(IN)SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 22 - September 2009

DIGITAL CERTIFICATES

THE NMAP PROJECT

TWITTER THREATS

CLOUD SECURITY

DATA RECOVERY

TABLE OF CONTENTS

Welcome to (IN)SECURE 22
the digital security magazine

Summer is nearly over and we're all getting back to our offices wondering how the holidays ended so quickly. To get you up and running with security insight, we bring you a collection of articles covering an assortment of themes, from cloud security to multi-enterprise application security.

For us, just like for many of you, the next several months are going to be filled with a multitude of events spread worldwide. We're going to cover BruCON in Belgium, RSA Conference in London and San Francisco, the Storage Expo in London, InfosecWorld in Orlando, just to name a few. If you'd like to arrange a meeting, bring us some products for review or just say hello, drop me a line.

Mirko Zorz
Editor in Chief

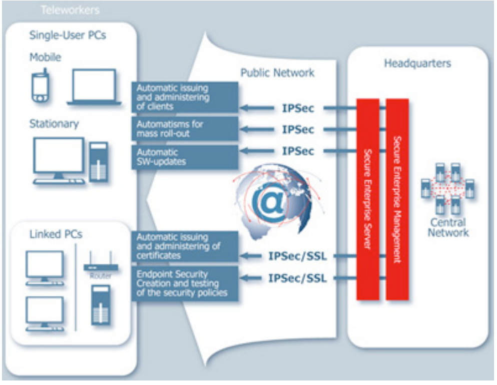
Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts

Feedback and contributions: Mirko Zorz, Editor in Chief - editor@insecuremag.com
News: Zeljka Zorz, News Editor - news.editor@insecuremag.com
Marketing: Berislav Kucan, Director of Marketing - marketing@insecuremag.com

Distribution

VPN management for Linux networks

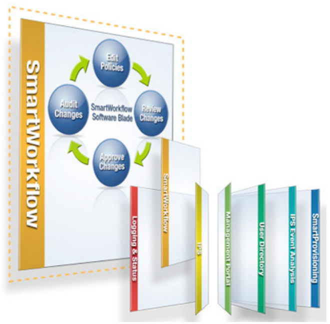

Teleworkers
Single-User PCs
Mobile
Stationary
Linked PCs
Router
Automatic issuing and administering of clients
Automatisms for mass roll-out
Automatic SW-updates
Automatic issuing and administering of certificates
Endpoint Security Creation and testing of the security policies
Public Network
IPSec
IPSec
IPSec
IPSec/SSL
IPSec/SSL
Headquarters
Secure Enterprise Server
Secure Enterprise Management
Central Network

NCP engineering released a new version of the software-based NCP Secure Enterprise Management System for Linux-based systems. Developed from the ground up to make hybrid IPSec / SSL networks powerful yet easy to manage, the system can plug-and-play with any existing network infrastructure or stand on its own as a new component. A single administrator is enabled full control over tens-of-thousands of secure connections, policy setting and enforcement, client updates, configurations and a host of other NAC management activities from one dashboard interface. (www.ncp-e.com)

The most physically and cryptographically secure USB flash drive

IronKey launched its S200 device for government and enterprise customers, featuring hardened physical security, the latest Cryptochip technology, active anti-malware and enhanced management capabilities. IronKey S200 is the first and only USB flash drive to meet the rigorous government security requirements of FIPS 140-2, Security Level 3. It comes with hardware-based AES 256-bit encryption in CBC mode and it features the secure management of encryption keys in an amper-resistant and tamper-evident rugged metal case. (www.ironkey.com)

SmartWorkflow: New security management software blade

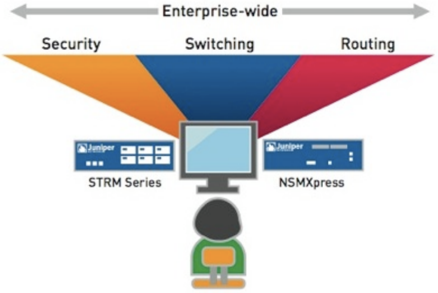


Check Point announced SmartWorkflow, a new security management software blade that provides customers the option of extending their security infrastructure with policy change management functionality.

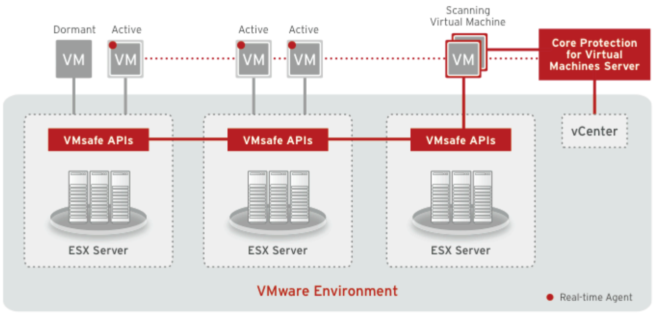
It enables an automated process of tracking, approving and auditing policy changes within the security management console, minimizing configuration errors and optimizing the integrity of network security. SmartWorkflow includes reporting and auditing capabilities that help customers ensure compliance with corporate policies and regulations. (www.checkpoint.com)

Juniper's adaptive threat management solutions for distributed enterprises

Juniper Networks Adaptive Threat Management Solutions, based on a dynamic security infrastructure, deliver security at scale that is identity aware and application aware, enabling consistent application delivery and performance across the distributed enterprise - including data center, campus, branch, remote and partner/extranet locations. (www.juniper.com)

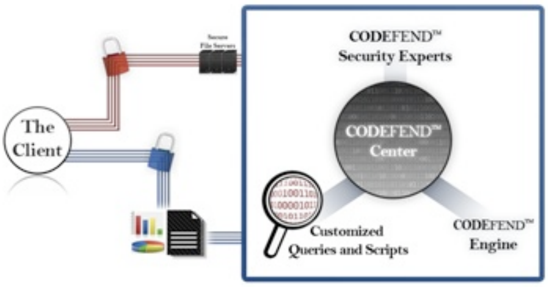


Trend Micro's protection for virtual machines



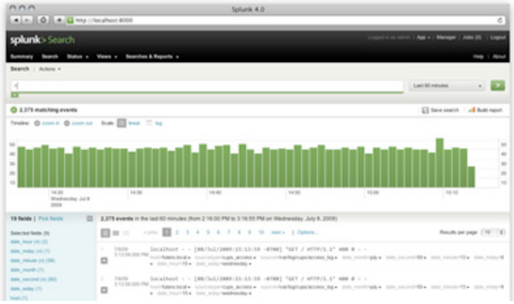
Trend Micro is expanding its virtualization security portfolio with a content security solution to protect VMware ESX/ESXi environments. Core Protection for Virtual Machines is designed to secure VMware virtual machines, both active and dormant. The product leverages the VMsafe APIs from VMware to offer layered protection through the use of dedicated scanning VMs coordinated with real-time agents within the VM. (www.trendmicro.com)

Security code review service for threat identification



Comsec Consulting launched CODEFEND, a new application security service which combines technology and expert human analysis, for Outsourced Security Code Review and Threat Identification. CODEFEND is an on-demand service allowing developers to securely send their non-compiled code to Comsec, where it is analysed for security vulnerabilities and threats. Fusing the latest generation of code analysis tools, customised rules and Comsec's proprietary methodologies, the service delivers more accurate reporting and identifies vulnerabilities not routinely picked up when using a "tool only" approach. (www.comsecglobal.com)

Splunk 4 supercharges IT search



Splunk 4 improves an organization's ability to manage, secure and audit their entire IT infrastructure. Re-architected and supercharged, Splunk 4 has infused IT search with speed and a customizable user interface. It offers users the ability to create custom dashboards for anyone in fewer than five clicks. The release also shatters the speed of previous releases with up to 10x faster search and 2x faster indexing, radically enhancing IT issue resolution times and incident investigations, giving users the power to index terabytes per day and search on massive amounts of IT data to deliver results in seconds on low-cost commodity server hardware. (bit.ly/17x8jx)

RSA SecurID software token for iPhone

RSA released the RSA SecurID Software Token for iPhone Devices that enables an iPhone to be used as an RSA SecurID authenticator, providing convenient and cost-effective two-factor authentication to enterprise applications and resources.

The app is now available on the App Store at no charge. The required RSA SecurID software token seed as well as RSA Authentication Manager - the software that powers the RSA SecurID system - are both available for purchase worldwide. (www.rsa.com)

Sourcefire and Qualys deliver real-time risk analysis

Sourcefire and Qualys announced that Sourcefire has become a Qualys Solution Partner and the companies have integrated the Sourcefire 3D System with QualysGuard. The combination of Sourcefire and Qualys enables organizations to reduce the number of actionable network threats by leveraging Sourcefire Defense Center to correlate threats detected by Sourcefire's intrusion prevention system (IPS) against host vulnerabilities identified by QualysGuard. (www.qualys.com)

Open source project to secure the Domain Name System

The OpenDNSSEC project announces the development of open source software that manages the security of domain names on the Internet. The project intends to drive adoption of Domain Name System Security Extensions (DNSSEC) to further enhance Internet security.

Industry leaders including .SE, NLNetLabs, Nominet, Kirei, SURFnet, SIDN and John Dickinson have come together to create open source software that promises to make it easier to deploy DNSSEC. The group's primary aim is to further protect the Internet by increasing the security for end-users. (www.opendnssec.org)

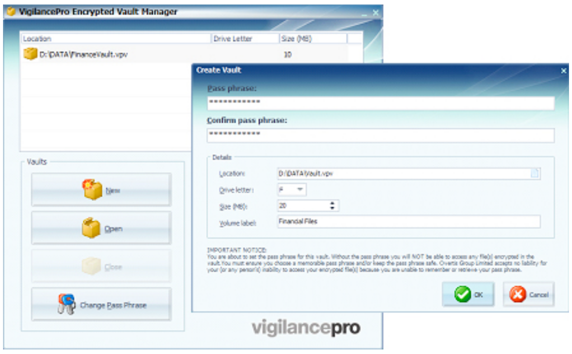
GFI MAX: Remote management and monitoring solution

GFI Software launched GFI MAX, a suite of remote management, monitoring and support tools for IT support organizations and MSPs worldwide.

Customers can use GFI MAX's real-time systems monitoring, automated daily health checks, asset tracking, patch management, own-brand client reporting and remote support solutions to build recurring revenues, drive down their operating costs and deliver best-of-breed IT support services. (www.gfi.com)

Virtual encrypted vaults for secure sharing

Overtis Systems launched the VigilancePro Encrypted Vault Manager (EVM), which provides means to encrypt, store and transmit data using virtual vaults. EVM also provides a way to share information securely on removable media, email and other means. EVM is also available as part of the full VigilancePro endpoint agent. When used as part of a full VigilancePro deployment all key management is handled centrally in line with ISO/IEC 11770 best practice. As a result, there is no need to enter passphrases when creating files. (www.overtis.com)



Location	Drive Letter	Size (MB)
D:\DATA\FinanceVault.vpv		10

Pass phrase: ***********

Confirm pass phrase: ***********

Details

Location: D:\DATA\Vault.vpv

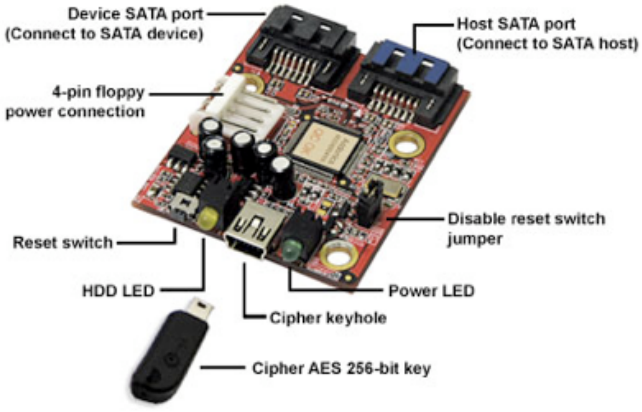
Drive letter: F

Size (MB): 20

Volume label: Financial Files

IMPORTANT NOTICE:
You are about to set the pass phrase for this vault. Without the pass phrase you will NOT be able to access any file(s) encrypted in the vault. You must ensure you choose a memorable pass phrase and/or keep the pass phrase safe. Overtis Group Limited accepts no liability for your (or any person's) inability to access your encrypted file(s) because you are unable to remember or retrieve your pass phrase.

