Bluetooth surfing. When Bluetooth is active, a hacker can access the device and all of its software completely unbeknownst to the owner of the device.

Sounds farfetched? Next time you're in a coffee shop have a Bluetooth sniffer check out all

the wide-open or default password Bluetooth receivers.

By design, most mobile devices have Bluetooth active all the time, and all use default passwords. Using a laptop, a hacker can access a mobile device still clipped to the owner's belt, trigger VPN or other software, and access corporate networks.

Educating the user on the risks, recommending Bluetooth be turned off when not in use, and pushing for password enforcement policies for Bluetooth devices is critical to managing this exploit.

## ONE OF THE MOST OFTEN MISSED SECURITY BREACHES VIA MOBILE DEVICES COMES NOT FROM THEFT, BUT FROM BLUETOOTH SURFING

### Best practices

Totally securing mobile devices is not practical in today's world, where any employee can buy the latest and greatest mobile device on the market and access his corporate email and network with just a few keystrokes. However, employing a few simple precautions, such as VPNs and encryption, can make the process safer without making the user's life miserable.

As encryption solutions for mobile devices become more prevalent, recommending these solutions for all employee devices will also become more common.

Educating employees about common risks, without being alarmist, will help raise aware-

ness. Finally, employing a reliable and flexible mobile device management solution, along with mandatory registration for any device accessing corporate resources, provides a way to not just control but also monitor and mitigate data leakages.

Mobile devices are now more commonly used than desktop computers, and while the venerable laptop is still used in corporate situations, smart mobile devices like tablets are quickly overtaking laptops in market usage.

Corporations have to adapt to this change quickly, but fortunately this is not an impossible task.

Dr. Tim Parker is the vice president of research and development for Absolute Software ([www.absolute.com](http://www.absolute.com)). He manages the ongoing innovation and new feature development for all Absolute products. Dr. Parker brings over 15 years of experience in R&D and CTO roles, including positions at CTO of TMA Solutions, vice president of development for Computer Sciences Corporation, vice president of development for First Consulting Group and senior engineering roles at other Fortune 100 companies. Dr. Parker has authored over 50 books and 3,500 articles on computer science and is a Six Sigma Master Black Belt.



# 2011

BARCELONA 

*The anti-malware event of the year*

5-7 October 2011 Barcelona, Spain

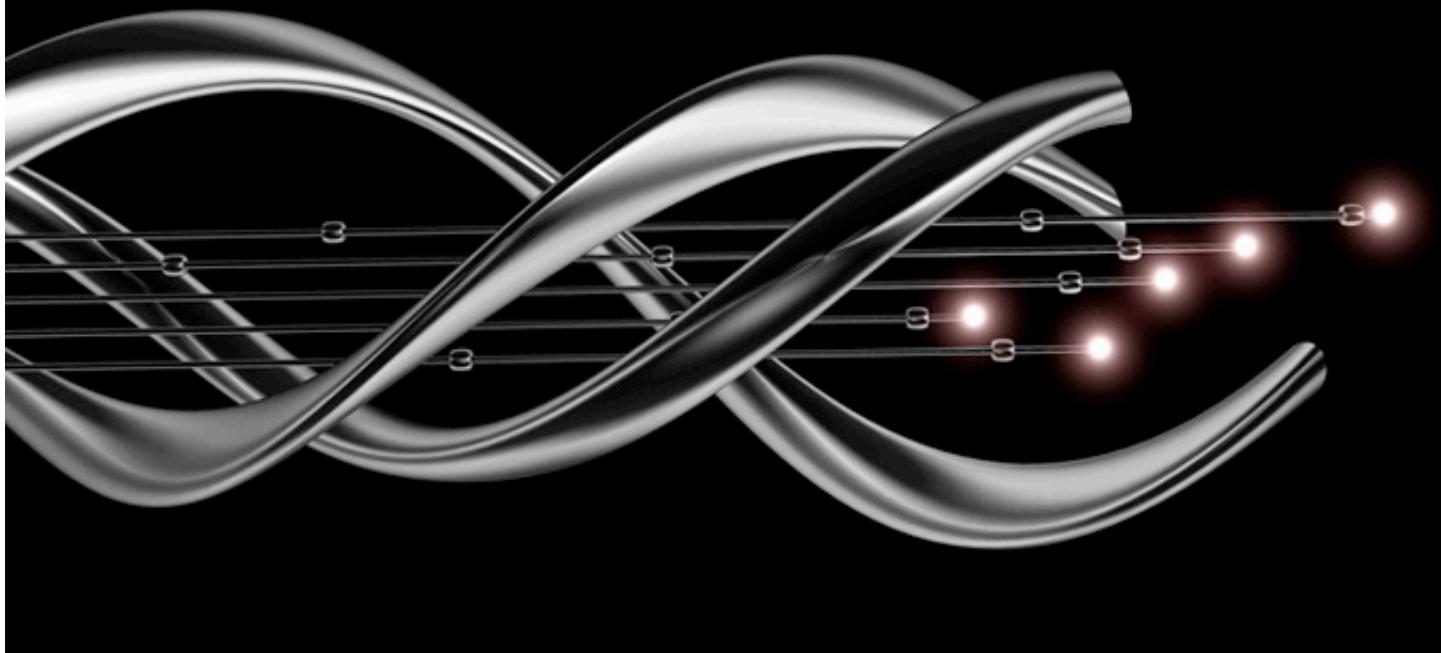
- Three full days of presentations by world-leading anti-malware and anti-spam experts
- Botnets
- Rogue AV
- Mobile threats
- Mac threats
- Stealth attacks
- Snowshoe spam
- Targeted attacks
- Last-minute technical presentations
- Networking opportunities
- Full programme at [www.virusbtn.com](http://www.virusbtn.com)

**EARLY BIRD RATES APPLY UNTIL 15 JUNE**

**REGISTER NOW AT [WWW.VIRUSBTN.COM](http://WWW.VIRUSBTN.COM)**

# Security needs to be unified, simplified and proactive

by Zeljka Zorz



IT security powerhouse Check Point is on a mission to make the management of security products unified and simplified, and nowhere has that message been more clear than at its annual conference in Barcelona, where some 1,100 attendees - and (IN)SECURE Magazine among them - had the opportunity to see and hear everything they wanted to know about the company.

Established eighteen years ago, the company has made history with its first product - simply named FireWall-1 - which was the first commercially available software firewall to use stateful inspection.

