

(IN) SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 19 - December 2008



**HOLE IN WINDOWS LOGIN CONTROLS
WEB FILTERING IN A WEB 2.0 WORLD
THE FUTURE OF AV**

RSA[®]CONFERENCE

WHERE THE WORLD **TALKS SECURITY**

Do more than
keep pace.
Set it.

In a security environment where every day brings new challenges, staying ahead isn't just an option, it's mandatory. As the information security event of the year, RSA[®] Conference 2009 is your opportunity to engage with the greatest minds in technology. You'll focus on critical issues and formulate strategies to create solutions that will influence the industry now and in the future. And you can do it all at RSA Conference 2009.

- Learn the latest trends at over 240 targeted sessions
- Discover practical solutions from 500+ speakers
- Get the tools for success from over 350 exhibitors

REGISTER

APRIL 20-24, 2009 | MOSCONE CENTER | SAN FRANCISCO
WWW.RSACONFERENCE.COM/2009/US
ENTER PRIORITY CODE: HN128

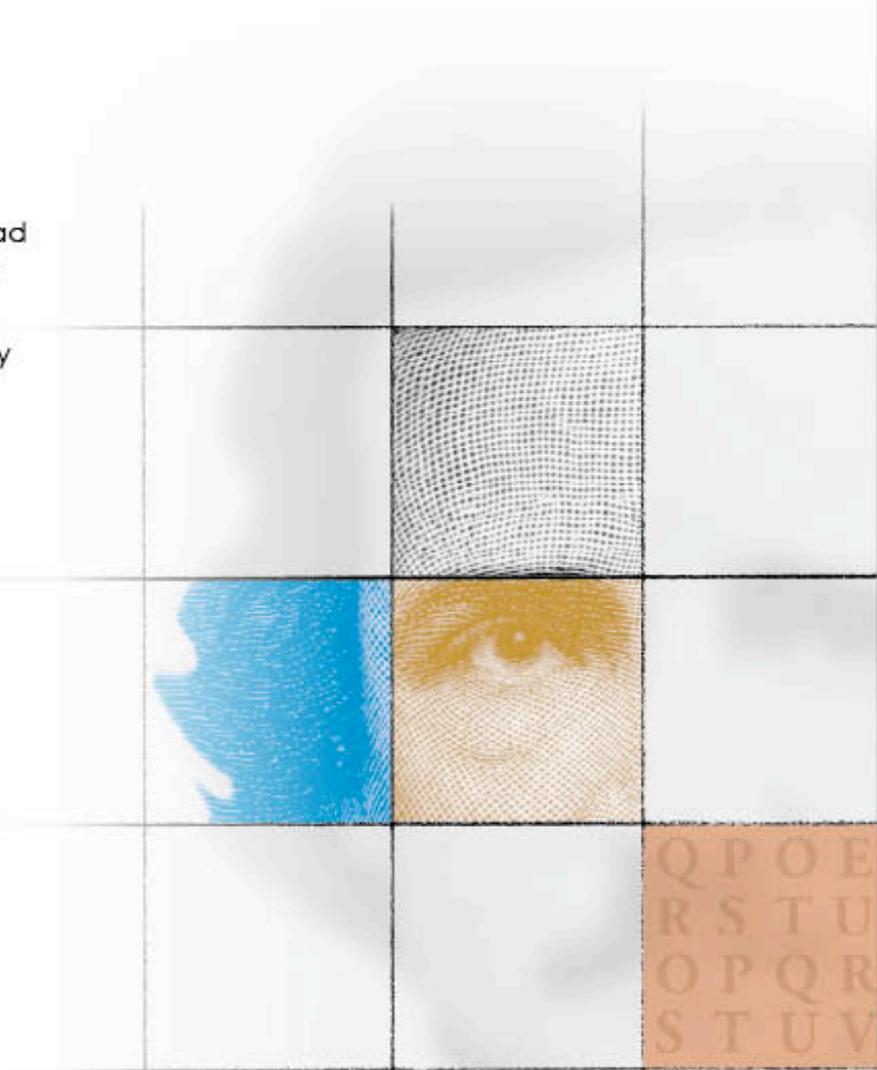


TABLE OF CONTENTS

Page 05 - **Corporate security news**

Page 11 - The future of AV: looking for the good while stopping the bad

Page 14 - Security standpoint by Sandro Gauci: How security can hurt us

Page 18 - Review: Eikon To Go

Page 28 - Eight holes in Windows login controls

Page 35 - **Latest additions to our bookshelf**

Page 36 - Interview with Giles Hogben, an expert on identity and authentication technologies working at ENISA

Page 41 - Extended validation and online security: EV SSL gets the green light

Page 46 - Web filtering in a Web 2.0 world

Page 50 - RSA Conference Europe 2008

Page 54 - The role of password management in compliance with the data protection act

Page 59 - Interview with Rich Mogull, founder of Securosis

Page 61 - **Events around the world**

Page 62 - 5 strategies for proactively embracing failure

Page 68 - The present and future of Web application security discussed in Portugal

Page 72 - Securing data beyond PCI in a SOA environment: best practices for advanced data protection

Page 80 - Navigating a sea of fake codecs

Page 83 - Role Based Access Control

Page 90 - **Security software spotlight**

Page 92 - How to build a security strategy to grow your career, success and results

Page 95 - Three undocumented layers of the OSI model and their impact on security



Welcome to (IN)SECURE 19 the digital security magazine

It's almost the end of another busy year during which security professionals worldwide battled with an increasingly clever circle of cyber criminals unleashing elaborate malicious code. Combine this with the usual vast assortment of vulnerabilities in established products, as well as pressing compliance issues, and I think many will be happy to recuperate during the holidays. After all, we have to be ready for what lies ahead, there's no end to this game.

In order to provide you with food for thought during your hard-earned downtime, in this issue we bring forward articles covering a wide range of topics: the future of AV, best practices for advanced data protection, password management, extended validation, and much more.

We've been contacted by many companies interested in having their products reviewed and this issue contains the first of many reviews. If you'd like to have your devices presented in (IN)SECURE, do get in touch by using one of the e-mails below.

We wish you a successful end of 2008 and a great start of 2009!

Mirko Zorz
Chief Editor

Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts

Feedback and contributions: Mirko Zorz, Chief Editor - editor@insecuremag.com

Marketing: Berislav Kucan, Director of Marketing - marketing@insecuremag.com

Distribution

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

Corporate security news

Free security awareness materials from ISC2 Cyber Exchange



(ISC)2 is inviting businesses and consumers to download free security awareness materials that have been provided by some of the organization's 60,000 certified members worldwide. The materials are available on the new Cyber Exchange, an online security awareness resource center.

The Cyber Exchange houses free security awareness tools from around the world, designed to be used by any organization or individual that wishes to promote online safety at work or within their community. (cyberexchange.isc2.org)

New firewall from Stonesoft - StoneGate FW-310

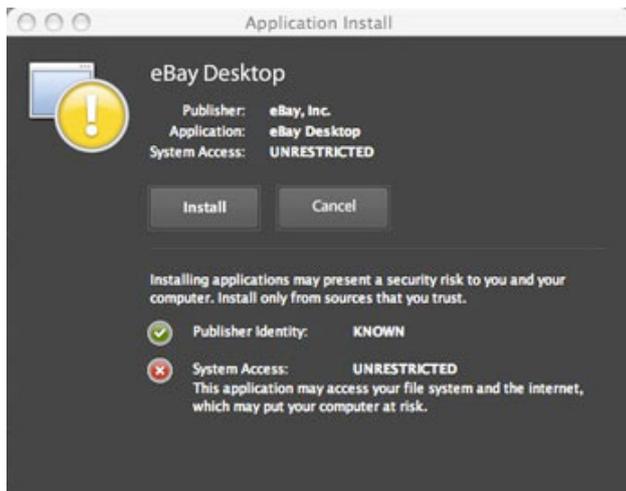
Stonesoft introduced the StoneGate FW-310 for remote offices with increased throughput and improved performance in connecting employees to the central office network.

Remote offices cannot afford service downtime or security threats any more than central sites can, but they often lack local resources for on-site administration. The

StoneGate FW-310 has been designed to meet the needs of remote offices, providing full-scale network security and guaranteed always-on business connectivity. (www.stonesoft.com)



On-demand digital certificates for Adobe AIR applications



ChosenSecurity announced that it is issuing digital certificates for applications built on Adobe AIR software to ensure users that these innovative applications can be globally trusted and are safe to use.

Adobe AIR offers companies a new way to engage customers with branded, rich Internet applications outside of the browser without requiring changes to existing technology, people, or processes. AIR applications are built using proven Web technologies and can be deployed across all major operating systems. (www.chosensecurity.com)

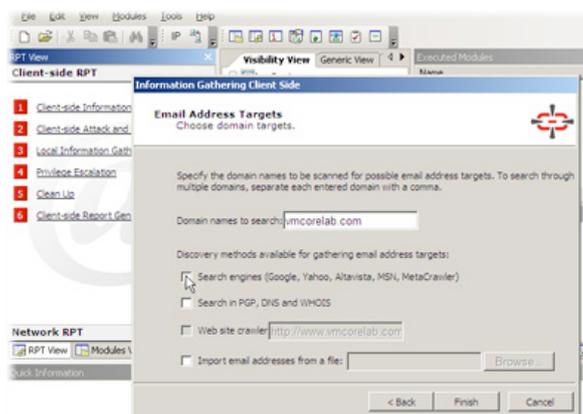
First dual-band secure Wireless-N solution

Netgear released the ProSafe Wireless-N VPN Firewall (SRXN3205) – the first product to combine dual-band Wireless-N with SSL and IPsec VPN. With this dual option, unmatched by competing security solutions for SMBs, the firewall provides 25-user offices with optimal, secure remote connections to their wireless networks. In addition to VPN flexibility, the SRXN3205 supports businesses transitioning from legacy networks to draft 802.11n networks.



The SRXN3205 Wireless-N VPN Firewall supports up to five SSL VPN tunnels and five IPsec VPN tunnels simultaneously for enhanced protection from network security threats. SSL VPN tunnels enable clientless, individual remote access to corporate data, anytime and anywhere - without needing to install a software client. (www.netgear.com)

New Core Security IMPACT Pro 7.6

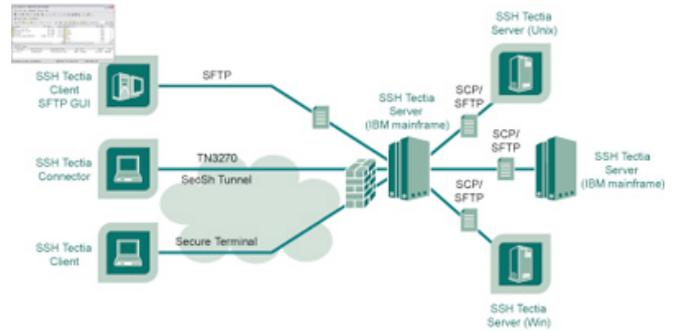


CORE IMPACT Pro 7.6 brings support for IPv6 infrastructure and extended the product's powerful web application testing capabilities. This release also includes a large number of newly developed, commercial-grade exploits. CORE IMPACT Pro is one of the most comprehensive software solutions for assessing the security of network systems, endpoint systems, email users and web applications. It takes security testing to the next level by using penetration testing techniques to safely identify exposures to critical, emerging threats and trace complex attack paths that can put your organization's most valuable information assets at risk. (www.coresecurity.com)

Enterprise security solution for Linux on IBM System z

SSH Communications Security introduced SSH Tectia Server for Linux on IBM System z. This new version provides a unified, end-to-end security model that extends from distributed platforms, to mainframes running the Linux operating system on the IBM System z platform, and also to virtualized environments.

The product delivers data encryption, secure file transfers, secure application connectivity, and secure system administration, all in a single, scalable, high-performance solution. It also utilizes the hardware crypto accelerator on the IBM mainframe, creating less overhead and optimal performance. (www.ssh.com)



New SSL VPN gateway - Connectra NGX R66



The Check Point Connectra NGX R66 is an access gateway that combines SSL VPN, IPsec VPN and intrusion prevention with centralized management. Connectra NGX R66 makes accessing the corporate network more secure and less cumbersome. It leverages an enterprise's existing VPN infrastructure allowing employees to connect from managed laptops using a traditional IPsec connection. (www.checkpoint.com)

Mobile security solution for 3G GSM/HSPA networks

Alcatel-Lucent announced a high-speed packet access (HSPA) version of its unique OmniAccess 3500 Nonstop Laptop Guardian (OA3500 NLG) designed to protect and recover stolen laptops and data.

This always on laptop security and management system for the mobile workforce leverages 3G (CDMA/W-CDMA/GSM) networks, allowing enterprises to overcome the 'mobile blind spot'. The mobile blind spot is defined as a condition where enterprises have no visibility or control over the location, use or configuration of employee laptops, increasing the risk of government fines, company reputation and hampering day-to-day operations of organizations. (www.alcatel-lucent.com)



Free log and compliance management virtual appliance



Q1 Labs released a free, downloadable, log management and compliance product that provides organizations with visibility across their networks, data centers, and infrastructures. With the company's new QRadar SLIM Free Edition (SLIM FE), IT professionals can collect, analyze, report, and store network, host, server, application, and security event logs, via syslog, from any source, including a wide variety of routers, switches, and security devices. QRadar SLIM FE's advanced analytics quickly turn confusing events into useful results that meet specific regulatory requirements. (www.q1labs.com)

Lockheed Martin establishes Center for Cyber Security Innovation

Lockheed Martin announced the establishment of its new Center for Cyber Security Innovation (CCSI). The center of excellence represents an evolution for the company and its cyber security capabilities as it organizes to centrally manage its enterprise practice for technology innovation, best practices, and talent management.



As cyber operations and reliance on networks extend throughout a diverse set of civilian, defense, and intelligence agencies, Lockheed Martin's internal infrastructure and best practices will remain critical to mission resilience for its customers. By utilizing integrated cyber security technologies and a defense-in-depth approach, the company will continue to apply real-time protection and attack management to its network and for its customers' networks.

(www.lockheedmartin.com)

USB-based PKI device for strong authentication



VASCO Data Security International unveiled the Digipass Key1, a USB-based PKI solution for strong authentication, digital signature and data protection. Digipass Key1 is the first solution which is launched in the VASCO PKI-based product line and can only be used together with Digipass CertiID, a client-based software suite offering digital signature capabilities.

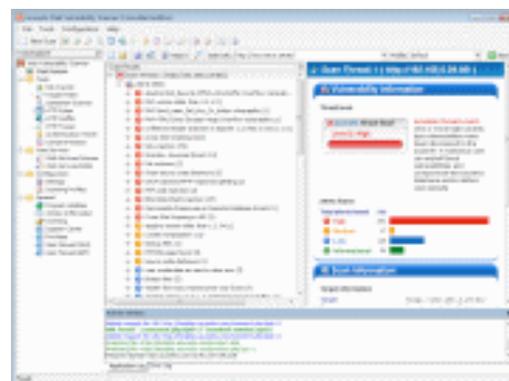
Digipass Key1 is an ultra-portable solution for strong authentication, secure access and secure transactions, offering the same capabilities as a smart card. It has been developed for large corporations, governments and banks providing two factor strong authentication for secure web login, windows PKI login to the desktop, e-mail signature, e-mail encryption and secure VPN access. (www.vasco.com)

New AcuSensor Web application scanning technology

Acunetix announced the release of the cutting edge AcuSensor Technology with the launch of version 6.0 of Acunetix Web Vulnerability Scanner. AcuSensor Technology consists of sensors that are strategically placed inside the web application source code and that send information to the web application scanner on how the applications handle the input during a scan.

The new Blind SQL Injector Tool is ideal for penetration testers as it is an automated database data extraction tool that allows further manual testing for SQL Injections; while with the Port Scanner and Network Alerts it is now possible to perform port scans against the web server, so that when open ports are found Acunetix WVS does complex network level security checks against the service that runs on that port.

(www.acunetix.com)



New Comodo Internet Security suite



Comodo Security Solutions has released Comodo Internet Security (CIS), a complete antivirus and firewall security package free to all PC users.

This security software detects and prevents malware such as viruses, adware, spyware, Trojans, bots and rogue software, and includes always-on, real-time protection against threats. (www.comodo.com)

Samsung ultra-lightweight fingerprint-enabled notebook

AuthenTec's small form factor AES1610 is integrated as a standard feature on the first Samsung consumer notebook to leverage the convenient security of fingerprint biometrics. Samsung's X360 weighs in at a scant 2.8 pounds and is the lightest notebook in its 13.3-inch class. Unlike the claims of some other "light" notebooks, the X360 includes 3 USB ports, a built-in HDMI connection, a 34mm express card slot and VGA output. (www.authentec.com)



3M ToughShield sleeves protect against information theft



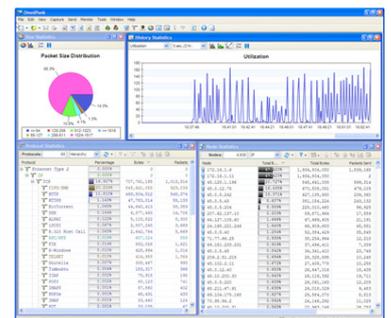
Data theft or "skimming" from smart cards and e-passports will be harder from documents kept in 3M ToughShield brand Protective Sleeves which offer reliable protection for RFID-enabled devices.

The 3M sleeves are lined with a thin copper-coated conductive polyester. This metallic layer effectively blocks radio frequencies used for unauthorized skimming of RFID-enabled applications. These sleeves were developed using 3M shielding technology used in a wide range of electronic devices. (www.mmm.com)

WildPackets launches NetFlow Analyzer for OmniPeek

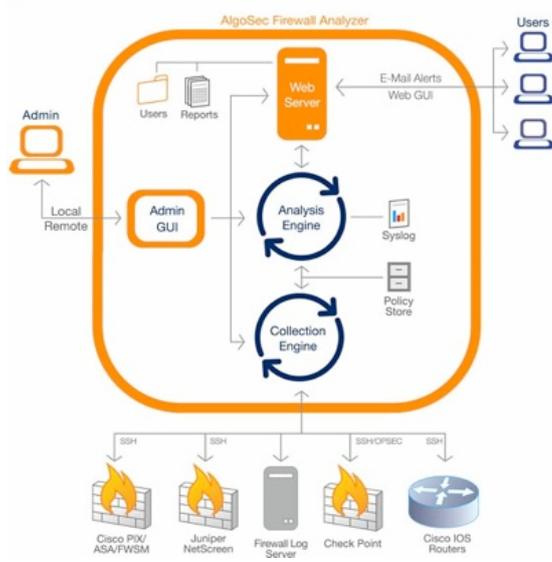
WildPackets released NetFlow Analyzer, an advanced extension for OmniPeek that allows users to analyze NetFlow statistics from Cisco networking hardware and seamlessly drill down to individual packet inspection for root cause problem analysis and resolution.

The NetFlow Analyzer identifies top talkers, protocols, and applications throughout the entire network making it easy to isolate and investigate excessive network bandwidth utilization and application traffic. Combined with the deep packet inspection of OmniPeek, IT professionals have complete visibility into usage, performance, and availability statistics and can set alerts to be notified upon suspicious activities and events within the network. (www.wildpackets.com)



New firewall matrix analysis technology

AFA Deployment Architecture

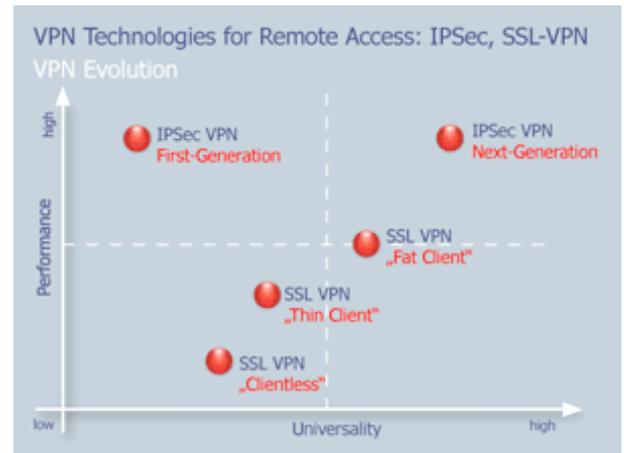


AlgoSec Firewall Analyzer (AFA) Version 5.0 extends the solution's capabilities to deliver the industry's first Matrix Analysis, or tiered firewall-specific analysis system. With Matrix Analysis, enterprises, managed service providers, consultants and auditors receive insight into multi-firewall and multi-vendor environments based on their relative hierarchy in the network.

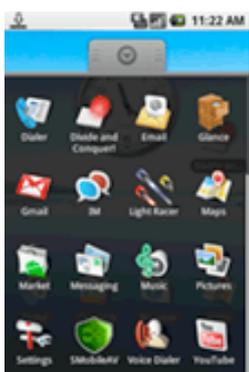
AFA Version 5.0 is available to businesses and organizations worldwide in multiple form factors and depending on the specific needs and requirements of each individual enterprise network. Delivered via the SaaS model or in virtualized environment or as software or an appliance, the AFA provides the flexibility that businesses need to manage multi-firewall, multi-vendor, including Check Point, Cisco and Juniper, security environments. (www.algosec.com)

Expanded IPSec VPN secure client for PCs and handhelds

NCP engineering announced the 9.1 version of the NCP Secure Enterprise Client. This major upgrade will provide users a flexible, intuitive, bundled client for any Windows-based (Mobile, CE, XS/Vista/32/64-bit) or Symbian system (S60 3rd Edition). The client is seamlessly compatible with any IPSec gateway on the market. The bundled solution is equipped with a dynamic personal firewall, intuitive and user-friendly GUI, data encryption and one-time password token and certificate support through a PKI. It can also be integrated with a NAC component to ensure highly secure access to central data networks. (www.ncp-e.com)



First antivirus for Google Android phones



For more than a year, Google has been touting its mobile phone operating system known as Android and how it would open up the platform to developers around the world, interested in developing Android applications. Two weeks ago, T-Mobile began selling its G1 handset, the world's first Android based cell phone.

VirusGuard is the first commercially available mobile security solution specifically developed to protect devices utilizing the Google Android operating system. Using the knowledge gained by developing antivirus and security applications for BlackBerry, Windows Mobile, Symbian, Palm and iPhone, SMobile engineers began development of VirusGuard for Android more than a year ago. (www.smobilesystems.com)

The future of AV: looking for the good while stopping the bad

by Carey Nachenberg



Contrary to some industry observers, antivirus software is not dead. It is, however, undergoing a game-changing transformation.

It has to. After all, the current model of detecting viruses through blacklisting simply cannot keep pace with the unprecedented volume of malware released every day. To continue to be effective, antivirus must transition from the current signature-based model to a new hybrid model that uses whitelisting to allow trustworthy applications, blacklisting to block prevalent known malware, and reputation-based ratings to automatically categorize the “long tail” of unknown malware and legitimate software.

Rapid growth of malware

By some measurements, the volume of malicious software is now outpacing the production of legitimate programs. Symantec recently measured the adoption rate of new software applications and found that out of almost 55,000 unique applications deployed during a weeklong measurement period on Microsoft Windows PCs, 65 percent were malicious.

In fact, there’s never been more malware. Nearly half a million new malicious code

threats appeared just in the last half of 2007, according to Symantec’s latest Internet Security Threat Report. That’s more than twice as many as were discovered in the first half of 2007 and five times the number detected in the last half of 2006.

It could get worse as attackers adapt. They have already shifted away from mass distribution of a small number of threats to micro distribution of millions of distinct threats. Using servers that generate a new malware strain every few hours - or minutes - they can unleash individual attacks against each victim. So far, cyber criminals have created millions of distinct malware strains, and antivirus software vendors are collecting tens of thousands more every day. If these attack trends continue, the public could face millions of new threats every year.

At the same time, antivirus vendors are feverishly working to generate up to 20,000 new virus fingerprints each day. However, most products detect only a fraction of new malware, even as many strains of older malware

go undetected. Furthermore, attackers can easily circumvent most generic signatures by tweaking existing malware files, scanning them with an antivirus scanner, and repeating the process until the scanner no longer detects the infection. Such modifications can be done by hand or, unfortunately, all too easily via automation.

As a result, whereas a few years ago a single signature could protect tens of thousands of users against a widespread threat, today a single signature typically protects less than 20 users against a micro-distributed threat.

Clearly, in such an environment, traditional signature-based detection - or blacklisting - alone is not enough.

ATTACKERS CAN EASILY CIRCUMVENT MOST GENERIC SIGNATURES BY TWEAKING EXISTING MALWARE FILES, SCANNING THEM WITH AN ANTIVIRUS SCANNER, AND REPEATING THE PROCESS UNTIL THE SCANNER NO LONGER DETECTS THE INFECTION

Finding the good

As the volume of malicious code continues to skyrocket, security techniques must increasingly focus less on analyzing malware and more on analyzing "goodware."

Whitelisting has traditionally been used on high-value servers because their static configuration makes a whitelist easy to build. Yet, even though most infections occur on desktops and laptops, whitelisting has not been extended to these systems.

Why not? Because desktop machines are far more dynamic than locked-down servers, employees download software packages on them to do their jobs, and desktop applications often self-update - thereby making it extremely challenging for an enterprise to create and update a whitelist for such machines.

Nevertheless, a comprehensive whitelist could virtually eliminate traditional infections on these endpoints. Some companies have taken a do-it-yourself approach wherein the vendor or customer manually constructs the whitelist.

Other vendors have chosen to partner with top software OEMs to build the list, while still others deploy Web spider software to gather files for the list. Unfortunately, thus far, none of these approaches have yielded a comprehensive enough and current enough whitelist that can reasonably be used to lock down desktops and servers without costly manual administration.

A new approach to building whitelists supplements whitelisting with new reputation-based protection technologies. Reputation-based protection is game-changing in that it leverages the wisdom of millions of users to provide customers with actionable information about the software they download and install. This helps customers make the right choices based on the experience of other, real users just like them. Early indications show that this approach, when complemented by traditional antivirus technology, radically improves protection, especially against the onslaught of personalized malware seen today.

The importance of reputation

One of the most difficult challenges of antivirus protection today is figuring out how to deal with threats that are on so few systems that they often go undetected using traditional blacklisting. After all, if only a handful of people in the world have a specific threat, a security vendor has little chance to discover that specific threat and write a signature for it.

Unfortunately, because there are so few common versions of today's malware, malicious programs tend to occupy this so-called "long tail" of software distribution. Similarly, it's difficult for security companies to locate less popular, yet entirely legitimate, software applications and add them to a whitelist. Imagine a small software vendor that caters to just a handful of customers. What are the odds that this vendor's software will be discovered and added to a whitelist in a timely fashion?

This is where the addition of reputation-based security looks promising. A reputation-based rating system for applications can provide users with an accurate security score, not unlike a credit rating, for every application they encounter on the Internet. This enables users to make more-informed decisions about the programs they download before installing them. Moreover, organizations can use the highest-confidence ratings to identify legitimate applications and then automatically populate their whitelists.

Most legitimate software is created for mass distribution and today's malicious programs have extremely limited distribution before they're mutated for the next user. To respond to this, a reputation-based system can leverage a prevalence-based reputation approach to assign lower ratings to less-prevalent software.

For example, an administrator could stipulate policy guaranteeing that only highly prevalent applications—for example, those with at least 10,000 other users—are allowed in an enter-

prise. Such a policy would weed out all but the most prevalent malware, which traditional fingerprinting via blacklisting can detect easily, yet allow the deployment of most popular legitimate applications.

As another example, a reputation-based system can derive reputation ratings based on the provenance, or source, of the application, and assign higher ratings to applications from known, trusted vendors. Using these and numerous other techniques, organizations can deliver highly accurate reputation ratings for applications that can fundamentally change the efficacy of security software.

With complementary blacklisting, whitelisting and reputation-based technologies safeguarding both enterprise and consumer endpoints, business and homes have a more formidable, long-term solution to the malware epidemic. Perhaps the greatest benefit of a hybrid approach is that it would finally return the burden of antivirus protection from the shoulders of weary customers back to security vendors.

Carey Nachenberg is a Symantec Fellow in the Security Technology and Response Group at Symantec Corporation (www.symantec.com).

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



Send your idea to editor@insecuremag.com



Security standpoint by Sandro Gauci: How security can hurt us



The more you spend on security does not necessarily equal more security.

At a recent presentation on web application firewalls (see enablesecurity.com/res/web), I was asked if deploying multiple web application firewalls would increase the security of a web application. Would deploying two or three products by completely different vendors compensate for the weaknesses of each security solution? Common sense would seem to dictate a definite “yes”. In fact, I could almost see the audience nodding. On the other hand, like many security matters, there is more to this than meets the eye.

The more you spend on security does not necessarily equal more security. In this article we outline cases where this might even lead to less security. Furthermore, we take a look at how the perception of security based on compliance requirements affects us all. Finally, we will take a realistic look at the state of our current systems and how to make future decisions based on all these variables.

How Defense in Depth matters

Defense in Depth is one of the terms that the Information Security community has borrowed from the military. In military terminology, Defense in Depth stood for methods which do not try to prevent an attacker from advancing but rather delay the attacker. In the information security industry, Defense in Depth is a popular concept where the security of a system does not rely on a single technology but rather relies on multiple layers of protection. The idea is that if an attack causes one protection mechanism to fail, other mechanisms will prevent the attack from being successful.

Most of us are familiar with the term and even if we do not use it in our day-to-day lingo, we probably apply this concept on a daily basis. The person asking me the question on web application firewalls was probably thinking in terms of Defense in Depth.

Implementing a firewall, an email security solution on the gateway and antivirus on the desktop is an application of the Defense in Depth theory.

The idea is that by making use of multiple security solutions we can prevent attacks on one product from becoming a real problem. Marketing departments in the security industry know this and present us with products that reflect these ideas.

In the past years, endpoint security became a regular part of our vocabulary. With endpoint security products one often gets software that does antivirus, antispyware, intrusion prevention, network access control, application and device control, encryption and a number of other features that were previously separate products. The security appliance market took heed and now sells devices that do some or all of the following at the perimeter: firewall, VPN, content security, intrusion prevention and antivirus under the name unified threat management.

THE WAY THAT MOST SECURITY SOLUTIONS ADDRESS ISSUES IS BY COVERING UP THE PROBLEM RATHER THAN ADDRESSING THE ROOT CAUSE

Poking holes in security products

If Defense in Depth consisted of a couple of walls placed in parallel that an attacker would have to bypass, then the easiest way to get inside would be to drill a hole in each wall that lets you in straight through. In the security world this would probably be a single security bypass which affects many products concurrently. If your security solutions are making use of a blacklist approach, then the chances of finding a way to bypass the protection is greater no matter how many products are in place to protect your system. However this is not limited to just security products relying on blacklists.

The way that most security solutions address issues is by covering up the problem rather than addressing the root cause. Web application firewalls do not fix SQL injection vulnerabilities; they prevent them. Intrusion prevention systems do not patch exploitable code but look for network traffic that appears to be trying to exploit known vulnerabilities.

Security products cannot fix the underlying problems simply because they are external to the vulnerable system. While in theory the idea of having external security solutions protecting another system is very attractive, it has a major flaw. Systems that need to be protected are complex and therefore it is not an easy job for the security solution to predict how the vulnerable system will react under certain conditions. If a security solution is to

protect a vulnerable system, then it needs to emulate the way that that system works. In the case of complex systems, this is not an easy task and that is why web application firewalls or antivirus on an email gateway can be bypassed.

In 2004 iDefense Labs published an advisory detailing a zip file that bypassed McAfee, Computer Associates, Kaspersky, Sophos, Eset and RAV Anti virus. The zip file had a header that specified that the uncompressed size of the archived files is zero. WinZip and Microsoft Compressed Folders still opened this malformed zip file, while the Anti virus products simply let the file through. A year later someone by the alias of fRoGGz published details on bypassing Anti virus products by adding fake headers to compressed RAR files. Both of these vulnerabilities impacted Anti virus solutions on gateways such as those filtering email or web traffic.

In November 2007 Avi Douglan published a paper titled "SQL Smuggling" which outlines attacks on the SQL server that web application firewalls and even input validation on the web application might not prevent. The reason is that the web application or web application firewall does not take the SQL server's specific unique properties into perspective. During his research Avi found out that certain SQL servers will translate Unicode characters that look similar to other characters based on heuristics.

For example Unicode Å character (U+0100) may be translated to the regular ASCII A (U+0041). A web application or web application firewall that does input validation searching for quotes might be bypassed by sending Unicode characters which are then converted to quotes by the database server itself. This can obviously lead to an SQL injection vulnerability even though the web application might be doing input validation by searching for quotes.

When security products reduce security

Many security vendors (correctly) claim that software that is totally secure does not exist and their products mitigate this condition. However that same argument also applies for their security products too! Several security products have been found to have security vulnerabilities that can lead to a system being compromised. Sometimes, like in the case of the Anti virus, they are vulnerable to the same type of security vulnerabilities that they try to protect against, such as memory corruption issues and privilege escalation.

Why do security products have vulnerabilities? To protect a system, many security products try to emulate the system. If an Anti virus solution needs to scan a compressed file, then it needs to decompress that file. In turn this means that they need to parse various file formats, interpret different network protocols without affecting the performance of the system. Writing bug-free security software with all these requirements is not an easy task by any means.

One of the concerns is that we trust our security software for protecting our data. A popular way to setup a web application firewall is by placing it between the client and the server as a reverse proxy. In any case, a security solution such as a WAF is going to need to watch all HTTP traffic. If it is meant to protect against attacks on the HTTPS server, it will need to terminate the TLS/SSL connection from the client and start a new one with the HTTPS server. This means that in this case, WAF solutions act as a Man in the Middle. If the WAF is compromised then the result it is very similar to when the Web Server itself is compromised. The data that it is being inspected for intrusion attempts is the same data that con-

tains your customer's credit card details or private information.

How does having multiple security solutions in place solve this problem? The simple answer is that most of the times, it does not. The concept of the weakest link still applies, even though there is the perceived added security by making use of multiple layers of security. Just by having one compromised WAF it is enough for an attacker to gain access to the sensitive data in transit. Additionally, this will lead to a domino effect where one compromised security solution can affect the rest of the system. More often than not, we put so much trust in our security solutions that when one of them breaks, the whole system can crumble resulting in a single point of failure.

An advisory for Cisco Application Velocity System (AVS 3110 3120) detailed how the system has default passwords for accounts that can lead to root access. Apart from performing other functions, the Cisco AVS 3120 also serves as a Web Application Firewall. Back in 2004 ModSecurity, the opensource WAF, was found to be vulnerable to an off-by-one overflow that could lead to a remote root compromise. Symantec Mail Security for Exchange had its fair share of vulnerabilities especially when it comes to parsing file formats. McAfee VirusScan Enterprise was also found to be susceptible to a vulnerability in the decompression of ZIP files.

Sergio Alvarez and Thierry Zoller from N.runs presented at Hack.lu conference in Luxembourg on how antivirus software can lead to compromise to the underlying operating system. In their presentation they showed the various security issues that Anti virus software is bound to have and how (in the case of Anti virus products) the concept of Defense in Depth is flawed.