Versatile hardware encryption for any computer

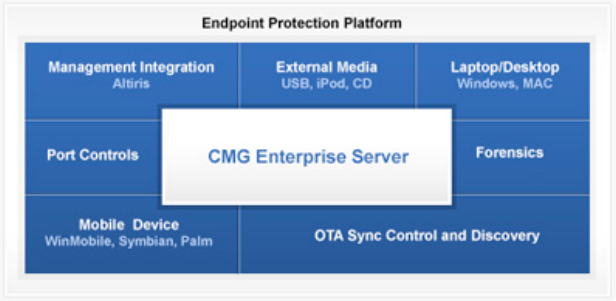


Addonics announced a 256-bit AES hardware full disk encryption solution for personal computers, servers, rack mounted systems, data storage equipment - basically, any computing equipment. CipherChain is a small module the size of a compact flash that can easily and quickly be installed into any system. Since it can be operated under any operating system, CipherChain is a security solution for organizations with legacy systems or in a heterogeneous computing environment. (www.addonics.com)

jCryption: Javascript HTML form encryption plugin

jCryption is a javascript HTML form encryption plugin, which encrypts the POST/GET-Data that will be sent when you submit a form. It uses the Multiple-precision and Barrett modular reduction libraries for the calculations and jQuery for the rest. Normally if you submit a form and you don't use SSL, your data will be sent in plain text. However, SSL is neither supported by every webhost nor it's easy to install/apply sometimes. With this plug-in you are able to encrypt your data fast and simple. jCryption uses the public-key algorithm of RSA for the encryption. (www.jcryption.org)

Mobile Guardian Enterprise Edition 6.5 for Mac released



CREDANT Technologies released Mobile Guardian Enterprise Edition (CMG EE 6.5), which includes full disk encryption and protection for Mac OS X. CMG EE v6.5 for Mac extends CREDANT's data protection to all Mac OS X environments including Mac OS X 10.4 Tiger and 10.5 Leopard Systems. The new edition requires no additional IT overhead beyond software deployment, and enables enterprises to secure their Mac environments with the same level of data protection that CREDANT provides for Windows workstations, handheld devices and removable media. (www.credant.com)

Mobile Guardian Enterprise Edition 6.5 for Mac released

CompTIA announced today an update to its certification CompTIA A+ with new content that reflects changing job requirements for tech support workers. Approximately 725,000 individuals around the world are CompTIA A+ certified. The updated version consists of two tests: CompTIA A+ Essentials (220-701) and CompTIA A+ Practical Applications (220-702). The new exams are now available worldwide. (www.comptia.org)

Portable smart card readers from SCM Microsystems

Smart cards are being used worldwide to secure identities in many applications, such as bank payment cards, employee access badges, government identity cards and healthcare IDs.

SCM Microsystems is expanding its smart card reader product family with three new models. The new handheld, USB or Near Field Communication connected readers are designed to be carried on key rings and used every day with contact or contactless smart cards, regardless of technology or manufacturer. In many instances, users insert the card and leave it in the reader - leaving them with a single small device for all smart card-related needs. (www.scmmicro.com)

New model of the BlackBerry Smart Card Reader

RIM unveiled a new model of the BlackBerry Smart Card Reader - a lightweight, wearable, ISO 7816 compliant card reader that enables proximity controlled access to a user's BlackBerry smartphone and computer.

The BlackBerry Smart Card Reader uses Bluetooth 2.0 technology with advanced AES-256 encryption to enable secure pairing and communications between the reader, the BlackBerry smartphone, the computer and PKI applications. (www.blackberry.com)

SanDisk Cruzer Enterprise enhanced for requirements of government employees

The SanDisk Cruzer Enterprise secure USB flash drives are now enhanced to meet the unique requirements of government employees. The Cruzer Enterprise design was independently tested and certified under Military Standard 810-F environmental standards in addition to being suitable for use by the visually-impaired under Section 508 requirements. Cruzer Enterprise drives feature industry-leading cryptographic modules and encryption algorithms, durable waterproof design, and are fully compliant with Trade Agreements Act (TAA) requirements for purposes of U.S. Government procurements. In addition, the Cruzer Enterprise line of flash drives is listed for Common Criteria certification, which it is expected to receive next month. (www.sandisk.com)

Freeware network discovery and IP address management tool

The Infoblox IPAM freeware application replaces manual processes, custom scripts, and spreadsheets with out-of-the-box automation and graphical tools for monitoring and managing IP devices and networks. The new, free VMware version of the Infoblox IP Address Manager module provides a graphical user interface, with a customizable dashboard, that consolidates and automates layers of traditionally manual IP address management tasks. (www.infoblox.com)

Wireless LAN security solution for remote wireless security testing

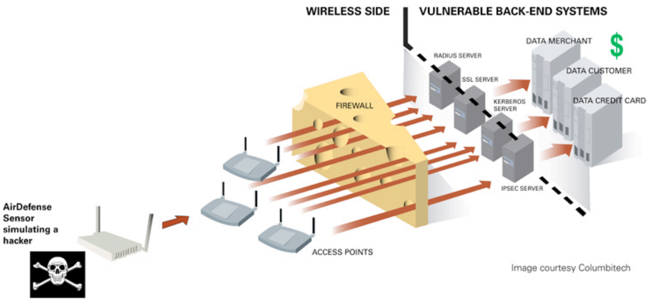


Image courtesy Columbitech

AirDefense simulating a hacker and running wireless scans against the network to identify network vulnerabilities

Motorola announced the AirDefense Wireless Vulnerability Assessment solution, a patented wireless security technology aimed at proactively assessing the security posture of wireless networks. The solution provides a completely new method to secure wireless networks against real-world threats by introducing active wireless testing capable of evaluating every deployed wireless access point. (www.airdefense.net)

Database security for Microsoft SQL Server

Sentrigo announced Hedgehog 3.0, which now supports Microsoft SQL Server 2008 running on Windows Server 2008, as well as SQL Server 2005 and SQL Server 2000 running on earlier Windows platforms.

Additionally, the virtual patching solution Hedgehog vPatch now includes dozens of additional protections specific to SQL Server. (www.sentrigo.com)

InfoWorld
2009
TECHNOLOGY
OF THE YEAR
AWARDS

Using real-time events to drive your network scans

by Ron Gula

Integrating the results from a vulnerability scanner into a higher order system such as a Security Information Management (SIM) tool, Network Based Anomaly Detection (NBAD), Network Access Control (NAC) or a Network Intrusion Detection System (NIDS) is commonplace on modern networks. Data from the vulnerability scanner can help populate asset tables and identify vulnerable targets. However, watching real-time events or trends in events over time provides much more insight from vulnerability scan data. This article describes some techniques to make your scanning program more effective by using information gathered from real-time systems.

Are you scanning the right targets?

Devices that monitor packets on your network such as a Network Intrusion Detection System, packet analyzers, firewalls and even proxy devices produce logs. These logs typically include reports about top IP addresses seen, all IP addresses seen, IP addresses that could be in the demilitarized zone (DMZ), IP addresses that connect to the Internet and so on.

It is a very good practice to compare this list of IP addresses obtained from a passive or logging device with the list allocated to the team running the vulnerability scanners. This list is extremely useful because it is very accurate and near real-time.

Security auditing teams that are provided lists of IP addresses to scan are often also provided routing tables, CIDR blocks, DNS domains information and so on. Network topologies and protocols can change over time and a security auditing team may have been made aware of these changes.

If you run a security auditing team and have been given a large IP address space, you may be conducting “quick” scans of this network. By “quick” I mean using simple detection techniques such as an ICMP or TCP pinging. Many vulnerability scanners can be configured to sacrifice accuracy for speed by just sending a few packets and then waiting for a response to see if a server or target is indeed active. I’ve seen many networks where devices such as routers, subnets, desktops were configured not to respond to these types of probes and were completely undiscovered by the auditing team’s scans.

Are you scanning the right ports?

There are two types of network vulnerability scans – those with credentials and those without. Credentialed scans login to the target system with a username and password to identify missing patches. Most vulnerability scanners support usernames and passwords for Unix and Windows servers. Some also support Kerberos, SSH public/private keys and other types of authentication. Uncredentialed scans must make a network connection to every port they wish to detect vulnerabilities on.

A common optimization when performing port scans is not to scan them all. There are more than 65,000 potential ports on any given host. If you consider there are both UDP and TCP ports, this number doubles.

Many vulnerability scanners can be configured to sacrifice accuracy for speed by just sending a few packets and then waiting for a response to see if a server or target is indeed active.

Most network scanners come with a “default” list of ports to target. These are typically related to the ports in a UNIX /etc/services file, or concentrated in the lower “0 through 1024” range. However, no list of ports to target is perfect and scanning all 65,000 ports can be time consuming and potentially cause network issues. If you have a scanner that can leverage credentials to perform a “netstat” style network scan, this means that you don’t need to put all of these probing packets on the wire.

Identifying an open port or a closed port is not difficult, but it is difficult to do it rapidly for thousands of hosts and thousands of ports.

Most NBAD solutions and network monitoring solutions have the ability to filter on certain types of network traffic and summarize the most common ports that are in use. Even SIMs that process logs from firewalls and NIDS can perform this type of task. The ability to summarize specific ports that are open on target networks is extremely useful. They are doing the hard work for you.

In some cases, you may have an NBAD sitting in front of an entire network spread across two Class Bs. It may identify 4000 unique ports in use on the network. Feeding this list to your scanner means that you don’t have to guess which ports to scan. The NBAD system can also report on more discrete parts of the network. This allows you to fine tune your scans for specific targets. For example, the list of ports for one of the Class Bs may be only 3000 ports and the other may be only 2500 unique ports.

The ability to tell your active scanner to only look at certain ports will dramatically reduce the amount of time it takes to perform a scan. There is one caveat however. NBADs, SIMs and NIDS only report on the traffic they see. For example, a Windows server with a vulnerable version of VNC may be serving as a backup to the Windows server that everyone is using and it won’t show up in the NBAD. This is not as bad as it sounds though. If you incorporated this sort of monitoring into your ongoing scanning process as soon as the unused devices started to have traffic to them, you will see the ports being used.

Use real-time events to scan things that changed

If your scanning solution and policy allows you to scan as often as you want, with credentials and with all checks enabled, you are already getting a lot of very good data. However, for many organizations that I speak with, continuous scans are expensive, they impact the network and the actual regulatory requirement driving the scans may dictate intervals of 30 days, 90 days or even more.

If you want to gain more security knowledge about your network, but you don't have the time, resources or permission to do a full scan every day, you can use your SIM, NIDS or NBAD to obtain a list of hosts that have changed.

Change detection can come in several forms

The simplest list is the detection of new IP addresses. A mature feature would be to identify truly new systems that have been added to the network as compared to identifying a laptop that has given up its DHCP (Domain Host Control Protocol) lease and obtained a new IP. Scanning these IP addresses lets you know what got added to the network. Consider performing a full scan of these devices because you don't know much about them, although a good SIM or NBAD may be able to fingerprint the device based on logs or network traffic.

Change can also come to an existing host in the form of new services. SIMs and NBADs and NIDS may have the ability to identify when a new port has been opened on a host, or generate an event when a firewall rule change is permitting traffic to a server that was not occurring before. Scanning these systems can help identify what the new service was.

Most SIMs can also detect internal changes. These types of changes include new software installation, applied software patches, configuration changes and new user accounts. Scanning these types of servers can help identify changes that have occurred and weakened security. For example, it's possible that applying some patches actually rolls back previous patch fixes and reintroduces security issues. However, most patches actually fix security issues and this type of rapid scanning can help you minimize exposure in your otherwise regular audit period.

Real-time security monitoring systems have a variety of methods they can use to monitor trust relationships.

Perform deeper scans on popular and trusted servers

Real-time security monitoring systems have a variety of methods they can use to monitor trust relationships. These can include analysis of NetFlow data, packet traces and system logs.

If you have limited time and resources for performing scans and you can obtain a list of these popular and trusted services, the ability to perform deeper audits of them can help maximize your overall auditing efforts.

Common services that everyone in an organization uses may include:

- Intranet data nodes such as trusted web sites, discussion portals, and Wikis
- Common mail servers
- Common file sharing servers
- Internally deployed chat servers and video conferencing.

The list in your organization depends on what type of network you have and what sort of applications your users have.

The point is to look deeper at the services that are being used by many people. For example, you may have identified twenty-five FTP servers that your scanner has identified as having "Anonymous FTP" access enabled. If you are using a SIM or NBAD, you may realize that four of the twenty-five FTP servers are directly connected to the Internet and three others account for 95% of the Internet traffic. Using credentials to perform patch audits, performing full port scans, or configuring your scan to perform a more "thorough" test mode would be more in order for these more important FTP servers.

Scan for policy violations

NBAD and NIDS solutions identify the use of popular P2P software such as Bit Torrent and potentially illegal or unauthorized Web or FTP servers. In some cases, identifying file sharing that could contain illegal copyrighted content is a political and legal problem for the network security staff.

As with our other examples, you need to have the resources to perform a full and thorough scan of your network that includes the identification of P2P and other file sharing applications and performing thorough scans on the list of potential abusers to have an accurate enumeration of potential abusers.

Network vulnerability scanners that identify P2P applications can often fingerprint the exact type of software being used, vulnerabilities associated with it, and in some cases, identify some of the files being explicitly shared. Some vulnerability scanners can even enumerate Web, FTP and Windows file sharing folders to identify the types of files being shared such as movies, songs, electronic books and images.

Scan compromised systems

If you are a NIDS, NBAD or SIM user, then you know that these products rarely directly identify a compromised system with 100% accuracy. Instead, they identify a series of events that may be against policy, are a statistical anomaly or evidence of attacks in progress.

Some NIDS and SIMs do incorporate the use of vulnerability data for enhanced correlation. The concept is to alert on IDS events that are inbound to services that have exploitable vulnerabilities. This type of correlation is often automated and leverages detection of the operating system or the specific vulnerability. For example, a scanner may identify that a specific vulnerability is present on a specific host and port. The SIM or NIDS then highlights IDS events related to this vulnerability that targets this host yet ignores or deemphasizes the same events going to non-vulnerable servers. If your SIM or NIDS is dependent on this type of vulnerability data and you can't perform a full scan as often as you'd like, consider using the techniques in this article.