Because of this, they were - and are - known as "The Firewall Company", but after it executed a number of acquisitions (ZoneLabs and the Nokia Security Appliances division - among others) that allowed it to offer software and hardware for data, network and endpoint security, and security management, its CEO hopes that people will come to know it as a company that offers security on many fronts.

Gil Shwed, Check Point's co-founder and CEO, has put a lot on emphasis on the fact that the company's approach to security is based on an effective and seamless integration of policy, people and enforcement. They call it 3D security, and they stress that users

need to be engaged and educated on security policy enforcement.

As I was able to see, a lot of their solutions include education directly into the program, which usually takes the form of warnings popping up when users are about to do something that could endanger the enterprise - for example, send out confidential data to a private email.

It is not enough just to say to the user that he can't do something, says Shwed. He argues that an explanation about why the alert has popped up is necessary, along with an elucidation of the implications of the attempted action, and an offered solution. "Users should be made to take ownership and responsibility for their actions," he says.

It is not a foolproof method, to be sure, but he insist that it helps inform users who don't yet

know what they are expected to do or not to do and makes malicious ones think twice about proceeding. The system also logs all these actions and/or attempts, leaving a mark



"Security today is a collection of many different technologies, many point solutions bought from different vendors. But that is no longer enough," he says. "Security is not just about technology, security should become a business process."

And why are people at the center of this vision? For Shwed, the answer is obvious - "They are the ones who use the technology, and they are the ones that usually make mistakes that lead to insecurity."

When talking about policy as the anchor of security, he insists that corporate policies must be simple, meaningful and usable. "And

that may help solve questions in the future or allow the company to react in time and prevent further damage caused by the action.



not too long. At Check Point, for example, every new user that joins the company must read some security material - which takes about half an hour - and before he can access the network, he must go through and answer correctly some 20 questions (online) in order to get access to the network," he says.

When it comes to enforcement, he believes that Check Point is on the right track with its software blade architecture.

IPS, DLP, mobile access, firewall, application control and more - all working within the same architecture, the same environment, managed from the same console.



He not only considers it more effective and easier to manage, but cheaper, too. Instead of 15-20 point solutions on its network, an enterprise can have five and add software blades



as the need arises, paying for the additional capability less than for additional appliances that do only one thing.

Both Shwed and John Vecchi, Check Point's head of global product marketing, point out that the time for proactive security has definitely come, and the 3D security vision that they began implementing with the introduction of Check Point R75 network security suite in February is a way to change an enterprise's approach to security, make it proactive.

Comparing the state of security today to a picket fence - a range of point products with gaping holes between them - Vecchi says that the biggest challenge today is managing the complexity of security. Instead of dealing with threats, enterprises are struggling to manage and coordinate the bevy of point products they have, and to solve that problem, security unification is crucial.

Having listened to a number of presentations of various Check Point technologies and solu-

tions, I couldn't help but be a little impressed with how the company practices what it preaches.

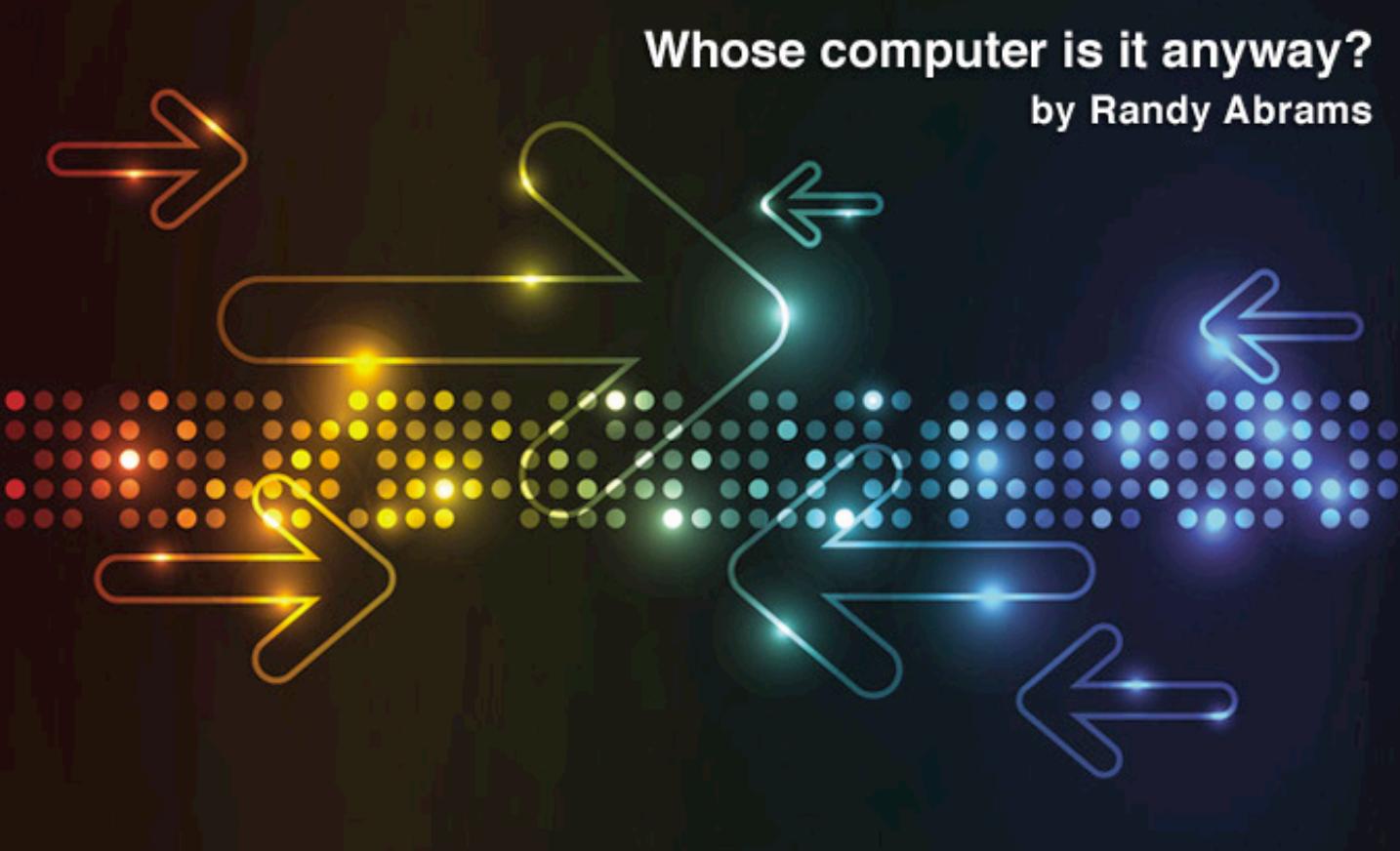
Theory is all good and well, but when you are given examples of how those technologies work in an actual enterprise environment - Check Point's enterprise environment - it's easy to see where their confidence comes from.