How compliance can add to the problem

Compliance requirements such as the Payment Card Industry's Data Security Standard (PCI DSS) try to ensure that certain security mechanisms are in place. Many believe that compliance is a necessary evil because organizations would otherwise avoid addressing security issues until it is too late.

The truth is that compliance and regulations are a one-size-fits-all solution. They need to be applicable to many different organizations all of which have different requirements. In turn compromises need to be made to be able to apply to so many organizations. In the case of the PCI DSS, in order to address the web application security issues the payment card industry gives the option of making use of an external auditing team or implement a web application firewall. If there is something that we should have learned by now, it is that security mechanisms should reflect the business requirements of the organization. Therefore a "one size fits all" approach can only work if such regulations are meant to address the bare minimum when it comes to security. That is exactly what many compliance and regulations do.

It is easy for these compliant organizations to point at the regulations and claim that they conform to the regulations when security concerns arise. The truth is that being compliant does not mean that your system is sufficiently secure against the attacks that might apply to your system. By making use of a Web application firewall to comply with the PCI DSS, organizations get an easy way out without needing to fix the underlying security holes within their web applications. However, even if web application firewall products have impeccable security (i.e. they not not increase the vulnerability surface) and have no known security bypass, they can only detect security flaws resulting from incorrect implementation.

What about design flaws? Verified by VISA is a mechanism that confirms the buyer's identity with an extra password on each online transaction. In October 2008, various news agencies covered stories where this password can be reset by simply providing the date of birth of the card holder and a new password. A web application firewall will never catch such a flaw because it has nothing to do with Cross Site Scripting, SQL injection or any of the other at-

tacks that such products are meant to address.

Should we ditch our security products?

By now you are probably asking yourself if I am suggesting that all the security products in place are useless. Security products tend to add a lot to perceived security, without necessarily adding enough to real security. The truth is that most organizations need a desktop antivirus if they are to make use of common off the shelf products without relying too much on luck and employee (or end-user) education. All successful security products try to address real issues. However the more products - including security products - you add to a system, the more complex that system becomes. In short, complexity breeds vulnerability.

When implementing a new system, we should be thinking twice before bloating that system with security products. Many security problems can be mitigated without adding more to the system. The expression "less is more" does not only apply to architecture, but can easily be applied to security. Rather than looking at the security of a system on its own, it is important to take the business requirements of such a system and tailor solutions to any security issues that apply to that system instead of simply loading your shopping cart with a myriad of security products and heading for checkout.

As the old adage states "if anything can go wrong, it will". In the case of security, the chances of something going wrong tends to increase with complexity. It is therefore paramount that instead of aiming towards a system that is impenetrable, we shift an adequate amount of our focus towards accountability. We cannot guarantee that a system cannot be compromised but we can increase the chances that if it does, we are promptly notified and can assess the extent of the problem.

Sandro Gauci is the owner and Founder of EnableSecurity (www.enablesecurity.com) where he performs R&D and security consultancy for mid-sized companies. Sandro has over 8 years experience in the security industry and is focused on analysis of security challenges and providing solutions to such threats. His passion is vulnerability research and has previously worked together with various vendors such as Microsoft and Sun to fix security holes.

Sandro is the author of the free VoIP security scanning suite SIPVicious (sipvicious.org) and can be contacted at sandro@enablesecurity.com. Read his blog at blog.enablesecurity.com

Review: Eikon To Go

by Mark Woodstone



Fingerprint authentication and digital privacy on the go.

Besides the regular software reviews, from this issue of (IN)SECURE Magazine we will be writing about a variety of security hardware devices. A number of infosecurity companies have been emailing us with requests for product reviews, so from now I will be testing them.

UPEK is one of the leading providers of biometric fingerprint security solutions, with their hardware being deployed in various computers from Asus, Lenovo and Toshiba. We have received a copy of Eikon To Go, a convenient portable version of Eikon Digital Privacy Manager. Portable Eikon comes with the appropriate software application Protector Suite QL and is aimed towards notebook use.

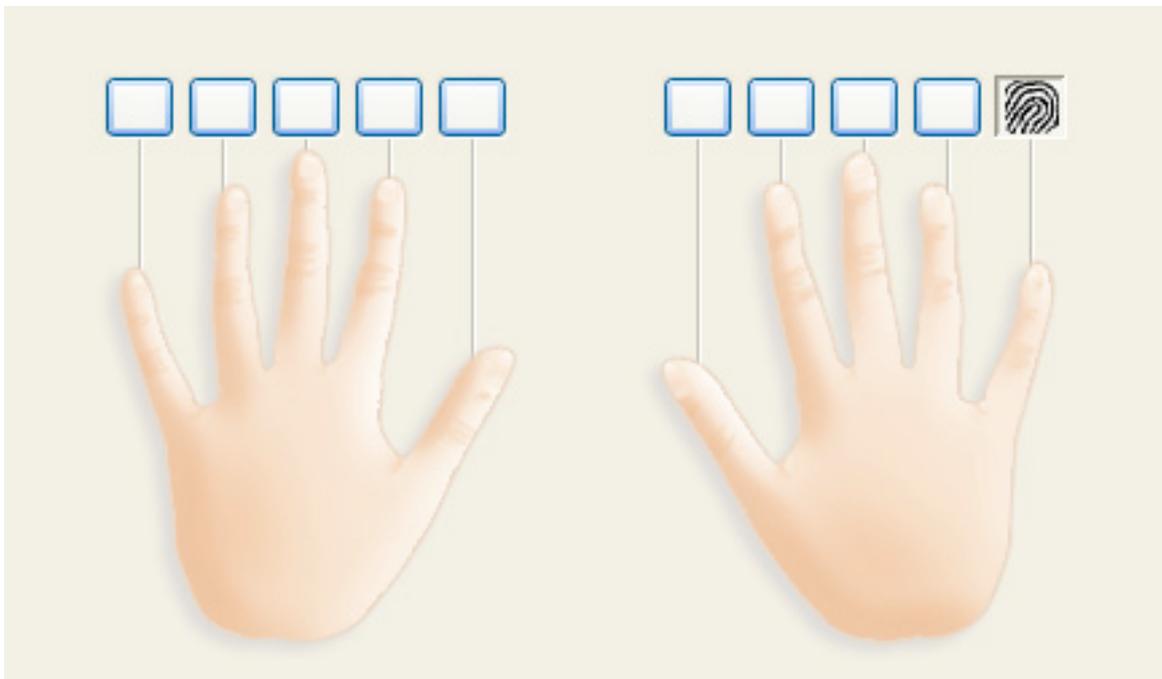
More and more hardware devices are being developed for multiple operating systems and Eikon To Go is one of them. This product review will be divided into two parts - the vast majority of the text will go towards extensive Windows XP usage, while Mac users can get a scope of the product's features running on Mac OS X Leopard. Besides these popular operating systems, the device works on Windows 2000, 2003 Server, Vista, as well as Mac OS X Tiger.

Hardware device

Eikon To Go looks like your typical USB key, but UPEK has managed to step up the design part and made it into a rather attractive gadget. The fingerprint reader is not located on the outside - it is unveiled when you slide the upper portion of the device. The same move opens up the USB connector which can be directly inserted into the USB port.

With the device comes a 20 cm USB extension cable, just in case your USB slot is located on a "busy" part of your notebook computer. If you are planning to use the device with your desktop computer, you will need a new cable to better position it for the finger swiping procedure.

When the device is not inserted directly into the notebook and used with the small extension cable, it is also easy to work with it. The USB key has a rubber bottom so you won't have any problems when swiping your finger through the reader. From the physical perspective, the device is one of the lighter USB keys I have come across.



Fingerprint biometric authentication

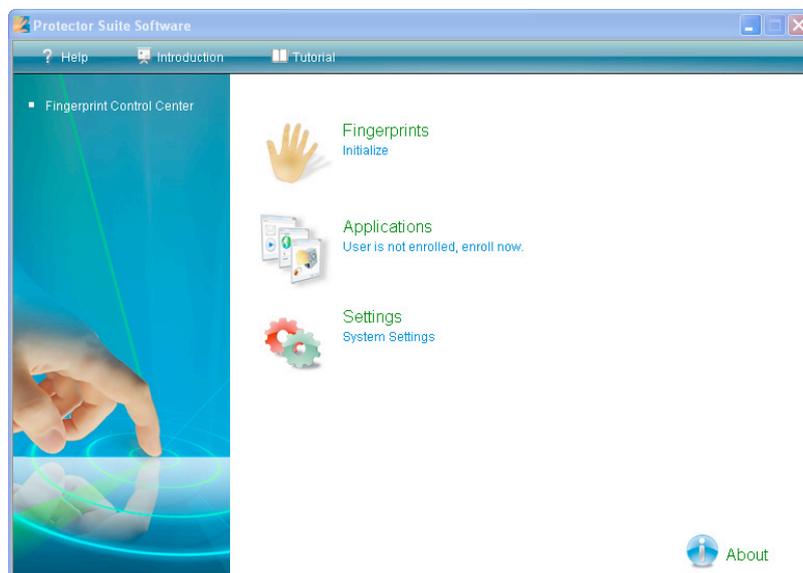
I mentioned earlier that the device has its full potential on a Windows computer, while on the Mac OS X it provides just limited functionality. I have used Eikon To Go on both of my work computers and I will go through all the options and utilities it provides on both operating systems. Although I also tried it on Microsoft Vista, XP is my preferred Microsoft OS so all the usage scenarios and screenshots are done on it.

Before I go deeper into UPEK's neat little device, here is a crash course in what can you expect out of Eikon To Go: Windows Logon, Password Bank, RSA SecureID support, Workstation (un)locking, file encryption and fast user switching. Still interested? Read on.

Initial setup and enrollment

The package consists of an Eikon To Go device, a simple 15-page start-up guide and a CD with the needed software suite. For the purpose of this review I used Protector Suite QL 5.8, which was the latest version at the time of writing this article (mid-November 2008).

This application works with a number of UPEK biometric readers and in case you misplace the CD, you can always but the software online for less than \$20. The default language used by the software is English, but the GUI is translated into more than 15 languages.

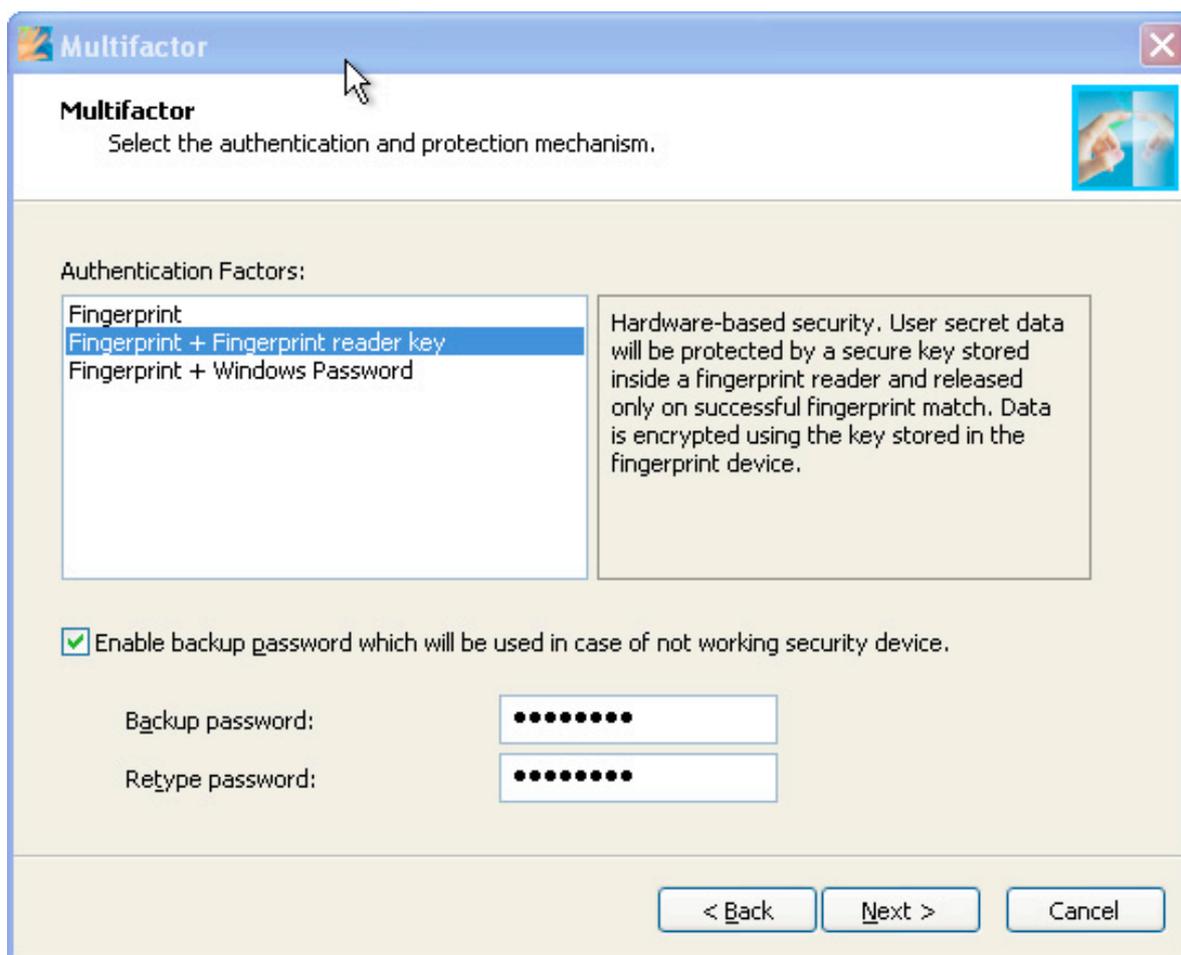


The Protector Suite command center before enrollment

After successfully installing the application you can plug in the Eikon To Go and start up the initial setup. Naturally, the first thing you need to do is to enroll at least one of your fingers to work with the device. I liked the fact that the user was given a choice of saving the fingerprints directly onto the device (obviously the default way of doing things), but you could also save the fingerprint schematic to the hard drive. If using the latter option, the stored fingerprints will be encrypted by the software. This option should be used if you plan to store

a larger number of fingerprints, as the device has its limit of stored data - 11 slots.

Before scanning your fingerprint, the application will check with you whether you are interested in just using your fingerprint as an authentication method, or you would like to go the multi factor authentication way. Depending on the level of your security awareness (or paranoia), you can combine the fingerprint with a special reader key that you need to input or with the Windows password that is associated with your user account.



Setting up regular or multifactor authentication

Enrolling was never easier - UPEK asks you to scan your finger of choice for five times, just in case it can record the real schema. I am stressing out schema because the actual fingerprint image is not stored, only a handful of unique features called a "template" which are extracted from your fingerprint and cannot be used to reconstruct an image.

I haven't used fingerprint based biometrics since my rather bad HP iPAQ 5550 experi-

ence, but I can say that UPEK's scanner worked perfectly. When using my point finger I had a 100% success ratio over the course of couple of weeks and with using other fingers I had maybe two or three situations when my scan wasn't recognized.

It is recommended that you scan at least two fingers just in case Murphy's laws hit your finger of choice.



Fingerprint is OK after five successful swipes

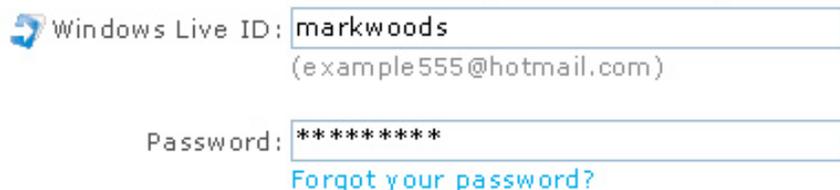
Windows logon

This is the first and to some the most important function of this kind of a device. When the computer is started, Windows will ask you to swipe a finger to successfully logon.

Password Bank

This utility provides a password manager function that is being safeguarded by your finger-

print. I have been using a similar tool on one of my computers, so I was really curious to see how UPEK implemented application-browser relations. From my thorough testing, this utility worked just fine. The process has two different tasks - remembering and restoring passwords. Password Bank automatically understands which pages have forms inside, so when you fill user/pass combination it will save them inside its database.



Password Bank save data procedure

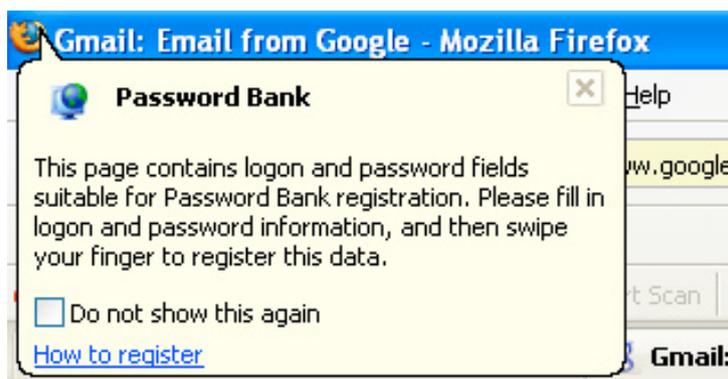
For restoring the passwords inside web applications, webmail services or anything online that needs authentication, you can choose one of the two ways.

The first is to open Password Bank, authenticate yourself via a fingerprint and click one of the saved profiles. This will open your favorite browser and automatically send the form

with your credentials. In case your favorite browser is not one of the compatible browsers such as Internet Explorer and Firefox 2, you will just get a regular page without any auto-filled data.

The second way works like this: When you open a web site for which you have already saved user/password data, the browser should automatically fill and send the form. Password Bank should understand that you

opened a page for which you have password data, the borders of the browser will flicker in a red color and the data will automatically be filled in. The flickering of the border is one of the two "hint methods" the software is trying to tell you that you already have saved data for the current page. The other method is a popup balloon in the left corner which is a better looking option. You can change these settings and chose your hint type within the Password Bank menu.



Sample balloon giving a hint to the user

By the way, if you don't logon to your computer via the biometric fingerprint you will have troubles using the Password Bank. It looks like this is the needed step as you won't be able to follow-up on any password filling - automatic that is, opening links from the "Registrations" menu of the Password Bank will still work.

File Safe

Besides the Windows logon, File Safe provides the best usage for this kind of a security

device. Biometrics combined with encryption is the way I like it and I found this a very quality options of securely encrypting and storing encrypted files.

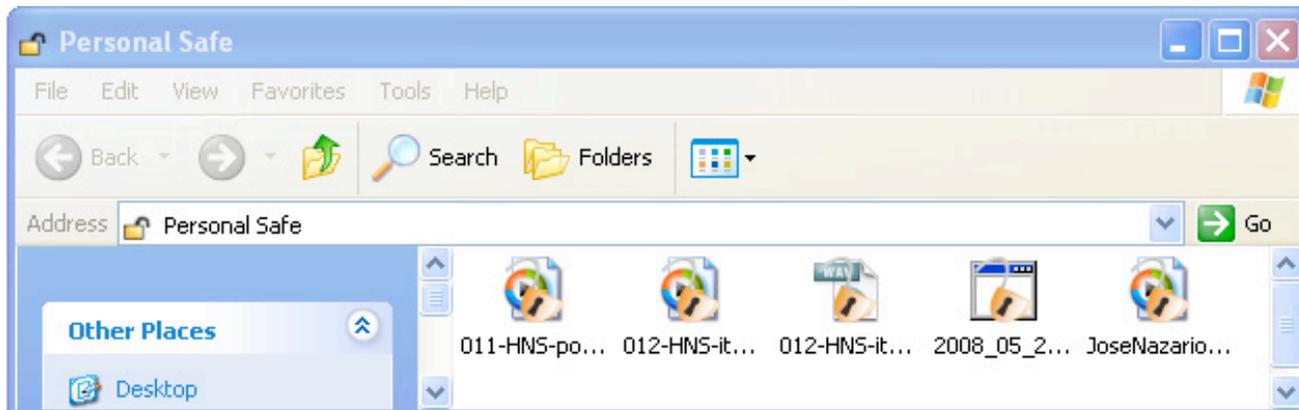
Technically, File Safe offers two separate, but similar options. The first adds the encrypt/decrypt menu to the Windows shell, so you can easily chose to work with any specific files. Crypto is based on both the password you can enter, as well as fingerprint slide that is needed to successfully decrypt data.



Encrypting a file with a backup password

Personal Safe is a variation of File Safe option which gives users possibility to create hidden folders in which you can store files. Of course, all the files are encrypted in the same manner and they can be accessed after suc-

cessful authorization to the application. Encryption is rather quick and 256 bit AES cipher is being used. A nice addition to the concept is that encrypted files can be shared to specific users.



Files located in the encrypted personal safe

Security tokens

The Eikon software enables token code generation and automatic form filling after you swipe your finger over the fingerprint sensor. The token code generation can be carried out by the fingerprint hardware chipset or by

software. To use this feature you must be registered with a provider that accepts token codes. This sounds like a nice feature. I didn't get the chance to try it, but I just wanted to mention it, as I know it makes a difference to some readers.



Ready to create new RSA SecureID token

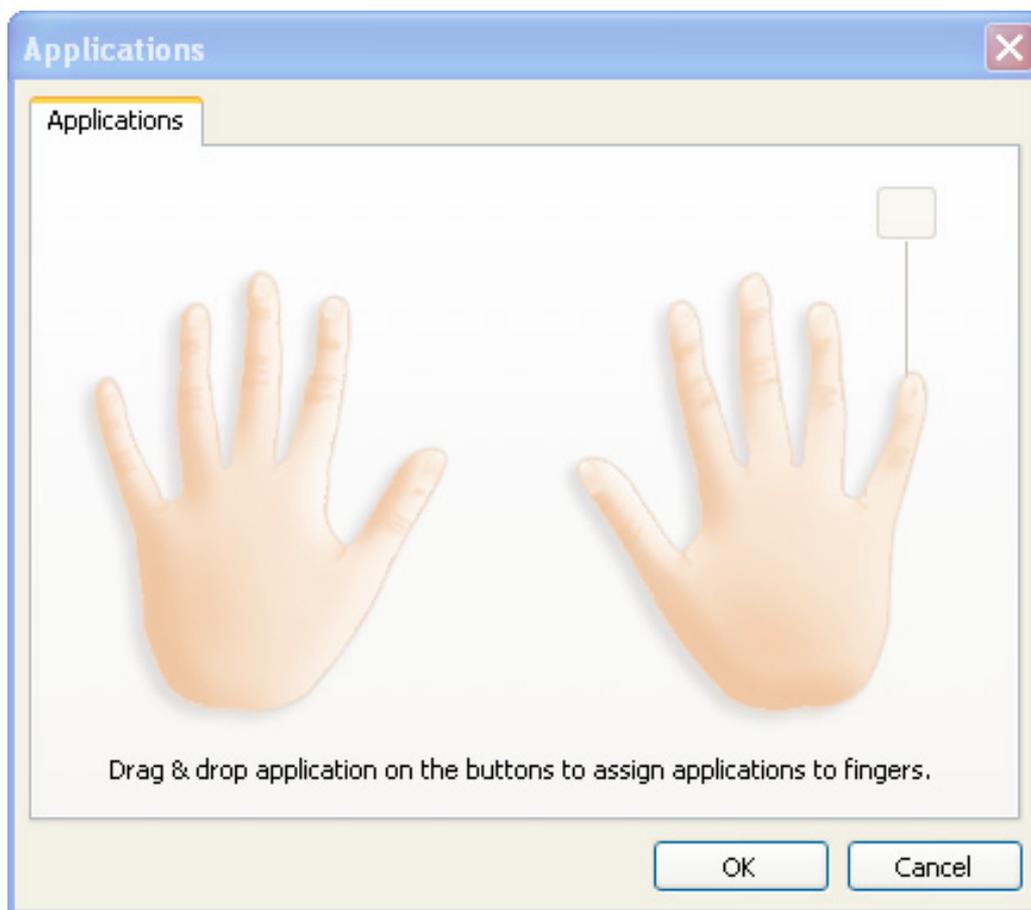
Bonus (eye candy) usage

When you already have a fingerprint reader stuck in your notebook, why not make it even more useful. There are two additional usage scenarios where the Eikon To Go can be useful:

a) Scrolling: fingerprint reader can be used for scrolling through web pages and documents

b) Application launcher: you can drag and drop applications to the specific finger, so by swiping it, applications get automatically launched.

Like I said, not very useful, but the functionality is there if you need it.



Setting up application launcher for the selected finger

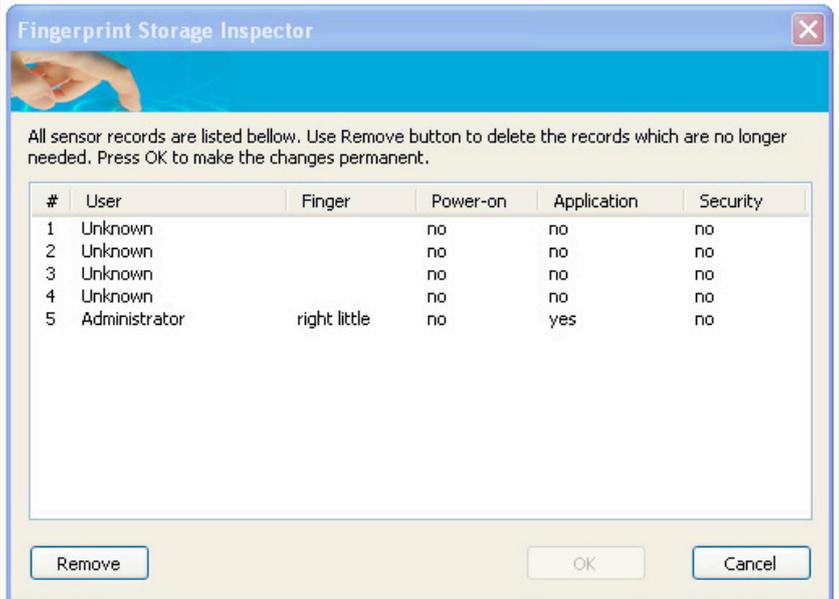
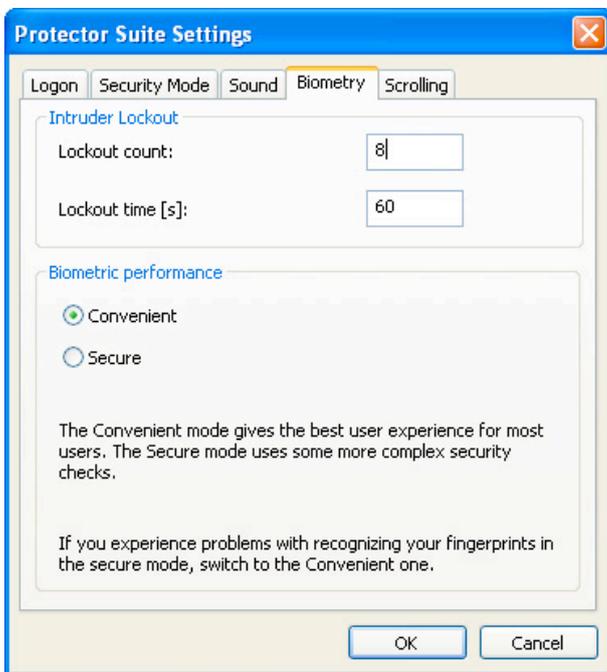
System settings

I have discussed all the practical uses of Eikon To Go and Protector Suite QL combo, but configuration options are a last valuable set of information I would like to share with you.

You never know what can go wrong with Windows logon, so the appropriate tab in the settings can be a of great help. In some cases it is good to have a backup and while a password bypass for the logon denies the sole purpose of using a biometric logon solution it could be useful in some bad situations.

Besides the mentioned fail-safe option, user can setup different security modes in which you can basically set some basic policies for login and enrolling of new users. Earlier in the text I mentioned that my fingerprint enrollment went by like a charm - that is because the default selection for biometric performance was put to "convenient". If you want extra security, chose "secure" and make the authentication more extreme.

Fingerprint Storage Inspector is a tool that lists all the sensor records and gives you a detailed list of users, fingers, applications and accompanied security levels.

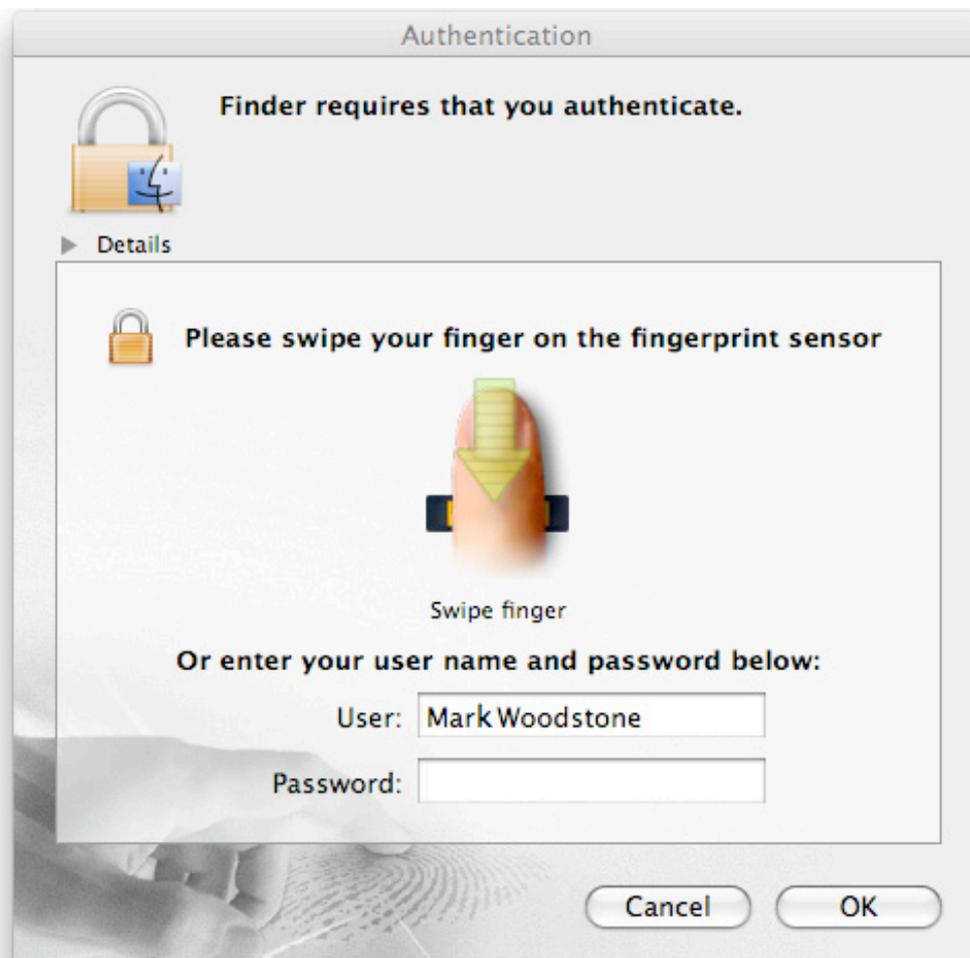


Biometric settings tab (left) and the of sensor records stored on the biometric device (right).

Mac OS X and Eikon To Go

I was glad to see that UPEK made an application for Mac OS X and that their devices are

compatible with it. Unfortunately (for now?), usage is very limited and while I would gladly like to use File Safe on my iMac, we are "stuck" with just the biometric logon process.

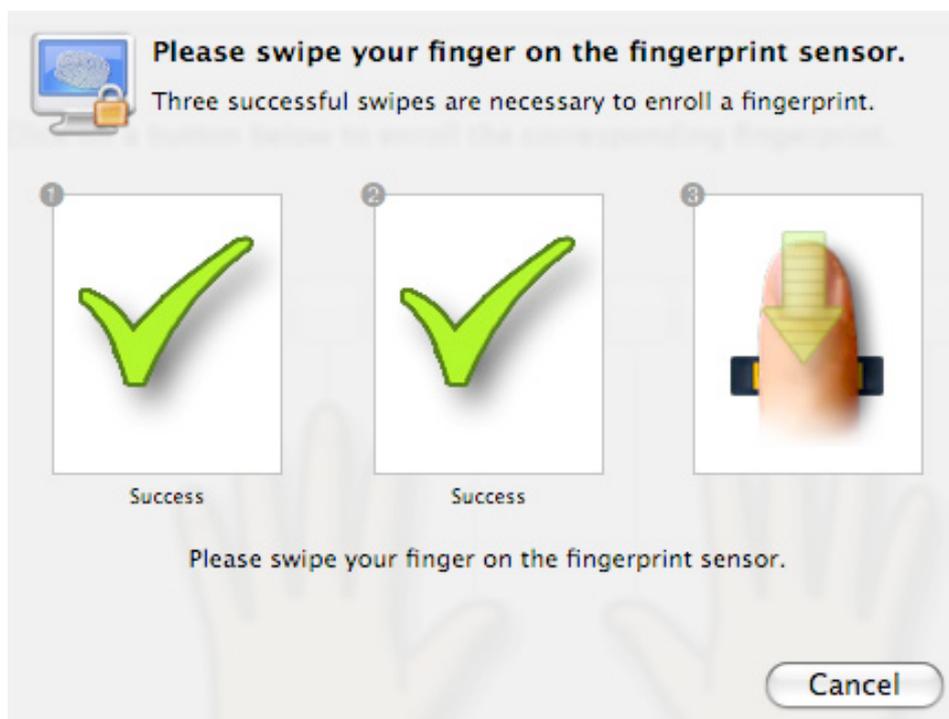


Mac OS X authentication with a fingerprint

The procedure is practically the same as on Windows computers, but the GUI looks much better, while there is less options for the initial phase. Mac OS X users are used to see far more superior interface designs and Protector Suite for Mac isn't here to prove them wrong. Every aspect of the enrollment process works

as a charm and the biometric menu mimics itself perfectly into the logon window.

While setting up the application, user can automatically chose a number of keychains (default, as well as third party such as from 1Password) that will automatically be unlocked after successful authentication.



Fingerprint sensor enrollment interface on the Mac

Final conclusion

Eikon To Go is a rather elegant little device that can come in handy in a number of situations.

During my usage I came across a couple of minor bugs, but nothing special. It would definitely be nice to see support for the latest

Firefox, as well as other browsers such as Google's Chrome.

While Windows users get all the good features, basic support for Mac OS X is a notable thing. A number of my colleagues must use Windows notebooks for work, while they use Macs at home, so this can be a good solution for them.

Mark Woodstone is a security consultant that works for a large Internet Presence Provider (IPP) that serves about 4000 clients from 30 countries worldwide.