However, if your SIM or NBAD has detected attacks, consider performing a vulnerability scan in the following situations:

- An increase in attacks of a certain type: If you can determine the type of vulnerability these exploits are attempting to take advantage of, scanning the hosts targeted by the attacks could identify a potential security issue.
- Systems that have been compromised: perform a vulnerability scan to identify high-risk security issues. Vulnerability scanners that support credentialed scanning can also identify backdoors and services installed by Trojan or viruses and well as changes made to system configuration files.

Regardless of the reason, the ability to perform a vulnerability scan of potentially compromised hosts can identify vulnerabilities that are present throughout your organization. This could provide political evidence of the need for more scanning or the need to patch certain services. In the case of a compromised server, the scan can also serve as initial forensic evidence for an investigation.

Conclusion

If you are resource constrained to a limited number of vulnerability scans you can perform or the thoroughness of the scans you perform, using data from an NBAD, SIM or NIDS can make your scanning more effective and efficient. Data obtained from these relevant scans can also be fed back into your security monitoring solutions to enhance the accuracy of their correlation and asset databases.

Ron Gula is the CEO of Tenable Network Security (www.tenablesecurity.com), which offers the Nessus vulnerability scanner and a wide variety of enterprise solutions for large scan vulnerability monitoring, continuous passive network monitoring and real-time log analysis for firewalls, NetFlow and many other sources. Mr. Gula also was the original author of the Dragon Intrusion Detecton System of Enterasys Networks.

Review: Data Locker

by Mark Woodstone

The fine folks at Origin Storage shipped us a review copy of their Data Locker security hard drive solution. This was one of the most talked about devices shown in this field at this year's Infosecurity Europe event held in London, so we decided to test it and feature it in this post-summer, "back to work" issue of (IN)SECURE Magazine.

Data Locker is a hard drive solution with a unique security twist - it features an LCD display used for PIN based authentication and, besides the hard drive, the enclosure contains a hardware based encryption chip.

This device is available in a couple of sizes and sports different types of encryption. The Pro version works with 128 bit AES encryption, while the Enterprise one uses the tougher-to-break 256 bit AES cipher. Depending on your storage needs, each of the flavors is available in 160GB, 320GB and 500GB versions. For the purpose of this article, I have been playing with the 160 GB Enterprise version.

Look and feel

I was pleasantly surpised when I saw that the Data Locker box doesn't contain a big, puffed up enclosure- its size is approximately 0.5 inches wider, longer and thicker than my iPhone. It's weight is about the double of an iPhone. As you can see from the accompanying product photos we shot, besides the rather impressive size and weight characteristics, the device is an aesthetically pleasing addition for your work environment.

It comes with a USB cable (mini to standard), with an additional Y cable that could be of use for some computers and USB hubs for extra energy. From my tests on different Mac and PC computers, one USB connection was just enough. For those that don't have luck with one or even two USB cables, there is a DC input slot that supports power adaptors. The last feature on the back side is something that is often disregarded with this type of smaller hard drives – the on/off switch. Including this switch is a good move - I dislike pulling USB

cables out of the computer or devices just to shut them down and plugging them back in to switch them on.

Now we are coming to the most interesting part - the LCD touch screen display. When the disc is powered on, the display starts-up and provides a simple menu. The touch screen works well and the keys are quite large so there shouldn't be any usage problems.

Just a little heads-up to users of iPhone and similar devices - you will need to press this LCD display a little bit harder than you are used to.

Setting up Data Locker

Data Locker's main task is providing a secure storage space for your personal files. It demands a secret PIN code and until you successfully authenticate, the disk can't mount and therefore doesn't "exist". The device comes preloaded with a default password of 000000. Accessing the menu is easy - just authenticate by punching in the default PIN and quickly tap the setup button. After you do that, you will get access to a couple of options:

Change PIN: When you're thinking of PINs, you are probably thinking of a sequence of 4 numeric characters. In Data Locker's case, the PIN must be at least 6 characters long and can take up to 18 numbers.

Change encrypt key: The drive contains data encrypted with your PIN code and the current encryption key. Changing the encryption key should be done when changing the owner of the disk, if you think formatting and changing the PIN is not enough. Modifying the encryption key instantly renders the current data on drive absolutely unusable.

Further customization

There is an additional menu option located on the bottom of the the setup screen. Hitting "other" will give you three possibilities you can toggle on and off:

Key tone: Every successful tap on the display generates a rather generic computer audio sound that confirms that something was done. It is turned on by default and if the sound becomes annoying, you can turn it off.

Self-destruct: If turned on, this option will destroy the data on the disk after nine unsucessfull login attempts. The anti brute force mechanism cannot be fooled into restarting after a couple of failed tries. The device remembers the attempts and after the ninth the decryption key is deleted and you can say bye-bye to your data. If this happens, you will need to reconnect the device to your computer and login with the password you previously used.

Random key-pad: Although it is hard to see what is happening on the LCD display if you don't have it right in front of you, this option is another security mechanism that works against those who would want to snoop on you. Every time you open the PIN code input form, the number position will be scrambled, so it will almost impossible to approximately position your PIN code. Also, this type of character scrambling would work pretty good against someone analyzing fingerprint marks to try to "hack" your device.

Data Locker usage

The entire process after the login can be described in just a couple of words - it acts just like a normal hard drive. After authorizing to the device, the drive mounts and you can use it for whatever purposes you had in mind.

When you want to remove the disk, or just lock it so no one can use it, you need to hit the appropriate button on the LCD display and voila'! The only consideration you should have is to always use "safely remove device" or "unmount" functions before locking the device. This is a healthy way of taking care of your data.

Data Locker is a multi-platform device - as it doesn't use any type of application for the cryptographic processes and it can be connected to any operating system. There is just one thing I need to mention and it is related to Mac OS X users. The Data Locker drive is NTFS formatted, so you won't be able to use it out of the box on your Mac computers. This is, of course, nothing specific to Data Locker, so you will have one of the usual two solutions: re-format the disk with FAT32 (or HFS+ if you will just share data on Macs) or install the NTFS-3G driver that provides NTFS read/write capabilities on non-Windows systems.

This being a hard drive review, you are probably expecting some benchmarking data. I recently read an article in an upscale IT magazine, in which it was said that the file transfer speeds for this disk are slower when compared to other robust hard drives. I guess they forgot that this is a security solution with a crypto operation, so it is expected to be slower than the regular drive.

FYI - transferring 1 GB file from my 2.4 GHZ Intel Core Duo iMac to Data Locker (NTFS) took 88 seconds, while the same procedure to another disk (XFS+) took 37 seconds. The difference is substantial, but like I said, from my point of view this is not a big issue.

By the way - what to do if your device gets into some kind of a rumble? When the LCD display ends up being smashed and if the hard drive is intact you should get yourself a new Data Locker enclosure and access to your data will be spot-on.

Final thoughts

Over the past couple of years I have evaluated a number of secure data storage devices, but this was the first time I crossed paths with a hard drive empowered by a PIN authorization mechanism. Built on an exceptional idea, the unit works very well and it is a tough and robust solution for keeping your data and backups highly secure.

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

RSA CONFERENCE EUROPE 2009

20-22 OCTOBER | HILTON LONDON METROPOLE | U.K.

GET ANSWERS TO THE CHALLENGES YOU FACE EVERY DAY

The most valuable three days of your year.

RSA® Conference Europe 2009 taking place from 20th - 22nd October at the Hilton London Metropole, is the de facto security forum for enterprise and technical security professionals.

- Choose from 70+ educational sessions
- Hear keynotes from industry thought leaders and guest speakers like Nick Leeson, rogue trader
- Meet with experts, peers and vendors
- Leave with critical insights that can help you in your everyday job

REGISTER BY 18TH SEPTEMBER AND SAVE £100

www.rsaconference.com/2009/europe/hn

Nick Leeson Photographer Sinead Lynch.

The Nmap project: Open source with style

by Mirko Zorz

When you think about celebrities, you probably think about actors and rock stars. Although definitely not as mainstream as movies and music, the information security world has its celebrities as well. They don't get followed around by the paparazzi, the 20-million dollar checks are just the stuff of their dreams and they don't usually go around dressed to kill, but we certainly have individuals that can be defined as security rock stars. One of those is Gordon Lyon aka Fyodor, the creator of Nmap, a free and open source utility for network exploration and security auditing.

Setting aside the big security events and the countless mentions in books and on the Internet, his software has the added distinction of being featured in major motion pictures such as The Matrix, Battle Royale and Die Hard 4. Not to mention that it's probably one of the most used tools in the software toolkit of every security professional out there.

Although it's being updated and refined on a regular basis, Nmap recently reached version 5 that brought a considerable number of fixes as well as principal improvements. When discussing the development of this big update, in a conversation with (IN)SECURE Fyodor said: "Our last major release was 4.50 in December 2007. But we've been working on some of the new 5.00 features even longer. For example, we started Ncat development 2005 and we finally feel that it is ready for production use."

Features

Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. Here are the top improvements in Nmap 5:

1. The new Ncat tool aims to be the Swiss Army Knife for data transfer, redirection, and debugging. A users' guide detailing security testing and network administration tasks with Ncat has been released.

2. The addition of the Ndiff scan comparison tool completes Nmap's growth into a whole suite of applications which work together to serve network administrators and security practitioners.

Ndiff makes it easy to automatically scan your network daily and report on any changes (systems coming up or going down or changes to the software services they are running). The other two tools now packaged with Nmap itself are Ncat and the much improved Zenmap GUI and results viewer.

3. Nmap performance has improved dramatically. Since the most commonly open ports have now been determined, Nmap now scans fewer ports by default while finding more open ports. Also, a fixed-rate scan engine has been added. Now you can bypass Nmap's congestion control algorithms and scan at exactly the rate (packets per second) you specify.

4. The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts to automate a wide variety of networking tasks. Those scripts are then executed in parallel with the speed and efficiency you expect from Nmap. All existing scripts have been improved, and 32 new ones added.

The Nmap Scripting Engine is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts to automate a wide variety of networking tasks.

While plenty of users still prefer to run Nmap strictly from the command line, things are changing. "Back in the days of the old Nmapfe GUI, I always used Nmap from the command line. It was just easier to use that way for me, and the GUI didn't really gain me much. In fact, back then, I always considered the Nmapfe GUI to be like training wheels for your bike. People new to Nmap used it to learn the tool and get rolling, but after a day or so of playing in the GUI, they'd move to the command line," said Ed Skoudis, the founder and Senior Security Consultant with InGuardians.

"But, with the release of the Zenmap, the latest GUI for Nmap, I'm rethinking this approach entirely. Sure, I still use Nmap from the command line for the vast majority of my work. It's just easy to kick off and script that way. But, I do find myself using the Zenmap GUI more for setting up scanning templates for clients and doing network visualization. So, back two years ago, 99% of my Nmap work was at the command line. Today, about 80% of my usage is at the command line, while the remaining 20% is in the Zenmap GUI," he added.

The development process

Some may think that Fyodor is the only person behind Nmap. This couldn't be farther from the truth as the project is a group effort with a myriad of contributors from all over the world. Coordinating such a sizable venture is far from easy.

"Organizing such a big project is difficult, but we manage by making extensive use of the Subversion revision control system, mailing lists, and chat meetings," said Fyodor. "Also, different people specialize in different parts of the code. For example, David Fifield basically runs Zenmap while Ron Bowes has been writing more NSE scripts than anyone lately. So we each have responsibilities for different subsystems."

Users are generally very satisfied with the pace new releases of Nmap see the light of day. Ed Skoudis commented: "Sometimes, I'm a bit overwhelmed at the relentless pace of Nmap updates. I also try to focus on full releases for my production work, rather than the beta releases which seem to come out every few days. For software stability and predictability, those full releases (not the betas) are the way to go."

The ultimate guide to Nmap

Besides working on the new release of Nmap, Fyodor also took the time to write an all-embracing book - "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning." (bit.ly/11NNXu)

From explaining port scanning basics for novices to detailing low-level packet crafting methods used by advanced hackers, this book suits all levels of security and networking professionals. It comes out at 468 pages and it's a no-brainer if you're serious about Nmap.

A look to the future

Since Nmap is one of those projects with a huge user-base and very dedicated developers, it's only natural for the community to constantly ask for new features and fixes. When talking about future versions, Fyodor noted: "We're already back at work developing new features and applications for the Nmap suite. These include a high speed network authentication cracker named Ncrack and a tool named Nping for exploring and troubleshooting networks by sending many types of raw packets and monitoring the responses. We're also expanding our Nmap Scripting Engine to inspect web servers more deeply and discover more vulnerabilities in them."

Every now and then, someone wonders if there will be a commercial edition of Nmap somewhere down the line. This is especially important for government agencies, some enterprises and certain military groups that are prohibited from running free software.

Every now and then, someone wonders if there will be a commercial edition of Nmap somewhere down the line. This is especially important for government agencies, some enterprises and certain military groups that are prohibited from running free software.

Some are not excited with the idea, others would embrace it. Andrew Knapp, an Analyst with CGI says: "Commercial tools, while often easier to use and with better technical support, require more red-tape when adding features that you may find useful for your own uses and environment that the vendor might not find as important to include. I would probably just go out and find other tools that were open source with the features I was looking for."

On the other hand, we have Ed Skoudis that has a different view of this hypothetical situation: "I'd certainly be open to a commercial version of Nmap, if it would provide me more or better support. I also think that a commercial Nmap would allow it to gain more use inside of organizations that are forced to pay for their software."