Sharing some of the results of the latest NSS Labs tests of IPS and firewall solutions, Shwed proudly says that their firewall is the only one that passed the test, and that, for the first time, an integrated IPS solution proved to be more effective than a dedicated one - whether when out-of-the-box or fine-tuned. "It shows you that when we speak about security is not just words - it's real."

---

Zeljka Zorz is the News Editor for Help Net Security and (IN)SECURE Magazine.

An advertisement for net-security.org/infosecuritynews.php. The background features a blue and green abstract design with a large, ornate padlock in the foreground. The text reads: "DAILY OR WEEKLY SECURITY NEWS RIGHT IN YOUR INBOX" in large white letters, and "net-security.org/infosecuritynews.php" in yellow. A small URL "www.insecuremag.com" is at the bottom left, and the page number "54" is at the bottom right.



# Whose computer is it anyway?

by Randy Abrams

This article explores employees' usage of company assets for personal use, and the challenge employers face with balancing potential cyber threats that may arise from lax workplace security policies and the morale problems that can result when companies adopt stricter regulations.

In February 2011 we detected an interesting download attempt: a customer was trying to download some software through the Microsoft Update Catalog and it triggered our alarms. But, what's interesting about it is that it wasn't a false positive.

It is actually extremely rare to find infected software available for download from Microsoft. The user in question was trying to download software for the Energizer Duo - a charger that allows one to charge NiMH rechargeable batteries using AC or USB sources.

The original software for this device was found to have a backdoor built into one of the drivers - the incident is detailed in US CERT Vulnerability Note VU#154421 ([www.kb.cert.org/vuls/id/154421](http://www.kb.cert.org/vuls/id/154421)). In order for the software to function properly (or improperly) it had to have a valid Microsoft digital signature. Microsoft, knowing the reputation of the Energizer (AKA Eveready) Corporation, as well as having run the files through the batter-

ies of antivirus products which detected no known threats or heuristic behavioral threats, signed the files.

The detection on the Microsoft Update Catalog in February 2011 was not the actual vulnerable file. That file had been pulled, but some of the other software tried to call the vulnerable DLL, so if an attacker were able to get the DLL onto a system, the other software would again enable the back door.

To properly speculate on how and why the software was shipped with such a backdoor requires a bar, plenty of beer, and a bunch of geeks. However, it could have easily been an incompetent programmer who thought he was writing some cool update functionality.

People who like to ascribe more sinister motivations to the event might conclude that this was a targeted attack. As a targeted attack it really could be quite perfect. The attacker sends the victim a charger for any made up reason and the victim is none the wiser.

I actually received one of these chargers from a relative. I couldn't understand why I should install software in order to charge batteries, but a lot of people believe they must install software if the hardware came with software so they do not give it a second thought.

This incident draws attention to an ongoing debate about the appropriate use of corporate resources. Should employees be allowed to install software of their choosing on a company asset?

The Energizer Duo incident is an extreme example. However, there are thousands of programs with vulnerabilities that are not intentional and can lead to compromise if not patched. While the thought of a targeted attack against a smaller business may seem

far-fetched, there are a number of factors that may trigger such an attack.

Not all attacks are financially driven. In one case a hospital worker installed a malicious program on her work computer when tricked by a stalking ex-boyfriend into installing the software. As a result, confidential hospital records were compromised.

There are multiple schools of thought on the issue of whether or not employees should be allowed to install software of their choosing on their work computers, especially when it is a laptop and they travel extensively. Let's start with the draconian mandate that includes policy and technology to prevent employees from installing anything but pre-approved software on their computers.

## EMPLOYEES GENERALLY DO NOT FEEL TRUSTED IN ENVIRONMENTS WHERE THEY CAN'T CONTROL THEIR OWN COMPUTER.

Fundamentally, we are talking about a white-listing approach. While not perfect, it is probably the safest approach from a simplistic security model.

But, whitelisting software is a task that requires a lot of time and work. When a program is updated to patch a security vulnerability, the patch must wait until it has been whitelisted.

Most companies that employ this approach have an exception process whereby an employee can request that a software package is added to the whitelist. Had an employee asked for an exemption for the Energizer Duo product, and explained that he or she travels on company business extensively and desires the functionality of the software package, it is probable that many organizations would have approved the package.

In addition to the security benefits of whitelisting, there are also performance benefits. Less software means less of conflicts and something to go wrong, which can make things quite a bit easier for IT administrators.

The downside to the whitelisting approach is a decrease in employee morale and – potentially - innovation. Employees generally do not feel trusted in environments where they can't control their own computer. The assurances that the reason is for the protection of the company and the employee are rarely seen as truly being for the protection of the employee at all.

Depending upon the environment and the particular job, a lack of access to specific web sites and programs may significantly decrease the effectiveness of an employee or an entire department. Finally, the whitelisting approach must be recognized as having its deficiencies and must be implemented in a defense in depth approach to security.

On the other side of the scale there are companies - such as Microsoft - who allow their employees to install software and visit most websites. The approach Microsoft takes results in an atmosphere where employees are able to explore new technologies and approaches to solve problems.

Employees feel more trusted (despite knowing that there is monitoring as well) and are happier than they would be if things like Facebook and YouTube were off limits. The approach comes with considerable risk and malware is no stranger to the internal Microsoft network.

Microsoft seems to feel that their approach is working for them and their employees, and arguably, despite some pretty high stress levels at Microsoft, the situation would be worse with an autocratic approach to corporate resources.

A different approach that some companies have begun taking is to give the employees a budget for a computer. The employee is responsible for the computer. The employees choose their security program, they choose their applications, and they choose which web sites to visit.

Regardless of the approach taken, the goal is to protect all that is of value while not spending more than the value of the data trying to protect it. The advent of the Internet and mobile technologies has made data security a far more daunting challenge than it once was.