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

HELP NET SECURITY

WWW.NET-SECURITY.ORG

HELP NET SECURITY **GFI MailEssentials** The #1 server based anti-spam solution! Download a free trial

HOME NEWS ARTICLES SOFTWARE HOWTO CLAMS EVENTS NEWSLETTERS STORE ABOUT ADVERTISE SEARCH RSS

SUBSCRIBE BY E-MAIL

- Spies served as virtual enemy
- IT security spending on the rise
- Knowledge Systems acquires Softland product line
- Netcom Computing to acquire Security
- The RFID Security Alliance (RFISA) formed

GRAB OUR RSS FEED

Reverse Engineer's Backs Arms Kicks
net-security.org

REVIEWS

- Security Prozer Tests
- Network Monitor
- Google Apps Suite
- Comodo: Understanding How Attacks and Defenses
- Big Book of Windows Hacks

REVIEWS

- LAMPand Network Security Scanner 4
- Password Safe 3.1d
- Data Protection Manager Pro 2008 1.2.0
- Data Guardian 1.0.3
- TopGuard 2008 Professional 7.4.0
- Outpost Firewall Pro 5.2.008.076.0007
- Anti-Archives Free Edition 4.106.1000

REVIEWS

- Mandriva Linux Security Update Advisory (advisory 2008-028-100)
- Gentoo Linux Security Advisory (MYSO: 2008-02-26-000004)
- Debian Linux Security Advisory (Debian-Security: 2008-02-26-000004)

Discovery and fusing for SQL injections with Web 2.0 applications
Tuesday, 11 September 2008, 10:29 PM (EST)

This paper describes some techniques and approaches to perform effective assessment on Web 2.0 applications on the basis of the recent experience and cases which were analyzed on the field.

Router evolution
Monday, 1 September 2008, 10:25 PM (EST)

Router evolution is following the same path as servers. First, vendors were identified as a separate class of hardware. Then there was a lot of media hype which led to a large number of anti-router tools and products, together with a noticeable reaction from the antivirus industry. Today both toolsets and servers have merged into the general malware domain and no longer reside any particular development "niche"; the concept of avoiding system features to hide something is obviously still valid and we are very busy to get new threats implementing stealth.

Deploying enterprise software security
Monday, 27 August 2008, 11:07 PM (EST)

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

Most organizations fail to stop interior network threats
Tuesday, 26 August 2008, 9:33 PM (EST)

A survey by Core Consulting revealed nearly half of the IT professionals who responded had endpoints connecting to their corporate networks without their knowledge. Not compared to other security issues, 80 percent of respondents said controlling network access ranked as a high priority.

Security risks for mobile computing on public Wi-Fi's
Monday, 25 August 2008, 10:40 PM (EST)

This article summarizes the effectiveness of VPN security mechanisms, data encryption, strong authentication and personal threats and shows how optimal protection can be achieved by dynamically integrating each of these technologies.

Reverse engineering: Smuggling the signature
Monday, 25 August 2008, 10:39 PM (EST)

Many antivirus and anti-spyware solutions identify malicious programs by looking for known virus signatures contained inside them. These signatures are stored inside a database which is constantly updated. This tutorial guides you through a number of steps to encrypt the executable file code section in order to evade antivirus signature checking techniques reflective against identifying the malicious code.

Internet terrorist: Does such a thing really exist?
Tuesday, 19 August 2008, 10:20 PM (EST)

In this article, a former CISO discusses the notion of worrying about the potential risk of terrorism against his organization and how it seems to be the general priority given the choices of hard, usually, terrorism today seems to be an emerging concern in the commercial world and many are actively pursuing methods and technology to help mitigate the problem. As a result, he began to research this trend to determine its drivers and possible implications to information security as we know it today.

Reputation attacks: A little known internet threat
Monday, 18 August 2008, 10:19 PM (EST)

Reputation attacks target both individuals and companies, and their goal is to run the victim's reputation. While attack techniques are varied, the consequences are often the same: a damaged reputation resulting in major losses to the victim's life. Attackers can use several methods to run a company's reputation.

Qualys Free WebScan: Proactive Vulnerability Management getting key aspects, analysis and implementation

Help Desk Reviews

QUALYS GUARD
On Demand
Vulnerability Management
Policy Compliance
PCI Compliance
14 Day Trial!

GFI EventsManager
Download your FREE trial today!

User attempted access to **Microsoft Windows** security updates
Failed to install Windows security updates

NO SECURITY
FREE SECURITY MANAGER
DOWNLOAD HERE!

Secure Email
Secure, reliable, fast, unbreakable.
No setup fees, free 1000 support.
www.Credentia.com

© 2008 GFI Inc. All rights reserved.
Vulnerability Scanning
Network Vulnerability
Event Log Security

Help Desk Reviews
Security Prozer
Network Monitor
Google Apps Suite
Comodo: Understanding How Attacks and Defenses
Big Book of Windows Hacks
LAMPand Network Security Scanner 4
Password Safe 3.1d
Data Protection Manager Pro 2008 1.2.0
Data Guardian 1.0.3
TopGuard 2008 Professional 7.4.0
Outpost Firewall Pro 5.2.008.076.0007
Anti-Archives Free Edition 4.106.1000
Mandriva Linux Security Update Advisory (advisory 2008-028-100)
Gentoo Linux Security Advisory (MYSO: 2008-02-26-000004)
Debian Linux Security Advisory (Debian-Security: 2008-02-26-000004)

10 years of information security coverage

Eight holes in Windows login controls

by François Amigorena



Windows has more security features than any other operating system but is strangely lacking the fundamental and classic login session controls found in other environment like mainframe and midrange systems, UNIX and Netware.

Windows indeed lacks:

- Concurrent logon control
- Logon/logoff reporting
- Logon session monitoring
- Remote logoff of workstation logon sessions
- Logon time restrictions by group
- Workstation restrictions by group
- Forcible logoff when allowed logon time expires
- Previous logon time and computer display when user logs on.

These are although important security controls that are required for an Information System to comply with major regulatory constraints (HIPAA, SOX, PCI, NISPOM, DCID 6/3, GLBA, US Patriot Act, FISMA) and can efficiently mitigate insider threats.

And the threat of attack from insiders is real and substantial. The 2007 E-Crime Watch Survey, (tinyurl.com/6cu9zg) conducted with the U.S. Secret Service, Carnegie Mellon University Software Engineering Institute's

CERT Program and Microsoft, found that in cases where respondents could identify the perpetrator of an electronic crime, 34% were committed by insiders (outsiders 37%, unknown 29%).

39% of these rogue insiders used compromised accounts to commit e-crimes, like unauthorized access to/use of corporate information, systems or networks, theft of intellectual property, theft of other information (including financial and customer records) and fraud.

Among best practices for the prevention and detection of insider threats recommended in the Common Sense Guide to Prevention and Detection of Insider Threats published by Carnegie Mellon University's CyLab (tinyurl.com/4er8vt) appear:

- Restricting employees' access to only those resources needed to accomplish their jobs, as access control gaps facilitate most incidents

- Logging and monitoring access to all of the organization's critical electronic assets, so that suspicious access can be detected and investigated
- Making all activity from any account attributable to its owner
- Enabling auditors or investigators to trace all online activity on any account to an individual user
- Logging, monitoring, and auditing employee online actions in order to lead to early discovery and investigation of suspicious insider actions
- Using techniques that promote non-repudiation of action in order to ensure that online actions taken by users can be attributed to the person that performed them
- Following rigorous termination procedures that disable all open access points to the
 - Networks, systems, applications, and data
 - Collecting and saving usable evidence in
 - Order to preserve response options, including legal options.

Major holes in Windows native login controls unfortunately do not allow to efficiently implementing such practices.

Hole #1: No concurrent login control

There is no way in Windows to limit a given user account from only logging on at one computer at a time. In terms of interactive logins at desktops and laptops, a system administrator cannot prevent a given user from going up to one computer, logging on there, letting somebody work as him or just leaving the computer unattended, and then walking up to another computer and logging on there.

The reason is because of the architecture of Windows: there is no entity keeping track of all the places where a user is logged on, as each workstation basically handles that individually.

Workstations have to talk to the domain controller, but the domain controller is only involved in the initial authentication. Once the domain controller tells the workstation that "Yes, this user is authentic" or, "No, he's not, his credentials were not good," then the domain controller just forgets about that logon session. It does not keep track of the fact that the user still logged on at that computer. Each

computer does that on its own. That is probably why there is no concurrent login control built into Windows in the first place.

Windows logon

Microsoft originally tried to address this major issue with an unsupported tool called Connect, provided in its Windows NT/2000 Resource Kit. However, due to the complexity to implement, the limited and poor functionality, the constraints and the additional flaws the application actually generated, few and far between are those known still actually using it. With the venue of Active Directory, Microsoft has been back to the drawing board; and whereas one would have thought that they would have properly addressed the issue, they are in fact back with another unsupported tool based on logon scripts, responding only partially to requirements and equally awkward to deploy and maintain: LimitLogin.

LimitLogin is indeed cumbersome to set up and use: For one thing, it performs an irreversible Active Directory Schema modification. For another, it creates a new partition in Active Directory. It also requires configuring a Web server with the .NET Framework and ASP.NET and setting it up to perform delegated Kerberos authentication. Finally, it requires distributing client packages that support communicating with the Web server via SOAP (a lightweight protocol for exchanging structured information in a distributed environment).

Why is controlling concurrent logins so important?

- It reduces the ability of users to share their credentials, and avoid situations like this one: a manager does not want to approve purchase requisitions and so just logs one of his subordinates on as himself and then allows him to sit there and just mindlessly approve each purchase requisition. And so, the whole business control that was intended in that case, just goes out the window.
- Some application controls depend upon controlling concurrent logins. These applications are written with the assumption that the same user will not be logged on through different sessions.

- It is necessary to enforce accountability and make sure that Bob really is Bob. In fact, sometimes investigations have been hampered because a user was able to claim, or at least try to make the claim, that someone else was logged on as them at the time that something happened, because they can show that they were logged on at their own computer.
- Not controlling concurrent logins creates a whole accountability and non-repudiation issue.

That is why this feature is required for an Information System to comply with major regulatory constraints, including:

- NISPOM (National Industrial Security Program Operating Manual – 8-303, 8-602 and 8-609 sections)
- DCID 6/3 (Director of Central Intelligence Issued Directive 6/3 – “Identification and Authentication” and “Enforcement of sessions controls” sections).

Hole #2: No logon/logoff reporting

There is no way in Windows to get a report saying “John logged on at 8:00 and he logged off at 11:00.”

The reason is again that the domain controller does not keep track of the fact that John is still logged on here at this computer. Some of you might think that if we combine the security logs on those domain controllers and filter the events correctly, we could get a report of all of the initial logons that will also show us all of these connections to other servers.

If you have tried, you know how problematic it can be just to get a list of all the initial logons from looking at your domain controller security logs, unless you have the capability to correlate multiple events down to one row on your report.

Some others might suggest that we could just track all of the network logon and logoff events and then put together a report from that that shows all logon sessions, showing us not only when John logged on but how long he stayed logged on and then when he logged off.

Well, that doesn't work. When a user maps a drive to a server, opens up a file on this server and then closes it, the file server closes (within just seconds or at the most a couple of minutes) that logon session and logs a logoff event (in the security log).

If you have tried, you know how problematic it can be just to get a list of all the initial logons from looking at your domain controller security logs, unless you have the capability to correlate multiple events down to one row on your report.

The user is still sitting at his workstation and has just no idea that he just logged off from the server. When he next tries to open up a file over here on the server, the workstation notices that he has been disconnected and the workstation silently reconnects him to the server, which generates yet another logon event on the server.

And then once he closes that file and does not have any other files open on the server, the server closes that connection again, generating another logoff event in the file server. That is why file servers usually show hundreds of logon and logoff events for the same user throughout the day. There is absolutely

no way to piece together the user's overall logon session by looking at the domain controller logs or file server logs.

And that leaves the security logs on all of your workstations. Except for some very high-security, government-related, small networks, I have never seen any company that collects all of their workstations' security logs.

That is not to say it is impossible, but you can imagine the storage and licensing costs on of trying to do that and it is therefore pretty impractical to try to use the security log to generate this important report in the first place.

Now, why is logon/logoff reporting so important?

It gives the ability to answer crucial questions when it comes to investigations following an incident. Who was really logged on? Where were they logged on? When did they log on? How long did they remain logged on? When did they log off? At any given time, which people were actually logged on at their systems? And that is what we are not getting with Windows native Windows functionality. This feature is nonetheless required for an Information System to comply with major regulatory constraints, including:

- Sarbanes-Oxley (section 404 and 802)
- LSF (French Financial Security Law – “control implementation” and “reporting” sections)
- Bâle II (European regulation for financial establishments – “Collect and log incidents” and “Reporting” sections)
- PCI (“Surveillance” and “Tracking and archiving” sections)

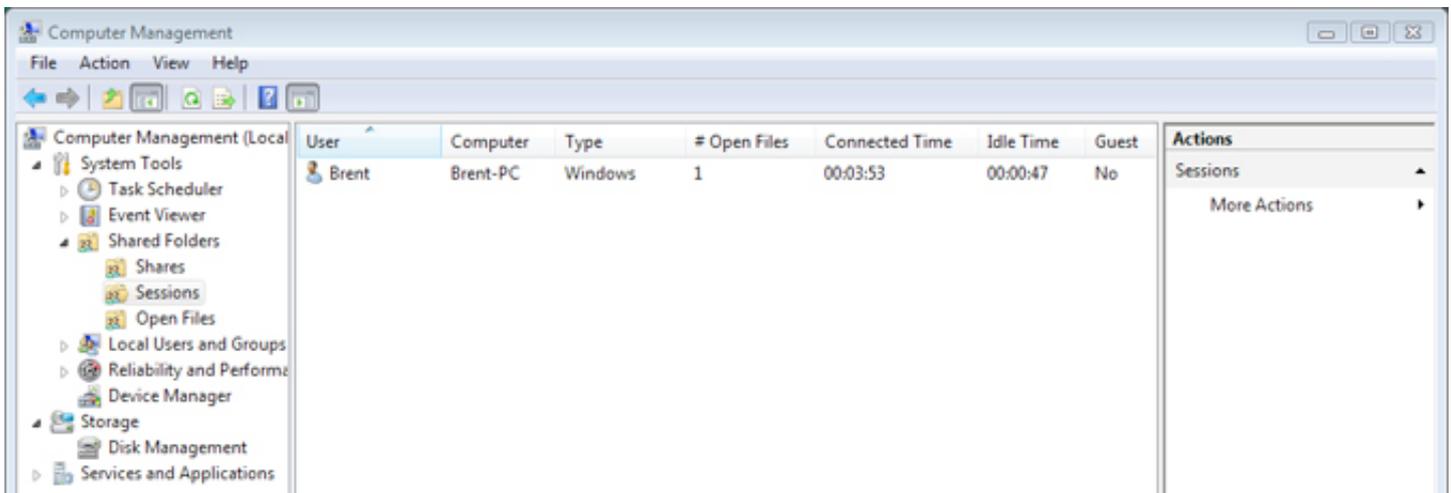
- US Patriot Act (“User monitoring and management” section).

Hole #3: No logon session monitoring

Logon session monitoring is different than logon session reporting. Logon session monitoring is being able to say, in real time, who is logged on at which computers and to answer two questions:

- What are all the computers that a given user is currently logged on at?
- Who are the users currently logged on at this particular computer?

And for the same reasons, there is no way to do that with your native Windows functionality. Instead, what you have to do is figure that out one server at a time. You can go to a given single server, go to Computer Management > Shared Folders > Sessions, and you can look it up that way. Think about how difficult that is if you have to check each computer individually.



This is even more important in some ways (for instance, with job terminations) when you need to determine immediately where is this specific user, what are all the computers where this user is potentially logged on, and you have to get him off your network.

It can also be about a resource contention issue: if a resource is currently locked by a user but that user is not at his usual workstation, a System Administrator cannot raise him on the phone or whatever to get him off.

Logon session monitoring is nevertheless required for an Information System to comply with major regulatory constraints, including:

- FISMA / NIST 800-53 / FIPS PUB 200 (“Access control” domain)
- GLBA (Gramm-Leach-Bliley Act - “Access control” section)
- HIPAA (Health Insurance Portability and Accountability Act – “Medical data protection” domain)
- US Patriot Act (“User monitoring and management” section).

Hole #4: No remote logoff of workstation logon sessions

If a system administrator needs to get a specific user off his computer, unless he has some kind of utility, he is going to have to walk down there to that building, to that floor, to that cubicle, and log him off that computer. And there are many good reasons you may want to log users off their workstations:

- Securing computers that are left unattended (even though hopefully they have a password-protected screensaver mandated)
- Freeing up locked-down resources
- Handling emergency situations.

Imagine for example that an employee (let us call him Jack) is fired and knows that his dismissal is coming. Jack is logged on at 04:00 pm and at 04:05 pm a system administrator disables and/or deletes his account.

Guess what happens? Jack is still logged on to that workstation and maybe connected to some servers. All he has to do is unlock that workstation, and typically workstations do not go and check unlock requests with the domain controller. Jack is still going to be there on that computer, even though his account has been disabled and deleted. The ability to

perform remote logoffs is nonetheless required for an Information System to comply with major regulatory constraints, including:

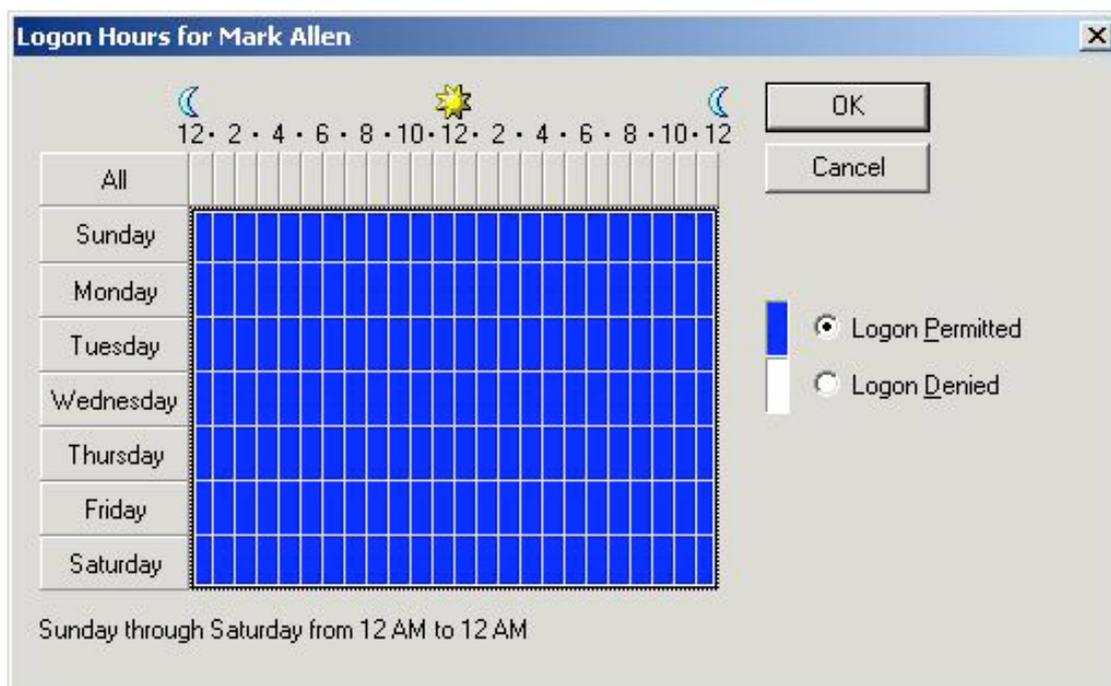
- FISMA / NIST 800-53 / FIPS PUB 200 (“Access control” domain)
- GLBA (Gramm-Leach-Bliley Act - (“Access control” section).

Hole #5: No logon time restrictions by group

Windows does provide logon time restriction functionality on a user-by-user basis.

A system administrator can go into a user’s account and restrict him to only being able to log on at certain times of the day and days of the week. But there is no way to do it by group. The best thing that can be done in Windows is selecting multiple users at the same time but I am sure you see the reasons why that is still nowhere near as manageable or as practical to use as on a group-by-group basis, especially on large and very large networks.

Enforcing time restrictions is nonetheless part of Information System requirements for compliance with major regulatory constraints, including:



- Sarbanes-Oxley (section 409)
- LSF (French Financial Security Law – “surveillance” section)
- PCI (“Surveillance” section)
- FISMA / NIST 800-53 / FIPS PUB 200 (“Access control” domain)
- GLBA (Gramm-Leach-Bliley Act - (“Access control” section)
- HIPAA (Health Insurance Portability and Accountability Act – “Medical data protection” domain)
- US Patriot Act (“User monitoring and management” section).

Hole #6: No workstation restrictions by group

Here again, Windows does provide logon workstation restriction functionality on a user-by-user basis. A system administrator can go into a user’s account and restrict him to only being able to log on from specific computers, but there is no way to do it by group and this is a real deterrent to implement and enforce an efficient access security policy.

It is indeed very relevant to reduce the number of computers on which an account could

be attacked or exploited if someone guesses the password or gets it using social engineering techniques and therefore reduce your Windows network attack surface.

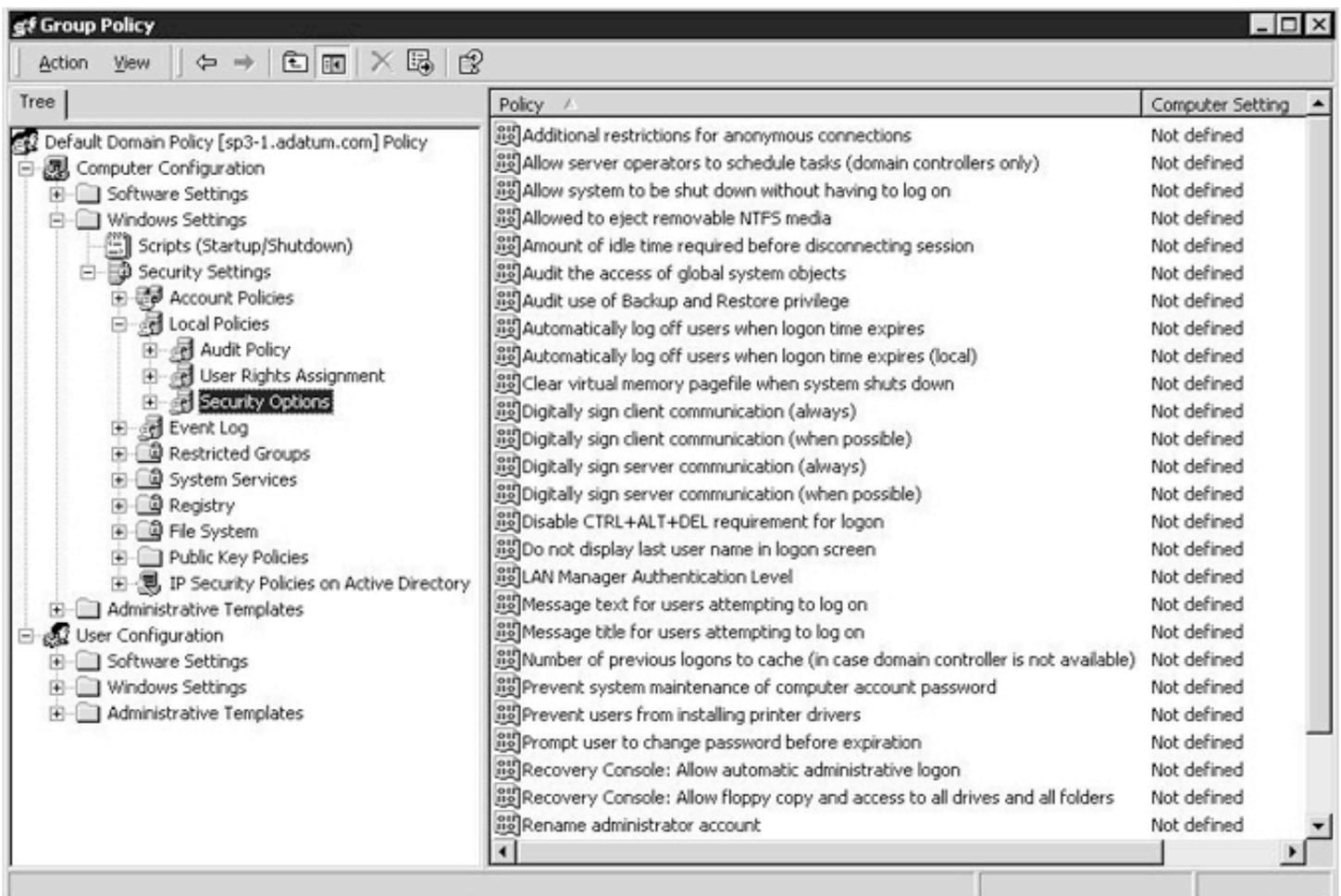
This feature is nonetheless and logically required for an Information System to comply with major regulatory constraints, including:

- FISMA / NIST 800-53 / FIPS PUB 200 (“System and information integrity” domain)
- GLBA (Gramm-Leach-Bliley Act - (“Protection against menaces” section)
- HIPAA (Health Insurance Portability and Accountability Act – “Medical data protection” domain).

Hole #7: No forcible logoff when allowed logon time expires

Using Active Directory functionality, a system administrator can define that a user (let us call her Carol this time) is limited to only being able to work from 07:00 am to 05:00 pm.

What really happens if Carol logs on at about 01:00 and remains logged on past 05:00?



Windows will not log her off of his workstation at this time, because there is no native control in Windows to perform that.

There is a setting (Local Policies > Security Options) though that might make you think that it would work that way: "Automatically log off users when logon time expires."

This setting only applies to file and print servers (SMB component). Carol logs on at her workstation and accesses a file server. If she remains logged on and accessing this file server past 05:00 pm (provided she has no files open on that file server), when 05:00 pm rolls around, the file server will disconnect her and prevent her from reconnecting to the file server itself. There is absolutely nothing in Windows that will log her off of her workstation where she is interactively logged on at the console.

This feature is nonetheless required for an Information System to comply with major regulatory constraints, including:

- FISMA / NIST 800-53 / FIPS PUB 200 ("System and information integrity" domain)
- HIPAA (Health Insurance Portability and Accountability Act – "Medical data protection" domain)
- US Patriot Act ("User monitoring and management" section).

Hole #8: No previous logon time and computer display when user logs on

Imagine the following scenario: a user is coming up to his workstation and after he correctly entered his username and password, the computer prompts a dialog box saying:

"Hello John Smith, you have been authenticated. The last time that your account was successfully logged on was at 2 am, from computer such-and-such."

What if this user recognizes that he had not logged on at that time? That would indicate that someone else had successfully logged on as him and impersonated him. This is one of the most effective ways to detect people impersonating other user accounts, providing your users are reasonably security aware. That does not exist in Windows although this feature is required for an Information System to comply with major regulatory constraints, including:

- NISPOM (National Industrial Security Program Operating Manual – 8-609 b3 section)
- DCID 6/3 (Director of Central Intelligence Issued Directive 6/3 – 4.B.4.a section).

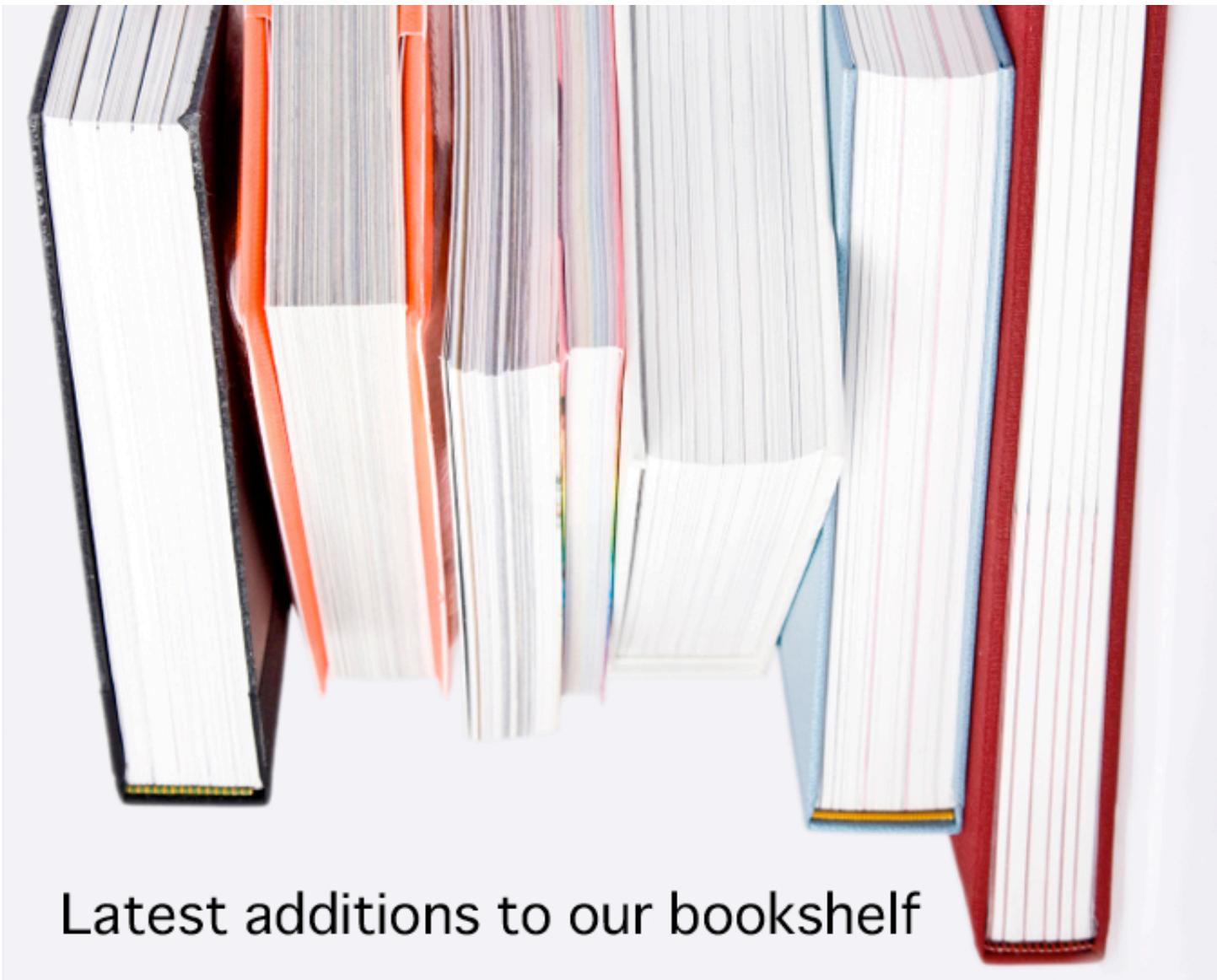
Windows does lack the mandatory session controls that would empower system administrators to efficiently mitigate insider threats and to introduce, develop and maintain IT compliance programs in their organization.

The current economic background makes the implementation of such features even more crucial. As Mark Raskino (Vice President - Gartner) recently said "An economic downturn and recovery create massive churn. The processes and tools for managing and disabling access [to IT networks] are going to be critical."

That leaves knowledgeable IT pros with no choice but to look at appropriate third-party solutions.

François Amigorena is the founder and CEO of IS Decisions (www.isdecisions.com), an Independent Software Vendor specializing in security and change management solutions for Microsoft Windows infrastructures. The IS Decisions portfolio includes UserLock (www.userlock.com), a software solution designed to secure access to Windows networks by restricting simultaneous sessions, by limiting user access to the network and by providing administrators with remote session control, alert options and advanced reporting for session analysis.

More than 500,000 UserLock licenses are already used worldwide by clients of all sizes and in all business sectors, including: BAE Systems, Ball Aerospace, Lockheed-Martin, Navy Marine Corps, NY State Organized Crime Task Force, Raytheon, Time Warner, United Nations Organization, US Bureau of Alcohol, Tobacco, Firearms & Explosives, US Department of Justice, US Department of Veterans Affairs, US State Department.

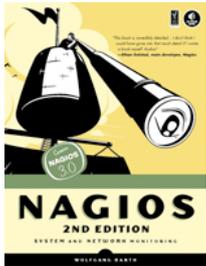


Latest additions to our bookshelf

Nagios: System and Network Monitoring, Second Edition

By Wolfgang Barth

No Starch Press, ISBN: 1593271794



Nagios, an open source system and network monitoring tool, has emerged as the most popular solution for sys admins in organizations of all sizes. Nagios can be configured to continuously monitor network services. It can also supervise host resources (processor load, disk and memory usage, running processes, log files, and so on) and environmental factors, such as temperature and humidity. This book is your guide to getting the most out of this versatile and powerful monitoring tool.

Voice over IP Security

By Patrick Park

Cisco Press, ISBN: 1587054698



Voice over IP Security focuses on the analysis of current and future threats, the evaluation of security products, the methodologies of protection, and best practices for architecture design and service deployment.

This book not only covers technology concepts and issues, but also provides detailed design solutions featuring current products and protocols so that you can deploy a secure VoIP service in the real world with confidence.



Interview with Giles Hogben, an expert on identity and authentication technologies working at ENISA

by Mirko Zorz

Giles Hogben is an expert on identity and authentication technologies working at ENISA, the European Network and Information Security Agency in Greece. He has published numerous papers on Identity Management, Privacy and the Semantic Web, including a widely cited report on "Security Issues and Recommendations for Online Social Networks". Before joining ENISA, he was a researcher at the Joint Research Centre in Ispra, and led work on private credentials in the EU PRIME project (Privacy and Identity Management for Europe), managed by IBM Research, Zurich. He graduated from Oxford University in 1994.

Along with a massive adoption of social networking comes a new dimension of threats. What are the most alarming tactics you've seen during the past year?

Actually the most alarming thing about social networks is not the malicious attacks. These tend to be the usual suspects affecting Web 2.0 applications - cross-site scripting, worms, spam etc. In fact the incidence of social network worms and XSS attacks seems to have decreased recently.

What is more alarming is the amount of personal data which ends up being either totally public or accessible to an unexpectedly large "audience". This is fueled by tools for tagging

images based on automatic face recognition and the freedom with which people are willing to trust what are essentially extremely weak access control systems and transfer highly personal data in plaintext.

Another alarming trend is the fact that people are willing to give away their email password simply in order to access their address book. People also give away social network account passwords to social aggregators in order to simplify management of their various profiles. In the absence of a more fine-grained mechanism for delegating authorization, they are left with little choice, but this is actually a very dangerous thing to do from a security point of view.

We need to see tools for more fine-grained delegation of authorization to help solve this problem.

The protection of private information is at risk because of a serious lack of both security awareness and common sense. Users tend to trust social networking sites and post an abundance of confidential data that makes them susceptible to identity theft. What can be done to mitigate this growing problem?

Firstly we can raise people's awareness of the problem so that they don't post things they might later regret. They should be told about the lifetime of data in social networks and the difficulty of erasing profiles and posts made on other people's message-boards. ENISA co-operates with various safer internet bodies which run campaigns to educate end-users about issues such as these.

Secondly, we need to find ways to give users more control over what happens to the data they do post. Currently if you want to set privacy controls over your profile, it can take a lot of effort. If you then want to move to another

social network, you have to start all over again. That's why it's very important that we move to portable formats for social networks, which are also able to transport privacy settings.

Third, a lot of privacy is lost through the actions of other people on a person's network. There is a huge increase in tagging of images for example which is something people have very little control over. I can't stop you tagging an image you post of me. Face recognition software which has now become mainstream and improvements in image upload software have made this a lot easier. Another way to give users a little more control might be to experiment with ways of licensing your own personal data - in a similar way to the way software or media content is licensed.