To make things official, when asked about this commercial possibility, Fyodor dispelled all myths for (IN)SECURE readers: "Nmap has been free and open source since I released it in 1997, and that isn't changing. The only companies who pay are those who can't comply with the GPL-based license and instead want to redistribute Nmap as part of their proprietary software or appliances." There you go - at least for the foreseeable future, Nmap will stay open source only, and Ed Skoudis added: "I think it is important, so that we can look under the hood and see how the tool does its work. Sometimes, when trying to glean a detailed understanding of how a given option actually functions, or to determine how a few different options may interwork in a way the documentation doesn't describe, it can be useful to review the code. Also, if there is a particular problem that causes Nmap or even a scan target to crash, having the ability to tweak the code is immensely helpful."

Mirko Zorz is the Editor in Chief of (IN)SECURE Magazine and Help Net Security.

Enterprise effectiveness of digital certificates: Are they ready for prime-time?

by Jim Peterson

Ever-expanding audit and regulatory requirements leave enterprise IT departments with increasing security compliance concerns. At the same time, budgets are decreasing as a result of current economic conditions. Security standards such as the Payment Card Industry Data Security Standard (PCI DSS) and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 focus on ensuring sensitive information is protected at all times, regardless of physical location. Increasing demands coupled with reduced resources strain IT departments, constantly requiring them to do more with less.

The combination of increased compliance requirements, reduced resources, and little tolerance for gaps in data security forces enterprises to adapt by rethinking their security strategies. As technology has evolved, needs have changed and risks have multiplied; approaches rejected in the past based on complexity or cost concerns must be reconsidered. While many rejected Public Key Infrastructure (PKI) in the past, the need for persistent, easy-to-use credentials for encryption and identification prompts a second look.

Mature security technologies (e.g., firewall, anti-virus, anti-spam) assure enterprises that their systems are safe from compromise. These systems reliably protect the standard data infrastructures of most organizations. With these trusted protections already in place, IT managers might consider themselves safe from most attacks aimed at any of the standard ports and protocols carrying and storing today's critical business information. In the face of new security challenges, such as the dramatic rise of insider threats and increased regulatory requirements, these protections alone are no longer enough. While many of these technologies provide continuous protection within the band they are designed to work, they cannot safeguard information wherever it is or wherever it goes.

Protecting sensitive data from threats both inside and outside the organization, throughout its lifecycle, is a difficult and daunting task. This task cannot be met fully by solutions routinely deployed. Reliable IT solutions of the past can be applied on an as-needed basis in an attempt to address new security requirements; however, this approach is costly and is not flexible enough to meet ever-expanding data protection needs.

SECURITY IS NOW MORE THAN JUST THE RESPONSIBILITY OF ENTERPRISE IT DEPARTMENTS

Consider, for example, just a few of the different ways in which a sensitive data file can be exchanged during a typical course of business. It can be delivered through email, using an email security solution that will protect it while in transit to its intended recipients.

Once opened at its destination it can no longer be protected by the email security solution. Alternately, that same file can be delivered using a portable storage device (e.g., CD, tape) that cannot be protected by the email security application. This potentially leaves the data at risk, unless additional solutions are in place for protecting portable media. How would that same data be protected if it must move to the cloud or if it is sent via Instant Message (IM)? Implementing numerous point solutions for each case may address individual problems today, but cannot address the problem as it evolves. They also cannot protect information pervasively as it moves beyond the reach of a given end-point solution. A security framework built on a series of point solutions leaves many opportunities for gaps that leave data vulnerable as it moves from point to point.

Further, security is now more than just the responsibility of enterprise IT departments; it has rightfully become the responsibility of everyone within an organization to ensure the sensitive data they work with is used appropriately.

Often times, IT does not know the nature of sensitive information used by trusted end-users. In fact, in most organizations, the majority of this sensitive information being exchanged both internally and externally should not be accessible by IT workers. IT must be reliable and diligent in providing appropriate tools and technologies, but they are not the appropriate resource for making critical decisions about protecting sensitive data. Consequently, IT must select and deploy flexible, comprehensive security solutions for their enterprises, and then appropriately train users on how and when to use them. Individual users must recognize the responsibility they hold for the data they work with. This approach to security will only be effective when the ability to apply protections is part of the users' standard workflows. User responsibility can be augmented by point solutions such as Data Loss Prevention (DLP), but cannot fully or effectively be replaced by them.

As this approach to data security expands to include all users within an organization as well as external parties with whom sensitive data is shared, the need for appropriate credentials for individual users becomes increasingly important. This need drives forward-thinking data security professionals to reconsider how digital certificates can meet this need. In an effort to combine a scalable data security solution with user accountability, organizations are adopting digital certificates and finding them effective. Certificates provide their users with the security credentials useful for both identification and data encryption.

Digital certificates are based on the concept of public/private key cryptography. This concept utilizes a mathematically related pair of keys. One key, the public key, is used when encrypting data which only the other key, the private key, can open. A digital certificate is issued by a trusted third party, a Certificate Authority (CA), that validates the identity of the holder of the private key. This provides a verifiable chain of trust behind each certificate.

A digital certificate provides a much more durable level of security than traditional methods such as password authentication or encryption systems. Passwords remain a familiar, but vulnerable means of protecting data due to the inherent difficulties of managing and using passwords. Password-based systems also pose a security risk due to on-going susceptibility to common password cracking methods such as brute-force or dictionary attacks that will reveal a password if the attacker is persistent.

Digital certificate technology has evolved over the past 20 years. It is now a stable and mature technology that has become an important security component embedded within many popular IT functions such as web browsers with SSL, Virtual Private Networks (VPNs), secure FTP, email, and many other systems widely used today. Given the increasing use of digital certificates for enterprise security, how do they measure up in their effectiveness for deployment within large scale individual security?

A forum at RSA Conference 2009 brought together technology experts and IT administrators for an informal peer discussion on how digital certificates are meeting industry security needs. This open discussion offered useful insight into the current state of the enterprise readiness of digital certificates from the perspective of those that are actually implementing them to solve real business issues.

PASSWORDS REMAIN A FAMILIAR, BUT VULNERABLE MEANS OF PROTECTING DATA

The specific needs of attendees for credentials ranged from security for corporate websites and portals to individual end-user credentials for securing email and unstructured data files. A critical goal shared by attendees was a need to effectively provision end-users with end-to-end data protection. Forum participants agreed that digital certificates offer the most viable option available for providing both identity verification and data privacy.

Few issues were raised with using digital certificates for web security or other embedded systems. Most attendees reported they can easily and routinely obtain and deploy SSL certificates sufficient for their organizations' needs. Forum participants voiced concerns of how effective the same technologies are when used for individual user credentials. These concerns aligned with three key topics of discussion:

- Misconceptions about PKI
- Usability of digital certificates
- Management & control of digital certificates.

Identifiable gaps in digital certificate technology leave barriers in the path of wider adoption. These gaps block the ability of IT to support and maintain secure systems and inhibit the ability of organizations to effectively elevate the responsibility for security beyond just the domain of IT.

Misconceptions about PKI

PKI is an acronym for Public Key Infrastructure, a method for issuing and managing verifiable digital certificates issued by a trusted Certificate Authority (CA). Despite both the maturity and stability of PKI, it is still routinely spoken of negatively and, as a result, enterprises often resist implementing a security strategy utilizing digital certificates. Stories of failed PKI projects, cost overruns, and lack of benefits have created a perception that key management is too difficult and too costly to implement. These perceptions are mostly based on experiences of early adopters of the technology that had only a few choices for obtaining certificates.

Implementation options for PKI today have expanded and largely mitigate the issues encountered by those early adopters. Organizations can now choose a certificate management solution that fits both their budget and their administrative needs. Available options range from internal PKI solutions purchased from any of the leading industry vendors to externally hosted services that can provide any quantity of certificates from just a few up to large numbers. Today, internal options for hosting PKI are now bundled with major enterprise operating platforms such as Windows and IBM System z. This option is suitable for larger organizations that need to issue many certificates and that prefer to manage their certificates within their internal IT group.

Choosing an external certificate source can reduce the administrative costs by removing the need to purchase and internally manage a PKI solution. This approach provides a good solution for organizations that plan to adopt certificates gradually through a pay-as-you go model and ensures certificates are associated with an established global trust source.

USERS HAVING CERTIFICATES MAY STILL OFTEN USE THEM INAPPROPRIATELY

Usability

To some, digital certificates are still considered too difficult to use and maintain within most organizations where technical complexity of any kind introduces costly end-user training concerns. Despite the advances in available options and improvements in setting up and maintaining a PKI as a certificate source, the end-user component - digital certificates – may still be viewed as an obstacle. Too many steps and administrative touchpoints with users still exist in the delivery, use, and exchange of certificates.

Opportunities for user error abound in both the enrollment and use of certificates in environments where there is user resistance to adopting a new technology - most users are comfortable with using a password for data privacy and protection, while a digital certificate is unfamiliar and is perceived as complicated. Forum panelists pointed out that one benefit offered by digital certificates is that they can be integrated more transparently into user workflows, removing the need to remember or retrieve a password. This transparency requires readily available access to both the public and private key pair of the certificate, as well as the public keys of other certificate users. Private keys may often be available only from a single system which restricts where a user may effectively use it for protecting information. Increasing availability of portable, hardened certificate storage options in the form of a smart card or smart token offer the promise to remove this restriction; however, interoperability with these devices remains limited to only a few applications today.

Public key access can be impeded by limited availability of hosted public key directories. This leaves users few options other than resorting to complex, technical key exchange steps. Alternate solutions offering the promise of simplifying the use of public/private keys through easily available identifiers (e.g., email address), unfortunately, fall short as a result of their inability to scale to meet the needs of a large and often widely dispersed population of internal and external users.

Management and control

Managing data security across disparate applications that integrate inconsistently, if at all, with centrally issued certificates, increases the cost and complexity of administration and can leave gaps in protection. Few applications make use of certificates today for end-user encryption or authentication (digital signing), yet data often moves between different applications and passes through many hands during normal use. This presents areas of risk as data moves between users and between cross-platform and cross-vendor applications possessing varying levels of certificate support. Applications that attempt to reduce perceived end-user complexity by “hiding” their use of digital certificates inside the application provide only limited data protection - protection that is lost as the data moves beyond the boundaries of that application.

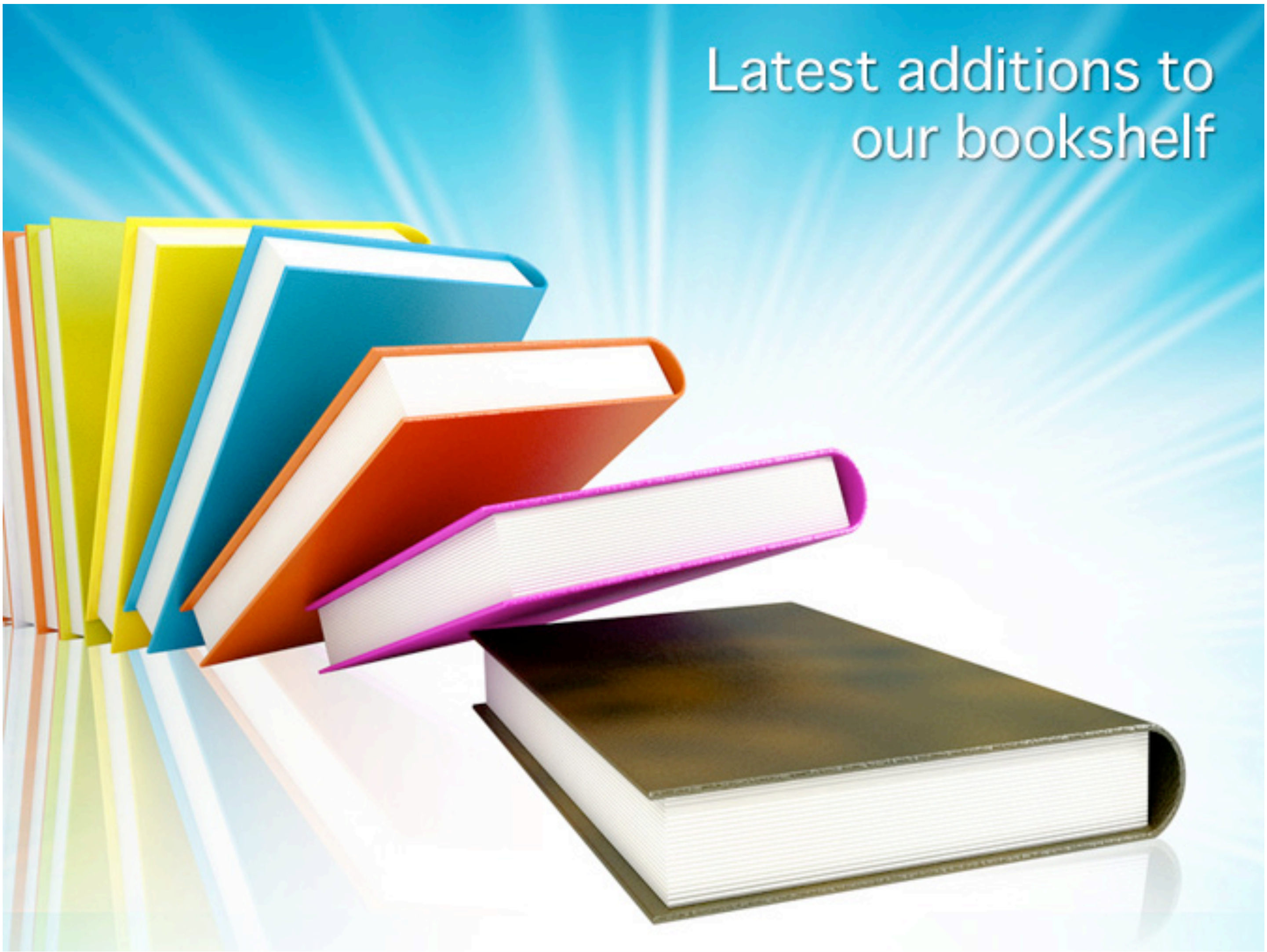
Users having certificates may still often use them inappropriately. Lack of policy support to ensure appropriate use and contingency access to encrypted data complicate audit and regulatory compliance efforts.