Recognizing the emerging realities of the changing landscape, in 2003 a group of corporate CISOs got together and formed the Jericho Forum ([www.opengroup.org/jericho](http://www.opengroup.org/jericho)). The forum advocates using technologies in ways that are cognizant of the realities of today's computing environment. That said, it would be foolish to believe that one size fits all, but the approaches advocated by the forum definitely must be considered by any IT manager or they are simply negligent in their fact finding.

The Jericho Forum talks a lot about de-perimeterization, and this is an important concept to grasp. Even if your workforce has no mobile users, if they have Internet access, then an attacker can breach the perimeter. In the security model that the Jericho Forum puts forth, it is a given, in many instances, that the user may be installing software on

their computer, but the idea is that the data is still protected from user error.

Once the security of data has been removed from the equation, the argument as to whether or not you allow employees to choose to install software becomes a bit more difficult. Factors such as productivity can be argued either way, however employee retention is more likely to be adversely affected in a shop where machines are tightly locked down.

There are strategies to mitigate morale hits. A clear explanation of the reasons for the policies and procedures is a good starting point. In some environments, a few computers that employees can use for personal purposes during break times may help alleviate negative consequences of draconian policies.

The more difficult issue is corporate risk. If an employee has pirated software on a corporate resource it can be a huge liability for the corporation. Perhaps this is a part of why some companies have gone the route of an allowance for the employee to buy their own laptop and required software.

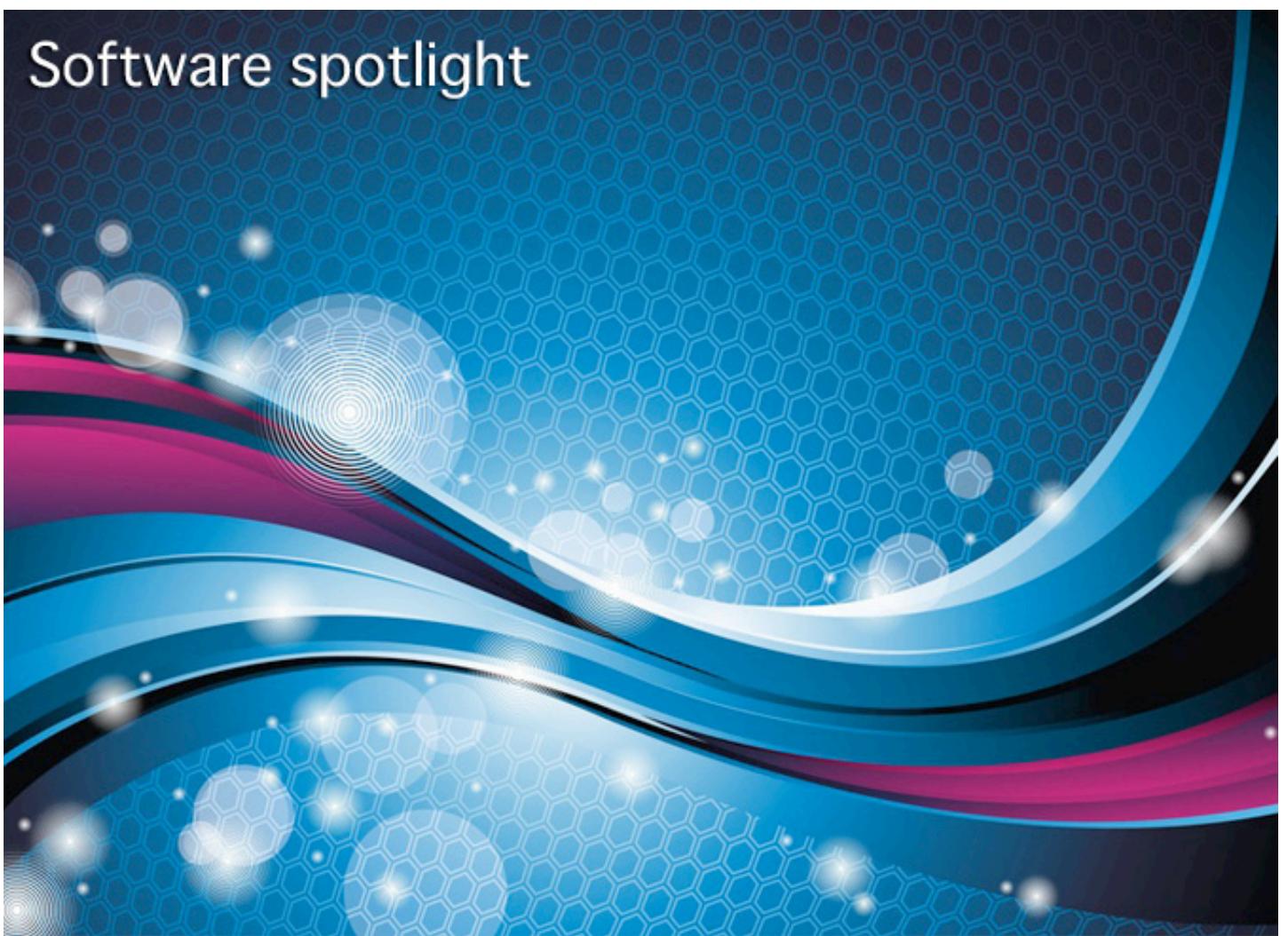
Employee morale is the most difficult aspect to measure and perhaps the most important metric at the same time. Morale affects productivity, and more than just that. If you are in an information field, then you probably need some pretty smart people. These people often attract other smart people.

If you are repelling intellectual talent, how long do you think you will be successful in your business? How effective do you think you really will be in attracting and retaining talent?

The question of whether or not employees can install software of their choosing is not an easy one to answer. There is not one right answer for all businesses. There are examples of successful business on both sides of the fence. As is the case with all security decisions, it comes down to a risk management equation that is specific to your environment.

Randy Abrams is the Director of Technical Education, Cyber Threat Analysis Center, ESET North America ([www.eset.com](http://www.eset.com)).

# Software spotlight



## Malwarebytes Anti-Malware

([www.net-security.org/software.php?id=757](http://www.net-security.org/software.php?id=757))

Malwarebytes' Anti-Malware is an anti-malware application that thoroughly removes advanced malware and spyware. It's fast and effective, capable of recognizing malicious applications and distinguishing between them and false positives. It can scan multiple drives and remove locked files.