Finally, there is some interesting research available on how combining seemingly innocuous snippets of a person's data can allow you to derive very private things about them. This is a very difficult problem to solve, but we need more research on how to control privacy in so-called mashup scenarios.

IDENTITY THEFT AND AUTHENTICATION IS A VERY FUNDAMENTAL PROBLEM IN SOCIAL NETWORKING AND IS AT THE ROOT OF MANY OF ITS SECURITY PROBLEMS

With identity theft running rampant and malicious users opening social networking accounts under the names of other people in order to exploit their connections, is it feasible to expect the creation of some sort of online passport at some point in time? Some kind of mechanism that will allow us to prove our identity.

Identity theft and authentication is a very fundamental problem in social networking and is at the root of many of its security problems. There have been proposals to pilot the use of identity cards in Social Networks, but none of them have got off the ground. This could be because people have an instinctive aversion to using ID cards in an area which is supposed to be fun. It could also be because the technology infrastructure simply isn't there yet - I can't use ID cards across border for example and few people have a smart-card reader attached to their computer. I personally think it

would be worth testing out the use of some kind of stronger authentication tokens in social networks. It might only work in certain kinds of social networks - but something is better than nothing.

Unfortunately, though, the people who are most vulnerable might not be protected: adults often lend credit cards complete with PIN to children and there's currently no way to stop this kind of delegation with ID cards.

Another, perhaps more promising idea is the use of web-of-trust techniques for establishing identity. This is a complex problem to solve, but the social network itself (the network of contacts) could be used to establish identity. One would have to choose end-user metaphors carefully but social networks might actually be a good tool to build up trust in keys which could then be used to identify the user.

Each user could vouch for the identity of their own network of contacts using a PGP-like model for trust.

There's a multitude of social networking websites out there and many users would like to have the option to export their data to other sites and applications. What's your opinion to data portability?

I think this is an extremely important issue. There is a tendency towards a lock-in effect inherent in Social Networking revenue models, which is detrimental to user privacy and security. Business models which depend on amassing increasing amounts of personal data do not favor any measures which inhibit the viral spread of the Social Network – something which privacy and security measures often tend to do.

ENISA recommended that open formats and standards should be developed to break the data lock-in effect and counterbalance this economic and social pressure. Somewhat surprisingly, we are now seeing a few companies offering this functionality. In the last six months, three of the biggest providers, Facebook, Myspace and Google, have all issued so-called 'data portability' Application Pro-

gramme Interfaces (APIs). That is, they allow third parties to integrate a user's social network profile data into external web applications. For example Google's Friend Connect system is based on a triad of open specifications – OpenID, OpenSocial and oAuth, which allow users to display social profile information from members of their network on any web page.

It remains to be seen how much providers will actually allow the export and open transfer of their data stores rather than 'framing' them into pages (where it is still drawn from a central repository) or exposing interfaces only to selected corporate partners.

Whatever happens, in opening up these personal data stores, it is crucial that the confidentiality and privacy of the data continue to be respected; i.e. (as I mentioned before) portable access control and privacy rules must be provided along with portable data. As Nipon Das wrote in the New York Times, "Social Networking is like the Hotel California. You can check out, but you can never leave". Open standards allow users to "leave the Hotel California" but they also need a secure suitcase to take their data with them.

PEOPLE SHARE A LOT OF INFORMATION ON SOCIAL NETWORKS AND THIS CAN INCLUDE CORPORATE SECRETS

Are social networking tools becoming so important that they may impact the way security professionals approach the security of their organization's network? What advice would you give them?

From the point of view of network security, there are 3 main issues I'd highlight:

First, social networking sites are Web 2.0 style applications, with a very rich client-side. There are lots of opportunities for end-users and attackers to inject malicious content. This means they can easily carry malware into your network. Your network needs to be particularly strengthened against attacks through the browser such as cross-site scripting attacks and cross site request forgeries.

Second, people share a lot of information on social networks and this can include corporate secrets. Sometimes people might believe that the information is only shared among an intimate circle, when in fact it is accessible to a very large number of people. You should have a clear policy on what data can be published on social networks and make sure people are aware of that policy.

Finally, people spend huge amounts of corporate time on social networks. There is some debate about how harmful this really is to the company, since the value of developing social capital is difficult to put a figure to, but Global Security Systems estimated that use of Social Networking sites costs UK Corporations 8 billion Euro every year in lost productivity (infosec 2008).

Each company should consider their policy on this on a case-by-case basis. They might also experiment with different options ranging from open usage to specific times when usage is permitted (enforced by the firewall).

How do you approach your research of social networking security? How does it differ from other security-related analysis you've done in the past?

We identify the threats using a group of experts in the topic area coming from both the academia and industry. We try to use a standard risk-assessment methodology based on eBios, first identifying the assets (what to protect), then the vulnerabilities (systemic weak-

nesses) and the threats (the impact of the actual attacks exploiting the vulnerability). The expert group never actually met in person but did all our research separately and combined it using phone conferences, a mailing list and a wiki. I spent a lot of time actually trying out different social networks and we invited social networking providers to present their most important security issues at a workshop.

In our more recent studies on Gaming Security and Web 2.0, which are coming out this year, we've also used a contractor to collect information about what real end-users have experienced (you can see the results of our end-user survey on Gaming security here enisa.europa.eu/doc/pdf/other/survey_vw.pdf).

THERE IS NO TECHNOLOGY WHICH CAN SUBSTITUTE PARENTS EDUCATING THEMSELVES ABOUT SOCIAL APPLICATIONS

With the explosion of online meeting places it's becoming increasingly difficult to protect children in these environments. What can be done to make sure a youngster doesn't become the victim of cyber bullying or worse?

Some recent research we conducted in the area of online games has shown that most people trust age-verification mechanisms to protect children. Our investigation showed, however that these mechanisms are not as effective as people believe. There is no technology which can substitute parents educating themselves about social applications and at least occasionally, supervising the child online.

There are also standard help-sheets for parents available and we collected a few tips from these in our paper. For example children should be told:

- Tell a trusted adult about the bullying – and keep telling until the adult takes action.
- Do not open or read messages from cyber-bullies.
- Tell your school if it is school-related. Schools have bullying policies in place.
- Do not erase the bullying messages – they may be needed to take action.

- Never agree to meet with the person or with anyone you meet online.
- If you are threatened with harm, inform the local police or ask your parents to do so.
- Parents should look carefully at any pictures their children are posting. Is there more information in the picture than was intended, such as the location of their school?

Based on your expertise, in which way do you think social networking threats will transform 5 years from now? What's waiting for us on the horizon?

Actually I think the most important development might be that Social Networks become a security tool rather than a security threat:

Social Networking is becoming the preferred way to manage personal data. It's an area where people take an active interest in how their personal information is managed and displayed rather than being passive account-holders as in most identity management systems. I think therefore that we'll see Social Networking merging more and more with the Identity Management space. It already has all the major components of an identity management system and it's by far the biggest store of personal data on the planet.

I also think that there are huge amounts of untapped trust data in social networks. Most people can tell quite easily if a friend's profile is faked. There are many ways in which this trust data could be exploited. We might see social networks being used to build up key trust (as I mentioned above), as an alternative to PKI - for example. Also reputation built up on social networks is an important, and largely unused source of trust information.

I'm also keen to see ways of encrypting data in social networks to strengthen privacy. One dream I have is a tool for encrypting data in social networks so that your friends can see the data, and even the service provider can't. This could be combined with a smart web-of-trust scheme for key management.

One area where I do think that threats may emerge is in the merger between Social Networks and online worlds. Avatars tend to give people a false sense of security and encour-

age them to disclose even more personal data about the real user behind the avatar. We are seeing a growing number of social applications using 3D worlds and more and more real-world data appearing inside virtual worlds. ENISA has just published a paper on security issues in online games and virtual worlds, which has been extremely interesting to work on.

Also as social networks migrate onto mobile phones, we're likely to see more location data and images involving unsuspecting (and possibly unwilling) subjects. The number of images published and specifically those which have been automatically tagged with personal data using face-recognition software is increasing very rapidly. The use of image search technology (with face-recognition included) is only just starting to make itself felt. I think this will become a more important threat in the future.

Everything is vulnerable

OSVDB is an independent and open source database created by and for the community. Our goal is to provide accurate, detailed, current, and unbiased technical information.

WWW.OSVDB.ORG



Extended validation and online security: EV SSL gets the green light

by Melih Abdulhayoglu

I am proud of my role in the genesis of my brainchild, the CA/B Forum and its offspring, the EV SSL certificate.

One morning in the spring of 2005, I shuffled into the spare bedroom in my pajamas to begin working on my dream, of an Internet where users move around freely, buying and selling without fear. Before this, any fraudster with \$20 in his or her pocket could buy an SSL certificate. They could set up a spurious website to con people out of their hard-earned money. Internet users deserved more security than that, and I believed that Certificate Authorities and Internet Browser providers could provide it.

I called my contacts at VeriSign first. I explained the need for establishing trust online. I invited them to join me in my effort to set industry-wide standards. A month later, the whole industry turned up to this very first industry gathering.

And so, the CA/B Forum (Certificate Authorities & Browsers Forum), which eventually

grew to 25 Certificate Authorities and Internet Browser vendors, was born. Thanks to close cooperation by all members, the CA/B Forum arrived at a new, higher standard of protection for all Internet users – the EV SSL certificate.

On June 12th, 2007, the CA/Browser forum officially ratified the first version of the Extended Validation (EV) SSL Guidelines.

Understanding Extended Validation

Extended Validation Secure Sockets Layer or EV SSL is the industry's response to tackle the rising problem of Internet fraud. It is built on existing SSL certificate standards, and aims to eliminate shortcomings in the current authentication process. The standard SSL format operates between the browser and the website, and secures all information in transit. The browser uses the SSL certificate to not only verify the credentials of the Certificate

Certificate Authority (CA) but also confirm that the URL displayed in the address bar corresponds with the domain mentioned in the certificate. The golden padlock, familiar to users everywhere, displays on the webpage to indicate that a secure connection has been established between the browser and the website.

While SSL certification assures users that any information they transmit during an online transaction is protected against tampering by a third party, it does nothing to identify the website to be what it claims to be. Users, for all practical purposes, might be sending confidential data to a phisher rather than the organization they think they are transacting with. Even though the communication process is secure, no one has checked that the web site is trustworthy.

Minimal verification of applicant websites has undermined the very purpose of SSL over the years. CAs agreed that they could do better. There are standard verification processes prior to SSL certification, but no compliance norms. The ease of acquiring SSL certificates has even encouraged phishers and other malicious entities to use them in officially establishing their credibility. Going strictly by the padlock, can shoppers on a retail site for instance, be absolutely sure that their credit card information is indeed being communicated to the right website? Are they on the same page? Maybe not.

MINIMAL VERIFICATION OF APPLICANT WEB SITES HAS UNDERMINED THE VERY PURPOSE OF SSL OVER THE YEARS.

The next generation EV SSL certification incorporates some of the highest standards in identity assurance to establish the legitimacy of online entities. With EV SSL, Certificate Authorities put the websites through rigorous evaluation procedures and meticulous documentation checks to confirm their authenticity and ownership. This systematic authentication process, also known as the Extended Validation Standard is based on a set of guidelines prescribed by the Forum for member CAs to adhere to when they receive a request for a digital certificate from an organization or business entity.

These include:

Customers of organizations such as banks and financial institutions have been at the receiving end of phishing scams and online fraud. These attacks not only place the reputation of these businesses at risk, they diminish customer confidence in transacting online. Studies indicate that a significant number of Internet users – business, commercial or social – do not trust existing online security processes. Moreover, they think online businesses are not doing enough to secure the information they are required to send during a transaction.

Research shows that the average online retailer loses over half of its potential customers to lack of user confidence in the web site's security infrastructure. Some current verification processes for SSL certification obviously are not enough to prevent identity and data theft by fraudulent websites. Perceptions, however, vary about the utility of SSL: most network experts consider it as a complete tool for online security. Agreed it's quite efficient; is it sufficient as well?

The CA/B Forum was the result of our efforts in securing the Internet for every user. Consisting of a consortium of leading CAs and Internet browser providers, the Forum aims to address user concerns by raising the bar on standard SSL validation processes through the Extended Validation SSL Certificate.

- Establishing the legal, physical and operational existence of the entity
- Verifying that the entity's identity matches official records like incorporation and business licensing information
- Confirming that the entity owns or has exclusive rights to use the domain mentioned in the application for certification
- Confirming that the request for an EV certificate has been authorized by the entity.

Since it is mandatory for the CAs to enforce the uniform issuance process, all entities requesting EV SSL certificates go through the same intensive verification check prior to validation.

All information provided by the company making the request is independently checked and verified by third-party resources. Consequently, the turnaround time for issuing an EV certificate is a tad longer than typical instantaneous SSL certification. The EV issuance policy also contains a revocation clause that empowers the CA to revoke the EV SSL certificate in the event of malicious use or expiry of validity.

The objective of the EV issuance process is to enable users to distinguish legitimate websites

from phishing sites, building their trust in on-line commercial transactions and increasing participation. Certification is provided only for a maximum of two years. Websites with SSL certification can choose to upgrade to the EV format provided they satisfy the eligibility requirements. A CA can issue an EV SSL certificate only after successfully completing an independent WebTrust audit every year. Additionally, it is allowed to issue EV certificates only in those countries where it has a legal presence.

CONSEQUENTLY, THE TURNAROUND TIME FOR ISSUING AN EV CERTIFICATE IS A TAD LONGER THAN TYPICAL INSTANTANEOUS SSL CERTIFICATION.

Recognizing an EV SSL-certified website

Green is good to go

An EV SSL certification works at two levels: a. It assures the user of the web site's authenticity through third-party verification, and, b. It provides a clear visual representation of the web site's identity on the browser. High-security browsers read EV-SSL standards differently, the primary focus being to project the web site's security profile in a more visible way. To enable users to immediately identify an authenticated website, the address bar on the browser is displayed in bright green. The web site's security status is also displayed alongside, with the tag alternating between the identity and location of the authenticated entity, and the CA that provided the validation. A mouse rollover on the security status bar will also reveal detailed information about the company operating the website. Additionally, EV SSL incorporates the SSL feature of encrypting information moving from the user to the website's server.

...white, yellow and red

EV-ready browsers support SSL just like before. In the IE 7.0 browser, a white address bar on a non-SSL website indicates to the user that the site may be safe to browse, but there is no identity information available. The address bar on an SSL-certified website is also white and carries the padlock against a blue background, but the user has to make the call on the genuineness of the site. When the address bar is yellow or red, it's the browser's

phishing filter warning the user about a possible or known phishing site.

IE 7.0 was the first browser to recognize EV SSL certification. New generation browsers like Firefox 3.0, Opera 9.5 and Google Chrome also support EV certification, displaying the green address bar for validated websites. Not all browsers recognize it though; older browsers will continue to display the SSL padlock even for EV-certified websites. The format has found support among major Internet browser vendors with newer versions offering browser interfaces incorporating EV display requirements as well as enhanced security features. Since user safety is an important component of browser development, the introduction and implementation of EV SSL standards has added more power to online security.

Operating systems running on Windows XP will not recognize EV SSL certification even on an IE 7.0 browser. Windows Vista on the other hand, has been designed to support EV standards and display the authenticated information of the validated website. All EV SSL solutions provide an upgrade tool for XP users to enable compatibility.

With Extended Validation, users are assured that the confidential information sent to an EV-certified website is protected from third-party access; they also have authenticated confirmation about the identity of the site. Additionally, they are warned when re-directed to a phishing site from an EV-certified site.

Businesses on the other hand, can be absolutely sure their websites cannot be hijacked by malicious entities on the Internet.

How EV SSL establishes trust online

The CA/B Forum mandates that EV SSL certificates are issued only to entities with a particular profile. They may be private organizations, government agencies, businesses, partnerships and even unincorporated and proprietorship companies. Regardless of size or background, any entity has to fulfill certain criteria to be eligible for the certification including presenting documentary evidence. Strict guidelines specified by the CA/B Forum govern the issuance of EV SSL certificates. A rigorous vetting process precedes the certification of a website. The clear intent of the exercise is not only to establish the authenticity of the website, but also to confirm the identity of the people or entity owning the website. EV SSL solutions are offered by all the members of the CA/B Forum.

Currently, over 50% of web browsers support EV SSL. Users will continue to upgrade to high-security browsers to ensure a safer Inter-

net experience. More and more Internet users recognize the 'green' browser as one that completely addresses the twin concerns of information security and website identity. This translates into higher user participation, conversion and online sales especially for online businesses, without fear of the visitor abandoning the transaction mid-way. When trust is established, customer retention is the result.

Online sales and security cannot exist in mutually exclusive zones. How a business fares on the Internet is entirely dependent on the perception of the user about the web site's security environment. The EV SSL certification is currently the highest standard authenticating a web site's identity in the marketplace. Adoption of EV standards ensures that small businesses have a level-playing field in the context of competing with larger organizations. Likewise, customers are more likely to choose a 'green' site against one that doesn't indicate its identity or security status. EV SSL is by far, the best defense against phishers for every business with an online presence; the competitive advantage in terms of increased customer activity and sales is substantial.

THE CA/B FORUM MANDATES THAT EV SSL CERTIFICATES ARE ISSUED ONLY TO ENTITIES WITH A PARTICULAR PROFILE.

Keeping the faith

EV SSL certification is especially relevant for online entities that allow commercial transactions, store personal data of users, share confidential information or are required by law to meet regulatory compliance standards. This is not to say that SSL certification has outlived its purpose. But phishers are getting savvier by the day; identity and data theft can have serious repercussions on the company's reputation, business and even its very survival. As more users move towards the new generation

browsers and expect an EV-authenticated site when they transact or share information, online business entities will need to look at the big picture – one where the customer moves into the website, or moves on.

EV SSL is all about re-establishing customers' trust online. By letting Internet users know about the true identity of each website they visit and transact on, EV SSL standards have introduced a new environment of security, confidence and reassurance on the web.

Melih Abdulhayoglu created Comodo (www.comodo.com) in 1998 with a bold vision of making the Trusted Internet a reality for all. He is the CEO and Chief Security Architect of the Comodo companies which provide the infrastructure that is essential in enabling e-merchants, other Internet-connected companies, software companies, and individual consumers to interact and conduct business via the Internet safely and securely. The Comodo companies offer PKI SSL, Code Signing, Content Verification and E-Mail Certificates, award winning PC security software, vulnerability scanning services for PCI Compliance, secure e-mail and fax services.

MIS TRAINING INSTITUTE'S

INFOSEC WORLD

March 7-13, 2009, ORLANDO, FL
Disney's Coronado Springs Resort

CONFERENCE & EXPO 2009

Featuring Practitioner-Led Sessions from the Following Organizations: (partial listing)

American Express	Lockheed Martin	Siemens Financial Services
Bancshares, Inc.	Macy's	Starwood Hotels and Resorts
Bank of New York Mellon	Mayo Clinic	State of California
Burton Group	McAfee, Inc.	State of Montana
Cardinal Health	Memorial Sloan-Kettering Cancer Center	State Street Bank
Carnegie Mellon University	Merck & Co., Inc.	Stevens Institute of Technology
Coca-Cola Enterprises	Michigan State University	Susquehanna
Department of Veterans' Affairs	Mitre Corp	Texas Instruments
DeVry, Inc.	Motorola	The Nemours Foundation
eBay	National Aquarium	The Timken Company
EMC ² Corporation	NIST	Towers Perrin
General Dynamics	Oak Ridge National Laboratory	University of Arizona
HSBC	PremiereTec Companies	University of Michigan
Humana, Inc.	Progressive Insurance	University of Nebraska at Omaha
Internal Revenue Service	Prudential	Wachovia Corp.
JPMorgan	Purdue University	ZipRealty

KEYNOTE SPEAKERS



DR. WHITFIELD DIFFIE
Vice President, Sun Fellow,
Chief Security Officer,
Sun Microsystems



MICHAEL T. ROCHFORD
Director, Office of
Counterintelligence;
Director, Field Intelligence
Element, Global Initiatives
Directorate, Oak Ridge
National Laboratory

CISO SUMMIT CHAIR



PROF. HOWARD A. SCHMIDT
CISSP, (ISC)²
Security Strategist;
former White
House Cyber
Security Advisor



CO-LOCATED SUMMITS:

CISO EXECUTIVE SUMMIT, March 8

SUMMIT ON IT GOVERNANCE, RISK & COMPLIANCE, March 12

SUMMIT ON KEEPING GOVERNMENT DATA CONFIDENTIAL, March 12



EARN UP TO 51 CPEs WITH
THE WORLD PASS!

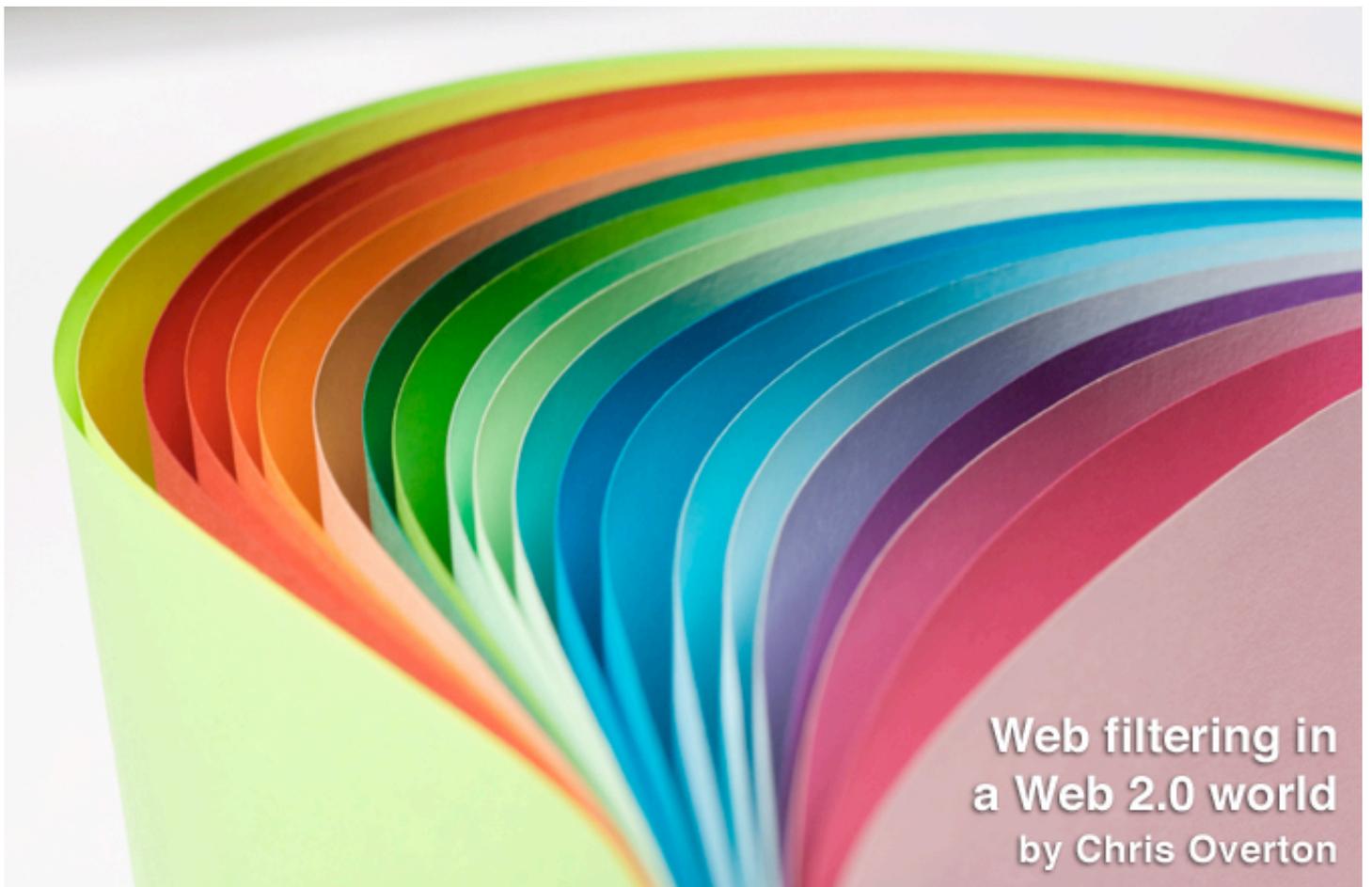
www.misti.com/infosecworld



The International Leader
in Audit & Information
Security Training

PLATINUM SPONSORS





Web filtering in a Web 2.0 world by Chris Overton

First introduced by Tim O'Reilly at the first O'Reilly Media Web 2.0 conference in 2004, Web 2.0 has become a widely used term, with a variety of definitions. The term Web 2.0 is a buzzword more than the name of a technology. What has changed is the way software developers and end-users utilize the Web, presenting both technical and social vulnerabilities.

It is the dynamic and interactive nature of Web 2.0 technologies that makes these applications inherently difficult to secure. Couple that with the use of AJAX (and other similar technologies) and the speed with which new 2.0 applications and widgets are created and launched, and it becomes apparent why consumer-focused web-apps and social networking sites are a serious threat to business IT systems and to corporations themselves.

Security challenges

Consumer-oriented Web 2.0 tools like Facebook, YouTube, Craigslist, LinkedIn and Wikipedia, as well as interactions through blogs, RSS feeds and other technologies such as Twitter, are increasingly being used in and by business. Sometimes this use is condoned or even encouraged when used as a business networking tool. In other instances, employees are simply using these tools for personal

benefits as they would use them at home. Many companies are doing little or nothing to prevent the use of these sites at work.

The implications are serious. A new study by Facetime Communications reveals that 60% of IT managers surveyed report employee use of social networks at work. And with the growth in usage, has come an increase in the number of security incidents. Nearly one quarter of the organizations had been hit by at least one web-borne attack costing the business an average of \$50,000 per month, according to the report. The main attacks were viruses, Trojans and worms (59 per cent), and spyware (57 per cent).

By increasing the availability of social networking tools, Web 2.0 sites are unwittingly providing a forum for hackers to practice social engineering.

Social networks, whether for business or personal use, rely on trust, and it is proving all too easy for attackers and botnet owners to push out new threats wherein, for example, a Facebook member unwittingly becomes the distributor of malware, or an infected fake application.

In a Web 2.0 world where users upload code themselves, and drag application code from other places – often with no idea what they are bringing in to their site or network – there is no way to patch this vulnerability.

Web 2.0 technology vulnerabilities

Web 2.0 sites typically feature a rich, user-friendly interface based on AJAX (asynchro-

nous JavaScript and XML), Adobe Flex, OpenLaszlo or similar rich media.

The JavaScript hijacking vulnerability in Ajax has been relatively well documented. Research suggests that most “Ajax like” technologies are vulnerable to it. In order to protect against this type of vulnerability, security solutions must have the ability analyze content as it comes across the wire.

Even if sites with malicious code have been identified and taken down, cached copies of the pages probably exist in many locations across the web. This caching problem can defeat security solutions that depend on the idea of identifying the original source of the content to determine whether to allow or deny access.

Social networks, whether for business or personal use, rely on trust, and it is proving all too easy for attackers and botnet owners to push out new threats.

Social networking exploits and malicious attacks

The famous “Samy” MySpace worm in 2005, in which a MySpace user named Samy created a worm that automatically added millions of MySpace users as his friend was a wake up call to the dangers of Web 2.0. Samy's code utilized XMLHttpRequest - a JavaScript object used in AJAX, or Web 2.0, applications.

Since then the threats to corporate and individual security and privacy have continued to expand and evolve. In June 2007, a MySpace worm turned 100,000 MySpace users' sites into zombies hosting malware. How to block such fluid attacks is still a question.

In January 2008 there was a social networking attack targeting Facebook users. The exploit – called “Secret Crush” – duped users into inviting friends to join them in downloading the “crush calculator.” This catchy application turned out to be a malicious widget that downloaded adware.

According to web security company Fortinet, who revealed the problem, the widget, which acts as a social worm, was being used by three per cent of the Facebook community or around one million users. Unsuspecting users

“freely” chose to install the widget at the cost of disclosing their personal information.

In August 2008, a new worm was discovered that targeted Facebook and MySpace users.

According to Kaspersky Labs – “The messages look like they contain links to video clips. When clicked on they prompt the recipient to download an executable file that purports to be the latest version of Flash Player. Instead, it is the worm itself, infecting yet another victim.

This social networking worm is another vector for installing an actual executable on your computer and turning your machine into a zombie. When infected machines log onto the social networks the next time their computers automatically send the malicious messages out to new victims grabbed from the friend list.”

The security aspects of social networks and the use of social engineering to hack these networks is a reality. In the face of these socially engineered attacks it is not unreasonable for some companies to consider blocking employee access to social networks.

The business risks of Web 2.0

The implications for business of not managing and securing employee access to the Internet can be substantial. The un-tested nature of many Web 2.0 tools and social engineering represent a justifiable reason for concern.

Business is necessarily focused on reducing costs and limiting risks, both in terms of Internet security breaches and liability. Reduced employee productivity, bandwidth drain and compliance issues are the other major reasons of concern by business, and why a sizeable number of companies currently block social networking sites (Dark Reading, November 2007 - 50 per cent of companies block social networking sites).

Security breaches - Threats include Viruses, Trojans, Spyware and phishing attacks that result in lost financial or other proprietary data. In addition to compromising your network a security breach can result in reputation damage and loss of profit.

Employee productivity – Business productivity is at risk from unfiltered and unmonitored use of the Internet:

- Use of social sites such as FaceBook, LinkedIn, YouTube, Flickr, Craig’s List, Wikipedia, Twitter, and IM, VoIP and chat, can impact time spent working. The same applies for time spent surfing the Internet, shopping

online, viewing pornography, gambling or playing games online at work.

- Breaches also consume significant IT resources in troubleshooting and recovering from an intrusion.

Bandwidth utilization – Use of high bandwidth P2P sites can lead to bandwidth congestion, additional costs for bandwidth utilization, and a compromised customer experience.

Legal Liability - Uncontrolled use of network resources can raise a variety of legal issues:

- Unauthorized access and distribution or disclosure (inadvertent or purposeful) of information assets, proprietary information, passwords and research data.
- Exposure to unwanted and often offensive content such as pornography can lead to a sexual harassment complaint because an employee is exposed to pornography through another person’s computer, and claims against the business under Employment and Sex Discrimination legislation (if employers do not proactively manage Internet access), as well as claims resulting from the transmitting of viruses and claims for denial of service.

Regulatory compliance - A growing raft of government regulations dictate effective systems and processes for data control, including the security of client or customer data.

Breaches also consume significant IT resources in troubleshooting and recovering from an intrusion.

Web 2.0 and Web filtering – the challenge

The primary approach used by web filtering companies has historically been crawling. Crawlers canvas the Internet and use a set of rules to analyze the content that they find and put it into a category. This category information is then stored and used to filter the sites that users see. This approach works well for sites that are fairly static. If the site content doesn’t change often, or the site has a static theme (e.g.: cnn.com will always mean “News”), this approach will deliver quality

categorization and filtering. However, because of their interactive nature, the content of Web 2.0 sites changes rapidly. Also, many of these sites (YouTube, FaceBook, MySpace, etc.) don’t really have a standard theme. They may deliver content related to literally anything.

The result of this is that standard methods of crawling to determine site content don’t do an effective job of categorization, and therefore don’t lend themselves well to filtering these sites.

AJAX provides a way for web developers to pull content from any number of back-end systems asynchronously, and display it. The web development approach exemplified by AJAX (and other similar rich web development methodologies) allows web page content to be pulled out of a database asynchronously and displayed dynamically. This causes major problems for categorization companies that rely on crawlers, because the content of the page is almost never going to be exactly the same when you visit it.

Some filtering companies use heuristic methods to categorize page content as it is loaded. This is a reasonable approach, but can yield lots of false categorizations (and therefore false blocks) and is much slower (from the end user's perspective) than crawler/database categorization.

Web 2.0 user-contributed content means that the content on the hundreds of thousands of URLs is constantly changing. Web filtering solutions are having to evolve to respond to the dynamic content that characterizes Web 2.0 sites, and to do so in a way that can monitor and control employee access to web sites without impacting network performance or employee productivity, as part of a comprehensive approach to Internet threats.

Domain Name Service (DNS) based web filtering software provides a security tool to help mitigate Internet risks and keep employees away from potentially harmful sites altogether - blocking questionable or undesirable content. DNS filters may be deployed and managed entirely offsite and provide a near real time protection to current web threats.

New domains are detected and classified at centralized locations and then pushed out to the DNS filters in near real time. Requested user sites are then compared against a list of allowed or known malicious sites.

Users are prevented from visiting the harmful sites by the return of a blocked server address rather than the actual server address.

This process is fast, transparent to the user, and requires no third party software installation on the client machine. This filtering capability complements any secure firewall and eliminates the threat of known malicious web-sites by preventing access to them.

Additional filter categories may allow the business to prevent users from visiting good, but time wasting, categories like auction sites as well.

For many companies, the best way to mitigate Internet risks is still to keep people away from potentially harmful sites altogether.

Balancing risk with flexibility

Currently web filtering services and software remain among the best ways to mitigate Internet risk, particularly for small business, while providing companies with the ability to customize filtration settings. The fact remains that although we are in an era in which applica-

tions are moving to the Web, a large number of web sites, applications, and social networks have vulnerabilities.

For many companies, the best way to mitigate Internet risks is still to keep people away from potentially harmful sites altogether.

Chris Overton is VP Product Development at CyberPatrol (www.cyberpatrol.com) a provider of web and content filtering software and services.

Chris has 10 years of experience in developing successful commercial security software. Prior to CyberPatrol he served as a software architect at Computer Associates where he led the effort to develop CA's next generation Anti-Spyware and Anti-Virus SDKs. Earlier his work as lead architect for PestPatrol developing an Anti-Spyware SDK and Version 5.x Consumer products was a key factor in PestPatrol's success. He is a graduate of East Tennessee State University, with a Master's Degree in Computer Science.

RSA Conference Europe 2008

by Sandro Gauci



RSA Europe is one of the major conferences taking place in London where experts share their knowledge on various topics that inadvertently fall under the permissive hood of Information Security.

Compared to other security conferences such as Black Hat, RSA Europe seemed to take a more general view of security by having panels on subjects such as Privacy, EU's telco legal frameworks and authentication issues faced by the financial industry. In that aspect, I found out that RSA Europe offers more diversity and tries to address the real issues rather than focusing on the more sensational security exploits for its content. On the other hand, at this conference one can easily find himself in a marketing driven presentation if he or she is not too careful.

During the three days between 27th and 29th October, I was able to attend a variety of presentations, panels and the occasional keynote. There were 10 tracks in total which sometimes made it quite a challenge to choose which presentation to sit through. The tracks consisted of the following:

- Developers and Applications
- Security Services

- Business of Security
- Hosts
- Hot Topics
- Governance
- Networks
- Professional Development
- Research and Threats
- Sponsored Sessions

The following is a taste of some of the presentations I personally attended.