Finding an effective solution

Questions remain about how to effectively use digital certificates to ensure data is both secure and remains available to efficiently respond to business needs. More specifically, how can digital certificates be used without resorting to multiple vendor solutions with varying levels of certificate support? The answer is data-centric security.

Data-centric security always stays with the data, protecting it wherever it is, wherever it goes, and however it gets there. Applying security directly to the data reduces the need to rely on certificate solutions for each application, reducing the complexity and cost of using and managing digital certificates. Use of digital certificates with data-centric encryption applications does, indeed, confirm that digital certificates are an answer for enterprise security. Data-centric solutions that fit seamlessly into existing user workflows avoid certificate enrollment and management complexity; they ensure appropriate use through policy and provide the level of usability, management, and control necessary for making digital certificates an effective enterprise data security solution. A few solutions are now available that offer usable certificate solutions and control, making digital certificates ready for primetime.

Jim Peterson is the Chief Scientist at PKWARE (www.pkware.com). He has been developing commercial software products for over 20 years and has spoken on data security issues at a number of industry forums.

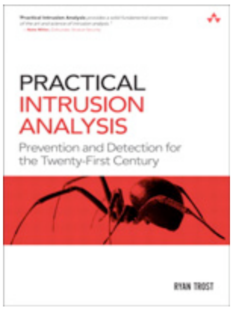


Latest additions to our bookshelf

Practical Intrusion Analysis

By Ryan Trost

Addison-Wesley Professional, ISBN: 0321591801

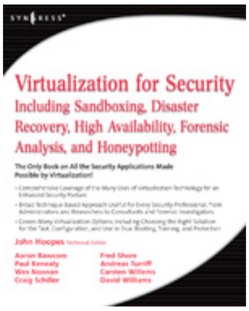


In Practical Intrusion Analysis, the author brings together innovations in intrusion detection and prevention for the first time and demonstrates how they can be used to analyze attacks, mitigate damage, and track attackers. He reviews the fundamental techniques and business drivers by analyzing today’s new vulnerabilities and attack vectors, and he presents complete explanations of powerful new IDS/IPS methodologies based on Network Behavioral Analysis (NBA), data visualization, geospatial analysis, and more.

Virtualization for Security

By John Hoopes

Syngress, ISBN: 1597493058


SYNGRESS
Virtualization for Security
Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis, and Honeypotting
The Only Book on All the Security Applications Made Possible by Virtualization!
John Hoopes Technical Editor
Aaron Bawcom
Paul Kenealy
Wes Noonan
Craig Schiller
Fred Shore
Andreas Turriff
Carsten Willems
David Williams

This title combines the most important uses of virtualization for enhanced security, including sandboxing, disaster recovery and high availability, forensic analysis, and honeypotting. It outlines covering tactics such as isolating a virtual environment on the desktop for application testing, creating virtualized storage solutions for immediate disaster recovery and high availability across a network, migrating physical systems to virtual systems for analysis, and creating complete virtual systems to entice hackers and expose potential threats to actual production systems.

Growing Software: Proven Strategies for Managing Software Engineers

By Louis Testa

No Starch Press, ISBN: 1593271832

Growing Software is a guide for technology leaders that gives advice on how to juggle the day-to-day challenges of running a software company while managing those long-term problems and making sure that your business continues to grow. With practical, hands-on advice, the book will teach you how to build and lead an effective team, define and sell your products, work with everyone from customers to CEOs, and ensure high-quality results. The author combines big-picture advice, specific solutions, and real-life anecdotes.

Security Monitoring

By Chris Fry, Martin Nystrom

O'Reilly Media, ISBN: 0596518161

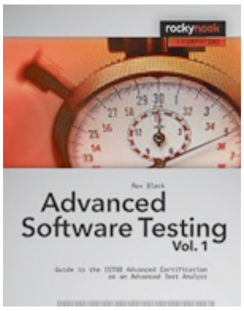
In this book, security experts from Cisco Systems demonstrate how to detect damaging security incidents on your global network--first by teaching you which assets you need to monitor closely, and then by helping you develop targeted strategies and pragmatic techniques to protect them.

It offers six steps to improve network monitoring, that will help you develop policies, know your network, select your targets, choose event sources, feed and tune and maintain dependable event sources.

Advanced Software Testing - Vol. 1: Guide to the ISTQB Advanced Certification as an Advanced Test Analyst

By Rex Black

Rocky Nook, ISBN: 1933952199

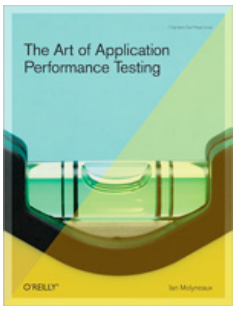


This book is written for the test analyst who wants to achieve advanced skills in test analysis, design, and execution. With a hands-on, exercise-rich approach, this book teaches you how to analyze the system, taking into account the user's quality expectations. You will learn how to evaluate system requirements as part of formal and informal reviews. You will be able to analyze, design, implement, and execute tests, and determine the appropriate effort and priority for tests. You will be taught how to report on testing progress and provide necessary evidence to support your evaluations.

The Art of Application Performance Testing

By Ian Molyneaux

O'Reilly Media, ISBN: 0596520662

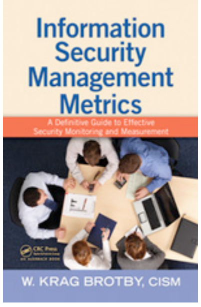


This title explains the complete life cycle of the testing process, and demonstrates best practices to help you plan, gain approval for, coordinate, and conduct performance tests on your applications. You'll learn to set realistic performance testing goals, implement an effective application performance testing strategy, interpret performance test results, cope with different application technologies and architectures, use automated performance testing tools, test traditional and web-based applications, and web services, recognize and resolves issues that are often overlooked in performance tests.

Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement

By W. Krag Brotby, CISM

Auerbach Publications, ISBN: 1420052853

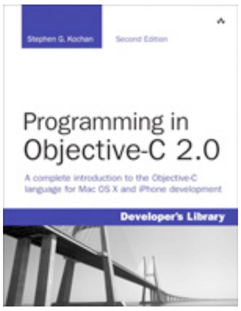


Information Security Management Metrics offers a step-by-step approach to developing and implementing relevant security metrics. With case studies and tools for monitoring specific items, this book offers practical guidance for implementing metrics across an entire organization, thereby improving budget and resource allocation, and reducing the possibility that unanticipated events will have catastrophic impacts. The book presents metrics that complement those used by IT managers, and demonstrates how to make adjustments to metrics without interrupting business processes.

Programming in Objective-C 2.0 (2nd Edition)

By Stephen Kochan

Addison-Wesley Professional, ISBN: 0321566157

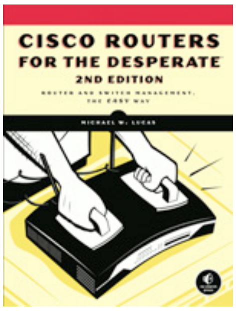


This title provides the new programmer a complete, step-by-step introduction to the Objective-C language. The book does not assume previous experience with either C or object-oriented programming languages, and it includes many detailed, practical examples of how to put Objective-C to use in your everyday programming needs. The second edition of this book has been updated and expanded to cover Objective-C 2.0. It shows how to take advantage of the Foundation framework's rich built-in library of classes and how to use the iPhone SDK to develop programs.

Cisco Routers for the Desperate, 2nd Edition

By Michael Lucas

No Starch Press, ISBN: 1593270496

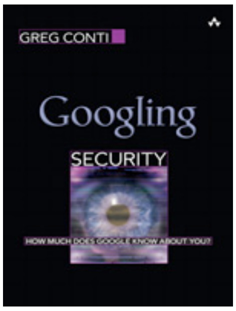


Just like the original, this second edition of the highly acclaimed Cisco Routers for the Desperate is written for the administrator in crisis mode. Updated to cover switches and the latest Cisco terminology, with a tighter focus on the needs of the small network administrator, this second edition covers installation, troubleshooting routers and switches, security concerns, and how to implement basic network redundancy to reduce the risk of network downtime. Cisco Routers for the Desperate, 2nd Edition is designed to be read once and left alone until something breaks. When it does, you'll have everything you need to know in one easy-to-follow guidebook.

Googling Security: How Much Does Google Know About You?

By Greg Conti

Addison-Wesley Professional, ISBN: 0321518667

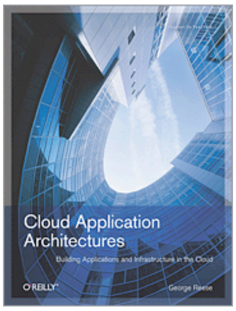


Googling Security is the first book to reveal how Google's vast information stockpiles could be used against you or your business, and what you can do to protect yourself. Unlike other books on Google hacking, this book covers information you disclose when using all of Google's top applications: Gmail, Google Maps, Google Talk, Google Groups, Google Alerts, Google's new mobile applications, and more. He shows how Google's databases can be used by others with bad intent, even if Google succeeds in its pledge of "don't be evil."

Cloud Application Architectures

By George Reese

O'Reilly Media, ISBN: 0596156367

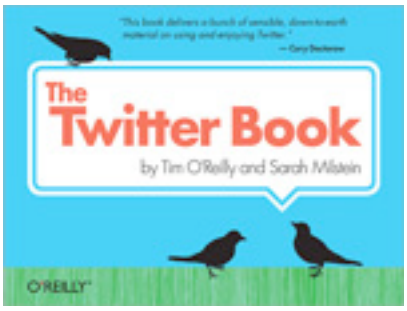


If you're involved in planning IT infrastructure as a network or system architect, system administrator, or developer, this book will help you adapt your skills to work with these highly scalable, highly redundant infrastructure services. With this book you will understand the differences between traditional deployment and cloud computing, determine whether moving existing applications to the cloud makes technical and business sense, analyze and compare the long-term costs of cloud services, traditional hosting, and owning dedicated servers, earn how to build a transactional web application for the cloud or migrate one to it, and hange your perspective on application scaling.

The Twitter Book

By Tim O'Reilly, Sarah Milstein

O'Reilly Media, ISBN: 0596802811

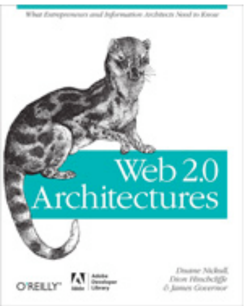


This practical guide will teach you everything you need to know to quickly become a Twitter power user. It includes information on the latest third party applications, strategies and tactics for using Twitter's 140-character messages as a serious - and effective - way to boost your business, as well as how to turn Twitter into your personal newspaper, tracking breaking news and learning what matters to you and your friends. The book consists of clear explanations and examples of best practices.

Web 2.0 Architectures

By Tim O'Reilly, Sarah Milstein

O'Reilly Media, ISBN: 0596802811



This book finally puts substance behind the phenomenon by identifying the core patterns of Web 2.0, and by introducing an abstract model and reference architecture to help you take advantage of them. The authors examine what makes services such as Google AdSense, Flickr, BitTorrent, MySpace, Facebook, and Wikipedia tick. This book reveals how the classic client-server model has evolved into a more detailed Web 2.0 model and talks about Web 2.0 reference architecture and the specific patterns of Web 2.0.

Regular Expressions Cookbook

By Jan Goyvaerts, Steven Levithan

O'Reilly Media, ISBN: 0596520689

This book provides help for programmers on how to use regular expressions to manipulate text and crunch data. With recipes for programming languages such as C#, Java, JavaScript, Perl, PHP, Python, Ruby, and VB.NET, this book offers step-by-step solutions to scores of common tasks involving regular expressions. This cookbook will help you understand the basics of regular expressions, learn how to validate and format input, find solutions for using regular expressions in URLs, paths, markup, and data exchange, learn the nuances of more advanced regex features, and write better regular expressions for custom needs.

HACKING FOR B33R

BRUCON

BRUSSELS
18-19 SEPTEMBER 2009
WWW.BRUCON.ORG

SECURITY AND HACKER CONFERENCE

BRUSSELS, 18-19 SEPTEMBER 2009

WWW.BRUCON.ORG

BruCON is an annual two-day security and hacker conference offering lectures and workshops on a multitude of topics about computer security, privacy, information technology and its implications on society.

Come and join us for 2 days of exploring: privacy, web2.0 security, cloud computing, kiosk security, cyberwarfare, application security, social engineering, IPv6 vulnerabilities, RFID, VOIP, MPLS hacking, identity theft, dissecting botnets, hackerspaces and much much more.

In addition to a first class speaker track, we will provide workshops on VOIP, RFID, wireless security, lockpicking and physical security. Meet us in Brussels on 18 & 19 September.