## Password Manager XP

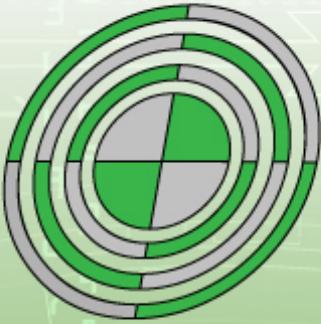
([www.net-security.org/software.php?id=70](http://www.net-security.org/software.php?id=70))

Password Manager XP is a program that will help you systematize secret information. You will forget about all your headaches which were caused by loss of passwords, access codes and other sensitive information. You'll be able to store all your logins, passwords, PIN codes, credit card numbers and their access codes, and any other confidential information in one place.

## John the Ripper

([www.net-security.org/software.php?id=11](http://www.net-security.org/software.php?id=11))

John the Ripper is a fast password cracker. Its primary purpose is to detect weak Unix passwords. Besides several crypt password hash types most commonly found on various Unix flavors, supported out of the box are Kerberos AFS and Windows NT/2000/XP LM hashes, plus several more with contributed patches.



# SOURCE Barcelona 2011

Security You Can Use

**Trainings: November 1st-2nd, 2011**  
**Conference: November 3rd-4th, 2011**

Museu Nacional D'art de Catalunya, Barcelona, Spain

for more information please visit [www.sourceconference.com](http://www.sourceconference.com)

## Training Spotlight

### Lessons In Mobile Penetration Testing

Jon Oberheide - Duo Security  
Zach Lanier - Intrepidus Group

### Grepping for Gold

Xavier Mertens - C-CURE  
Wim Remes - Ernst & Young

## Conference Spotlight

Exclusive Access To Speakers

Networking Events

Advanced Session Topics

Practical Real-World Solutions

Intimate Environment

Learn From Industry Leaders



## 10 golden rules of information security

by Gideon T. Rasmussen

Establishing an information security program is a complex undertaking. It is easy to get lost in the details and neglect a critical component of the program. This article focuses on high-level guidelines or tenets. Its framework can also be used to provide an overview for senior management and employees.

**1. Focus on the information security program as a whole.** Program design should start with a control framework such as ISO 27002. Frameworks are essentially information security best practices. Layer on compliance requirements and add safeguards as the outcome of risk assessments. Compliance considerations include laws, regulations and contractual obligations. Ask your attorney for support. Program documentation should include policies, standards and guidelines.

Document security safeguards in a control baseline. Refer to NIST SP 800-53 as an example. It has high, moderate and low impact control annexes. Ensure compensating controls meet the intent and rigor of the original requirement. Evaluate processes and procedures by the COBIT maturity model and improve the program over time.

**2. Identify and manage risk.** Compliance with security regulations and frameworks is meant to address risk from a generic perspective. It is also necessary to consider risk to your specific business and operations. Consider a retail scenario where competitors are

suffering payment card breaches by a sophisticated threat. Management may decide to implement an associated countermeasure given the threat, vulnerability and potential business impact. Do not try to eliminate risk entirely.

Adapt your risk model as the threat landscape changes to do more with the same resources. Refer to NIST SP 800-30 and the ISACA Risk IT Framework for additional guidance.

**3. Follow the data.** When asked why he robbed banks, Willie Sutton's response was, "Because that's where the money is." Protecting assets starts with knowing where they are. Document where data flows throughout the company and when it is shared with third parties. Maintain an inventory of applications, databases and related systems, with mapping to sensitive data and intellectual property. Discover unstructured data through automated scans. Classify data by confidentiality, integrity and availability ratings. Refer to NIST SP 800-60 for sample ratings and impact definitions. Label consumer records with home state and country to enable compliance with privacy regulations.

**4. Apply defense-in-depth measures.** This tenet addresses adversaries and the insider threat, inclusive of human error and social engineering. Ensure appropriate controls are in place to protect data from disclosure or modification as it flows internally and when shared with third parties. Layer on a comprehensive blend of preventive, corrective and detective controls based upon risk.

For highly sensitive intellectual property or confidential information, consider strict controls such as air gaps and two-person integrity. Ensure security language is included in contracts and cannot be deleted in negotiations without risk evaluation and sign off. Design applications to adhere to consumer data sharing preferences and website privacy statements.

**5. Align with business products, services and objectives.** This is necessary to accomplish the goals of information security and to stay relevant within the company. Expand beyond merely protecting what is mandated,

such as credit card and social security numbers. Learn how the business functions, including how revenue is generated. Align recommendations for security initiatives with threats to strategic business objectives. Protect the intellectual property of the company.

Understand risk to strategic objectives, how that is quantified, monitored and mitigated. Consider embedding risk and security professionals within lines of business.

## **6. Anticipate, be innovative and adapt.**

Threats, vulnerabilities and business practices evolve over time. Focus personnel and budget where there is the greatest return on risk mitigation. Establish a function to track security advisories, research compromise trends and network with the security community from a threat perspective.

When an advanced persistent threat is identified, take it seriously. Establish a process to accept, mitigate or transition identified risks.

## **For highly sensitive intellectual property or confidential information, consider strict controls such as air gaps and two-person integrity.**

**7. Establish a culture of security.** Reinforce policy and educate personnel about threats with a security awareness program. Start by asking a senior executive to send a message explaining the company has a low risk tolerance and everyone is responsible for security. Require all personnel to sign-off on security policies. Conduct training upon date of hire and repeat annually.

Be mindful of your audience. Communicate in layman's terms, avoiding unnecessary use of technical terms. Speak in terms of business risk versus fear, uncertainty and doubt with no context. Include a testing component to evaluate training comprehension. Find ways to keep security topics front-of-mind throughout the year such as awareness tips sent by e-mail. Document a training plan by audience.

**8. Plan for a rainy day.** Low probability events occur over the course of time. Ensure

critical dependencies are accounted for within business continuity and disaster recovery programs. Establish an incident response team, including preparation for denial of service attacks. In the event of a compromise, preserve forensic evidence and comply with applicable data breach notification laws.

Prepare to present details of the security program in court and how it provides "reasonable" protections. Test business continuity, disaster recovery and incident response at least annually.

**9. Trust but verify.** Internal audit should consider control frameworks and industry best practices when determining the effectiveness of the information security program. Evaluate compliance with laws, regulations and contractual obligations. Follow data flow to ensure operational risk is appropriately identified and mitigated.

Conduct penetration tests of hosts, networks, applications and physical security controls. Use social engineering assessments to evaluate the security awareness program. Conduct assessments of third parties to ensure they adhere to company standards.