Locking the back door: new backdoor threats in application security

One of the first presentations that I attended was by Chris Wysopal, CTO of Veracode. The presentation went through some historic backdoors such the one in Quake that was published back in 1998. It also covered the more recent vulnerabilities such as one in Wordpress 2.1.1. By looking at backdoors from the past, one can get an idea of how to identify and track backdoors in larger



applications where code review is not feasible. An example of this is if you are reviewing an application for backdoors, you would probably want to look at network traffic which is passed through cryptographic APIs. The presentation shifted to explaining how with web applications some conditions change because the application in question is remote and the researcher does not necessarily have access to it. This means that the victim might not be able to inspect the application since it is remote. Overall, an excellent presentation supported by a large amount of public content.

Web 2.0 security testing

Next up, Billy Hoffman from Hewlett Packard gave a presentation on Web 2.0 security testing. This presentation was delivered very well and explained the main difference between testing traditional websites and Web 2.0 websites. With traditional websites or web applications most of the logic resides on the server-side.

Conversely, with Web 2.0 websites a lot of work is now being done on the client-side and this presents a major paradigm shift when it comes to security testing. Billy was able to captivate the audience by providing excellent examples of atrocious mistakes that Web 2.0 developers make, some of which were based

on his first hand experience. For example, one administrative interface at an online casino was basing its authentication on a Flash SWF file which could be inspected and bypassed by anyone accessing this SWF file. Another example was the case of the coupon codes for Macworld Conference and Expo being hidden in Javascript within the registration website, granting free passes to the conference for anyone who understood the system.

Regular expressions as a basis for security products are dead

The presentation by Steve Moyle of Secerno was mostly an exercise in attacking the naive usage of Regular Expressions. This talk was listed as an “Advanced Technical” track, but in reality it boiled down to showing the severe limitations of string matching through regular expressions. Some of the examples given were usage of comments and char() functions to bypass regular expressions that do not try to handle such scenarios.

The audience was then introduced to an alternative to regular expressions, which is obviously what Secerno uses in their products. They explained how SQL servers can be protected by a security solution that knows the grammar of the SQL statements and which uses the operating context.



Bruce Schneier in action.

Beyond username and password: what European financial institutions are doing to protect customers

This panel included panelists Marc Cramer from ING, Mark Stanhope from Lloyds TSB and Xavier Serrano Cossio from Banco Sabadell.

This panel covered phishing extensively and the panelists examined how it is evolving to more targeted and sophisticated social engineering attacks. In fact, some of the techniques mentioned sounded very similar to techniques used for targeted marketing.

There was also mention of how one time passwords or OTP are still vulnerable to Man in the Middle attacks. In one particular case, the fake (phishing) website asked for the one time password which was then relayed to the legitimate bank's website. The fraudster was then able to access the victim's accounts. The obvious conclusion at the end of the panel was that online banking is a very challenging area and no single technology will solve the security issues.

The future of privacy

The keynote room during by Bruce Schneier's presentation was standing room only. The keynote was titled "The Future of Privacy" and outlined how technology is constantly lowering our privacy barriers.

Bruce mentioned many privacy unfriendly technologies such as CCTV, mobile phones and social networking and debunked some of the myth surrounding the idea of Privacy versus Security. Of course, if you ever read any of his recent blog posts or books, you'll notice that it's all been said before and this keynote was just a rehash of previous publications. At some point to me it felt as if I've already been through this keynote in some other conference or by reading one of his papers.

Real-life social networking

Of course I attended other presentations, but what about the people attending the RSA Conference? One of the main reasons that many visit these conferences is not simply the content of the presentations, but the social



aspect. However, if you are the antisocial type you might want to look at the airwaves for clues about the sort of neighbors made it to RSA Europe. When I did that for 10 minutes by gathering wireless traffic which showed people checking their email through Outlook Web Access, Gmail and POP3 with no encryption. One could also notice the VPN traffic and a large amount of SSL traffic too.

On a less geeky level, I met a few old faces from Infosec Europe and Black Hat Europe. Apart from the receptions held by the RSA Conference, there was a security bloggers meetup that I attended. It was an excellent experience as it is always good to meet fellow security professionals. Additionally, thanks to mobile devices one could get coverage of

session tracks that they missed by following the “#rsa” tag on twitter. Various people in different rooms were giving live updates and one can still read these short posts by searching for #rsa on search.twitter.com.

To summarize, RSA Europe had a good mixture of business, management and technical content. Most of the presentations were of high quality and it was a good chance to hear from and speak to the experts themselves. Additionally, RSA Europe is an excellent event for networking with others who are passionate about security and do not necessarily work in the same industry. If you are looking for a change of pace from traditional security conferences I recommend that you try an RSA event local to your continent.

Sandro Gauci is the owner and Founder of EnableSecurity (www.enablesecurity.com) where he performs R&D and security consultancy for mid-sized companies. Sandro has over 8 years experience in the security industry and is focused on analysis of security challenges and providing solutions to such threats. His passion is vulnerability research and has previously worked together with various vendors such as Microsoft and Sun to fix security holes.

Sandro is the author of the free VoIP security scanning suite SIPVicious (sipvicious.org) and can be contacted at sandro@enablesecurity.com. Read his blog at blog.enablesecurity.com



USERNAME:
PASSWORD:

The role of password management in compliance with the data protection act

by Stephane Fymat

Many organizations collect personal data as part of their daily business. Names, addresses, phone numbers, income and credit histories, and bank account details are all collected and stored in a database. Because this information is very sensitive, it is governed by the 1998 Data Protection Act (DPA). The Act gives people the right to know what data is held about them and to make changes to any inaccurate records. It also requires the organizations themselves to maintain stringent security to protect the personal information they gather.

All organizations that hold or process personal records of any form – electronic or paper based - must comply with DPA requirements, whether they operate in the public or private sector and regardless of their size. Enforcement is the responsibility of the Information Commissioner's Office (ICO), which has the right periodically to audit compliance and issue fines to any organization found to be in breach of the law.

Unfortunately, the ICO has its work cut out for it. Far too often the IT security measures put in place to secure personal data from unauthorized use have failed to keep pace with data volumes and developments in storage, networking and data manipulation technologies. The pervasiveness of complex network-

ing technology, widespread internet-based services and the ability to integrate electronic records has transformed data management, but highlighted systemic weaknesses in IT security measures.

Even the kiosks that have been widely adopted by public bodies to provide access to publicly available information have become a problem. Library or hospital staff who use a kiosk to open up applications containing personal information can easily step away, leaving the data exposed to anyone who passes by.

These and other issues have led to highly publicized breaches of personal information privacy such as disclosures of credit card

details, network hacking incidents, and misdirected emails. A number of high profile cases have highlighted what can happen when passwords are misused.

For example, in 2007 TJ Maxx admitted that hackers had stolen credit and debit card numbers from the company over an 18 month period putting over 45 million customers at risk. The security breach, which cost the firm an estimated \$4.5 billion, was put down to TJ Maxx's failure to secure its network from attack. A TJ Maxx employee later revealed the shocking extent of the company's lax security, claiming employees were able to log on to company servers with blank passwords and

passwords and usernames were written on post-it notes.

Incidents such as this one have intensified the public's privacy fears, yielding a recent finding that 95 per cent of individuals rank personal data protection among their top three concerns.

That, of course, is where the DPA comes in. The Act mandates protection of the integrity, confidentiality and availability of individually identifiable information. Organizations need to make sure that only authorized personnel can access the data, and that accurate records show who has seen the records as well as what changes have been made.

Password protection of all applications, databases and systems is the first step in preventing improper access to personal records, but this on its own is not enough.

Users: the weakest link

Password protection of all applications, databases and systems is the first step in preventing improper access to personal records, but this on its own is not enough. Sharing passwords remains a common office practice.

When given the freedom to choose their own passwords users will go for easy-to-remember "obvious" choices. Most people will use their birthday, name, or some combination of the two because it's the first thing that comes to mind – and far easier than taking the time to think up a complex password. Their very simplicity and obviousness however make them easier to hack and therefore provide a fairly low level of security.

In addition, lazy users tend to pick the same password, or a close variation of it, for every application on their desktop. This might reduce the complexities faced by the IT department, but computer hackers are well aware of the phenomenon – routinely relying on it to breach security systems through passwords derived from easy-to-discover personal data.

The alternative – more complex passwords – is also fraught with problems. Although hack-

ers have a tougher time figuring them out, users often forget them.

Broadly speaking, there are two types of users: those who write down their passwords, and those who don't. The latter rely on memory for password recall, the performance of which declines in direct proportion to both the complexity and number of passwords. This results in frequent calls to the help desk for password resets, which industry analysts estimate cost £10 to £20 per call for IT support alone. Added to that figure is the cost of lost productivity as the user waits for a new password to get back into the application he needs. If each user in a company of 10,000 employees makes one password reset call to the IT help desk per month, and the cost is £10 per call, the annual password reset bill comes to over £1 million a year.

As for those users who write down passwords, they naturally do it in easily remembered places: an index card in the top desk drawer, a sheet of paper taped to the cubicle wall, or a sticky note on the side of the PC monitor. It's a gift for unauthorized users, who pirate these passwords for illicit network access with almost no effort at all.

The rise of the profit-turning hacker

If employees are one source of weakness, then deliberate malicious attacks are another. In addition to the kudos that drove many 'old-school' hackers, there is now money to be made from cracking passwords and infiltrating systems. If a firm is unfortunate enough to be the victim of a hacker who is prepared to put the work in, then even memorized and complex passwords are vulnerable. Hackers will call unsuspecting users, pretending to be computer support staff, and ask for the password. Or, the hacker will call the help desk, pretending to be a user who forgot his password.

In addition, many desktops allow Windows to fill in password data automatically. If the passwords for individual applications are stored on the desktop in unsecured cookies, then spy-ware, worms, and other malicious

code can easily steal account information, including log in details and passwords.

The more advanced cyber-thieves have access to a wide range of "password crackers" with software specifically designed to decipher passwords: applications like John the Ripper, Brutus, and Russian Password Crackers are becoming increasingly common. Phishing is another common and profitable method for stealing passwords.

However, the underlying problem with passwords and the weakness that every hacker exploits, is that they do not fulfill the fundamental requirements of IT security. To protect systems each user should have an identifier that is unique to him. But no password or PIN really meets that requirement: anyone who possesses that password or PIN can get into the system.

If a firm is unfortunate enough to be the victim of a hacker who is prepared to put the work in, then even memorized and complex passwords are vulnerable.

The Holy Grail of passwords: Enterprise Single Sign-on

The solution to the password problem is not to eliminate passwords but to eradicate the need for users to remember them, as this instantly removes the majority of problems associated with password management.

One of the easiest, fastest and most-effective ways to do this, and to achieve and document DPA compliance, is Enterprise Single Sign-on technology (ESSO). ESSO allows users to sign in once with a single password and access all their applications, databases and systems. Not to be confused with password synchronization, a method for distributing and synchronizing a main password to other systems, true single sign-on solutions enable users to have different passwords for every application.

ESSO automates password entry by responding to each log-in prompt without user intervention. This approach eliminates the need for employees to remember multiple passwords and reduces the likelihood of them ignoring

basic security procedures by writing down passwords or aides-mémoires. Instead, they gain immediate access to the information they need without even knowing any password except the one they need to log on for the day.

What's more, ESSO enables new passwords to be automatically generated when old ones expire. As the process of password management is automated, strict selection criteria can be enforced on both the password's composition and frequency of change. That means that alphanumeric passwords that are hard to guess can be readily deployed, and changed regularly, making it more difficult for unauthorized users to gain access. With a different, complex credential for each user and each application, systems are more difficult to breach, and data is more securely locked down.

The user ID and password for every application is stored in a secure central repository enabling an organization to provide secure access to an individual's personal information with confidence.

In addition, ESSO can provide full session control to kiosks with automatic closure of open applications and session termination after an elapsed period of inactivity. It can also provide enhanced workstation security with strong authentication, enabling a second-level security device like a smart card, token or biometric to be attached to a workstation and providing access only to employees who are able to authenticate. This is a particularly effective solution because - unlike an ID and passwords - strong authentication devices cannot be shared without accountability.

ESSO systems also maintain audit logs that are vital to comply with DPA mandates giving individuals the right to examine and obtain a copy of their own personal records. Since ESSO technology executes application access on the user's behalf, it can capture in

real time data that shows which employees access various applications and when. It provides comprehensive reports on password-related activity and full audit trail visibility about the issuance and use of passwords, ensuring that security policy is maintained over time. This audit trail can then be supplied to ICO to demonstrate DPA compliance.

ESSO has often been seen as too costly and labour-intensive to ever be truly attainable in large enterprises, and this was certainly the case with the first generation of single sign-on solutions. However, the software has moved on and industry-standard sign-on platforms upon which an enterprise can build a full suite of single sign-on solutions that address all their password-related requirements are now available.

The easiest way to calculate the ROI of freeing the user from password complexity is to measure the reduction in password reset calls to the help desk.

The death of passwords

The easiest way to calculate the ROI of freeing the user from password complexity is to measure the reduction in password reset calls to the help desk. Our experience and analysis over the last ten years shows that as much as 40 per cent of help desk calls may be password related. At the world's largest enterprise, the United States Postal Service, implementing ESSO saved the organization millions of dollars a year in reduced support calls. Most organizations experience payback in less than six months, and triple-digit ROI after three years.

This is not to say that ESSO is a magic bullet. Multiple layers of security are still necessary to protect an organization from the consequences of privacy breaches. But it is a key first step – in no small measure because it can be rapidly deployed at reasonable cost so that the minimum standards mandated by the DPA can be met. There is no burden of application

integration so organizations can leverage their current infrastructure, making it far less time-intensive and more cost-effective than biometrics, smart cards and public key infrastructure. It is also compatible with all of those technologies when and if organizations have the budget to implement them in the future.

Technology alone rarely solves operational problems, and data privacy is no exception. Implementing technological solutions will not guarantee the privacy of personal records. But properly implemented, ESSO can be a vital tool that provides the foundations necessary for maintaining the security of countless applications, tracking and logging access to personal records, and speeding access to critical information. It is an effective method of authorizing personnel and holding staff accountable for their activities. And by deploying an ESSO solution, an organization can demonstrate, categorically, that it has made a reasonable effort to protect customers' privacy.

Stephane Fymat is the VP of Business Development and Strategy at Passlogix (www.passlogix.com), the developer of the v-GO Accelerator Suite, a robust, scalable and easy-to-deploy enterprise single sign-on platform with successful installations in hundreds of organizations of all sizes and in all industries around the world.

SCALE 7x

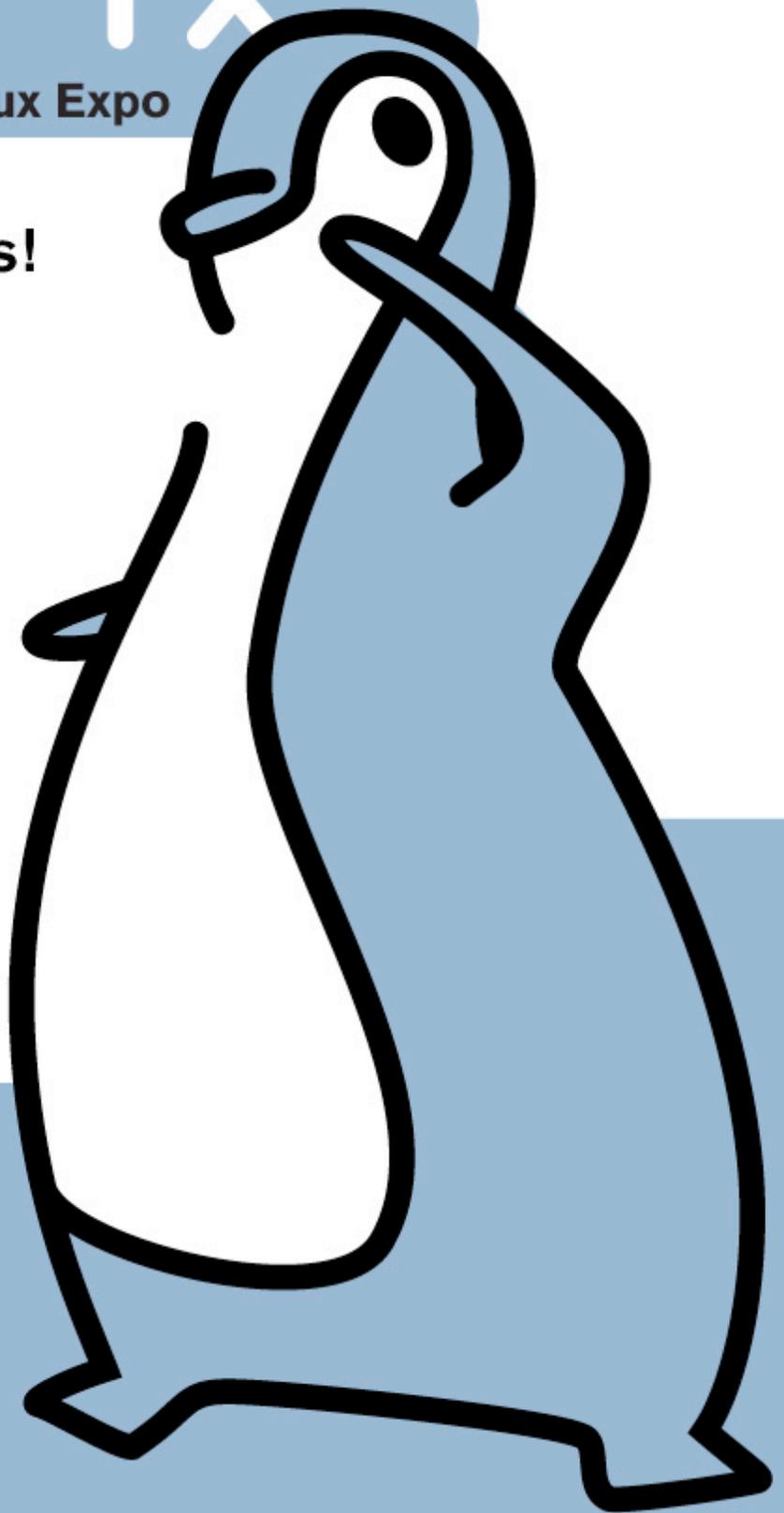
The Seventh Annual
Southern California Linux Expo

Mark your calendars!

**The 7th Annual
Southern California
Linux Expo
is coming!**

More session tracks!
More speakers!
Same great location!

February 20–22, 2009
Westin LAX
Los Angeles, California



<http://www.socallinuxexpo.org> for more info

Use Promo code NETS for a 30% discount on admission to SCALE



What will 2009 bring?



**Interview with Rich Mogull,
founder of Securosis**
by Mirko Zorz

Rich Mogull has over 17 years experience in information security, physical security, and risk management. Prior to founding Securosis, Rich spent 7 years as one of the leading security analysts with Gartner, where he advised thousands of clients, authored dozens of reports and was consistently rated as one of Gartner's top international speakers. He is one of the world's premier authorities on data security technologies and has covered issues ranging from vulnerabilities and threats, to risk management frameworks, to major application security.

Based on what you've seen all year long, how has the overall threat landscape transformed and what kind of evolution can we expect for 2009?

I kind of have to break this down into two parts- the evolution of vulnerabilities, and the real world threats/attacks. On the real world side we've just seen consistent evolution- basically, anything that worked for the bad guys in 2007 worked in 2008, and is likely to work in 2009. We've moved past the phase where the bad guys had to develop their infrastructure, and now they are just profiting off those investments and the organization of the criminal underground. What concerns me is we heard more hints in 2008 of quiet attacks- such as the active exploitation of the 0-day that lead to

Microsoft RPC patch. I highly suspect that in 2009 we'll see more of these very advanced, and very quiet, targeted attacks, which won't be very public, but we'll hear rumors of behind closed doors.

In terms of macro trends, it will still be mostly about web application attacks, client-sides, and going after common desktop applications to circumvent operating system anti-exploitation controls.

On the vulnerability side, 2008 was the year of the design flows- from DNS, to BGP, to Click-jacking. I highly suspect this trend will continue in 2009 as we see a lot of what we may have considered minor design issues from our past become major routes for exploitation.

In your opinion, what will be the broad implications of the worldwide economic crisis when it comes to IT security? What can organizations do to prepare themselves to these upcoming issues?

I don't see a dramatic reduction in security budgets, but the belt will definitely tighten. Basically, if it isn't something that stops a highly visible threat (like spam, viruses, etc.), meets a compliance requirement, or directly results in measurable cost reductions, you won't get money for it. This includes security professionals- if you aren't saving money, stopping an obvious threat, or essential for compliance, you are at risk for a reduction.

Finally, we'll also see a lot of impact on the vendor side- a lot of M&A activity, especially

as startups run out of operating capital, can't get more credit, and are faced with either selling themselves for a fraction of their desired value or just going out of business.

To prepare, I really recommend organizations evaluate their security programs and start trimming the fat and coming up with business justifications. Especially in large organizations we have a lot of extraneous pet projects that do little to improve our practical security. It's time to focus on the basics, optimize what you have, and learn how to communicate your value to the business. FUD won't work, you really need to show how you can operate more efficiently and what value you provide. Metrics will be your friend, but don't fall into the trap of making bullshit ROI justifications based on potential losses.

The web is a wonderful vector for attack due to its basic design and we'll continue to see all sorts of creative attacks. We definitely haven't hit the peak of web based malware as a threat.

The concealment of malicious code on websites is still a significant issue. Can we expect more trouble in 2009? What features should Internet browsers and operating systems incorporate in order to slow-down the infection rates?

Absolutely. The web is a wonderful vector for attack due to its basic design and we'll continue to see all sorts of creative attacks. We definitely haven't hit the peak of web based malware as a threat.

I've got some pretty strong opinions on how to work on this problem. On the browser side we need to start looking at session isolation/virtualization. This will really piss off the advertising/tracking networks, but I don't see any other way around the problem. Basically, we need to place more limits on cross-tab/window communication and, especially, iframes.

The truth is we face major design issues on the browser side and even these kinds of fixes will only help with parts of the problem.

Basically, we need more sandboxing and isolation- the bad guys will still be able to compromise the browser, but they'll be much more limited in what they can get away with.

I also have some kind of out-there ideas on what we can do with our web applications, but that's probably another (longer) conversation. It's a concept I call ADMP- Application and Database Monitoring and Protection. Basically combining a bunch of technologies like WAF, SSL-VPN, database activity monitoring, and web application security services to create a combined web application security stack, instead of all the little point pieces that don't work all that well right now because they none of them really see the full application.

What would be your most outrageous security-related prediction for 2009?

President Obama hires me to run our national cybersecurity :)

Events around the world



RSA Conference 2009

20 April-24 April 2009 - Moscone Center, San Francisco
www.rsaconference.com/2009/US/ (enter priority code: HN128)

InfoSec World 2009 Conference & Expo

7 March-13 March 2009 - Disney's Coronado Springs Resort, Orlando, FL
www.misti.com/infosecworld

Southern California Linux Expo (SCALE 7x)

20 February-22 February 2009 - LAX Westin, LA
www.socallinuxexpo.org

The Fourth International Conference on Availability, Reliability and Security (ARES 2009)

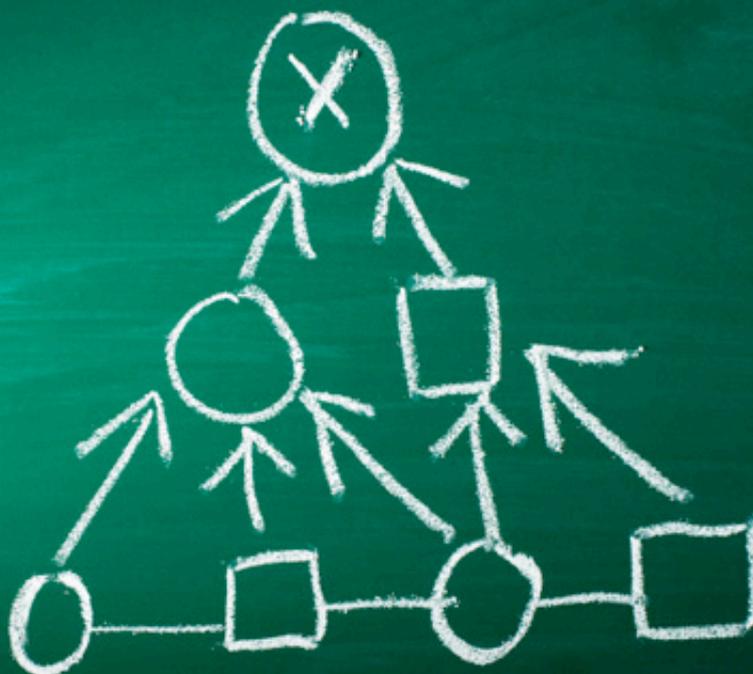
16 March-19 March 2009 - Fukuoka, Japan
www.ares-conference.eu/conf/

2009 European Workshop on System Security (EuroSec)

31 March-31 March 2009 - Nuremberg, Germany
dcs.ics.forth.gr/eurosec09/

5 strategies for proactively embracing failure

by Steve Shillingford



As information security professionals, we constantly ask, “Are we doing enough?” To which, the answer is usually a resounding “No.” So, we embark on an often endless cycle of product and process evaluation, purchase and implementation only to end up plagued by our initial insecurity - that we’re still not doing enough, that we’re still not secure.

This paranoia is driven by a multitude of factors. Beyond the desire to succeed in our professional roles, consider the influence of highly publicized breaches, the endless succession of "next generation" security toolsets, the barrage of threats including the next "zero-day" exploit, and the evolving government regulations meant to ensure information security in the first place. Collectively, these factors breed an industry-wide fear of catastrophic system failure. Naturally, we are inclined to embody this fear by building systems aimed solely at preventing it.

This logic is flawed. The preventative security solutions that we employ today only protect against “known threats” - or those that have already been identified by our existing info security systems. Meanwhile, attackers continue to persevere, relentlessly. Admitting susceptibility to these security loopholes, or “unknown threats”, that facilitate failure, may prove more useful than focusing so much on known

threats. Viewed in a broader light of environmental adaption in complex systems, we begin to recognize that planning for failure is not only important, it's fundamental in addressing our objective of comprehensive security.

Armed with the handful of strategic initiatives outlined here, IT security professionals can begin accounting for the inevitability of failure, improving their overall security posture.

Understanding failure

Before we begin planning for failure, we must learn to accept that information security is an imperfect entity; that, despite our best efforts, any defense measure we employ will fail; and that if this failure is unavoidable, it must be factored into the information security process. For the same reasons banks use video surveillance while simultaneously deploying prevention measures (guards, alarms, etc.), IT organizations need to embrace the notion that

prevention is not a credible stand-alone measure. Educating ourselves, our teams, and our departments about the various theories and studies that lend creditability to this contrarian thinking is imperative. There are many complex systems outside IT where failure preparation is standard practice. Why should the network be viewed any differently?

We should first consider the factors that drive innovation in the information security products landscape. The rules that govern economics and natural selection help eliminate the inferior, unaffordable and ineffectual offerings. We are able to select from a range of best-of-breed defensive solutions that, upon deployment, instill a sense of reasonable confidence in our information security systems.

This confidence sets the stage for a less-than-desirable consequence. The more fit a security product is perceived to be, the more likely it is to recklessly reassure us that we are secure. And while we're caught up in a fleeting sense of security, the same market dynamics that drive product innovation are fueling the evolution of pervasive and agile threats.

To overcome their adversaries, attackers have become increasingly covert, both in the means through which they're infiltrating our systems and their intended end result. Typically, an information security system's ability to detect and protect against these attacks depends on deterministic strategies, where products are configured to address only known threats or events. If attacker's operations are unknown, and therefore go undetected, preventive countermeasures cannot be adapted to thwart their attacks.

In an attempt to counter such deficits, hybrid products have appeared - those that include deterministic and heuristic strategies, such as behavioral- or anomaly-based methods. Currently, the time it takes these products to help us accurately identify and resolve malicious network activity is insufficient in containing the damage caused an attack. But when these hybrid technologies become pervasive - as the competitive product ecosystem suggests they will - attackers will adapt and evade, becoming simultaneously able to impersonate "normal" behavior and remain relatively undetectable.

Van Valen's Red Queen hypothesis helps explain information security product developers' and hackers' tendency to one-up each other. It suggests the balance between competing species evolves dynamically - a state where adaptive improvement is always possible for both species so they continually evolve in relationship to one another and keep up with the evolutionary improvement of their counterparts. In the context of information security, product vendors and attackers continually compete for survival, each incrementally trumping each other's more advantageous attributes without driving their competition into extinction. So as quickly as a system can be updated to protect against an identified threat, an unknown, more adaptable threat can compromise the systems' effectiveness.

In this way, active countermeasures to known threats only provide the illusion of control. Bruce Schneier explains this well in his book *Beyond Fear*, when he outlines "security theater." According to Schneier, security theater describes countermeasure solutions that provide the feeling of improved security while doing little or nothing to actually ensure safety. This is not to say that a firewall doesn't, in fact, protect against the known threats for which it's configured against; instead, it draws attention to our tendency as information security professionals to be blinded with confidence in our defensive efforts and ignore the potential vulnerabilities of our current systems to unknown threats.

Industry reports lend additional credibility to the insidious and pervasive nature of network attackers and can often provide clues to what isn't working on an industry-wide level. A June 2008 security survey conducted by InformationWeek reported that while 95 percent of the organizations surveyed had security budgets that were the same or increased from 2007, 66 percent of them suspected their vulnerability to breaches to be the same or worse as they were in 2007. The same survey participants suggested that firewalls, antivirus tools, encryption and VPNs were only effective about two-thirds of the time, providing ample opportunity for successful attacks.

Or take, for example, the recent findings about a non-dictionary attack on the popular wireless encryption method Wi-Fi Protected

Access (WPA), which were presented at the PacSec Tokyo 2008 conference by academic researchers Erik Tews and Martin Beck. In their paper, entitled "Practical Attacks against WEP and WPA," they report finding a hole in part of 802.11i that forms the basis of WPA. Leveraging this weakness, they were able to break the temporary Key Integrity Protocol (TKIP) in under 15 minutes.

These findings carry implications for information security professionals in enterprises worldwide. Sure, we can upgrade to WPA2 if we haven't already, but how long until this encryption method is cracked?

Findings from both industry and academic research encourage us to more closely scrutinize our own security systems and processes. Combined with exposure to theories, such as Red Queen and Schneier's security theater, we begin to understand the ever-evolving nature of attackers and their ability to evade the security products we employ to detect and protect against them. As a group we should acknowledge the imperfect nature of our information security systems and processes. Equipped with this new perspective, we can more effectively address questions like those around securing wireless networks - we can begin accounting for inevitable failure as a fundamental tenet of design.

As a group we should acknowledge the imperfect nature of our information security systems and processes.

Risk mitigation

Evaluating security infrastructure in accordance with risk management theory provides a valuable framework with which to start accounting for system and process failure. As long as we are trying to protect assets, we must accept that some combination of existing threats (or attacks from which we are trying to protect our assets) and vulnerabilities (or the way in which an attacker prevails), can put those assets at risk. Identifying our organizations' assets, calculating their individual risk and employing a risk management model can help us determine our organizations' specific threshold for risk.

ISO International Standard ISO/IEC 15408-1:2005, also known as Common Criteria Part 1, offers a straightforward formula for calculating the relationship among variables, such as threats and vulnerabilities that account for an assets' quantitative risk (standards.iso.org/ittf/PubliclyAvailableStandards/). Similarly, the NIST Special Publication 800-30 provides a simple decision chart for determining an organization's acceptability of risk (csrc.nist.gov/publications/nistpubs/).

A recent adaptation of these basic risk mitigation theories—issued by the American National Standards Institute (ANSI) and the Internet Security Alliance in a guide called

"The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask" (webstore.ansi.org/cybersecurity.aspx) - takes a more holistic approach. The guide suggests that organizations calculate network security risks for specific attacks or events by first asking questions of every department or group within the organization that might be affected. This comprehensive pooling of data seeks to ensure better accuracy in determining the organizations' potential risks, and the costs associated with them, because it involves everyone who might be affected by a security breach.

This equation, supported by the basic theories outlined in the Common Criteria Part 1 and NIST Special Publication 800-30, can help information security professionals in determining what risk management actions, if any, should be executed.

The formulas inform allocation of resources - essentially, helping us assess the type of protection we can afford in terms of time, money, energy and space consumption, human resources, tolerability and sustainability. They allow us to arrive at an acceptable level the cost associated with our organizations' specific risks while also directing us to where vulnerabilities persist.

Devalue data

We should not be surprised when we're faced with reports about the information security risks of Internet communication, such as VoIP, SMS-linked micro-blogs or social networks. We should anticipate them because, by nature, network information is highly vulnerable.

Consider the characteristics of posting data on the Internet. Technology makes instant communication simple. This communication can be private, and often private communication is centered around sensitive matters. Communication can also be public, and sometimes public communications can reveal too much information. As such, Internet communication is becoming increasingly transparent. Because we're inclined to capitalize on the simplicity it provides, what, as information security professionals, can we do to ensure that sensitive enterprise data remains relatively private?

We can turn to Red Team exercises—or security practice drills issued by the US government. An example is the confidential report that recently spurred an onslaught of “Potential for Terrorist Use of Twitter” stories in the media. However, we should proceed with caution when directing our attention to such exercises, as we don't want to adopt their alarmist perspective.

We must also avoid making it easy to hack a system. This may seem obvious, but it's a surprisingly common oversight. In the recent Sarah Palin hack, the hacker simply reset Palin's password using her birth date, ZIP code and information about where she met her spouse—all information available through a simple Google search. It seems someone would have thought to adjust the password settings on her personal email accounts or take them down entirely.

Any amount of time wasted in implementing a patch widens the window of time during which an organizations' data is vulnerable to a known threat, and system failure.

We must heed these warnings. More specifically, we should use communication modes other than the Internet when transmitting sensitive enterprise data. To help ensure that all employees take such precautions, not just those of us in IT, we can block users within our network from accessing non-corporate email, VoIP, micro-blogging and social network accounts. We can also provide warnings and education that deters them from using personal accounts to send company documents and information when working outside of the enterprise network.

Finally, and most importantly, we can try to devalue data whenever possible. We can use full-disk and database encryption so that when a loss or breach occurs, the thief finds the data inaccessible or, at least, very expensive. We can use unique passwords with the help of a password manager so that if one password is compromised, others aren't. We can use “one-time” data instances such as one-time passwords or one-time credit card numbers.

Accounting for known threats

We must ensure that failure doesn't occur because of a known issue. With risk mitigation theories, we can more accurately determine which information security product investments will lessen risks associated with known threats and events. Aggressively applying more- or less-comprehensive detection and prevention solutions based on these determinations is imperative.

Additionally, as the information security ecosystem evolves, more known threats are revealed. These threats are often brought to our attention by the security products' vendors in the form of a patch or signature file. Though it may seem obvious, staying abreast of these updates within our existing infrastructures is of equivocal, if not greater, importance to investing in new products or upgrades. Any amount of time wasted in implementing a patch widens the window of time during which an organizations' data is vulnerable to a known threat, and system failure.