Sponsors

belgacom

together with proximus telindus

DIMENSION DATA

ERNST & YOUNG
Quality In Everything We Do

f5

Media Partners

Hakin9

(IN)SECURE
www.insecuremag.com

HACK.LU 09
Open convention in computer security
28-30 October

HELP NET SECURITY
WWW.NET-SECURITY.ORG

A look at geolocation, URL shortening and top Twitter threats

by Fred Touchette

On a daily basis, online spammers and hackers are hard at work conjuring up crafty ways to compromise unsuspecting PC users. E-mail inboxes and social networking sites are two popular attack targets. This article looks at a selection of nefarious Internet activity that has made recent headlines, including geolocation and URL shortening e-mail attacks, along with emerging threats plaguing sites like Twitter. In each case discussed below, you will notice that the techniques used by scammers are actually simple by design, but are quite effective and can often have damaging effects.

Geolocation

In recent months, a malware variant known as Waledac has resurfaced. Believed to be a reincarnation of the infamous Storm Worm, the Waledac worm is embedded in an e-mail attachment and spreads using the infected computer's e-mailing networks. Waledac has generated several spam campaigns in 2009 - a number of which have featured a technique called geolocation.

Geolocation, also known as IP geolocation, is relatively simple. When in action, it looks at the IP address of a person visiting a Web page and cross references that IP address against a database that tells it exactly where the IP address is assigned. The result is a Web page that appears to be customized for you. This is similar to the frequently seen banner ads promoting dating sites, such as "Hot Singles in Kalamazoo are waiting for you," or something along those lines where "Kalamazoo" would obviously be your city of residence. By utilizing a visitor's IP address when they arrive at Waledac's target sites, the information can be customized to appear to be local to the visitor.

However, Waledac attacks do not usually wait for the user to download the malicious executable on his or her own. Oftentimes, a hidden iframe on the landing page will begin the download without the need to click any of the links. These domains are always on the same fast flux type of networks that this group has been using since the early days of Waledac, back when it was known as Storm.

Although there is no exact science to the timing of Waledac appearances, we have come to expect visits during major holidays based on previous incidents. One example of such a strike occurred during the last week of February 2009. A short e-mail barraged inboxes with a link to the "Couponizer" Web site.

In a feigned attempt to soften the economic blow, the "Couponizer" appeared to offer a slew of coupons for deals relevant to the recipient's locale. One subject line read, "I hope it will be useful for you," which directed readers to the malicious Web site. Each link on the page, however (which was really just one big link appearing to be many), led to the file download, "sale.exe." Interestingly, it was not necessary to actually download the file since a hidden iframe - as previously mentioned - pulled malicious binaries from another source, a fast flux site with the name chatloveonline.com.

Similarly, the March 2009 St. Patrick's Day spam campaign featured an attack that personalized its messages with recipients' locales utilizing geolocation. In this case, Waledac wanted its victims to believe that a terror attack had just occurred in their home town. The attack included a fake news story, supposedly from Reuters, that claimed, "At least 12 people have been killed and more than 40 wounded in a bomb blast near market in [insert your town here]." Directly below the Reuters story appeared a video claiming to contain footage of the reported devastation, which, in true spammer fashion, you were told to download the latest version of Flash in order to view it. Instead of Flash, however, a file named Run.exe (malicious payload) was downloaded.

Though geolocation is not a difficult task to implement, it is a new and effective touch for Waledac. It would not be a stretch of the imagination to assume Waledac, or any other botnet, may bring this highly effective social engineering tactic back when we are more than sure to see new malware campaigns attempting to get the better of us.

ONE CAMPAIGN UTILIZING THIS TECHNIQUE CAME IN WITH A BANG IN JUNE 2009, ARRIVING AT NEARLY 10,000 PIECES PER MINUTE WITH AROUND 18 MILLION PIECES CAUGHT IN APPRIVER FILTERS

URL shortening

A second effective spammer technique involves URL shortening, which essentially exchanges an original URL for a shorter version. URL shortening is free through services such as ShortURL, TinyURL or Bit.ly, to name a few. When someone clicks on the short URL, the Web site looks up the longer URL and redirects the user to the actual destination.

One campaign utilizing this technique came in with a bang in June 2009, arriving at nearly 10,000 pieces per minute with around 18 million pieces caught in AppRiver filters. The attack began as a plain text e-mail promising a financial way out of the current recession and displayed itself in two forms. In one form, it presented a link to a news article supposedly from "The Business News," and in the other form, it showed "proof" of its authenticity from a concerned friend.

In both forms, the e-mails used URL shortening services to provide a unique hyperlink to the Web-based story. The obfuscated links, by means of the shortening services, made it near impossible to block these spam e-mails based on the links themselves. In this way, spammers could keep the landing site on fewer servers and simply mask the redirection to them, thereby decreasing their workload and need for unique Web addresses.

In the example mentioned above, when the user follows the short URL, they arrive at a Web page that appears to be a news story titled "Jobs: Is Working Online At Home The Next Gold Rush?" Not only does the story sound compelling, but the fact that the page is arranged in the same manner that other reputable news sites are arranged in also gives it an air of legitimacy.

To illustrate the appearance of a reputable site, this particular campaign included a slew of supposed reader comments at the end of the article. Some sang the praises of the work-from-home system, while some provided slightly skeptical views, done to undoubtedly keep up the image of legitimacy. However, a look at the source code shows that these comments were written directly to the page and avatars were stolen from comment sections of various reputable Web sites, including the New York Times.

Another feature that helps with the legitimacy aspect is the use of geolocation in order to customize the story and site to appear to be local, making it more appealing to the reader. The article in this example discusses the success of a woman named Mary Steadman, who just happens to be from the same town as that of the reader (thank you, geolocation).

This is seen several times throughout the story, including the title of the publication, which is the [insert your state name here] Catholic Business Edition. The story continues to tell you how Mary "gets rich quick" using Easy Google Profit to post links on various Web sites, which most likely will aid the scammer later through Search Engine Optimization (SEO).

ALTHOUGH SHORTENED URLS WERE MADE POPULAR BY TWITTER'S 140-CHARACTER LIMIT, SPAMMERS HAVE TAKEN ADVANTAGE OF THIS SIMPLE TECHNIQUE TO POSE MORE DANGERS TO THE UNSUSPECTING

Although shortened URLs were made popular by Twitter's 140-character limit, spammers have taken advantage of this simple technique to pose more dangers to the unsuspecting. One danger associated with URL shortening is that users are blinded to the actual URL they are about to visit, since they click on an unknown link, which may contain a malware download, phishing sites or other spam-related material.

Since the proliferation of Twitter, where shortened links are commonplace, caution seems to have gone by the wayside, and often times, even the savviest users are too trusting and they click on shortened URLs without hesitation. Scammers capitalize on this fact, leading us to the second danger of shortened URLs: bypassing spam filters.

By shortening the URLs, scammers can bypass spam filters because the actual domain is not sent via e-mail. As a result, the malicious link is more likely to evade some filters. Currently, there are high volumes of spam utilizing many different URL shortening services.

Finally, and something worth noting, shortening services are typically free, do not check the link or utilize any CAPTCHA technology to prevent abuse. Such ease of access allows cybercriminals to conveniently utilize automation built-in by spammers, thereby allowing them to abuse the service with efficiency.

Twitter

In this final section, we will delve further into the topic of Twitter security as the craze surrounding this micro-blogging site continues to grow. 140-character "tweets" provide a unique way to share information and an innovative way for spammers, scammers and hackers to once again trick the unsuspecting user.

Recently, Twitter has faced scrutiny for lack of security, mostly surrounding password security. Not too long ago, a hacker made his way into a Twitter employee's Yahoo account by guessing the user's security question, and shortly before that, another Twitter employee's administrator account password was hacked because he used the simple dictionary word "happiness." This was followed with blog posts about the conquest, along with screenshots, showing that the hacker gained administrator access to such celebrity accounts as Aplusk (aka Ashton Kutcher), Barack Obama, Britney Spears, et al. All of this led to a media lashing about Twitter's inability, or lack of concern for network security. In reality, weak passwords and easily avoidable security flaws are frequently the result of lack of education on behalf of the user.

Placing controls in a business is becoming increasingly important, not only because of the latest federal mandates within a number of industries, but also because malware, spyware and other malicious online schemes continue to prove they are on the rise.

Today, innovative, multi-vector techniques are attempted on virtually everyone connected to the Internet, and employees who fall victim to these scams are frequently uneducated when it comes to Internet security protocol. This is why short URLs pose such a strong security risk; employees will click what appears to be a harmless link, e-mail or Web site, which can infect their machines and possibly harm the entire organization.

This leads to one key aspect to every network's security: education. To use a popular cliché, a network is only as strong as its weakest link. And when that weakest link is in charge of holding onto key financial or other sensitive information, as was the case with Twitter, it becomes of utmost importance that each person on the network understands best practices and current threats to prevent stolen or leaking data.

One such best practice that all companies should highlight is the importance of password security. The first step to create a secure password is to think about the length. For each character or symbol that is added, the security of that password rises exponentially. One piece of advice to abide by is to avoid creating a password with less than seven characters.

A second piece of advice is to have the password appear as nothing more than a random string of characters to someone else that may see it. By using a variety of lower and upper case letters, numbers and punctuation from all over the keyboard, is a unique way to enhance security. One thing to keep in mind, however, is to avoid sequential or repeating instances.

One good method in creating passwords is to use look-alike characters in substitution for other letters in your password, such as @ for 'a', $ for 's', 1 for 'I', zeroes for 'o', or the like. However, there is a risk when only using this technique in an attempt to obfuscate your password, as many password guesser programs are well equipped to be aware of these rather simple substitutions and may try to replace the symbols with letters themselves.

A good trick is a nice long acronym or partial words from a phrase to throw off any sort of dictionary-based attack. For example, take a nice long sentence that will be easily remembered, such as "I hate making up new passwords," and turn it into "!h8MunP@$s."

Another strong password usage habit is to never use the same password twice. It seems almost logical to avoid using the same password for a banking account and a MySpace or Facebook account. However, this is a strong point to make. If passwords are repeated, hacking in to one account can leave all other accounts with the same information (username, etc.) vulnerable. Although it is near impossible to make anything 100 percent secure, by utilizing multi-layered security practices, beginning with a password, it makes it much harder for anyone to get a hold of private data and information.

Conclusion

The need for general network security is consistently illustrated, especially as the latest threats continue to find their way in to disrupt a network. Geolocation, URL shortening, social networking sites and even micro-blogging sites, such as Twitter, all help to create a sense of personal connection and a false sense of trust for the potential target, making these simple techniques extremely effective.

Fred Touchette is a Senior Security Analyst at AppRiver (www.appriver.com) where he is primarily responsible for evaluating security controls and identifying potential risks. He provides advice, research support, project management services, and information security expertise to assist in designing security solutions for new and existing applications. Touchette holds several technical certifications, including COMP-TIA Security+ and GREM - GIAC Reverse Engineering Malware through the SANS initiative.

How "fake stuff" can make you more secure

by L. Brent Huston

Have you ever left the light, radio or TV on when you left home? The idea is usually that would-be burglars would see the lights or hear the noise, assume someone was there and move on to less dangerous targets. Over the ages, we humans have become very well versed at feeding our foes false stimuli, using trickery and deceit as a defensive technique. In the information age, little has changed, other than the medium. This remains a highly effective tool for adding to the security of an organization.

Using honeypot techniques in the corporate IT world has some challenges, but done properly, the capabilities are simply amazing. Honeypots have been around in the IT world for quite some time.

The Honeynet Project, probably the most significant work in the field, was founded in 1999. While their work is primarily focused on high interaction, academic study of attacker techniques by offering target systems and network environments up for exploitation, their implementations likely require more than most corporate organizations can manage in time, effort, forensic analysis and capability.

However, by simplifying honeypot technologies away from a systemic approach to emulation of specific services we can begin to pare down the requirements to a more manageable level.

Further, by refining the idea of what data the honeypot should gather from the deeply academic to the more focused “get what a corporate IT person needs” we can easily extend the idea of a “low interaction” honeypot into the corporate IT environment.

The underlying principle is easy to understand. If something is fake, then there is essentially no reason why anyone should interact with it. If we emulate a fake web server, for example, no legitimate users of the network should ever use it, since it holds no real data or significance for them.

Thus, any interaction with a fake service (hereafter referred to as a pseudo-service) is suspicious at best and malicious at worst. That means that from a detective standpoint, if you treat all connections to a pseudo-service as suspicious and investigate them as a potential security incident, they are actually helping you be more secure, even though they are “fake”.

Pseudo-services, and other low interaction honeypot technologies, can provide you with visibility into the security posture of your environment. They are very effective at capturing the details of attackers who might be performing reconnaissance against your systems.

They have proven to be capable of detecting human attackers probing for vulnerabilities and malware seeking to spread from system to system inside a network. Pseudo-services simply wait for interaction, after which they capture the essentials that are important to the corporate IT security team, such as source IP addresses and the frequency of the connections. Additionally, since they are able to log all commands and transactions, they often offer deeper insights into the intent and capability of the attacker or malware infection, allowing the security team the flexibility to take different actions as the result of specific threats. For example, they may create automated tools to shutdown the network switch ports for hosts that are clearly infected with a simple worm, while they might activate their full incident response team to handle a more focused, knowledgeable and clearly human attacker.