Evaluate processes with Failure Mode and Effects Analysis (FMEA). Establish a quality assurance program to address variation and defects within critical process steps.

**10. Tell the story and exert influence.** Report risk and compliance in a manner that it can be aggregated up through the company to provide an enterprise view. Include drill down capabilities to findings-level detail to facilitate remediation.

Use metrics to defend the program when annual budgetary requests are due. Influence starts with establishing professional relationships with business executives. Information security and business operations have the same objectives, to ensure products and services are consistently delivered.

Develop routines to ensure risk issues are clearly communicated. Send formal risk escalation reports and invite operations, risk and compliance contacts to meetings to discuss them. Track open issues in a risk registry. Document a communications plan by audience.

Business executives consider the cost of the security program with a focus on percentage of the operating budget. They are likely to ask what will be the consequence if a given requirement is not met. The answer must be framed in terms of compliance and operational risk, within a business case. Consider strategic and reputational risk as well.

For those of you reporting to a Chief Security Officer, realize that s/he has a finite budget and looks to mitigate as much risk as possible. Align your programs and budget requests with business risk mitigation clearly identified.

Follow the data, follow the risk. An ounce of prevention is worth a pound of cure.

---

Gideon T. Rasmussen ([www.gideonrasmussen.com](http://www.gideonrasmussen.com)), CISSP, CISA, CISM, CIPP is a Charlotte-based Information Security Manager with over 15 years experience in corporate and military organizations. The opinions expressed here are those of Gideon Rasmussen and do not necessarily represent those of his current or past employers.



**SUBSCRIBE TO (IN)SECURE MAGAZINE**

**[www.insecuremag.com](http://www.insecuremag.com)**



## The token is dead

by Andrew Kemshall

“The stars have aligned” is a phrase often used, but in 2011 it is the technology that has come together to hammer the final nail into the physical token’s coffin. The cynical among you would argue that this statement has been made before and yes, I concede that tokens have survived and are still prevalent. How is this year different?

Before we examine the evidence, let’s take a quick trip down memory lane:

- During the ‘70s tape cassettes were the medium of the day
- In the ‘80s VHS cassettes reigned supreme
- The ‘90s saw the introduction of DVDs
- And the millennium brought with it the BluRay Disc.

What does this demonstrate? That nothing lasts forever and two factor authentication isn’t any different. It too has experienced advancements, from the original complex and time consuming challenge tokens of the ‘70s to the time synchronized tokens of the ‘80s.

Thirty years later, and it’s as if time has stood still - the majority of physical tokens still rely on this out-dated technology. But, the tide is turning.

### If it’s not broken, why fix it?

True, there are few technologies that have withstood the test of time as well as physical tokens have, but that’s not to say they’re perfect.

The fact is that there are a number of issues with their utilization, some of which have been around since their introduction thirty years ago.

It’s time to present the evidence:

## SMS isn't new so what changed?

In 2000, the number of mobile phones started to increase sharply. In fact, according to gsmworld.com, there are over 4,947,400,000 GSM and 3GSM connections globally, with the figure steadily increasing every second. By the time you're reading this it wouldn't surprise me if that figure had topped 5,000,000,000.

By utilizing SMS technology, any mobile phone can be used as an authentication token. A passcode is sent to a user's device, eliminating the need for a physical token.

Other enhancements - including the option of reusing a user's existing password instead of remembering a separate PIN – are tied to its use. However, SMS technology alone isn't the answer as there have been instances when it

has proved to be unreliable. In a small number of cases, estimated at 4%, SMS messages can take longer than 1 minute to get through.

Other issues could be the network is temporarily suspended or the user may be in a signal dead spot, such as the basement of a building or computer room. This is an argument that has saved physical tokens in the past, but it can no longer stave off the Grim Reaper's scythe.

With the advent of pre-loaded codes, mobile phones are able to hurdle this final barrier. As soon as a user enters their authentication code, the system automatically forwards a new SMS message, overwriting the code in an existing message ready for the next session.

## By utilizing SMS technology, any mobile phone can be used as an authentication token

### Invested far too much in tokens to change?

It's always going to be hard to justify writing off an investment. Yet, it is the sensible thing to do if you don't want to continue hemorrhaging money supporting an old technology:

- For starters, it is estimated that moving to SMS authentication will reduce ongoing running costs by 40 – 60%! This is substantiated by Gartner with its belief that "SMS OTP approaches the security of a dedicated hardware token, but at a lower cost and with higher convenience."

- Due to their lifespan, you'll have to replace all your tokens within the next three to five years. With an SMS system, the majority of your users will already have a mobile phone. If for any reason a user does not have a mobile phone, a voice text can be sent instead to a number stored on the system.

- There is the argument that people do misplace their mobile phones but this is also true for physical tokens. It is people's attachment to their mobile that is the differentiator. As research by YouGov revealed, a third of the population would notice they'd lost their mobile phone within 15 minutes and 60% would within the hour. The emotional attachment to a physical token can mean its loss isn't discovered until the user actually needs to use it which could be hours, or even days, later!

- Using automation, an SMS system can be set up in a day (an average of 300 users per minute) instead of six months. The existing employee database is used with mobile numbers automatically identified. For records where a number is not listed, an email is automatically sent requesting the user to self-enroll.

- It can offer substantial benefits for organizations looking to reduce their carbon footprint. It would require 1673 trees to offset the emissions created in deploying 3000 tokens.

Andrew Kemshall is the co-founder of SecurEnvoy ([www.securenvoy.com](http://www.securenvoy.com)).



## Security videos

### Social media threats and targeted attacks

(<http://www.net-security.org/article.php?id=1585>)

In this video, Alexandru Catalin Cosoi, the Head of Online Threats Lab at BitDefender, talks about the new breed of social media threats and sophisticated targeted attacks.

Cosoi estimates that during this year we'll see a decrease of classical malware such as spam and file infectors. Cyber criminals will increasingly take advantage of social networking platforms like Facebook, and attack more using malicious applications.

---

### Securing the virtual environment

(<http://www.net-security.org/article.php?id=1600>)

In this video, Dimitri McKay, Security Architect at LogLogic, talks about vulnerabilities and the security challenges surrounding virtual environments: hyperjacking, VM hopping and VM theft.

---

### How secure is your browser?

(<http://www.net-security.org/article.php?id=1580>)

Qualys CTO Wolfgang Kandek talks about research which clearly shows that browser security is alarmingly bad. Browsers and plug-ins are frequently outdated and easily attacked.