What happens when a known threat infiltrates our systems during this window of vulnerability? Or, if it attacks before the patch itself is issued, when the threat is still unknown?

Though vendors may tout the idea of “zero-day threat detection,” more often than not evidence suggests the contrary. Rather, it points to an undefined time period before a patch was issued and implemented when vulnerable systems were successfully attacked and exploited.

The controversy surrounding the Microsoft MS08-067 emergency patch is an example of this. The patch was issued on October 23, 2008 to remedy the Windows RPC exploit. Yet, Trojans capitalizing on the flaw were identified the day following its release. Further analysis of these strains suggested that they may have been in circulation before the patch was issued, perhaps as early as September 29. The concept of “zero day” goes out the window, but the potential exploitations or events that occurred because of the vulnerability remain.

Incorporating an incident response plan into our information security practices and processes provides us with the ability to better identify the cause and extent of a breach.

Negative day threat detection and network forensics

Incorporating an incident response plan into our information security practices and processes provides us with the ability to better identify the cause and extent of a breach. With a plan in place, we can account for the fallibility of patches and defensive solutions as well as the pervasive nature of system threats and vulnerabilities.

A well-executed incident response plan incorporates a number of variables. Above all, it must contain the direct damage caused by an attack. It must provide the tools for a methodical and timely response, curbing the indirect damage, such as negative publicity, reduced customer confidence, or legal repercussions. If set up properly, it can also identify and resolve the root causes of an incident so repeat occurrences can be avoided. The hallmark of such a plan is network forensics technology - or more specifically, traffic capture, regeneration and search solutions.

Capitalizing on the advancements in data storage, which increase space at lower costs, these solutions record all data crossing a network and store it for later recall and analysis. This complete record of network traffic provides context to alerts or events. Once we identify a threat, we can navigate through traffic history and search evidence surrounding the actual event, not just superficial metadata such as log files and header information. We can use this evidence to view and replay, with

full fidelity, the events that predated classification of the threat.

In the case of vendor-issued patches, network forensics technologies offer “negative day threat detection.” That is, the patch serves as an incident or notification of a previously unknown threat. And we can go back, even weeks prior to the issuance of patch, and use the published threat patterns to search for instances of the offensive malware that might have crossed the network since the first reports of the incident.

But alert mechanisms that rely on pre-defined signatures, patterns or data or those that are identified by security vendors or researchers are hardly infallible. We can also leverage capture technology for surveillance - a process of continuously capturing and monitoring traffic for detection of any atypical activity or anomaly. Specifically in high-risk or vulnerable areas of a network, monitoring traffic records can help us proactively distinguish between legitimate alerts and false positives. They can help us uncover previously undetected, or unknown, breaches.

When prevention fails, detection is key. Network forensics tools equip us better in efficiently realizing known and unknown breaches. We can more effectively stem further loss or future loss of sensitive data and update existing controls to avoid repeat attacks. These tools provide necessary fortitude to any effective incident response plan and help us account for failure.

Complex systems reside in a state of equilibrium where events have individual and aggregate impacts. For example, why is it difficult to immunize against certain viruses? Because in many cases, these viruses evolve and evade the cocktails of drugs that seek to prevent them from successfully attacking healthy cells. This characteristic holds true for any complex system with multiple inputs and outputs.

Another system of moderate-to-sufficient complexity that's worth examining is security in a bank. A bank has a diverse collection of defenses to protect against robbery, including a vault, time-release locks, bulletproof glass and security guards. But it also employs a security measure that accounts for the failure of those defensive solutions: surveillance cameras. If the defensive measures fail to detect and prevent a robbery until after the money and robbers are long gone, authorities would

not turn to the security guard for eye-witness testimony. They'd rely more heavily on the forensic record of evidence provided by the cameras.

Why then, as information security professionals, do we think our organizations are any different than the virus or the bank? We should know better than to believe we're safe from network failure of some undetermined variety and magnitude. We must take into consideration education about the pervasiveness of threats, the specific risks that our organizations face in the wake of these threats, the importance of devaluing data and the role played by network forensics technologies. Once we realize the impediments to adopting these strategies are non-existent, we can move to implement them throughout our information security systems and processes - ultimately accounting for network failure.

Steve Shillingford has more than 15 years of experience in sales, operations and management in technology companies. He joined Solera Networks (www.soleranetworks.com) in early 2007 from Oracle Corporation, where he was responsible for some of the largest deals in the company during his tenure, all in the Rocky Mountain region. Steve was named top salesperson within Oracle in 2005 as a result of this success. Prior to joining Oracle in 2000, Steve had held several sales and operational management positions at Novell over the preceding seven years. Steve holds a B.S. with honors in Psychology from Brigham Young University.





The present and future of Web application security discussed in Portugal

by Carlos Serrão

The Open Web Application Security Project (OWASP), an open international initiative that identifies the top web application security vulnerabilities, develops tools to identify and correct these threats, and that advocates a set of good development practices to address security issues in the applications, has conducted its major meeting at the beginning of November.

This meeting, the OWASP Summit 08, has joined more than 80 security experts from over 20 countries from the five different continents, in the beautiful Algarve region in Portugal. The OWASP Summit 08 objective was to bring this community of expertise to join efforts to identify, coordinate and prioritize the efforts for the coming year (2009) to create a more secure and reliable Internet.

OWASP is a free and open community that focuses on improving application security. There is overwhelming evidence that the vast majority of web applications and web-services contain security holes that are increasingly putting people and organizations at serious risk. Securing web applications is an extraordinarily difficult technical challenge that demands a concerted effort. The mission of OWASP is to make application security visible, so that people and organizations can make

informed decisions about application security risks. Everyone is free to participate in OWASP and all of the materials are available under a free and open software license. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for the work being conducted.

During the event, OWASP has joined together international OWASP leaders as well as important industry partners that presented and discussed the most recent OWASP developments in terms of documentation and tools. The Summit featured more than 40 OWASP sponsored projects presentations in the application security research fields, as well as some specific working sessions to promote the cooperation between Summit participants, chapter leaders and OWASP supporters, towards the achievement of the current OWASP

project objectives and the definition of the future milestones. OWASP Summit 2008 was composed by several technical and business-oriented sessions offering the perfect environment for learning more about the multiple available OWASP resources.

OWASP came together for a week and produced a stunning amount of new ideas. The OWASP community is growing and organizing into a powerful movement that will affect software development worldwide. This summit marks a major milestone the efforts to improve application security.



An overview of one of the main conference rooms, with Dinis Cruz on the stage.

The major key results from the OWASP Summit are outlined below.

New Free Tools and Guidance - During the Summit, OWASP has announced the release of Live CD 2008, many new testing tools, static analysis tools, the Enterprise Security API (ESAPI v1.4), AntiSamy, the Application Security Verification Standard (ASVS), guidance for Ruby on Rails and Classic ASP, international versions of the OWASP materials, and much more.

New Outreach Programs - OWASP has expanded its outreach efforts by building relationships with technology vendors, framework providers, and standards bodies. In addition, OWASP has piloted a new program to provide free one-day seminars at universities and developer conferences worldwide.

New Global Committee Structure - OWASP recognized the extraordinary contribution of

the most active leaders by engaging them to lead a set of seven new committees. Each democratically established committee will focus on a key function or geographic region, such as OWASP projects, conferences, local chapters, and industry outreach.

Some of the topics that were presented and discussed on the working sessions, included the following:

- OWASP Roadmap for 2009
- OWASP Top 10 update for 2009
- OWASP ESAPI - Enterprise Security API Project
- OWASP ASDR - Application Security Desk Reference
- OWASP CLASP - Comprehensive, Light-weight Application Security Process
- OWASP ISWG Browser Security
- OWASP Orizon project (Summer of Code 08)
- OWASP Testing Guide (Summer of Code & Working Session)

- OWASP Code Review Guide (Summer of Code 08 & Working Session)
- OWASP .NET Project (Summer of Code 08 & Working Session)
- Threat Modeling.

During the meeting the integration of some of the most important OWASP documentation

projects took place. This discussion was mostly centered on the integration of the Develop, Code Review, Testing and Application Security Desk Reference (ADSR) guides. Also, OWASP is planning the internationalization of such guides, making them available in different languages (English, Spanish, Portuguese, French and others).



The OWASP Summit participants.

Another important topic discussed during this Summit was the OWASP Top Ten vulnerability update for 2009. The OWASP Top Ten lists the ten most critical Web Applications Security vulnerabilities. The actual list is the following:

- A1 – Cross Site Scripting (XSS)
- A2 – Injection Flaws
- A3 – Malicious File Execution
- A4 – Insecure Direct Object Reference
- A5 – Cross Site Request Forgery (CSRF)
- A6 – Information Leakage and Improper Error Handling

- A7 – Broken Authentication and Session Management
- A8 – Insecure Cryptographic Storage
- A9 – Insecure Communications
- A10 – Failure to Restrict URL Access

OWASP will continue to embrace the knowledge sharing as a way to carry its mission – to promote the security of web applications and web services. The community contribution to its documentation projects and tools will be available to everyone in an open manner.

Carlos Serrão is the OWASP Portuguese Chapter Leader.

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.

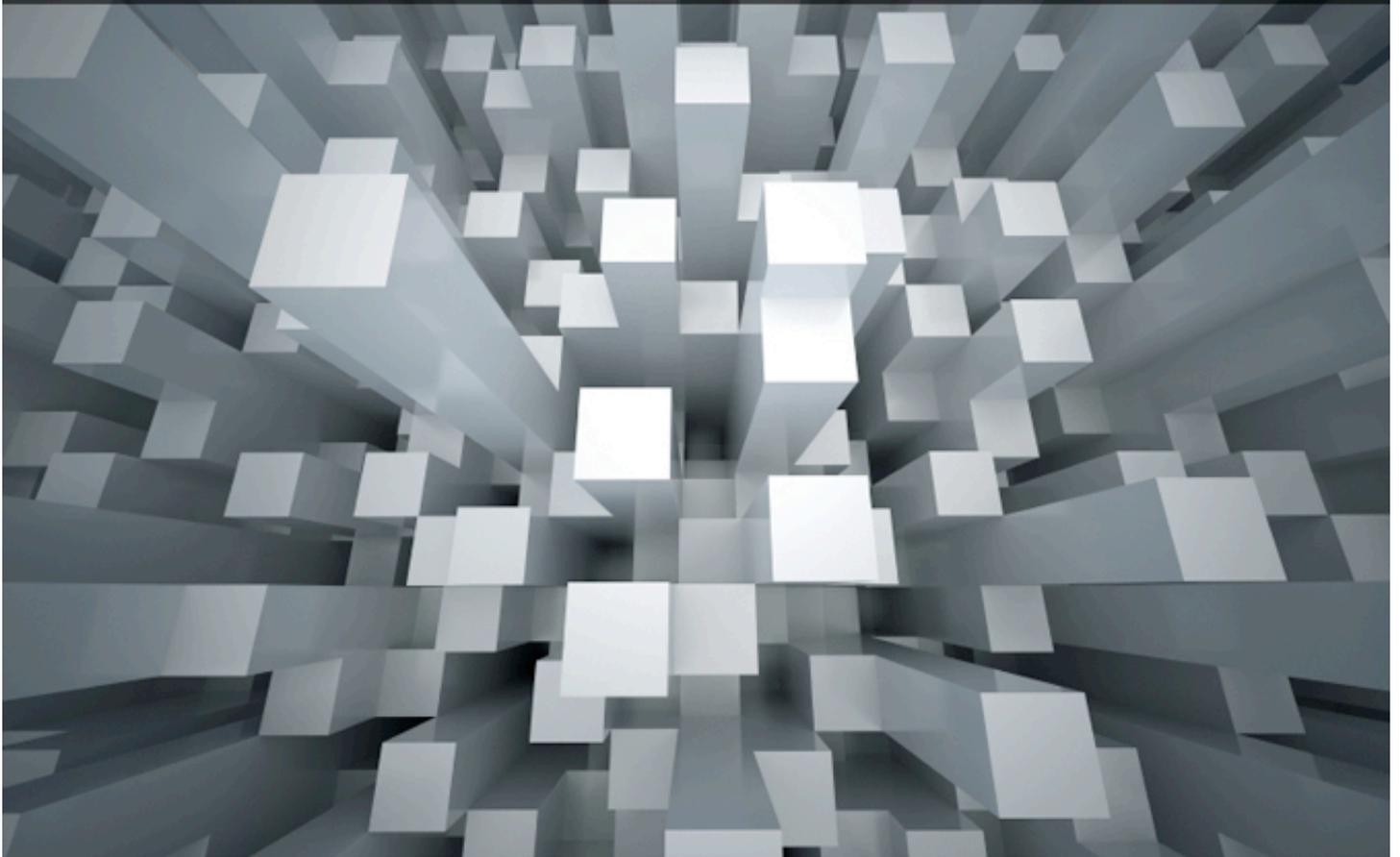
For a free trial, go to a browser near you.

www.qualys.com/SaaS_Trial



Securing data beyond PCI in a SOA environment: best practices for advanced data protection

by Ulf Mattsson



New business models rely on open networks with multiple access points to conduct business in real time, driving down costs and speeding responses to revenue generating opportunities. That's the good news. The bad news is that this modern business architecture is often riddled with vulnerabilities that can easily be exploited to gain unauthorized access to sensitive information.

To make life even more exciting, you can't rely on traditional best practices like establishing strong boundaries around critical applications to secure SOAs or you'll be defeating the features and flexibility that SOA brings to the enterprise.

Another attractive feature of SOAs is the use of standardized contracts and contract retrieval methods, which make life much easier for developers, authorized users and malicious hackers. Using a collection of freely available contract descriptions a hacker can target weakly authenticated or high-value services, easily penetrate an improperly secured SOA, eavesdrop on SOAP message traffic and see information that may be private. In addition, it is relatively easy to intercept a SOAP message in an unsecured SOA and re-

route it or transform its content for purposes of mischief or fraud.

Layers of security - including integrated key management, identity management and policy-based enforcement as well as encryption are essential for a truly secure SOA. This article reviews a practical implementation of a transparent, risk-based management approach that can be used to lock down sensitive data utilizing policy driven encryption and key management for data-at-rest and in-transit across enterprise systems.

Evolving data threats

We all know that malicious hackers are attracted to electronic commerce systems. Another category of applications that attracts

hackers' attention are those that deliver services on behalf of financial firms such as reward redemption, report delivery for banks, and merchant and bank information exchange. Unlike traditional static internet applications, many of these applications store and process information that is strictly regulated and must satisfy various compliance requirements. Typically, these applications compile databases containing hundreds, thousands, or even millions of credit card accounts and personal identifiable information. For hackers, these databases represent an excellent opportunity for theft and fraud.

And although the IT community is interested in SOA because of its promise of efficiency and improved IT management, security problems are causing many to proceed slowly, or not at all, with actual SOA implementations. Major systems have typically been designed to protect against unauthorized use, intrusion, and viruses. Today, however, the issue has taken

on even more seriousness in the wake of hacking-for-hire attacks and global viruses.

SOA's inherent security problems stem from the ways in which the SOA replaces traditional security parameters with new, open standards. The security problem is twofold in that not only are the new standards completely open-no one owns them but they were also developed without security in mind. Web services were developed over a period of years by industry consensus as a way to, among other things, enable the creation of reusable code, simplify development, and streamline system integration. Specifically, XML, SOAP, WSDL, and UDDI are open standards that enable the transmission and description of data and procedure calls between systems. However, none of these open standards contain any inherent security aspects of their own. If left alone, they are completely non-secure. In fact, web services were designed to be able to move data efficiently through firewalls.

SOA'S INHERENT SECURITY PROBLEMS STEM FROM THE WAYS IN WHICH THE SOA REPLACES TRADITIONAL SECURITY PARAMETERS WITH NEW, OPEN STANDARDS.

In the traditional security model, the system's security apparatus, such as a firewall or virtual private network (VPN), screens out unauthorized (human) users. However, an SOA demands that the architecture be more flexible and open to access from multiple systems to facilitate reuse and composition of new applications. If the systems are exposed as services but a new security mechanism is not enforced, a hacker could configure a machine to impersonate a vendor's system and make erroneous or fraudulent service calls.

While SOA security concerns abound, virtually all IT managers are realizing that they must soon identify and implement security solutions for SOAs because their developers are exposing applications as web services using the new generation of development tools. A pressing need exists, as noted in (tinyurl.com/666goy), to solve the security risks in the SOA.

Any security system is only as strong as its weakest link, and that is what attackers - from both inside and outside of the enterprise - look for; up to the application and even client level,

and down to the system internals and driver level. At the top level you have the world of web application attacks, where web applications are used as proxies to attack the underlying databases. The conventional risk model used in IT security is that of a linked chain - the system is a chain of events, where the weakest link is found and made stronger. We should question this approach because it fails to solve the problem of how to provide a secure IT system, even when a recognized weak link is made stronger.

The strengthening of any link, even if made much stronger, would not make the system less vulnerable. In fact it might make the system more vulnerable, because the security of the system would still depend on a weakest link (which might be the newly "hardened" link). Further, such solutions are actually based on the illogical presumption that "no part will fail at any time" - if a critical part fails, the system fails. In short, there is an inevitable single point-of-failure - that weakest link. Making the link stronger will not make the single point-of-failure go away - at most it may shift it.

Approaches to SOA security

It is critical to have a good understanding of the data flow in order to select the optimal protection approach at different points in the enterprise. By properly understanding the data flow we can avoid quick fixes and point solutions and instead implement a protection strategy encompassing protection all the way from the data sources.

Careful analysis of use cases and the associated threats and attack vectors can provide a good starting point in this area. A continuous protection is an approach that safeguards information by cryptographic protection or other field level protection from point-of-creation to point-of deletion to keep sensitive data or data fields locked down across applications, databases, and files - including ETL data loading tools, FTP processes and EDI data transfers.

Security policy refers to the issues that arise around authentication and authorization. In general terms, any SOA security discussion is going to have a component of security policy. Message-level security is a group of technology issues that relate to the integrity of the actual web service that is traveling across the

network. Message-level security is the necessary other half of security policy. Not only is this good business, it's also becoming part of the law in such areas as privacy and regulatory compliance. Message-level security, which involves such technological functions as encryption, keys, certificates, and signatures tackles the challenges of securing the specific web service interaction from meddling and eavesdropping. The goal of SOA security in the context of governance is to provide assurance that the SOA can deliver verifiable data that will stand the test of an audit.

If you want your SOA to have robust security, where you are confident that the users of your web service are properly authenticated and that the information flowing back and forth between web service and their invoking applications is not read by unauthorized people, then you will almost certainly need to apply the powerful tool of encryption to your SOA security solution. Below is a description of how end-to-end data oriented encryption provides end-to-end field confidentiality across the enterprise data-flow, including the SOA layers, while WSS (Web Services Security), TLS and proxy only provide message-oriented or point-to-point confidentiality.

IT IS CRITICAL TO HAVE A GOOD UNDERSTANDING OF THE DATA FLOW IN ORDER TO SELECT THE OPTIMAL PROTECTION APPROACH AT DIFFERENT POINTS IN THE ENTERPRISE.

XML message encryption

WSS is a communications protocol providing a means for applying security to Web services. The protocol contains specifications on how integrity and confidentiality can be enforced on Web services messaging. The WSS protocol includes details on the use of SAML (see below) and Kerberos, and certificate formats such as X.509. WS-Security describes how to attach signatures and encryption headers to SOAP messages.

In addition, it describes how to attach security tokens, including binary security tokens such as X.509 certificates and Kerberos tickets, to messages. WS-Security incorporates security features in the header of a SOAP message, working in the application layer. WS-Security however addresses the wider problem of maintaining integrity and confidentiality of

messages until after a message was sent from the originating node, providing so called end to end message level security. You can use this type of XML encryption if message protection is enough, or end-to-end data encryption if protection of the data flow is needed. WSS cannot protect a multi-tiered data flow from storage all the way to the client that is requesting the data.

Only point-to-point protection with TLS or proxy

In point-to-point situations confidentiality and data integrity can also be enforced on Web services through the use of Transport Layer Security (TLS), for example, by sending messages over https.

Applying TLS can significantly reduce the overhead involved by removing the need to

encode keys and message signatures into ASCII before sending. A challenge in using TLS would be if messages needed to go through a proxy server, as it would need to be able to see the request for routing. In such an example, the server would see the request coming from the proxy, not the client; this could be worked around by having the proxy have a copy of the client's key and certificate, or by having a signing certificate trusted by the server, with which it could generate a key/certificate pair matching those of the client. However, as the proxy is operating on the message, it does not ensure end to end security, but only ensures point-to-point security.

Security Assertion Markup Language

In some cases, the authentication process will result in the SOA security solution creating a Security Assertion Markup Language (SAML) assertion that expresses the authenticity of the user in a way that will be accepted by the web service that the user is invoking.

SAML is an XML-based standard that provides a framework for describing security information about a user in a standardized way. One

highly effective way to protect the security of core systems is to avoid letting anyone reach the service hosting platform.

Message monitoring and federated identity management system

To deal with the security challenges inherent in securing third parties, an SOA security solution can utilize federated authentication. Federated authentication is a process by which multiple parties agree that a designated set of users can be authenticated by a given set of criteria. Users of the federated authentication approach can create a Federated Identity Management System, which is a sort of pool, of authenticated users.

The SOA security solution can authenticate a user by checking with the Federated Identity Management System. In other words, a "federation" of systems, communicating with one another, can agree that certain individuals are okay. SOAP message monitoring based on SOAP interception is another way to build the foundation of an effective SOA security solution as noted in (tinyurl.com/666goy).

WE CANNOT RELY ON APPLICATIONS TO DO ALL THE WORK FOR US OR THROW MONEY AT THE DATA SECURITY PROBLEM AND HOPE IT WILL GO AWAY.

A holistic layered approach to security

We cannot rely on applications to do all the work for us or throw money at the data security problem and hope it will go away. A holistic layered approach to security is far more powerful than the fragmented practices present at too many companies. Think of your network as a municipal transit system - the system is not just about the station platforms; the tracks, trains, switches and passengers are equally critical components.

Many companies approach security as if they are trying to protect the station platforms, and by focusing on this single detail they lose sight of the importance of securing the flow of information. It is critical to take time from managing the crisis of the moment to look at the bigger picture. One size doesn't fit all in security so assess the data flow and risk environ-

ment within your company and devise a comprehensive plan to manage information security that dovetails with business needs. A data protection-driven holistic plan is the only way to truly secure data – it allows you to think strategically, act deliberately and get the absolute best return on your data security investment. Protecting the enterprise data flow is discussed in (www.ulfmattsson.com) and (tinyurl.com/6y6xdy) is looking at security beyond PCI.

A good starting point is to analyze and understand the flow of sensitive data and then identify critical assets and their vulnerabilities, assess the risk level for each attack vector and prepare a staged working plan to close each critical vulnerability in the order of the severity of the risk it presents to the most critical data.

Protection beyond PCI - issues and methods

End-to-end data encryption

The capability to protect at the point of entry helps ensure that the information will be both properly secured and fully accessible when needed at any point in its enterprise information lifecycle.

One important point is how end-to-end data encryption can protect sensitive fields in a multi-tiered data flow from storage all the way to the client that is requesting the data. The protected data fields may be flowing from legacy back-end databases and applications, via a layer of web services before reaching the client. The sensitive data can be decrypted close to the client after validating the credential and data level authorization.

In this scenario SOA is mainly a data transfer mechanism. The end-to-end data encryption is not SOA specific; it could be used for any protocol/data transfer mechanism. In some cases a partially protected credit card account number is passed between different applications, databases and files. This approach is described later in this article. The end-to-end data encrypted can have integrity and a key identifier added to the field or compressed into field, depending on the data types involved. You need to know which key the data has been encrypted with. The key management solution must provide the same key used for encryption to be used for decryption, and key rotation must be supported.

Protection against application-level attacks

The primary vulnerability of database- and file-level encryption is that they do not protect against application-level attacks -- the encryption function is solely implemented within the DBMS. The application protection solution institutes policies and procedures that enable software developers to effectively build security into enterprise applications, employing external filters to block attacks. Hackers, crackers, internal attacks and business evolution are facts of life; as a result, security threats, leaks and lack of scale will constantly plague user access control solutions based on pass-

word lists, access control databases, and shared secrets.

Different options for data field protection

A strategic approach is to implement solutions that are automated, integrated, scalable, and secure in an Enterprise Environment. A mature solution should provide a choice to balance and optimize the mix of different approaches to credit card protection across different systems in the enterprise, including tokenization, encryption and hashing.

Native database security mechanisms

Native database security mechanisms are very limited in defending successful data attacks. Authorized but malicious transactions can make a database useless by impairing its integrity and availability. Suites of the proposed solution may be deployed throughout a network, and their alarms managed, correlated, and acted on by remote or local subscribing security services, thus helping to address issues of decentralized management.

Hash values are non-transparent to applications and database schemas

Hash algorithms are one-way functions that turn a message into a fingerprint, usually several dozen bytes long binary string to avoid collisions. Hashing can be used to secure data fields in situations where you do not need the data to do business and you never need the original data back again. Unfortunately a hash will be non-transparent to applications and database schemas since it will require long binary data type string (longer than the 20 bytes for the broken SHA-1 or two-way symmetric encryption).

Minimizing changes to applications and databases

Give careful consideration to the performance impact of implementing a data encryption solution. First, enterprises must adopt an approach to encrypting sensitive fields only. Such a solution allows the enforcement module to be installed with the file level, at the database table-space level, or at column level to meet different operations needs. It allows the encrypt/decrypt of data as the database

process reads or writes to its database files. Decryption can usually be done in an application-transparent way with minimum impact to the operational environment.

Encrypting data and keeping the data length

If necessary to keep the length any stream cipher mode can help, but more care is needed in the implementation. Counter mode (CTR) turns a block cipher into a stream cipher. It generates the next key-stream block by encrypting successive values of a "counter". The counter can be any simple function which produces a sequence which is guaranteed not to repeat for a long time, although an actual counter is the simplest and most popular. CTR is a mode, which may be used with AES128 or AES256. If using CTR mode (and any other XOR based stream cipher) you need integrity. CTR is not providing any integrity protection. This means that an attacker who does not know the key may still be able to modify the data stream in ways useful to them, without any surety those alterations will be detected. It is now generally well understood that wherever data is encrypted, it is nearly always essential to provide integrity protection, as the risks from not doing so are high.

Stream cipher mode can help, but more care is required

For such secure operation, the IV and cipher-text generated by these modes should be authenticated with a secure MAC, which must be checked by the receiver prior to decryption. Using CTR without authentication tags is trivially malleable, and an adversary with write access to the encrypted media can flip any bit of the plaintext simply by flipping the corresponding cipher-text bit. Plain ECB (electronic codebook) mode also has a similar problem as CTR, but for ECB mode you need to exchange the whole block. For CTR it's per bit.

Both CBC (cipher block chaining) and CTR modes need proper IV management. Using a fix IV is never good for an XOR based stream cipher like CTR. With CTR mode you must have an IV if using the same key, and you should have (secure key based) integrity (MAC - message authentication code). You may compress a CCN (credit card number) before encryption if the requirement is to keep the data length. Compression may allow including a short form of integrity value, IV and/or key identifier to also support key rotation.

WHEREVER DATA IS ENCRYPTED, IT IS NEARLY ALWAYS ESSENTIAL TO PROVIDE INTEGRITY PROTECTION, AS THE RISKS FROM NOT DOING SO ARE HIGH.

Transparent data format that knows about itself

Some combinations of data types and lengths for the encryption input and output may allow including a reference to different meta data, including short form of integrity value, IV and/or key identifier. Some of this meta data can be stored in catalog. One formatting approach is called meta-complete data storage is a method of securely storing data so that the data contains information about the data and/or the encryption of the data, systems and methods of providing secure access to real world data through data transformations, and systems and methods of managing security parameters for data described in (Meta-complete data storage, United States Patent Application, 20080082834) addresses these demands with methods and systems of meta-

complete data, i.e., "data that knows about itself." Such data may be transported throughout the enterprise and beyond without additional "baggage," allowing for quick and secure transport of data and requiring minimal modifications of existing data infrastructure.

Encrypting data if a binary format is not desirable

Application code and database schemas are sensitive to changes in data type and data length. If data is to be managed in binary format, "varbinary" can be used as the data type to store encrypted information. On the other hand, if a binary format is not desirable, the encrypted data can be encoded and stored in a VARCHAR field. There are size and performance penalties when using an encoded format, but this may be necessary in

environments that do not interface well with binary formats, if support for transparent data-level encryption is not used. In environments where it is unnecessary to encrypt all data within a data store, a solution with granular capabilities is ideal. Some vendors provide transparent data level encryption with data type preservation that does not change data field type or length.

Encryption options

Format controlling encryption

Format Controlling Encryption (FCE) is based on a relatively new AES encryption mode that makes it possible to integrate data-level encryption into legacy business application frameworks that were previously difficult or impossible to address. Unlike traditional algorithms that expand data into binary fields, FCE enables encrypted data to retain its original format, on a character-by-character basis, so that encrypted data “fits” in existing fields, eliminating the need for database schema changes. For example, a 16-digit credit card number can be encrypted, with the output guaranteed to also have 16 digits; the credit card checksum can even be maintained.

FCE also preserves referential integrity, which enables encryption of foreign and indexed keys and ensures internal consistency in masked data. Through the use of FCE, Encryption vendors Solutions provides highly efficient, robust data encryption and data masking that can typically be implemented with a fraction of the effort of competing systems. FCE supports data of any format, including numeric and alphanumeric and allows format definition on a character-by-character basis. No database schema changes are required and the data “fits” in existing fields. FCE also guarantees against collisions through reversible encryption.

Partial encryption

There is an operational business need for a middle-ground between encryption and clear-text data. This can also strengthen the protection of the data. The same encryption that prevents human eyes and un-trusted systems and from reading sensitive data can also hamper trusted or semi-trusted systems, ap-

plications, which have a business need to review or operate on the data. A partial encryption concept can be applied to improve search performance on encrypted fields. Searching on one or more leading characters of a column will be much faster than performing full table scans and decryption of the full table. Depending on the distribution of the values within the column, different performance gains are accomplished due to the selectivity of such a “wild card” search.

Limit the exposure of sensitive data bytes inside applications and the LAN. Many applications have no need to view all bytes in every data field that is passed through. One approach to protect this information in application memory and in transit is to use masking or partially encrypt sensitive fields to hide the not needed bytes from exposure (Data type preserving encryption, November 2000, United States Patent 7,418,098). This can be enabled by using some mode of AES encryption algorithm that is providing full or partial format preserving encryption or preservation of length or data type. This allows arbitrary fields to be encrypted to a given the same or corresponding format. This alleviates the need to change the database, and minimizes the application end point changes to a minimum. Some of these types of encryption modes may not be secure to use when encrypting short data strings.

By encrypting different parts of a field with separate keys, a customer service representative could be allowed to decrypt and view only the last four digits of a Social Security or credit card number for verification, keeping the rest hidden. To make the scheme work, the same key should always produce the same cipher text when run against a number, without producing collisions - that is, no two numbers will produce the same cipher text. This allows use of the encrypted numbers for indexing. Finding a way to avoid collisions might be the most significant advancement in Format Controlling Encryption.

Replay attack protection and auditing

Usually, a tracking feature will monitor the sender of the SOAP message and the time that it originated. If the solution is set to block duplicate messages, it then becomes

impossible for the same message to be sent twice. If the SOA security solution is configured to track messages, then it should be able to generate usage logs and audit reports for SOA message traffic during specific periods of time.

A Multi-layer Security Advisory System can provide a framework to effectively deal with threats of some classes of attacks. The warning system could have 5 risk-of-attack-levels (Threat Levels) which when triggered, initiate specific actions by local servers within the same policy domain. Information about data security events is collected from sensors at different system layers (web, application, database and file system).

The Threat Level can be propagated to systems that are connected within a data flow. The Threat Level will also adjust for time of day, day of week, and other factors that are relevant. A score-card is maintained for each subject (user or service account/proxy-user, IP address, application, process I) and object (database column, file I) with a history of processing sensitive data. The score-card summarizes current and historical information about data access patterns for each entity (subjects and users).

The score-card also includes a 'fingerprint' that reflects historical deviation from acceptable access patterns at the level of s/i/u/d (select/insert/update/delete) operations. A high score-card value will initiate more extensive analysis before releasing data to the subject.

The dynamic and automatic altering of the protection policy between multiple system layers includes modifying the protection policy of data at one or several of the system layers. The modification is performed based on a result of the prevention analysis. The score-card

can also keep track of when a remote system need to reconnect to the central system to renew or recharge it's capability to encrypt and decrypt data. The policy may allow the local system to only operate stand alone for a certain time or processing a fixed number of crypto operations between each host connection and central password renewal. This behavior will act like a rechargeable key box and can automatically shut down the local access to sensitive data in case the local system is stolen, cloned or compromised in some other way.

Conclusion

Any system that's specifically built to support the effortless flow of data will also be eminently hackable - that's just the nature of the security beast. SOA provides real benefits and creates real security threats. The article above is just an overview of some issues to consider when developing a plan to secure your SOA environment - it is not intended to be a comprehensive guide to locking down the world's SOAs.

When developing your own risk-based holistic SOA security plan, make sure to factor in the demands of whatever regulations and standards affect your industry. Depending on how the enterprise uses SOA, it may also be vital to review security plans with partners, out-sourcers, remote offices and anyone who has authorized access to the system - how have they handled security on their ends?

Additionally, it is important to develop a clear policy that details SOA governance - management, maintenance and accountability - because SOA security cannot be purchased off-the-shelf, it needs to be built and carefully maintained. Like all security, SOA defense is an unending work in progress.

Ulf T. Mattsson is the CTO of Protegrity. Ulf created the initial architecture of Protegrity's database security technology, for which the company owns several key patents. His extensive IT and security industry experience includes 20 years with IBM as a manager of software development and a consulting resource to IBM's Research and Development organization, in the areas of IT Architecture and IT Security. Ulf holds a degree in electrical engineering from Polhem University, a degree in Finance from University of Stockholm and a master's degree in physics from Chalmers University of Technology.



Navigating a sea of fake codecs

by Pekka Andelin

Fake codecs provide everything but the satisfying access to adequate digital decompression.

The Internet has become a major scene for sharing all sorts of media files. These files may have been compressed using different codecs, some free and some commercial.

What is a codec? A codec, in this case, is used to decode compressed data streams in order to make them viewable and audible in a proper player.

Watching an AVI (Audio Video Interleaved) video and audio file with compressed data, or other compressed movie formats, may require a proper codec. The amount of codecs out there amounts to a level that makes it hard for common users to find and install the correct one required to play an eagerly awaited sequence of images. The situation gets even more complicated considering that unscrupulous individuals want to transform the common codec-eagerness into cash in, one way or another, by offering fake codecs.