With a small amount of analysis of the honeypot detection patterns and the observed events, it quickly becomes clear what type of threat is underway.

Pseudo-services, and other low interaction honeypot technologies, can provide you with visibility into the security posture of your environment.

Deployment of pseudo-services is often the first step in an organization’s leveraging of honeypot technologies. Usually, this begins by the security team deploying a few services on a dedicated laptop or desktop device and moving this “decoy host” from network to network. This approach is usually referred to as “scatter sensing”, since the idea is that you scatter these mobile sensors around the environment.

Once the security team becomes more familiar and comfortable with the honeypot tools, they typically move on to deploying additional decoy hosts on each network segment, or they begin to deploy pseudo-services on their existing production servers, workstations and devices.

Once the honeypot sensors are fully deployed, most organizations find that they are essentially low noise, high signal tools for detecting potential security issues. Most corporate environments with even a basic security program, identify between four and ten security events using the pseudo-service approach each month. Since any and all interactions with a pseudo-service are suspicious, they investigate each occurrence and do not suffer any false positive alerts. The best part of this technique is that the deployments are essentially “deploy and forget”. Little ongoing management and maintenance is required since there are no signatures to update or tune!

In my experience, once they get their feet wet in the honeypot world, organizations then typically begin to grow their capabilities beyond pseudo-services. Some begin to create specialized Trojan horse documents and executables to track unauthorized access to files or the movement of files around the world. Many create specialized PDF and HTML documents with embedded links to track who is reading their information in detail.

With some imagination, they create honeypot accounts in their Windows AD infrastructure that alert the security team if and/or when they are accessed. They might begin to use tools to send “fake” credentials across the wire, hoping to direct those attackers using sniffers toward their pseudo-services.

Their experiences vary depending on the effectiveness of the rest of their security program, but many organizations have reported much success with these techniques. Obviously, they have caught infected machines scanning their environments, worms attempting to spread to emulated pseudo-services and employees dabbling in off-the-shelf attack tools. Some have identified 0-day exploits that eluded both network defenses and anti-virus installations.

Others have found that their deployed pseudo-services have been connected to from the public Internet, exposing misconfigurations in perimeter firewalls, routers and port forwarding configurations. In many cases, internal employees and contractors have been identified that were simply “looking around the network” where they should not have been. Corporate honeypots, in my opinion, represent a vastly misunderstood and underutilized resource. Presenting the concepts to upper management may return anything from acceptance to dismay, and from curiosity to “it might make attackers mad”. The key to being successful is careful, concise communication of the value. Progressing the idea that these “fake” services can be deployed once, then depended on for ongoing security with little or no day-to-day effort has shown to be a powerful idea in the boardroom.

Starting small, with dedicated workstations and the scatter sensing approach is usually easy to do and requires the smallest of security investments. It also lends itself well to finding that first malware infected host that most security teams leverage to shed light on the proof of concept to their management.

Presenting the concepts to upper management may return anything from acceptance to dismay, and from curiosity to “it might make attackers mad”. The key to being successful is careful, concise communication of the value.

Products and services are widely available in the honeypot space. A variety of solutions, both open source and commercial are easily found with a simple Google search. Several consulting firms offer services around designing and implementing honeypot technologies and employing them effectively to help secure your informational assets.

Whether you choose to pursue them on your own or with the guidance of an expert, I believe that your organization will find great value and capability in corporate honeypots. My experiences have shown that they are effective, easy to manage and capable security tools. Give them a try, and please, share your findings with others.

Brent Huston is the CEO and Security Evangelist at MicroSolved (www.microsolved.com). Brent is an accomplished computer and information security speaker and has published numerous white papers on security-related topics.

Open Disclosure: I am the author of a commercial honeypot suite of products and techniques known as HoneyPoint Security Server. My opinions, do not represent any corporation or other entity. Your paranoia and milage may vary...

Gartner Information Security Summit 2009

21–22 September 2009 | Royal Lancaster Hotel, London, UK

Managing risk and securing information: your role, your priorities, your tactics

In today's climate, you not only have to be effective at protecting your organization, you have to be efficient at delivering effectiveness; you have to protect more aspects of your organization and do so with fewer resources.

The **Gartner Information Security Summit** will demonstrate the best practices, give you the strategic insights, and will provide you with a roadmap showing the actions you should be taking today to address your most pressing security challenges.

Summit highlights

- 13 Gartner Security Analysts
- Over 50 Conference Sessions
- End-User Case Studies from British American Tobacco, City of Göteborg, Centrica, Euroclear, Centrica Energy, RWE nPower, Banc Sabadell Group, Ericsson, and Swiss Federal Railways.
- Priority One-on-One booking with Gartner Analysts

Key Benefits

- Meet business needs
- Make wise investments
- Sound deployment of resources
- Make the business case
- Safeguard clients
- Deepen tactical knowledge
- Strengthen strategic vision
- Develop your knowledge and skills

Register now!

europe.gartner.com/security
Tel: +44 (0)208 879 2430
Email: emea.registration@gartner.com

Gartner
Information Security
Summit 2009

21–22 September | London

europe.gartner.com/security

Making clouds secure

by Alexei Lesnykh

The concept of cloud computing - just what every IT community is dreaming about these days - has a multitude of indisputable advantages over more traditional modes of software distribution and usage. But cloud computing has a long way to go before it takes over the market - not in terms of technology, but in terms of how it is perceived by potential clients. For the majority of them, cloud computing seems like an interesting, but not very secure idea.

If you were to review the evolution of the concept (which, incidentally, is considerably older than it might seem), you would see the close connections between cloud computing and information security.

As Enomaly founder and Chief Technologist Reuven Cohen has rightly noted, the cloud computing concept was first mastered by cyber criminals who had created rogue networks as early as ten years ago. Not much time passed before people started using cloud computing for legitimate purposes, and the technology is just now beginning to come into its own.

What is a "cloud"?

Let's take a look at the formal definition of the concept before we tackle the modern aspects of security and cloud computing. There is still no common or generally recognized definition of cloud computing in the IT industry, and most experts, analysts, and users have their own understanding of the term.

In order to come to a more precise definition, we first need to move from the general to the specific. In general, cloud computing is a concept whereby a number of different computing resources (applications, platforms or infrastructures) are made available to users via the Internet. While this definition seems to capture the essence of cloud computing, in practice it is much too abstract and broad. If you wanted to, you could include practically everything even vaguely related to the Internet in that definition. The definition needs to be made more specific, and in order to do so, we will first take a look at the position of the scientific and expert community.

The work "Above the Clouds," published by the RAD Lab at UC Berkeley, has identified the three most common features of cloud computing:

- The illusion of infinite computing resources available on demand, thereby eliminating the need for cloud computing users to plan far ahead for provisioning.

- The elimination of an up-front commitment by cloud users, thereby allowing companies to start small and increase hardware resources only when there is an increase in their needs.

- The ability to pay for use of computing resources on a short-term basis as needed (e.g., processors by the hour and storage by the day) and release them as needed, thereby rewarding conservation by letting machines and storage go when they are no longer useful.

The specifications for building a cloud platform, such as virtualization, global distribution or scale, are not so much features of cloud computing, but merely help put this paradigm into practice. In particular, the use of virtualization technologies helps achieve the "illusion of infinite computing resources" mentioned above.

The main features of any cloud service are the kinds of resources it offers users via the Internet. Depending on these resources, all services can be divided into a number of different categories (see Figure 1). Each of these carries the suffix *aaS, where the asterisk represents the letter S, P, I or D, and the abbreviation "aaS" means "as a service."

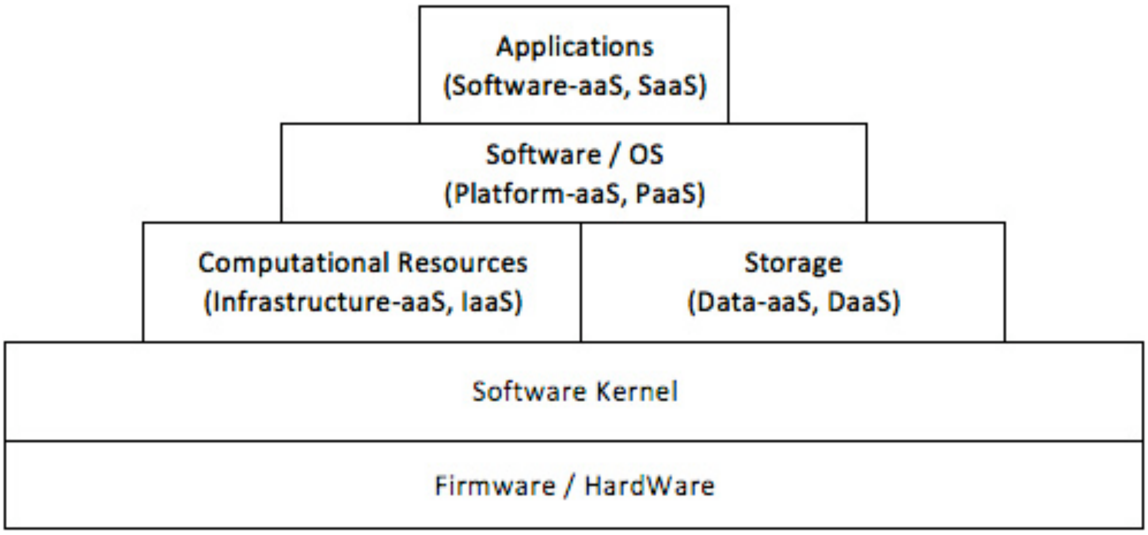


Figure 1. The ontology of cloud services.

Essentially, cloud computing makes resources available through the Internet and has three fundamental features, as noted above.

The types of resources made available may be software (SaaS), a platform (PaaS), an infrastructure (IaaS), or storage (DaaS).

Defining security problems on cloud servers

Practically every expert in the industry approaches cloud computing with their own interpretation of the concept. As a result, after examining numerous published works on the subject, one might get the impression that there is really no standardization at all. Questions regarding the security of Skype - a typical consumer cloud service - get jumbled up with the business aspects of installing SaaS, while Microsoft Live Mesh is already becoming a headache for companies that never even planned on using it in the first place.

That's why it would make complete sense to deconstruct the problem of cloud computing security into several high-level categories. In the end, all aspects of cloud service security can be put into one of four main categories:

- Security issues with consumer cloud and Web 2.0 services. As a rule, these problems don't have as much to do with security as they do with privacy and the protection of personal data. Similar problems are common among most major Internet service providers - just think about all of the accusations against Google or Microsoft that come up from time to time with regard to tracking user activity.

- Corporate-level security issues resulting from the popularity of consumer cloud services. This becomes a problem when employees get together on sites like Facebook and gossip about corporate secrets.

- Cloud computing security issues related to corporate usage, and the use of SaaS in particular.

- Issues concerning the use of the cloud computing concept in information security solutions.

In order to avoid any confusion or contradictions, we will address only the third category from the list above, since this is the most serious issue in terms of corporate information system security. Consumer cloud services have already won over Internet users, and there are really no security problems that could break that trend. The hottest topic right now is just how quickly cloud computing can become a corporate platform suitable not only for SMEs, but for large international organizations as well.

Deconstructing corporate cloud services

IDC analysts who spoke at the IDC cloud computing Forum in February 2009 stated that information security is the top concern among companies interested in using cloud computing. According to IDC, 75% of IT managers are concerned about cloud service security.

In order to understand why, we need to continue our deconstruction of the security issue. For corporations using cloud services, all security issues can be further divided into three main categories:

- The security of a platform that is located on the premises of the service provider;

- The security of workstations (endpoints) that are located directly on the client's premises;

- And finally, the security of data that are transferred from endpoints to the platform.

The last point concerning the security of transferred data is de facto already resolved using data encryption technologies, secure connections, and VPN. Practically all modern cloud services support these mechanisms, and transferring data from endpoints to a platform can now be seen as a fully secure process.

The platform: trust and functionality problems

Clearly, security issues related to service platform functionality are the biggest headache for IT managers today. For many, figuring out how to ensure the security of something that cannot be directly controlled is not a very straightforward process. The platform of a typical cloud service is not simply located on the premises of a third-party organization, but often at an unknown data center in an unknown country.

In other words, cloud computing's basic security problem comes down to issues of client trust (and verifying trust) in service providers and is a continuation of the same issues that arise with any type of outsourcing: company specialists and management are simply not accustomed to outsourcing something as crucial as the security of business data. However, one can be certain that this problem will be resolved since other forms of outsourcing for the same IT processes and resources no longer give rise to any fundamental concerns.

What is this certainty based on? First of all, it is considerably easier for cloud service providers to ensure the security of the data centers where available resources are located. This is due to the scale effect: since the service provider is offering services to a relatively large number of clients, it will provide security for each of them at the same time and, as a result, can use more complex and effective types of protection. Of course, companies like Google or Microsoft have more resources to ensure platform security than a small contracting firm or even a large corporation with its own data center.

Second, using cloud services between client and provider organizations is always based on their respective cloud services quality agreements (SLA), which clearly set out the provider's responsibility for various information security issues. Third, the provider's business directly depends on its reputation, which is why it will strive to ensure information security at the highest possible level.

In addition to verification and trust issues, cloud platform clients also worry about the full functionality of information security. While most in-house systems already support this feature (thanks to many years of evolution), the situation is much more complicated when it comes to cloud services.