The data was gathered by Browser Check, a free service which enables the end user to check the state of security of the browser. The results point the user to software updates that resolve security issues and offer recommendations in case a fix is not available.

Even though browser patching is very established and user awareness is growing, the basic data shows that roughly 70% of all BrowserCheck users were using a vulnerable browser.

## The fundamental failure of endpoint security

([www.net-security.org/article.php?id=1572](http://www.net-security.org/article.php?id=1572))

According to Stefan Frei, Research Analyst Director with Secunia, it's not the vulnerabilities in Microsoft's products we should worry about, but those in third-party software.

Even though the number of discovered vulnerabilities has slightly decreased in the last two years, the worrying fact is that 84 percent of all those found in 2010 can be exploited from a remote location, and that 69 percent are tied to third-party products that may or may not have a quality patching mechanism in place.

---

## Application security vulnerabilities

([www.net-security.org/article.php?id=1589](http://www.net-security.org/article.php?id=1589))

Rafal Los, Application Security Evangelist at HP Software, talks about application security vulnerabilities at the logic level.

The inner-workings of an application can only be seen through a combination of human input, static analysis, dynamic analysis and a new type of technology loosely termed run-time analysis - the type of 'deep inspection' that's required to truly see "inside" an application and determine how flaws relate, how they're exploited and where in the source code they can ultimately be fixed.

Building systems that really understand applications ultimately requires us to utilize our human brains and culminate information from technology, project requirements, developer interaction and simply 'using' the application by following use-cases.

Only through the collaborative approach of all these human and automated technologies can we start to build systems that are pseudo-intelligent and can perform the combinatory magic which allows iterating through millions or billions of combinations actions to determine negative variations.

This is no small feat - this problem has been worked on for well over a decade and only now through the bringing together of both static and dynamic analysis can we truly start to dig deep into a problem that has silently plagued application security for a very long time.

---





# DON'T MISS BEING PART OF INDIA'S LARGEST INFORMATION SECURITY CONFERENCE

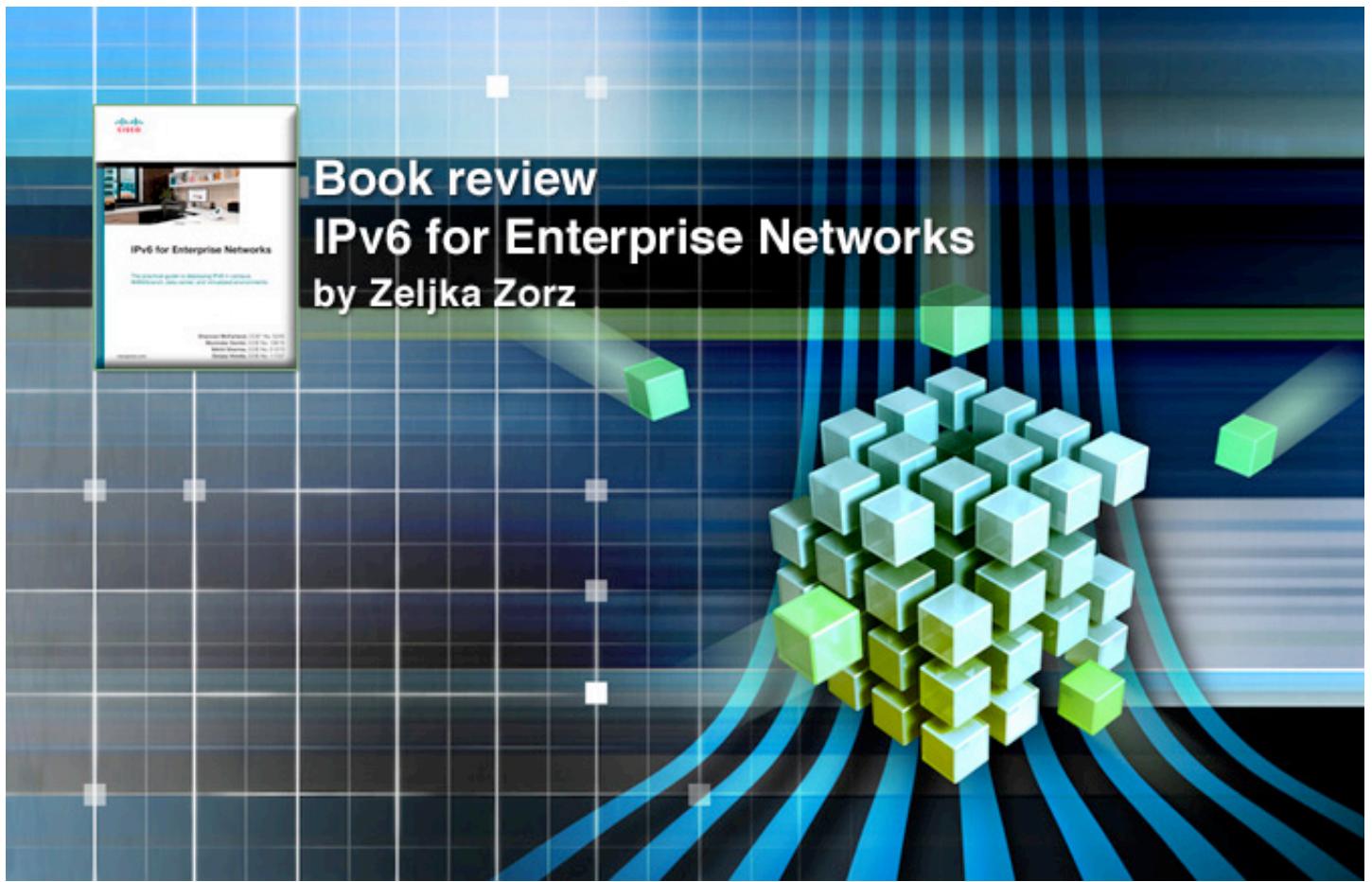
SEPTEMBER 6TH - 9TH 2011

**SECURITYBYTE**

CONFERENCE & WORKSHOPS

REGISTER AT [WWW.SECURITYBYTE.ORG](http://WWW.SECURITYBYTE.ORG)





## Book review IPv6 for Enterprise Networks by Zeljka Zorz

The February news that the last batch of IPv4 addresses has been distributed has resounded across the Internet as a final wake up call. It made everybody aware of the fact that IPv6 will very soon become the prevalent standard, and that the time has come to think about deploying it within the enterprise. This book explains why and most especially how to make that transition seamless.