A sea of fakes

Fake codecs provide everything but the satisfying access to adequate digital decompression. These fake codecs are lures that the dishonest net-trollers deploy in order to catch credulous people that fall for their social engineering skills. In the Lavasoft Research department, we work to continuously inform people about new threats.

The lure often consists of providing an easy way to watch a particular celebrity video. This can be presented actively via e-mail (where the addressee is spammed continuously with movie offerings) or passively via a compromised website. The enforced drive-by download represents a combination of these strategies. The latter is possible using malicious web-coding and by exploiting vulnerabilities in the users' web browser to enforce fake codec downloads.

Don't take the bait

Swallowing the lure may lead to a situation where the user has a severe system infection on their hands caused by hard-to-remove rogue applications or other dropped or downloaded malware. What is a movie-loving, codec-craving individual supposed to do in a sea of fake codecs?

The first step is, of course, always to secure the excursion-vessel in order to make the hunt for codecs as pleasant and secure as possible. A good starting point is to follow available online security guides to patch possible security glitches (in the system, browser, etc.).

Securing the system with proper security applications would be another.

I would, however, like to emphasize the need of obtaining knowledge in order to be less exposed for the traps laid out by the unscrupulous net-trollers. The trick is to acquire as much knowledge as possible, navigate to the right location in order to get the right codec, and then stick to that winning combination (i.e. something that is malware/adware clean and works well.) Developing - and trusting - a gut feeling for what is safe to install is also essential, but this must be combined with adequate knowledge.

DEVELOPING - AND TRUSTING - A GUT FEELING FOR WHAT IS SAFE TO INSTALL IS ALSO ESSENTIAL, BUT THIS MUST BE COMBINED WITH ADEQUATE KNOWLEDGE.

Learning by example

The following is a possible scenario of how a user could handle a situation where a movie is unplayable due to the lack of a specific codec. (Note: I have chosen to call this a possible scenario, not a recommendation or guide; this is due to the fact that codecs change on a regular basis and a codec or codec pack that is clean from malware at one moment may be infected or ad-infested at another.)

The movie X does not play as a suitable codec is not found on the system. The application Videoinspector (or Gspot) is used to pinpoint which codec(s) the media file in question requires. Videoinspector and Gspot (freeware utilities) can also be used to display the codecs that are already installed on a system. Each codec is usually represented by a four character code (FOURCC). Here's a bit more info on some of these codes:

- Xvid, DivX (belonging to the XMPEG-4 Part 2 standard) are commonly used to compress .avi files.
- MPEG-1 is used for Video CDs. MPEG-2 are used for the DVD and SVCD formats.
- WMV (WMV 7-9) stands for Windows Media Video supported natively by the media players from Microsoft.

- Files with the .mov extension are media files encoded in the Apple QuickTime video and audio format. QuickTime files could also be played using the QuickTime Alternative software.
- Files with the .rm extension are Real Media files which have to be played with Real Player (or by using the Real Alternative software).
- Files with the .mp4 extension are encoded in the MPEG-4 format and those could be played in several portable video players.
- Files with the .mpg or .mpeg extensions indicate that the file is either MPEG-1 or MPEG-2 video. If the .mpg or .mpeg files cannot be played with Windows Media Player it may indicate that a DVD software player has to be used in order to play the file.
- Files with the .vob extension indicate that the file is a DVD Video Object file. Those files belong to the MPEG-2 format and are usually stored on DVD discs. The .vob files may be played with a DVD software player or by using Media Player Classic with the proper codecs.

The file name does not always reveal the encoding method, sometimes for example DivX- and Xvid encoded files come with only the .avi extension. In other cases, the file-name itself can provide valuable information that could be used to pinpoint which codec to use.

Audio codecs are used to decompress digital audio data to allow the user to listen to the audio track that is accompanying a movie. The .mp3 extension stands for MPEG-1 Audio Layer 3, which is a common container format for audio. Many .avi files may come with .mp3 audio. The .ogg extension usually refers to the Ogg Vorbis audio file format. While .mp3 and .ogg are compressed audio formats PCM audio is an uncompressed audio format (commonly used in audio CDs). MPEG Layer II (.mpa) and AC3 are common audio formats that can accompany DVDs. The .wav extension stands for Waveform audio format which is a Microsoft and IBM audio standard.

The next step is to navigate to a selected, trusted location in order to get the correct codecs. Sites are dynamic in their nature and they change with time which could mean that a former “safe” site could be “malicious” at some other occasion. This is where awareness and use of gut-feelings come in handy. Sites like www.free-codecs.com offer links to many codecs, codec packs and freeware players.

The K-Lite codec pack is a common freeware codec pack that comes in three versions: Basic, Standard and Full. The Basic version comes with the most common codecs. Keep in mind, there is no need to install all of the codecs out there - only the ones that have been pinpointed with tools like Videoinpector or Gspot. The standard version of the K-Lite codec pack also includes the Media Player Classic which can be used as a media player. Security conscious users may check the codec

files by using online scanning services (such as virustotal.com) before installing them.

Users that do not want to deal with separate codecs or codec packs may use the freeware VLC (VideoLAN client) player to play movie files. This client has all the common codecs “built in”.

Removing codecs

You may be wondering if there is an easy way to remove codecs that are installed on your system. Codec packs are most easily removed by using their uninstaller (as in the case with the K-Lite Codec Packs), something that all trustworthy codec packs should come with. There are, however, some instances when it may come in handy to know how to remove codecs manually.

In order to uninstall codecs manually navigate to Start – Settings – Control panel and then to System. In the System Properties, click on the Hardware tab and then on the Device Manager button. In the Device Manager, expand “Sound, video and game controllers”. Clicking on the Audio Codecs opens the Audio Codecs Properties and clicking the Properties tab in that interface presents a list of the Audio Compression Codecs that are installed on the system. Now the user may remove or enable/disable a selected codec from the list. Video Codecs can be handled in the same manner by choosing “Video Codecs” from the Device Manager under “Sound, video and game controllers”.

IF IT SOUNDS TO BE TOO GOOD TO BE TRUE IT PROBABLY IS.

Simple codec tips & tricks

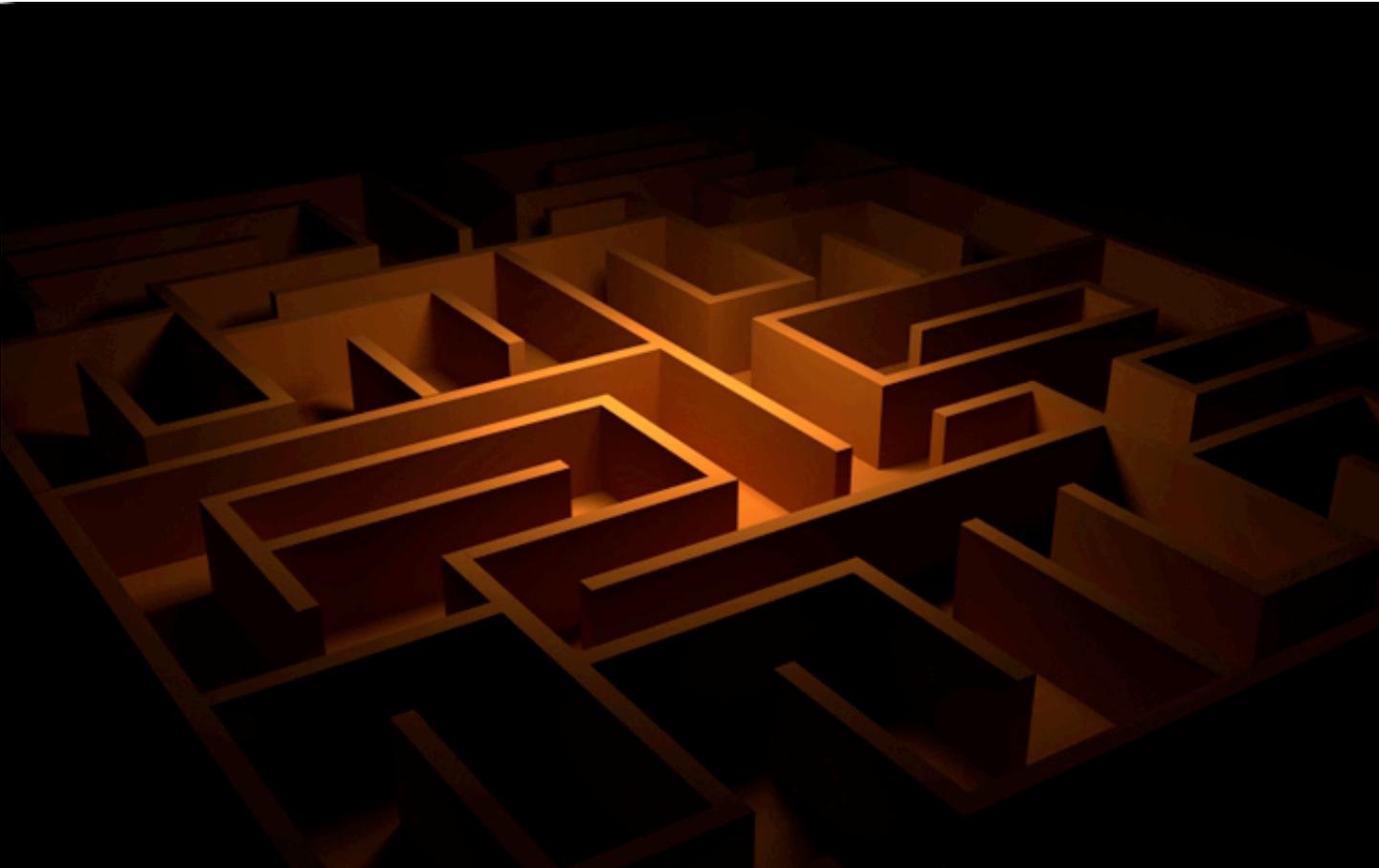
I hope that this article has shed some light into the comprehensive and often misunderstood area of codecs. Here are three important things to remember:

- NEVER download codecs on the fly. The same is true for when you’re prompted to add

obscure codecs automatically in order to be able to watch some spectacular movie.

- If it sounds to be too good to be true it probably is. Most of the online movie offerings stating to be movies of nude celebrities are just lures that are laid out to trick gullible surfers.

- Get the knowledge you need in order to be aware of the tactics used by unscrupulous codec scammers!



Role Based Access Control

by Steve Slater

One of the most common buzzwords in IT security and compliance is RBAC, or Role-Based Access Control. The concept of RBAC is very simple, and has even been codified into an ANSI standard. But what do roles and role-based access controls really mean to the end user? This article presents some of the business benefits of managing access rights via roles, discusses whether or not roles are right for you, and provides guidance for deploying role-based access controls.

What are roles?

First, we need to define a role. As mentioned above, the concept of RBAC is simple; a role is nothing more than a collection of user access rights. This collection of privileges could be limited to a single business application or include privileges from several applications or systems. In addition to access rights, a role could include other roles, leading to role hierarchies.

How do we define a role and which privileges belong in which role? Who decides which users are in which roles? What happens when users need privileges that are not part of their

current role? These and similar concerns are what make RBAC deployments complicated and challenging for any organization.

Why Role-Based Access Controls?

The business benefits of RBAC are potentially very great. The most obvious is the tremendous time savings when combined with an automated provisioning tool. System and application accounts for new hires are created immediately with the correct set of access privileges needed for their job, based on predefined roles for the user's title or responsibilities.

Furthermore, compliance and security controls are significantly enhanced by using role-based access control. The roles themselves are already pre-defined. When managers and business owners perform periodic certifications of access rights, they simply need to review a handful of roles to ensure the user is in the correct role, rather than reviewing tens or hundreds of individual access rights. Moreover, automated tools can very easily detect user privileges that are outside of the approved role and provide a mechanism for handling exceptions.

Both of these core drivers equate to improved security governance and a reduced risk of audit findings and compliance deficiencies. In addition, the extra automation leads to significant savings of both time and cost.

Our ideal end state for our organization is therefore a well-oiled machine wherein every user access right or privilege is included in one or more roles. Role hierarchies are utilized to create “roles of roles” that enable cross-application enterprise roles. A limited number of top-level roles will exist and each user in the company is assigned to a handful of these top-level roles. The role assignments are linked to job descriptions and functional requirements, and no exceptions exist wherein users are granted individual access privileges.

Unfortunately, this RBAC nirvana is extremely unlikely to happen. The reality of nearly any workplace is that the work still needs to get done and various skill sets across the company are leveraged to perform tasks that may not fit cleanly into any particular job description. This inevitably leads to either many exceptions to existing roles or the creation of a unique role for each user.

We therefore want to be sure to set realistic expectations and a plan for efficient handling of RBAC exceptions. As we’ll see later in this paper, we also know that including every business application in our RBAC deployment is extremely unlikely. Given this proper perspective on RBAC, we can follow the steps described in this paper to successfully evaluate and implement a role-based access control program and achieve the security and cost savings we expect.

The RBAC deployment process

The process of an RBAC implementation can be simplified into four basic steps, each with its own unique set of challenges and desired outcomes. Failure to complete any of these phases can lead to serious complications in the deployment process. Our recommended steps include needs analysis, scope, planning, and implementation. We will walk through each of these processes to identify common pitfalls and provide recommendations to ensure success.

Needs analysis

RBAC is not for everyone. Even though this paper is focused on enabling a successful RBAC deployment, and my company provides products and services to enable RBAC, some of us simply should not attempt such a potentially massive undertaking. Or perhaps the scope needs to be more limited. Whatever the case, conducting an honest needs assessment will guide us down the best path.

We need to ask ourselves a few key questions. First, what are the business drivers? What pain points are we trying to address with the project? We presented two common drivers above, and you likely have your own unique environment that has other imperatives. These pain points become the core of our project’s success criteria and should always remain forefront during subsequent project phases. One of the most critical tasks of the RBAC project manager will be to continuously refer back to the primary objectives and keep the team focused so that months don’t get wasted learning a “cool feature” that doesn’t really address a core problem.

It is also crucial to quantify the inefficiencies or compliance failures. An RBAC deployment can be time-consuming and hard-dollar cost savings will help keep executive support alive throughout the project and provide a true return on investment calculation.

The next question we should ask is, will RBAC really help me? We may have several struggles related to access rights, but are roles the answer? Let’s look at a few considerations.

- **Common functionality versus custom responsibilities:** What percentage of users can be grouped into common responsibilities and therefore common roles? Typical cases where this happens are in helpdesk or customer service positions. Often several people perform identical functions. In the medical community, most doctors and nurses need the same access privileges as other doctors and nurses.

Conversely, information security staff and IT administrators are some of the hardest positions to fit cleanly into roles. In smaller companies, often nearly every employee wears many hats and has custom access needs. A quantitative measure of the percentage of users that will be covered by roles provides a key needs analysis metric.

- **Employee change and turnover rate:** How often do employees and contractors come and go, and how often do roles for existing staff change? If changes are infrequent, it is much harder to justify the expense of a full RBAC deployment. Perhaps a simpler auditing or compliance tool is more appropriate.

- **Compliance and security benefits:** How much time will be saved or audit risks be

minimized through role-based access controls? For example, nearly every company must perform some type of periodic review and certification of user access rights. In many situations, each employee being reviewed could have tens or hundreds of individual access rights. Reviewing each privilege for every user in a company will either take an extraordinary amount of time for the reviewer, or else (more likely) the reviewer will simply “rubber stamp” the certification; in which case no security value is gained. Conversely, if each user has only several roles and a handful of exceptions, the approver is much more likely to stop and consider the request before blindly approving it.

By reviewing all of these factors, an educated recommendation can be made whether or not to proceed with the project. It is possible that the needs might not be great enough to warrant continuation of the project and potentially up to millions of dollars can be saved by avoiding a project with limited chance of success. On the other hand, the analysis may show an overwhelming potential for cost reduction and compliance improvement. Either way, our needs analysis has led us to our success criteria as well as provided metrics for an ROI calculation.

Information security staff and IT administrators are some of the hardest positions to fit cleanly into roles.

Scope

Armed with accurate knowledge of the true business needs, we now need to determine the scope of our project. Resist the temptation to take on every application in the company. As with nearly every identity-related project, an RBAC deployment conforms to the law of diminishing returns.

Some applications will simply take too much effort and offer too little benefit to be justified. Though the exact number will vary by company, a typical ideal scope will be between 60-90% of the key business applications.

Compliance regulations are often key aspects to consider and will narrow the scope to primarily compliance-critical applications.

Other factors to consider are the internal relationships between various business units. A key part of the RBAC project will be engaging business owners to help define which privileges should be part of which roles. Some applications will be either out of scope or part of a follow-on deployment phase simply because of expected challenges.

If you will be deploying commercial tools or relying on consultants to assist your deployment, this is an ideal time to begin engaging third parties. Now that we have identified our core business drivers and set our scope appropriately, the internal and external costs estimates can be weighed against the expected benefits.

Planning

The old adage that says “if you fail to plan, you plan to fail” was written with an RBAC deployment in mind. Be sure to allow for time in your estimates. For a typical RBAC project, well over 50% of the time will be spent in the planning phase. The goal of the planning phase is two-fold. The first is to plan the technical side of the project. Which access rights belong in which roles and which tools best fit our needs? The second goal is to determine if we can actually succeed in an RBAC deployment. Do we have support from application owners and administrators across the enterprise? Do the benefits exceed the expected costs?

An RBAC project is typically driven from the IT and/or information security team. Always remember that we are not an island. Specialized knowledge of a diverse set of applications will be necessary to move the project forward. Application administrators are essential to understanding often cryptic access rights profiles. Line of business managers need to approve the proposed role definitions. The successful RBAC project will have a large

virtual team that includes representatives from each of the in-scope applications.

Now that we have everyone on-board, it is time to achieve the primary goal of the planning phase and determine which privileges belong to which role. This is a very daunting task, especially at the beginning. Various automation tools have been developed to assist in the process and we will discuss several types later in this paper.

For the RBAC core team, this is the most critical phase to keep moving and the easiest place in the process for the project to spiral into analysis paralysis. Never underestimate the value of strong executive support. When other priorities begin to compete with the RBAC project, we must prevent it from being delayed. Stress the ROI numbers we calculated above to gain the support and ensure a high priority. But perhaps the most important tip in the planning phase is to be extremely clear and direct with our extended virtual team. We are often “borrowing” people’s time to complete this project and we need to give clear guidance to avoid wasting their time.

Application administrators are essential to understanding often cryptic access rights profiles.

For business owners, planning involves working with the RBAC team to define the roles. Some of the details we need to collect include:

- Total number of privileges in the application.
- Pre-existing roles within the native access rights definition.
- Types or categories of people that use the application.
- Access rights that are relevant to all users.
- Access rights that are assigned to only a subset of users.
- Existing users that we can use as a prototype, a starting point for a role. This is often a nurse, doctor, helpdesk user, customer service representative, or similar position.

Using this data, we perform access rights data mining and combine that with the business and administrator knowledge to accurately define the necessary roles for each ap-

plication. Remember to allow for exceptions when necessary. Our initial needs analysis most likely did not include placing 100% of user access rights into roles. More often we are striving for cost reduction and compliance improvement. These can be achieved even with exceptions as long as our exception handling process is simple and efficient.

I often hear claims that some tool or widget can automate this entire planning and role-mining process. Don’t believe the myth. Some tools are very useful for sorting and collecting data, and can save a tremendous amount of time. But no tool can explain the business-related uses of the application itself that are so essential to the process of defining roles. You should always plan on significant involvement from key application owners.

After completing role analyses for each application, we then combine these results across

the entire company and again look for commonalities. This is an iterative process where we seek to identify a percentage of common attributes based on key values such as job title, cost center, or organizational charts.

We use intelligent trial and error to attempt to fit a high percentage of common privileges into distinct roles. When we think we are close, we then verify with the extended project team to confirm and modify based on the irreplaceable human knowledge. Our end result will be a set of enterprise roles that group together various application-specific roles.

Remember that we are not seeking to have zero exceptions. But if we begin to see nearly as many roles as we have users in the company, we should not ignore that warning. Maybe we need to re-evaluate our role definitions. Perhaps our organization is not currently managed in a way where RBAC helps. It is far better to recognize that now before devoting resources to implementing a solution that can't achieve the project goals.

Implementation

If the first three phases were completed successfully, the implementation phase will be the easiest part of the entire RBAC project. All of the hard work is already complete. Our success criteria are defined, our scope is set, and

the majority of our enterprise roles have already been created. For those deploying a third-party RBAC tool, simply complete the installation and configuration. For others developing in-house systems, the required use cases are now defined.

Next, our provisioning and de-provisioning functions need to be altered to include the role definitions. This is where we realize a majority of true cost savings. The provisioning tool or process needs to integrate with the RBAC definitions.

For most commercial tools, this is easily achievable. For internally-developed tools or processes, be sure to consider the modification costs as part of the project planning. If the provisioning system is not RBAC-aware, the automation benefits will be difficult to realize.

Finally, the compliance and security benefits are significant. The periodic certification of access rights that previously involved certifying hundreds of privileges for each user now consists of certifying a handful of roles and exceptions. In addition, separation of duties conflicts can be defined at a role level and reports can instantly detect users with exceptions to the roles. Reports help identify users with excessive access rights before a catastrophic event occurs like the recent trading incident at Societe Generale.

Reports help identify users with excessive access rights before a catastrophic event occurs like the recent trading incident at Societe Generale.

Hazards and tips

We have just completed a four-step process to deploy role based access control. In some cases, it might go very smoothly. More than likely, however, one or more of the following pitfalls may threaten the project.

Bogged down in the details

At many places in the process, some applications will be very difficult to understand. The scope of the initial RBAC deployment therefore needs to be carefully and realistically set. If certain applications present unusual chal-

lenges, consider delaying them for later. If all applications seem to be overly difficult, consider if RBAC is appropriate and/or engage outside consulting help to view the project from a fresh perspective.

Too many exceptions

During the planning phase, it is unavoidable that certain users will not fit neatly into roles and will require exceptions. At SCC we coined the phrase "The Law of Exceptions." The number of exceptions is inversely proportionate to the number of roles.

Or more clearly, the more roles you have, the fewer exceptions, and vice versa. If you have too many roles in the organization, the RBAC efforts become pointless and you approach one role per user. If you have too many exceptions, RBAC again does not meaningfully improve upon the current situation. We strive for a compromise between number of roles and number of exceptions.

If a high number of users are requiring exceptions, consider this a warning sign. Especially for small and mid-sized organizations, RBAC is often not appropriate due to the many hats individual people must wear.

This highlights the importance of detailed planning to identify potential issues before committing significant resources.

Change and apathy

Change in any part of life should never be underestimated. While change is often good, it is also often resisted. As we attempt to modify internal processes and gain more efficiencies, we will inevitably be disrupting the status quo. We may be embraced by some and ignored by others.

The scoping exercise should anticipate resistance by thinking outside the box. Are people concerned about their job being eliminated? Do they have too many other priorities to fully engage in our RBAC project? Honestly consider these factors and ensure a strong executive support to help overcome possible apathy.

While role-mining tools look great in a demo, the value is extremely difficult to predict.

Tools

Technologists love tools. They make our lives more efficient and automate very labor-intensive tasks. But how do we know which tools we really need? In this section, I will give a brief description of the general classes of tools related to role-based access control, and provide some considerations for your own evaluation.

Role-mining tools

The mission of a role-mining tool is to analyze existing identity and access data within the organization and suggest role definitions. Using a variety of formulas, the tools will consider existing privileges, organizational charts, job title, cost center code, geographic location, and various other parameters. Since the first analysis is almost never correct, we look at the results, tweak some parameters, and try again. This process iterates until we are either satisfied with the results or give up trying.

While role-mining tools look great in a demo, the value is extremely difficult to predict. Sometimes they will provide a great starting point for mapping privileges into roles, while in other companies, nearly all of the work of the

role-mining tool needs to be re-created. In a highly centralized environment with many common classes of users (like helpdesk, customer support), they can typically perform better. When performing a cost-benefit analysis for role mining tools, consider some of the following points:

- How well did the demo/evaluation perform with your data?
- Do internal application owners already know what their application roles should be?
- Do you have limited support outside of your project team where this type of automation tool could help fill in the gaps?
- Role mining is typically a one-time task and the tool is not heavily used after the project is complete.

Identity management tools

Many books can, and have, been written about the various aspects of identity management (IdM) solutions. The commercial solutions have various levels of support for role-based access control. Some have no concept of a role while others have full integration with a role-mining tool and provide interfaces to manage the ongoing maintenance of the roles.

The decision to use an IdM tool is largely independent of your RBAC project since multiple types of solutions exist to manage the role definitions besides IdM products.

The costs of an IdM deployment typically run in the millions of dollars because of the high consulting effort required, but the benefits of an IdM solution are likewise potentially high. A solid cost-benefit analysis should be completed outside of the RBAC efforts.

As they relate to RBAC, the most important considerations of an IdM tool include:

- How hard is it to define cross-application enterprise roles?
- Does the tool support the concept of a role hierarchy, where roles contain other roles?
- Is the automated provisioning fully “RBAC-aware”?
- How well can the IdM tool help with the ongoing tuning and compliance efforts related to RBAC?

Audit and compliance tools

A new category of compliance tools has emerged in recent years that can also assist with managing your role-based access controls. Burton Group has named this category Identity Audit (IdA). IdA tools, such as SCC’s Access Auditor, were developed to automate security and compliance efforts including the periodic certification of user access rights, enforcing separation of duties (SOD), and alerting and reporting to access rights data across the organization.

Because these tools do not perform the provisioning like an IdM solution would, the cost and deployment efforts are a fraction of IdM solutions’ outlays.

These compliance tools usually have the support for managing roles as well. All of the certification, SOD, alerting, and reporting functions can be based on a combination of roles and distinct privileges, and exceptions are easily spotted. IdA solutions can operate independently of IdM products or interoperate to leverage combined strengths.

Do it yourself

The final option for managing a role-based access control deployment is to build your own system to keep track of the role definitions and perform the required security and compliance reporting.

While this is usually too large of an endeavor to be cost-justified, some companies have been extremely successful in building their own RBAC management system. The common success factors in these cases were a clear business case and limited scope.

Summary

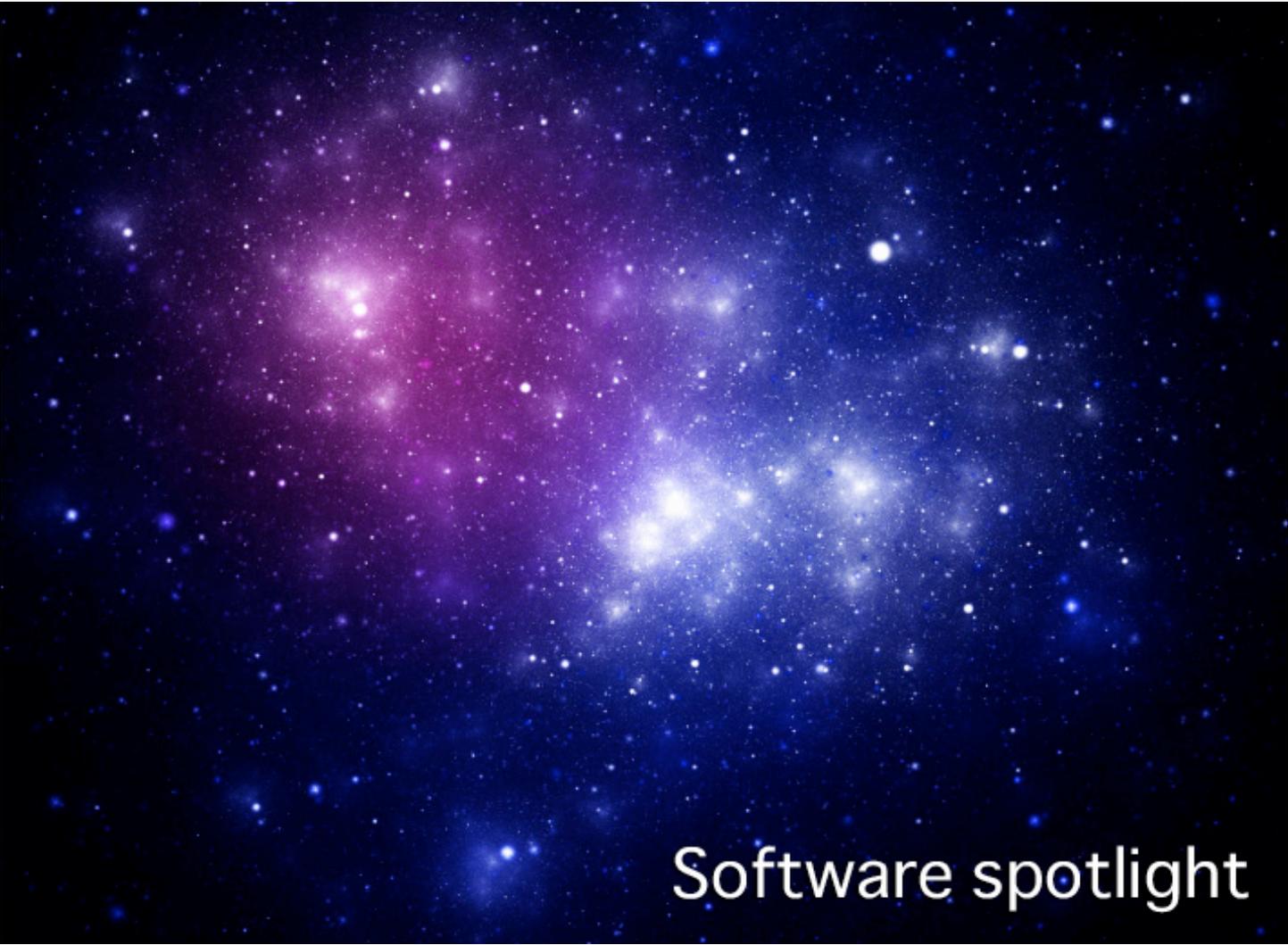
I presented a four-step process for leading a role-based access control project, and gave consideration to various tools to help you succeed. We need to remember two key points.

First, the ideal end-state of RBAC nirvana is not going to happen, but we can still make significant improvements in security, compliance, and automation.

Second, nothing is more important than an honest and accurate needs analysis to keep the project focused and ensure that we achieve a rapid return on investment. These items will become our rudder as we keep our project on course.

Dr. Steve Slater, CISSP, is the Founder and CEO of Security Compliance Corporation (www.securitycompliancecorp.com), a leader in the identity management market focused on user access rights, role management, attestation, and separation of duties. Over the past 15 years, Steve has provided a range of expert consulting including web application vulnerability assessments, penetration testing, regulatory compliance (SOX/GLBA/HIPAA), and PCI assessments for some of the world’s top companies, such as Bank of America and Visa.

Dr. Slater has written and taught Information Security classes for leading training organizations on topics including auditing techniques, LAMP, web application security, and secure development. In addition to security, Steve also holds a PhD in Nuclear Engineering from UC Berkeley and has several publications relating to high-performance computing and advanced numerical analysis. His scientific expertise earned the recognition of both the National Science Foundation and the Department of Energy.



Software spotlight

Drive Encryption (www.net-security.org/software.php?id=725)

DriveEncryption helps you encrypt the disk drives which are using FAT or NTFS File Systems.

Lutz (www.net-security.org/software.php?id=338)

Lutz is a small but full-featured portscanner for Linux. It uses some advanced scanning techniques like SYN, FIN, NULL, and XMAS scan and supports Protokol scanning. A simple OS Detection by TCP Fingerprinting is also included.

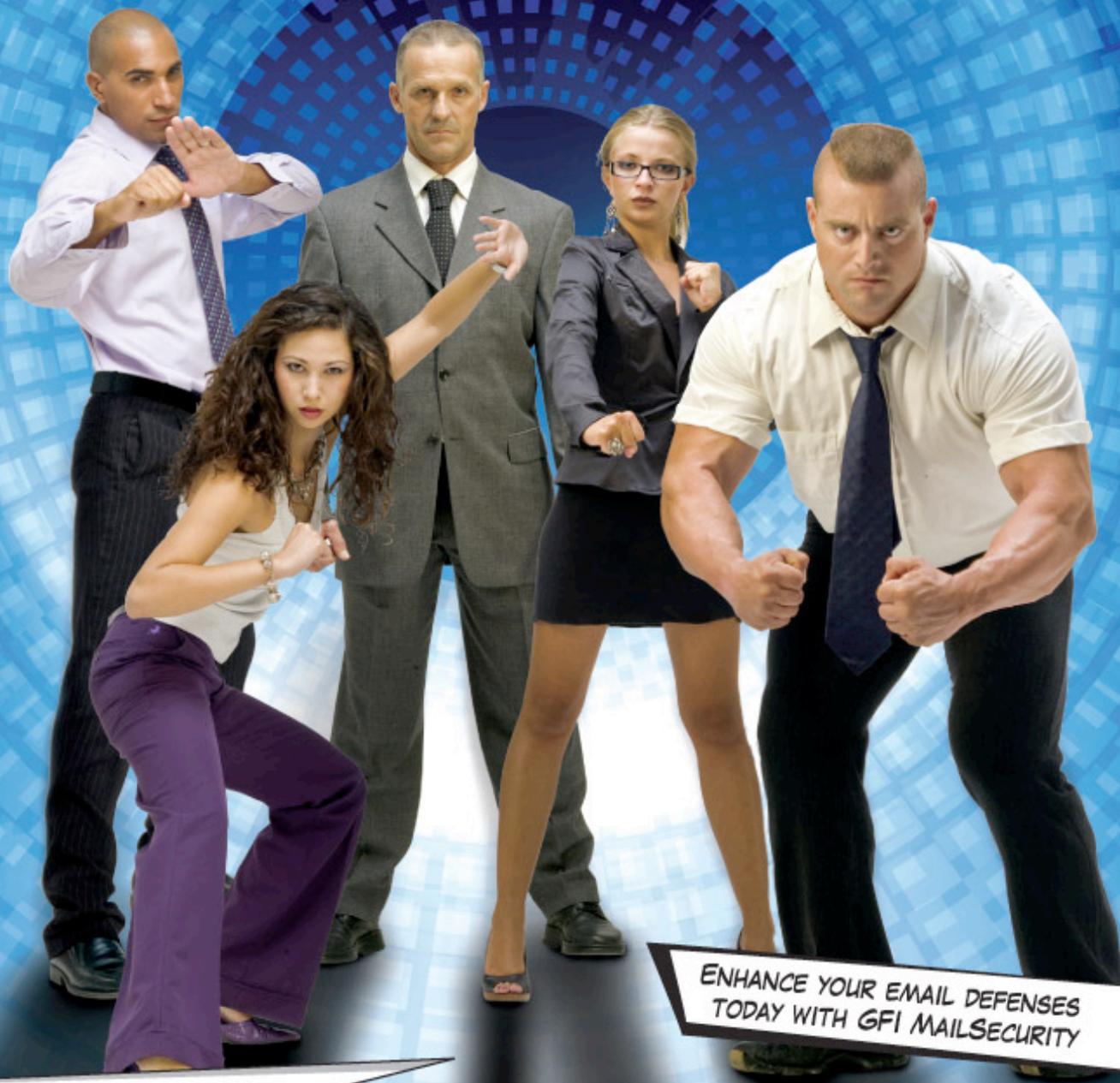
MacNikto (www.net-security.org/software.php?id=678)

MacNikto is an AppleScript GUI shell script wrapper built in Apple's Xcode and Interface Builder, released under the terms of the GPL. It provides easy access to a subset of the features available in the Open Source, command-line driven Nikto web security scanner, installed along with the MacNikto application.

segatex (www.net-security.org/software.php?id=697)

segatex is a tool to configure SELinux policy with the help of a GUI. At the push of buttons, it can generate a .te file in the /root/segatex directory. You can then edit your .te file, make a module, and install. You can make any module name and also edit present modules. You can install, update, and remove modules.

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



ENHANCE YOUR EMAIL DEFENSES
TODAY WITH GFI MAILSECURITY

GFI MailSecurity

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

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

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

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

Download your **FREE** trial version from www.gfi.com/ehns/



GFI NETWORK SECURITY
CONTENT SECURITY
MESSAGING



McAfee
NORMAN

bitdefender
secure your every bit

AVG Anti-Virus



How to build a security strategy to grow your career, success and results by Debbie Christofferson

Are you creating strategic advantage, or are you a simple firewall administrator, busy putting out fires? Are you a business enabler, and is your function tactical or strategic? Security strategy isn't about spending more, it's about focusing more.

To get started, focus on your organization's core business, priorities and pain points. Include hot buttons especially related to security. It does not matter if your business has no documented strategy, or if current plans make no mention of security. Your job is to define a risk-based security strategy that supports the business.

Decide how security can add value

Your company's core business and the related security drivers will underpin your strategy:

- Why does security exist, and why were you hired?
- Who is the customer of your business and where is security's role?
- Do you have intellectual property to protect, such as designs for computer hardware and software?
- What outsourced services are provided that impact security?

- Who are the critical vendors, suppliers and business partners to the business?
- Do you have open security audit findings?
- Is your organization subject to regulatory requirements?
- What is the cultural impact if you're a global company?
- What is the real risk if you do not comply?
- Where does reputation factor in, or monetary fines, loss of intellectual property or market lead time, or losing your license or ability to do business?

Know exactly what you need to protect and why, and what the priorities of the business are.

Collect stakeholder inputs on their security requirements

Define who those stakeholders are, including Legal, Compliance, Human Resources, Internal Audit, Information Technology and your

own chain of command, peers, and direct reports. Don't forget the business lines—those matter most. What major initiatives or projects does the business have going on? Define early on how security fits the business model.

Assess your security program's Strengths, Weaknesses, Opportunities, and Threats (SWOT)

Identify major risks and gaps, unrealized opportunities, and low hanging fruit that you can pick off with minimal time or money. Engage your staff fully. Seek quick wins to build early momentum.

Integrate trends affecting your industry and organization, as they affect security

These include rampant counterfeiting, an on-line criminal frontier that is growing in sophistication, wireless and mobility, virtualization, growing global regulation, and Software as a Service (SaaS) that also goes by the not-so-

new name of "Cloud Computing" or shared IT services.

Invasion of the laptop snatchers: If encryption isn't on your bill for laptop hard drive encryption, it's time to start making it happen. Encrypted databases, portable memory sticks, wireless and passwords all fall under strategy.

In addition to data centers reducing power use, green initiatives spill over to work-at-home, to reduce the office footprint. If a contracted Personal Assistant supports your CEO from a home office, how will you secure that access when it's not your PC or network? That's one example.

Cowboys still roam the range in developer security. Two certifications demonstrate a growing risk and demand for securing web-facing applications and the development life cycle. These are offered by SANS (www.sans.org) and ISC2 (www.isc2.org).

DEFINE EARLY ON HOW SECURITY FITS THE BUSINESS MODEL.

Define your action plan based on the outcomes for the value proposition, stakeholder feedback, and your SWOT analysis

- Use a 12-month period. If you've previously published a strategy, then increase this to a 24-36 month window for your strategy and supporting goals.
- Write a "draft" plan with major initiatives, and goals to support them.
- Seek stakeholder feedback, then update your plan and prioritize it top to bottom.

Publish and communicate your strategy

- Take advantage of existing venues, or create new ones.
- Write it to an executive level, in executive summary.
- Speak in plain English not geek-speak, be clear and concise.

Are you a superdork? If you're not the head of your company, or the owner's progeny, you might want to revisit your social skills and how you get the word out.

For your written plan:

- Send to key stakeholders, post to your organization's internal web site, and inform your team, up, down and across the organization.
- Publish an annual state of security report, or report out in a special meeting, one you create, or insert yourself into an existing meeting structure.

Your success depends on visibility, support and feedback from stakeholders and you must build streets to reach them.

Create a security steering committee or council, if none exists. This is made up of stakeholders and guides your strategy at a high level.

If you report to IT, include no more than two IT management representatives. Business units would ideally come from carrying the highest priority for business risk, due to materiality and impact to the bottom line. Choose security supporters not detractors. This forum balances security business risk, by focusing resources where they matter most.

Benchmark and measure your program, to manage results

Metrics increase visibility, define your focus, and motivate behavior changes. Choose wisely for a management view of security - apply metrics in their language, not yours.

Pictures count, with a clear compelling view of how your program impacts security risk from the top down. Define a baseline of where you are, identify gaps, and measure change. Report regularly to stakeholders.

Keep your plan current

Writing the plan is half the battle, now you need to execute it. Review your strategy at least quarterly, and update it annually with your stakeholders.

Creating a security strategy is free

It doesn't cost you a penny, and it's worth a million bucks in results for the impact to your career and security program. Security is about the business, not technology. It's critical to stay focused, and to manage security as a business, to break out of the pack.

Debbie Christofferson, CISSP, CISM, offers more than 15 years of information security management experience across the U.S., Europe and Asia in a global Fortune 500 environment. She's a current information security manager and serves the local and international boards for ISSA (Information Systems Security Association). Debbie shares her expertise as a published author, columnist and speaker, on future trends and strategies for careers and information security. You can contact her by e-mail at DebbieChristofferson (at) earthlink (dot) net.



OWASP

The Open Web Application Security Project

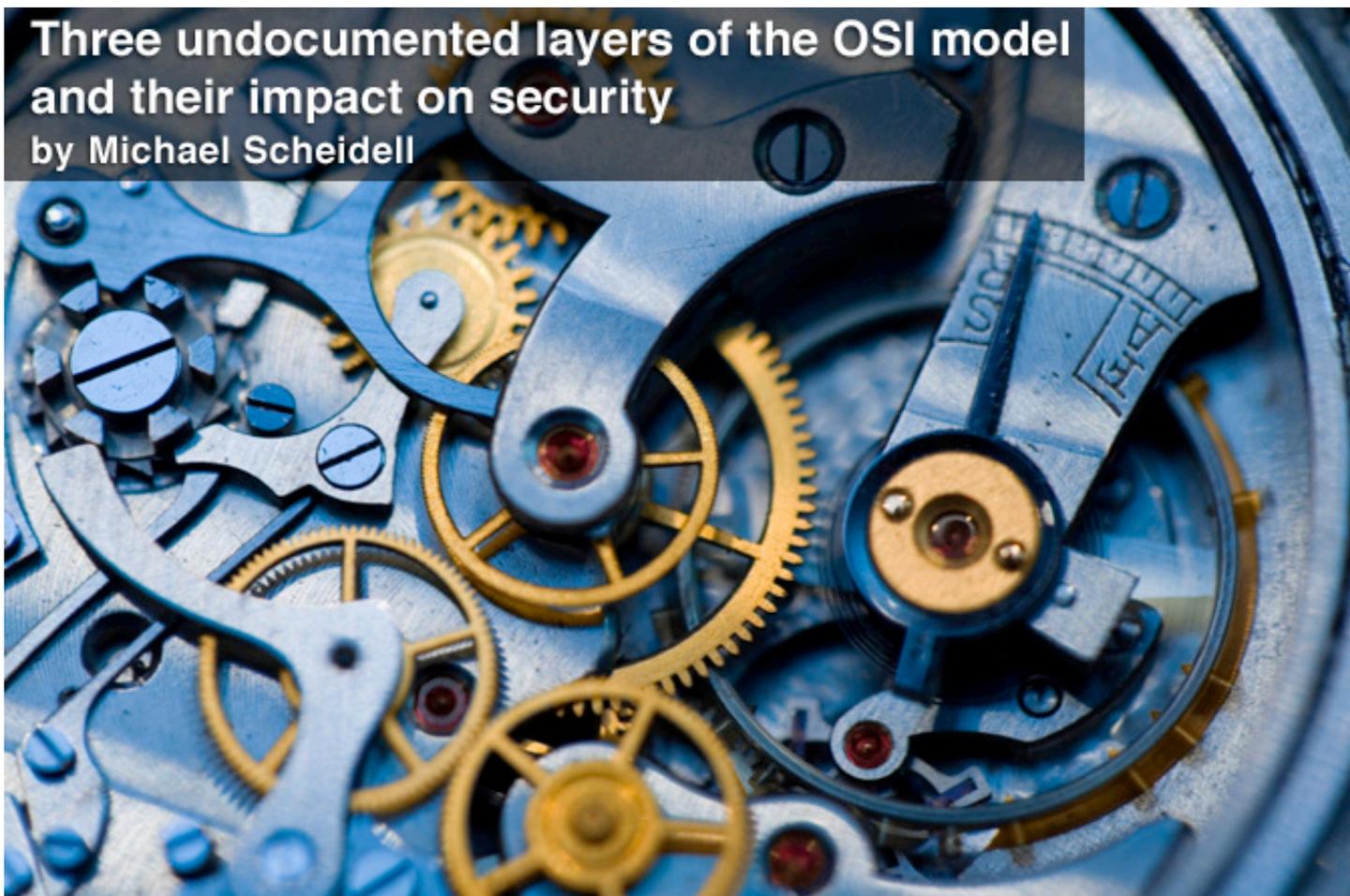
JOIN US! OWASP is a free and open community dedicated to improving application security for everyone.

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

www.owasp.org

Three undocumented layers of the OSI model and their impact on security

by Michael Scheidell



The single most serious threat to the security of sensitive information today is not individual hackers or gangs of cyber criminals. It is not an inadequate firewall, lack of logging or missing patches, or even the negligent employee. Nor is it found in Layer 7 of the Open Systems Interconnection (OSI) model - no amount of application filtering or testing can address this threat.

Instead, the most serious threat to data security lies in what we refer to as the undocumented layers of the OSI model: Layer 8 (Politics), Layer 9 (The Religion of Technology), and Layer 10 (Economics).

You can conduct GLBA, SOX, FACTA, HIPAA, FERPA and ISO audits until you are buried in reams of audit reports. You can recommend implementation of DOD or NIST standards until you feel like Dilbert trying to convince his boss to do something logical. The bottom line is that, if your executives are stuck in one of these layers - you (and your future) may be stuck as well.

This paper explores some of the issues unearthed during our security audits and offers insights to help you navigate the executive suite to overcome them. A quick word of advice: the last thing you want to do is present your executive team with a long list of recom-

mended changes they won't read - let alone approve. Organizations fear change even more than they fear hackers. Pick your battles, and learn to suggest improvements in bits rather than bytes. This strategy will help you gain traction over time and build solid success in your role within the organization.

Beyond the seven layers

The traditional seven layers of the Open Systems Interconnection (OSI) model for network architecture begin with the most fundamental - the physical layer - and move upward in complexity through data link, network and transport layers, and on to session, presentation and application layers.

The seventh layer, application security, is two-pronged, encompassing web application security and email application security. Web application security addresses risks such as SQL

injections and web-based attacks, while email application security focuses on viruses, worms, phishing and the like. Most IT experts are trained to consider the seven OSI layers when making decisions regarding information security solutions. This is a fine construct, but is just a beginning.

The three undocumented layers of the model exert a powerful influence on information systems and security decision-making. It is important to understand these hidden influencers, and how they can drive sub-optimal decisions, delay or derail projects, and open security gaps that can become security breaches.

The scourge of malware and high cost of cybercrime

The evidence is all around us. Cybercrime is rampant, ongoing, and expensive. Estimates by the Federal Bureau of Investigation suggest that cybercrime costs U.S. businesses a staggering \$67.2 billion annually. In its July 2007 report, the Federal Trade Commission declared that spam has become a substantial global tool in the propagation of financial crimes. And when the Internal Revenue Service published its 2008 report of the 12 most serious tax scams, phishing topped the list. Phishing is a prime tool in the exploding problem of identity theft.

We are all familiar with the growing body of knowledge surrounding email communication, and the spyware and malware that can plague it. As of October 2007, for example, almost 70 percent of email communications sent to businesses were spam, according to Gartner research. In residential households spam constituted 75 percent of all email received.

Research conducted by market intelligence firm IDC revealed that 10 of every 12 email messages are spam (83 percent), and one in 39 carries a virus. IDC also projected that consumers and businesses will spend more than \$305 million to detect and eliminate spyware between 2007 and 2011 - a figure that seems low in comparison to the degree of risk.

These numbers tell a disturbing story about the high cost of cybercrime. Among those costs are application costs such as the ero-

sion of network bandwidth, reduced network performance and diminished network storage (that malicious email has to be quarantined somewhere!).

There are the costs of lost employee productivity during hacker attacks or in dealing with destructive worms and viruses, and time wasted by technical help in remediating intrusion-related issues. There is also the inestimable cost of a system compromise due to the carelessness of just one employee—which affects not only the bottom line, but also a company's reputation and credibility among customers and partners alike.

How expensive is the perception among an organization's stakeholders that the business may be vulnerable to attack? What is the cost of lost business? Each week, it seems, news stories describe an endless series of network attacks on retailers in which sensitive customer data has been compromised. In response, embarrassed businesses are providing affected customers with free credit record monitoring services in an effort to protect them against identity theft. This is a bit like closing the barn door after the horse has escaped. Unfortunately, in most cases fines have yet to be imposed on the negligent businesses, but that pattern is expected to change.

There is little doubt that the cost of cybercrime has burgeoned in recent years and will continue to rise. According to Irida Xheneti, a research analyst for IDC's Security Services program, "The sophistication of the threat landscape, stringent regulatory mandates, the complex technology environment, and the potential impacts that security vulnerabilities present to corporations will force companies to invest heavily in IT security." Other voices echo this projection.

Regulation and responsibility

The Fair and Accurate Credit Transactions Act of 2003 (FACT Act) requires that a wide range of organizations - from banks and mortgage brokers, to telecom, gas and electric utilities, to automotive dealers - take serious steps to safeguard electronic transactions and credit information. The Red Flag rules, which must be implemented by May 2009 under the FACT Act, impose requirements on those

organizations to proactively monitor transactions in order to detect and prevent abuse.

The Gramm-Leach-Bliley Act (GLBA) of 1999, Sarbanes-Oxley Act (SOX) of 2002, Health Insurance Portability and Accountability Act (HIPAA) of 1996, Family Educational Right to Privacy Act (FERPA) of 1974 and the overarching Privacy Act of 1974 and subsequent amendments all impose privacy and protection requirements and most include penalties for non-compliance. To date, there has been no tendency to levy those penalties, although that pattern may change as security breaches continue to be publicized.

Gartner suggests that CIOs must manage IT risk as a business risk. Most security engineers, when performing risk analyses, use the seven OSI layers as a reference point for each link of the chain that needs protection.

For example, the application layer must have properly coded programs to prevent bugs from allowing unforeseen problems, such as exploits or faulty programs, to compromise a network. OSI provides the cornerstone for interoperability and communications decisions. This is why, when we are faced with information technology purchasing decisions, we evaluate the functionality a product will deliver in addition to the OSI layer in which it will operate. However, what is generally not taken into account on a conscious level - although they may be significant factors on the subconscious level - are the three additional OSI layers and the role they play in the IT decision-making process. By failing to be cognizant of these additional layers or, worse, ignoring them, we increase our risk of sub-optimal decision-making.

In its Special Report in April of 2008, CIO Magazine addressed these "hidden" layers of influence as they impact medical care inside California prisons. The problem? Substandard medical care kills one inmate every week - in large part due to the absence of medical records, inadequate medical data, and lack of access to online medical references.

The solution? Information technology was an integral part of a court-ordered prescription to ensure that prison doctors do no more harm.

The report concluded, however, that progress has been slow, and that "doing IT behind bars requires overcoming physical, political and cultural obstacles foreign to most CIOs." The hidden layers begin to be revealed!

OSI Layers 1-7 and their role in security

Before we investigate the additional OSI Layers 8, 9 and 10, let's examine two of the traditional layers of the Open Systems Interconnection model. Much has been written about the elements of each of these seven layers, and the SANS Institute has published an excellent article about applying the model to Information Security, including the relative merits of single-layer versus multi-layer security solutions at these layers.

Our security audits continue to confirm the existence of security issues in these layers and the importance of building security into each layer from the ground up. The following examples illustrate security gaps, encountered during our audits, in the lowest and highest layers of the basic model.

Layer 1 – physical

The door to the server room is propped open for convenience during maintenance work, when the requirement is that this door be closed and locked to restrict access to this secure space. Another example we've all been victims of is the hard disconnect caused by the network guy tripping over a critical cable.

Layer 7 – application

Your business is protected by a firewall that inspects the content of incoming packets. This firewall application must also be secured, by programmers observing software development life cycle best practices. A security gap or oversight may cost you \$1 to fix while you are writing code, but will cost \$100 to fix after a quality audit. And the cost of that security oversight will be immeasurable in the event of a future security breach.

Despite best practices applied in adding security to OSI Layers 1 through 7, the real devil is in Layers 8, 9 and 10, as we'll see.

Layer 8 – politics

The eighth layer of OSI becomes evident when technology meets a decision-making process that is not entirely in the hands of the users. When all previous layers have been addressed, compliance issues may remain in an organization due to political blocking, which is generally the result of executives or board members who do not fully comprehend the ramifications of the underlying decision or the technical issues in play. However, they are the final decision-making authority, and tend to cross-pollinate with other executives both within and outside the company. Following are some examples.

At one publicly-traded bank, a Gramm-Leach-Bliley Act (GLBA) compliance audit discovered severe breaches of compliance laws that ex-

posed the organization to attack as well as possible leakage of customer data. The incident was thoroughly documented, with remediation recommendations formulated and presented to the Director of IT, who agreed with the findings. However, the C-level executives were not convinced the problem warranted remediation because there had been no previous repercussions.

Two months later, the company was victimized by a successful Denial of Service (DoS) attack, which took their systems offline for two hours and cost an estimated \$1.2 million. The Board of Directors subsequently directed that the audit recommendations be implemented as soon as possible - a good decision - but the genie was out of the bottle and it took weeks for the negative media exposure to wane.

“Whenever PII (Personally Identifiable Information) is compromised, that can hurt customers in many ways...trash their credit reports, result in identity theft, or even physical crimes resulting from criminals having home addresses. Organizations entrusted with customer PII should take responsibility ... and err on the side of being overly cautious.” Rebecca Herold - Information Security and Privacy Expert.

In another example, a project team conducted an exhaustive evaluation of a software product to identify the “Must Haves” and “Want to Haves,” rank them, and narrow the search to three vendors. The team then evaluated the three vendors and ranked them as well. The lowest-ranked vendor provided the team with a product demonstration, during which the project team asked pointed and probing questions that should have resulted in elimination of that vendor. Unknown to the team, however, one of the vendor’s executives had a personal relationship with the executive to whom the project team reported. As happens frequently, discussions occurred above the team level to assure a decision in favor of that “preferred” vendor. Thus, while the project team comprehensively reviewed and evaluated the vendors and recommended a purchase decision in favor of the top-ranked vendor - justified by all the right evidence - the real decision was made at the next level and for reasons having little or nothing to do with OSI Layers 1 through 7. Instead, politics ruled this decision. As anticipated, the product chosen by the politically-motivated executive was

difficult to implement and never really met expectations. Later, when the user community began to identify implementation issues, the project team was blamed even though it was not the team who had made the ultimate call. Layer 8 - the political layer - had caused the decision to be redirected to a sub-optimal path.

Many employees of a certain private educational institution preferred short, easy to remember passwords, and because of their tenure had resisted changing their passwords. A password audit was performed to check for easily guessable passwords, and these particular passwords made the hit list. We suggested that the institution make users aware of their new complex password policy and establish a deadline for password expiration. To give the policy teeth, the IT team required approval from the president to ensure his support of policy enforcement - which they obtained. It was a small and modest beginning, to be sure, and stronger authentication methods would be preferable.

However, implementing the one policy improvement they were able to is an important step, and it won't be the last action the institution takes to strengthen its information security program.

In another case, a high-ranking executive allowed a visiting vendor friend to use an empty office and plug into the local network to catch up on her email between meetings. It turned out that the vendor's machine was infected.

Fortunately, the problem was detected quickly and the vendor was directed to remove her laptop from the network. The policy override that occurred at the political layer, however, created a security incident that could have had severe consequences had it not been detected so quickly. Later, a policy was approved - by the same executive - requiring visitors to acknowledge that they were not to connect laptops to the company network without approval and verification that their machine was up-to-date with all current patches. Other

companies have experienced similar security incidents and have implemented MAC address security on selected ports and in vulnerable areas such as conference rooms.

In another example, a small organization was permitted to share office space with a larger company, whose respective CEOs were friends. As an advance precaution, the larger firm implemented MAC address filtering on its network ports to prevent potential "cross-pollination" of malware from the smaller firm. This security precaution proved its value quickly, for the smaller company (which had no such filtering) had been infected by a visiting salesperson's computer. As a result, several of their computers had become infected and were being used in a spam bot network. Since they also had weak outbound firewall rules, the smaller firm was unwittingly spewing spam from its email addresses, which caused them to be blacklisted by various email filtering programs and unable to send even legitimate email from their addresses.

"Change is difficult. Change consumes time. Change requires investment. On the positive side, however, change can produce exciting new tools and applications. Change can jump-start new thinking. And if necessity is the mother of invention, change is the father." Michael Scheidell - CTO, SECNAP Network Security.

As a final example (although there are hundreds more), imagine a publicly-traded company whose CFO often takes home his laptop in order to work in the evening. Of course the laptop contains some of his company's financial data. Not unusual, and nothing to be concerned about, right? Not quite. As a C-level executive, he had invoked his executive privilege and obtained admin rights on his machine for his convenience in various job-related responsibilities.

One evening, he allowed his teenage son to use the laptop. The son installed peer-to-peer file-sharing software, thinking so little of the action that he never mentioned it to his father. Subsequently, the CFO was faced with the very real prospect that the company's financial information was able to be shared with others. The political layer allowed the CFO to override security policy and - because he works for a public company subject to Sarbanes-Oxley requirements - he could incur financial liability

for having overridden that policy in the event the information became compromised.

Layer 9 – the religion of technology

It may not occur as routinely as the experiences with OSI Layer 8 described above, but Layer 9 - what we call the religion of technology - can have as much impact or more. In this layer, the decision-making process makes a leap from objectivity and fact-based considerations to allow the selection of a specific supplier, almost as if the decision-maker was hard-coded to that supplier. Vendors such as Cisco, Citrix, Microsoft, SAP and others, through rich budgets and even richer marketing initiatives, have created an aura of entitlement that results in decisions being made to select their products based on faith. They are the first (and sometimes the only) to be considered and are the easiest to sell to C-level executives. After all, "No one ever got fired for buying IBM," as the axiom goes. No harm, no foul!

Faith-based decisions contributed to the wild-fire spread of Token Ring networking when Local Area Networks were first gaining traction. No doubt more than one project team was directed to evaluate LAN technologies and recommend the best option for the business - as long as it was Token Ring. Management was fanatical about IBM and they were not about to change their religion. However, time proved that the mainstream or most popular solution is not always the best answer. Eight years later Token Rings had been supplanted by Ethernet, but the religious layer had already done its work. We can only imagine what new and alternative technologies might have sprouted during that time, absent the powerful influence of nearly universal faith in a single vendor or product.

There are IT shops that employ only Microsoft servers, and those that only use Unix-based servers. And, yes, there are some sound economic reasons for standardizing on a particular platform or operating system. However, sometimes technology exists on one operating system that doesn't exist on another, or it may be less expensive in terms of labor or licensing to use one system over the other depending on the business functions to be supported. It is easy to become comfortable with the operating system we "grew up with" rather than one that objectively makes sense as a solution for the organization.

In the desktop world, discussions regarding MAC vs. PC often occur with religious fervor. In the beginning, the accepted religion was that Apple had an advantage over the PC in terms of security. With the passage of time, the balance has shifted somewhat, especially as significant vulnerabilities have made the news.

OEMs may encounter the religion of technology when installing their software on a particular hardware platform. Some IT shops are all Dell, others exclusively IBM, and often they are willing to pay more to maintain that consistency, with the reason often being that it is simply easier. However, we have seen organizations undergo conversions - becoming more tolerant of alternative hardware "religions" upon learning that their platform of choice would cost an additional 15 percent.

Layer 10 – economics

The final layer that is always a factor in a complete and compliant review, one way or another, is the operating budget. We're all familiar with examples.

The executive who finally understands the full range of security and privacy requirements that bear on the business, and accepts the various changes that will be necessary to bring processes and systems into compliance, but then balks at the costs associated with full compliance. The IT manager who has earmarked certain funds for a pet project and so sabotages the optimal business decision in favor of funding a sexier initiative.

It seems there is never enough budget to support full, proactive compliance. But money can always be found, somewhere, to repair compliance gaps when they become visible as the result of audits, security breaches, or worse. When those gaps occur, hindsight invariably tells us we should have spent the money on preventive measures, even if it was a larger investment than we had counted on. The results of compliance gaps can entail costs far beyond simple financial ones - although even those affect the bottom line eventually. Consider the impact of a worm or virus breaching your firewall and wreaking havoc in the user community, whether that consists of 20 employees or 20,000. Compare the cost of widespread employee downtime against the cost of the preventive measure that could have been implemented had an optimal purchase decision been made. Certainly, cost estimates may be and often are integrated into the purchase decision-making process in earlier layers. However, that doesn't preclude them from being considered later in a different light, such as the economic light cast in Layer 10.

Some security tests ask a question concerning the factor that has the most significant impact on security. Though you may be tempted to answer in terms of people, or policies, or some technological barrier, this can be a trick question - for the impact of economics on final security decision-making may outweigh other factors.

Consider the \$3.8 billion multinational corporation that allocates \$10,000 per year on security. What is wrong with spending less than one one-hundredth of a percent to protect your organization's information assets? Plenty! Or, there's the publicly-traded New York firm with \$142 million in annual sales that spends \$450,000 per year on director and officer insurance, but only \$15,000 to prevent unauthorized network intrusion. These numbers do not compare favorably with the rule of thumb for IT investment, which is generally based on the number of company employee workstations multiplied by \$200 per month. And the security investment should be 10 percent of the IT budget.

There was a clever cartoon circulating in the IT community a few years ago in which a CFO

sat behind a big desk, with an even bigger lighted sign mounted on the wall behind it. The sign flashed the word "No!" at the touch of a button. The CFO was sitting there anxiously awaiting his next visitor, so that he could have the satisfaction of flashing that big "No!" in answer to whatever funding they were requesting. Those organizations, and those CFOs, do exist - although the big lighted sign thankfully is pure metaphor. The more disturbing fact is that a request for funding may make complete sense for the organization, a business case may be well-constructed, and an expenditure may be perfectly timed to address a looming security need, but if there is no funding, none of that matters. This is Layer 10 - abandon hope all who enter here!

Consider the \$3.8 billion multinational corporation that allocates \$10,000 per year on security. What is wrong with spending less than one one-hundredth of a percent to protect your organization's information assets?

Keeping systems updated with patches, especially the recent spate of system band-aids, requires considerable effort. Yet, too often, companies will not invest in the labor or technology resources needed to apply the patches and thereby avoid the risk of a security incident. Then, one day, an infected machine is plugged into the network and the infection spreads like wildfire. Suddenly, the famed knee-jerk scramble is in full swing. Thousands and thousands of dollars are spent freely to react to a crisis that could have been prevented - had the upfront investment been approved for labor and technology resources.

One strategy for conquering a big "No!" obstacle like this is to tediously and relentlessly compile cost data until such a compelling, quantitative case for the expenditure is made that the CFO finds it increasingly difficult to refuse. Unfortunately, this takes time and persistence, but can ultimately pay off.

In South Florida, hurricanes are a fact of life—just as earthquakes are on the West Coast and tornados are in the Midwest. Yet there are companies who remain reluctant to pay for off-site hosting of critical servers and who have minimal battery-backup. In the South Florida

example, several years had gone by without the experience of a direct threat, and many firms had begun to "play the odds." Unfortunately, when severe storms did make landfall several years ago, some businesses were without power - and hence offline - for more than a week. Suddenly, the knee-jerk scramble was on, again. This time, IT VPs scrambled to locate a hosting facility anywhere, at any cost, transport their servers to the hosting facility, and try to get their systems up and running again. In the meantime, their web server and email servers were down and their websites dark. Customers had good reason to wonder if these businesses had blown away and weren't coming back.

Decisions to take calculated risks with network security programs can have similar consequences. For example, take the company that has a program in place, and decides that it provides an acceptable level of protection from unauthorized network intrusion. They go into deferred maintenance mode, saving money by avoiding upgrades and not investing in periodic audits of their systems and programs. When their system is hacked - as statistics indicate is more and more likely - customer data is compromised or stolen and

the horse is out of the barn. Too late, they close the barn door. Too late, they invest in system protection. But now there are additional costs, and they are costs that easily could have been avoided:

- Compensating victims for damages due to identity theft
- Purchasing credit monitoring service for affected customers for a year or more
- Creating expensive advertising and direct mail campaigns to counter the enormous toll of negative publicity
- Attempting to recover lost business.

The very real examples make headlines almost every week - from retailers and grocery stores, to high schools and universities, to government agencies. From the fake subpoena scam targeting C-level executives to the viruses that are pre-installed on some of today's hot gadgets. The creativity and persistence of hackers, phishers and spammers seem to have no limits.

Lessons learned

We have demonstrated the existence of three additional OSI layers in the information technology and security environment, which are often overlooked and undocumented. Real-life experiences have illustrated how those hidden layers can present obstacles to progress.

It is advantageous to be aware of all of the issues - including the non-technical - when developing a security project. This concept applies not just to hardware or programming, but to all project management. If political, religious or economic issues insert themselves into the mix, security architecture may be compromised and opportunities to implement improved technology may be lost.

Although the political, religious and economic layers of the OSI model wield considerable power in influencing security decisions, they can be effectively managed. Following are some tips.

Don't be the IT security expert who enters the room with all the right answers, a 700-page audit report, and a long list of shortcomings that need fixing and fast. Executive management really isn't willing to change anything.

(Remember, change is difficult, change consumes time, change requires investment.) IT security experts who stand their ground gain nothing. IT security experts who learn to leverage incremental progress - pushing for small changes a few at a time - ultimately will be much more effective in protecting their organizations.

Do your own due diligence when embarking on an IT security project. Are there relationships you should be aware of? Are there hardware, software or vendor biases you should be cognizant of? Is budget actually available? If not, what projects would have to be deferred in order to implement yours? Sometimes this type of research is as simple as asking for direction or guidance from an engaged executive. In other cases, conversations with colleagues who have been through similar experiences in attempting to effect change in their departments can provide insights into the biases or preferences of the decision-making executives in your company.

Do initiate a dialog up your management chain to begin "warming up" your audience and pre-marketing your main ideas or premises. Provide preliminary information or a few samples of findings to garner feedback in the early stages. This will enable you to make adjustments in your project description, audit scope, or final recommendations that will improve your chances for success. Communication is a vital component at all stages of a project.

Do begin building a solid business case for the security improvements that need to be made. Search the Internet for justification. The news is chock-full of detailed reports of identity theft, hacked systems, phishing scams, identity theft, hacked systems, phishing scams, identity theft, hacked systems, phishing scams - and the skyrocketing cost of these cyber crimes. Case studies can often be downloaded at no cost. Research is available from a variety of proven sources, and while the fully-detailed reports must be purchased, usually there are one or two compelling statistics or facts provided as part of the report marketing program. And don't forget to tap your vendors or consultants for assistance as well.

Don't become frustrated when the big "No!" sign keeps on flashing. To paraphrase the famous advice from Desiderata, "For all its sham, drudgery, and broken dreams, it is still a beautiful world. Be professional. Strive to be happy."

Finally, if you are a C-level executive who ultimately makes the decisions regarding information security, ask yourself if you have been guilty of being stuck in one of these treacherous OSI layers. Have you ever rejected a good proposal for political, religious, or economic reasons? Did that action result in a sub-optimal decision - one that was not necessarily in the best interest of the company, that didn't obtain all the bang for the buck it could have, or that eventually had to be re-thought in favor of a different course? We have all been guilty from time to time. The challenge is to keep an open mind, think outside the box, and try to make the right decisions for the right reasons. Empowering the talented professionals on your IT team to do their jobs is a good start.

Summary

Experience suggests, and strongly, that certain other factors affect information systems or security purchasing decisions, beyond the traditional seven layers of the OSI model. Most of us have seen evidence with our own eyes, whether as victims - such as the project team blindsided by the politics of a special vendor relationship - or as perpetrators, such as the executive team who has already made their decision but allows a process and recommendation to be completed for the record.

It is important to understand these factors and to be aware of the powerful influence they exert over information security decisions, even causing us to render sub-optimal decisions that are not in the best interests of our organizations. By considering the additional - and perhaps most influential - layers of the OSI model, CISOs, CIOs and IT professionals will afford themselves the best opportunity to make the right security decisions for the business, and thereby ensure optimal protection of their sensitive data.

Michael Scheidell is the President and CTO of SECNAP Network Security Corporation (www.secnap.com).

References

- www.gartner.com
- www.idc.com/research
- www.ftc.gov/opa/2007
- Hannaford Data Breach: An Inside Job? Linda McGlasson, Bank Info Security Newsletter (tinyurl.com/5usuak).
- Phishing Scam Targets Corporate Execs; Stefanie Hoffman, ChannelWeb (tinyurl.com/5tas9a).
- Can Technology Fix California Prison Health Care?; Kim Nash, CIO (tinyurl.com/6pps7x).
- FACT Act Identity Theft Red Flag Rules Alert; John Burnett, BankersOnline (tinyurl.com/5nlxoz).
- Consumer Alert: Phishing Attempts; Bank Info Security Agency Release (tinyurl.com/6hutlk).
- Student Accused of Hacking School District Database; Joel Marino, South Florida Sun-Sentinel.
- Phishing Scams, Frivolous Arguments Top the 2008 "Dirty Dozen" Tax Scams (tinyurl.com/22w928).
- Harvard Grad Students Hit in Computer Intrusion; Jaikumar Vijayan, InfoWorld (tinyurl.com/6d98g7).
- Some Viruses Come Pre-installed; Jordan Robertson, AP Technology Writer.
- FBI: Cyber Crime Causes Financial Pain for Many Businesses; Keith Regan, E-Commerce Times (tinyurl.com/5cjoq5).
- Applying the OSI Seven-Layer Model to Information Security; Damon Reed (tinyurl.com/6nnxdq)