### About the authors

Shannon McFarland is a Corporate Consulting Engineer for Cisco serving as a technical consultant for enterprise IPv6 deployment and data center design.

Muninder Sambi is a Product Line Manager for Cisco Catalyst 4500/4900 series platform, is a core member of the Cisco IPv6 development council.

Nikhil Sharma is a Technical Marketing Engineer at Cisco Systems.

Sanjay Hooda, a Technical Leader at Cisco, works with embedded systems.

### Inside the book

This book will not attempt to teach you about networking technologies and deployment - you're supposed to know that already. It is

also helpful if you have a general idea of what IPv6 means and which problems it aims to solve.

The book starts with a helpful chapter on the IPv6 market drivers and a number of frequently asked questions and, of course, answers about the technical benefits of the standard. If you already know all this, you can skip this chapter. And probably the next, too, because you're supposed to know about network design for various parts of the enterprise network and the various topologies.

IPv4 and IPv6 will probably coexist for quite some time yet, and here is your chance to learn about the mechanisms that will allow them to do it without creating problems for the users. Also very handy is a chapter on network services, that answers the question of how to use and configure multicast, QoS and routing with IPv6, by comparing the process to that in IPv4.

The chapter on planning and IPv6 development is a must - it tells you how to decide where to begin by doing some benefit, risks and cost analysis, and how to plan (and execute) a pilot phase of the deployment so that you can experiment addressing internally.

The remaining chapters deal with deploying IPv6 to the various modules that make a corporate network: campus networks and virtualized networks, WAN/branch networks and remote access VPN, and the data center.

These chapters are extremely technical and make the most valuable part of the book. They effectively translate all those IPv6 concepts into usable configurations complete with a list of benefits and drawbacks of each of the topologies presented.

Each of these modules have their specific idiosyncrasies, and each is thoroughly examined. In the end, you will be able to learn how to manage and monitor the modules effectively with a string of applications and tools helpfully presented here.

### Final thoughts

IPv6 for Enterprise Networks is an easy-to-read book and very thorough in its explanations. The authors have recognized the fact that the most difficult part for projects of this size is to choose an appropriate starting point, and have offered a constructive chapter on how to do that. The technical chapters are also very detailed and extensive, making this book a handy tome for anyone that is charged with ushering the corporate network into the age of IPv6.

Zeljka Zorz is the News Editor at Help Net Security and (IN)SECURE Magazine.

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



**Send your idea to [editor@insecuremag.com](mailto:editor@insecuremag.com)**



## Cyber security revisited: Change from the ground up

by David Lowenstein and Risu Na

This is the first in a series on cyber security that examines why comparable industry thought trends are hindering the space's progress - and why taking a novel approach to IT security will work.

The seeming inevitability of cyber insecurity makes it all too easy to externalize, requiring someone – somewhere – to do something. It almost seems like that we have gotten too complacent with cyber security and hackers are having a field day.

While we have gotten conditioned to saying “it’s impossible to secure everything,” what about our own personal roles and responsibilities as security professionals and consumers? How much of this problem do we personally own? We have been too trusting of our experts, too staid in our approaches, and too complacent in our demands for results. So what other factors are impacting the need for fundamental change?

1. Pithy marketing saying you do something-or-other isn’t quite the same as actually doing it. Casual observation of the “hack du jour” would seem to indicate that solution providers saying that they are anti-virus, or anti-spyware, or anti-whatever is having a similar effect on cyber security as anti-war sentiments have had on stopping wars.

2. It’s human nature to choose the path of least resistance; the proverbial “easy way.” Unfortunately, deep, difficult, complex, multi-domain problems like cyber insecurity are not solvable by the often simple, superficial and superfluous solutions proposed to date. Bluntly put, it’s time to stop treating symptoms with Band-Aids and start holistically focusing on root causes. And yes, we fully recognize that the cyber infrastructure was never designed to be secure, and as such, any effective solution must pragmatically be backwards compatible. Much easier recognized and said than done, but it really is time quit complaining and just get on with trying to solve the problem at hand.

3. Many know that you can’t fix what you can’t measure, and yet cyber security remains an industry befuddled in its development of even a rudimentary set of outcome oriented metrics. Case in point is a pretty good piece of recent work by Carnegie Mellon’s Software Engineering Institute that is in our view almost entirely negated by its lack of constructiveness.

- What percentage of bad stuff can we keep off our systems?
- What number and percentage of actual attack vectors can we stop (with an emphasis on the top 25 or so)?

Not perfect for sure, but a pragmatic start (if you have a better idea, propose it and let's get on with using it, but doing nothing isn't acceptable). Unfortunately, the truthful answer to both questions would self-evidently be "not much."

4. The digerati would have us believe that surveying industry leaders and then "benchmarking" their solution sets – even though they are known *a priori* not to work – is following some form of admiral best practices. Ditto for being "best of breed" among a mediocre, if not downright poor set of comparables.

Sure these measures satisfy compliance checklists and the "commercially reasonable-ness" test for legal liability – which we regrettably understand remain required objectives – but let's at least stop kidding ourselves that either actually improves cyber security or is something that should be lauded.

5. Markets often suffer from what has been described as the "suspension of disbelief"

such as, by way of example, the Internet valuation bubble of 2000 and the recent sub-prime mortgage debacle. Unfortunately, cyber security is facing a much more troublesome challenge that we call "the suspension of belief."

Simply put, very few people think that cyber security is a problem that can be "solved," even to acceptable levels of risk. In this regard, count us unapologetically in the visible minority, for we are deeply committed, actively engaged and manically optimistic that a secure end-state can be achieved.

Think about it – if Google and the U.S. government can't protect stakeholder data, then who can? What can we realistically expect IT managers with materially less resources to do?

In short, it's time for IT to stop cyber security's equivalent of "insanity," for as defined by Einstein, "the definition of insanity is doing the same thing over and over and expecting a different result." It's time for IT to embrace the reality that to make progress in closing the cyber security gap, new thinking, new models and new approaches are needed. When it comes to cyber security, we clearly and unequivocally both need and deserve better.

David Lowenstein is the CEO and Risu Na is the CTO of Federated Networks.



**Order today and protect your physical and electronic systems from attack!**



**Available at [Syngress.com](http://Syngress.com), [amazon.com](http://amazon.com) or your favorite online retailer!**

SYNGRESS