Gartner's brochure "Assessing the Security Risks of Cloud Computing" examines seven of the most relevant cloud service security problems, most of which are directly related to the idiosyncrasies of the way cloud systems function. In particular, Gartner recommends looking at cloud system functions from the viewpoint of access rights distribution, data recovery capabilities, investigative support and auditing.

Are there any conceptual restrictions that might make it impossible to put these things into practice? The answer is definitely no: everything that can be done within an organization can technically be executed within a "cloud." Information security problems essentially depend on the design of specific cloud products and services.

In addition to verification and trust issues, cloud platform clients also worry about the full functionality of information security

When it comes to cloud computing platform security, we should address yet another important problem with regard to laws and regulations. Difficulties arise because a separation of data takes place between the client and the service provider within the cloud computing environment, and that separation often complicates the process of ensuring compliance with various statutory acts and standards. While this is a serious problem, it will no doubt be resolved sooner or later.

On the one hand, as cloud computing becomes more widespread, the technologies used to ensure compliance with legal requirements will be improved. Legislators will have to consider the technical peculiarities of the cloud computing environment in new versions of regulatory documents.

In summary, the concerns about information security as it pertains to the platform component of the cloud computing environment lead us to the conclusion that while all of the problems that potential clients have identified do in fact exist today, they will be successfully resolved. There simply are no conceptual restrictions in cloud computing.

Endpoint: Difficulties remain and are getting worse

In the theoretically ideal "Cloud World," cloud computing security takes place on the platform level and through communication with edge devices, since data is not stored on the devices themselves. This model is still too premature to be put into practice, and the data that reaches the platform is de facto created, processed and stored on the endpoint level.

It turns out that there will always be security problems with edge devices in a cloud environment. In fact, there is another much stronger theory that these problems are actually becoming worse. In order to understand why this is happening, let us take a look at some conceptual diagrams of traditional in-house IT models compared to the cloud computing environment (Figures 2 and 3 on the following page).

In each case, most of the threats are coming from the global network and entering the client's corporate infrastructure. In the in-house system, the main blow is dealt to the platform, in contrast to the cloud environment, in which the more or less unprotected endpoints suffer.

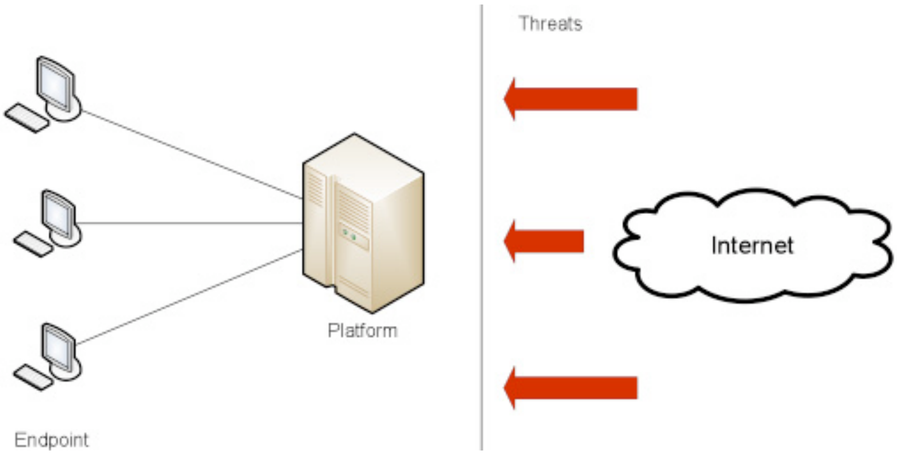


Figure 2. Security threats for traditional models for running software.

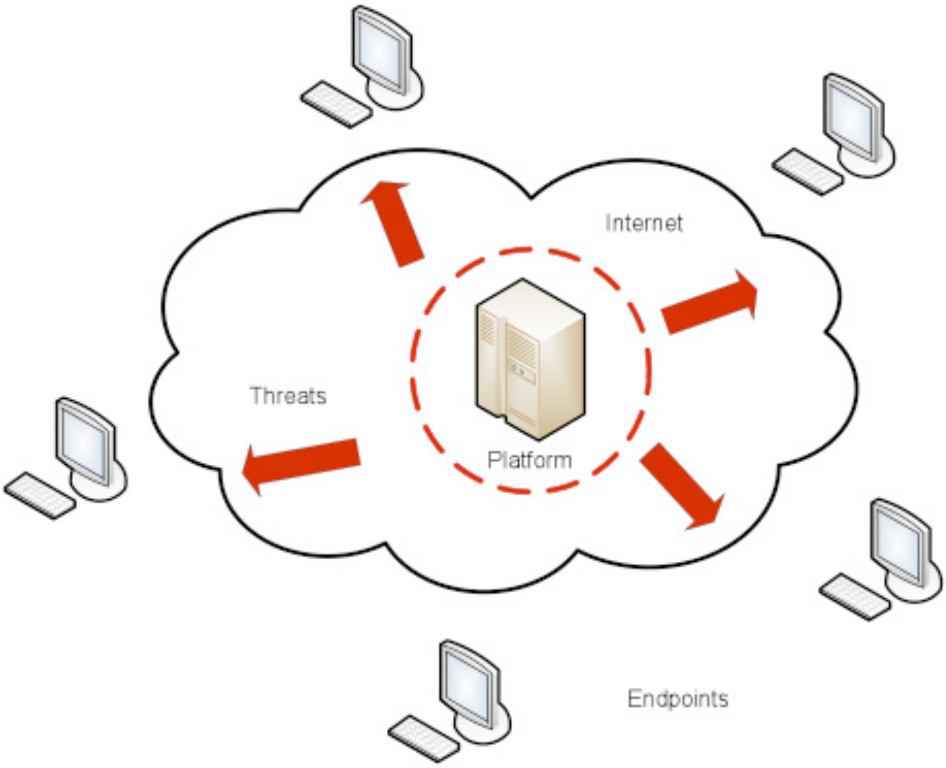


Figure 3. Security threats in a corporate cloud environment.

External attackers find it useless to target protected provider clouds since, as we noted above, the protection level of global cloud platforms like Google and Microsoft, due to the numerous capabilities, professional expertise and unlimited resources, will be significantly higher than the data protection supplied by any individual corporate IT system.

As a result, cyber criminals end up attacking edge devices. The very concept of cloud computing, which presumes access to a platform from wherever and whenever it is convenient to do so, also increases the probability of this type of scenario.

Having observed an increase in a variety of attacks on endpoint computers, corporate information security services have had to resort to focusing their efforts on protecting edge devices. It is this task in particular that, it would seem, will become a critical problem for corporate information security.

"I think a lot of security objections to the Cloud are emotional in nature, it's reflexive," said Joseph Tobolski, director for Cloud Computing at Accenture. Shumacher Group CEO Doug Menafee is also familiar with the emotional aspects:

"My IT department came to me with a list of 100 security requirements and I thought, Wait a minute, we don't even have most of that in our own data center".

Deciding to use cloud computing is just like getting behind the wheel of a car for the first time. On the one hand, many of your colleagues may have already made the leap, but on the other hand, getting onto a busy highway for the first time can be scary — especially when you keep seeing stories of horrible accidents on the news. However, it‘s not much more dangerous to drive than it is to drink coffee on a moving train or to wait at a bus stop.

For the most part, the situation with cloud computing is the same as with classic software usage models. The cloud environment requires attention to information security, but we`re totally confident that there would be solutions to the problems that currently exist.

There are specific nuances in cloud security, primarily related to a blend of priorities - from perimeter protection to edge device protection. But if data security developers help companies resolve this problem, the future for “clouds” will be sunny indeed.

Alexei Lesnykh, DeviceLock (www.devicelock.com).

Q&A: Dr. Herbert Thompson on security ROI and RSA Conference

by Mirko Zorz

Dr. Herbert Thompson, CISSP, serves as RSA Conference Program Committee Chairman and Advisory Board member. He is directly involved in the selection of session topics and speakers, and the architecture of Conference educational programming. Dr. Thompson is a world-renown application security expert, Adjunct Professor of Computer Science at Columbia University, Graduate Faculty member in Applied Mathematics at Florida Institute of Technology, Advisory Board member for the Anti-Malware Testing Standards Organization.

Although ROI is a term the majority of IT security professionals don't like for a variety of reasons, they still have to make sure the management understands what they're doing and why. In these tough economic times, what advice would you give to security personnel pitching a budget to their superiors?

Justifying the money spent on security improvement is a core challenge of IT security. If you can link an investment in security improvement to how that investment is going to help the company make or save money, or help reduce risk (avoid losing money), then that investment can compete on the battlefield of IT budget. There will always be activities that must be done to comply with a regulation or standard such as PCI DSS or Sarbanes Oxley. For these, security is more about compliance than risk reduction. Outside of compliance, the preventative nature of security can sometimes make it difficult to quantify and communicate its worth. One approach I've seen implemented successfully is the use of risk management frameworks to create benchmarks for applications, processes, etc. The data was then used to motivate individual business units to move in-line with the rest of the organization. When a group observes that they significantly fall below other areas of the organization from a security/risk perspective, it serves as strong motivation for risk-reduction practices and tools. Another thing to consider is that security can also serve as a differentiator. Business customers, and to some degree consumers, are starting to ask businesses hard questions about security. The answers that come back might make or break a sale.

As expected, cybercrime is soaring worldwide and at the same time, the recession is shrinking IT security budgets in most industries. Do you see any strategies that can fill the void as the money runs out? What recommendations would you give to organizations?

Now is one of the most critical times to not drop the ball on security. So much of security comes down to little decisions that employees make every day that inadvertently put a business or its customers at risk. Security tools, processes and technologies help to create a safety net for those mistakes, but when security budgets are cut, the net becomes tattered and leaky.

The key is to create a culture of security and help make it infectious in an organization. Some companies have managed to evangelize security and bring awareness through brownbag lunches, security awareness events and sending "influencers" in the company to industry events like RSA Conference.

Building awareness has the two-fold effect of helping employees make good security-conscious choices day-to-day and also keeping security in clear view of executives that need to make budgeting decisions.

Building awareness has the two-fold effect of helping employees make good security-conscious choices day-to-day and also keeping security in clear view of executives that need to make budgeting decisions.

Legitimate businesses are not the only ones impacted by an unstable financial system. What kind of ramifications is the economic downturn having on the underground economy? What type of remodeling can we expect to see in the near future?

Most indications are that the underground economy is thriving and growing rapidly. In some ways it's also becoming more efficient - meaning that the prices for certain types of stolen data have stabilized - making this type of data more of a commodity. This is a scary situation for businesses because it means that it's getting easier to turn customer data into cash, which means the motivation to steal data is strong.

There has also been a maturing in the underground services market, too. This means that someone that has malicious intent - who wants to launch a Distributed Denial of Service (DDoS) attack for example - but not the technical skills or resources to execute the attack can now outsource. The result is a broadened range of digital adversaries. All of this means that we're likely to enter a period of significant attacker innovation, making it more important to carefully monitor threats and keep up with the latest attack trends.

Achieving more on a smaller budget and keeping an organization protected at the same time is on the table of many security professionals. Can we expect talks related to budgeting security at RSAC 2010?

While we're still developing the content for RSA Conference 2010, budgeting for security is obviously top of mind for security practitioners.

Some organizations, pushed by today's challenges, have been forced to innovate in the areas of security metrics and risk management to better use their budgets and minimize risk. I'm looking forward to seeing the results of that innovation at RSA Conference 2010.

DATA LOCKER

PIN Protected AES Encrypted USB 2.0 Hard Drive

The World's Most Secure PIN Protected Portable Hard Drive

The Data Locker features a comprehensive set of innovative, proprietary technologies in order to provide users with the simplest to use, most secure portable hard drive on the market.

The Data Locker is the only portable hard drive which is 100% platform independent, all of its security measures are performed within the device itself. Unlike other secure devices which require authentication through the host system, Data Locker users must authenticate themselves via a touch screen LCD panel on the Data Locker to deactivate the security measures. Only after the authentication process is completed is the drive recognised or accessible by the host system. This allows the Data Locker to remain driverless and software free as well as being both PC and Mac compatible.

The Data Locker's unique authentication system eliminates the threat of infected systems, keyboard loggers or brute force attacks. This authentication system coupled with hardware based 128 or 256 bit AES (CBC Mode) full drive encryption provides unparalleled security.

Key Features

- 128 or 256 Bit AES Hardware Encryption
- Higher Level Encryption Using Cipher Block Chaining (CBC) Mode
- FIPS 197 Certified Encryption Chipset & FIPS 140-2 Applied For
- Up To 18 Digit User Defined PIN
- Unique User Generated Encryption Key
- LCD Touch Screen For Authentication
- Random Keyboard Layout
- One Touch Data Eraser For Redeployment
- Platform Independent Security Process
- Driverless And No Software Required
- PC And Mac Compatible

Technical Specifications:

Capacity:	160GB, 320GB, 500GB, 750GB & 1TB
Drive Specs:	2.5 Inch SATA, 5400 RPM, 8MB Buffer
Interface:	Hi Speed USB 2.0
Bus Transfer Rate:	Up To 480Mb/Sec
Dimensions:	127mm x 76mm x 20mm
Weight:	256 grams
OS Compatibility:	Compatible With All

Available Models

	Data Locker Models:	
Feature:	**Pro AES**	**Enterprise**
Encryption Algorithm	AES CBC Mode	AES CBC Mode
Encryption Key Strength	128 Bit	256 Bit
Self Destruct Mode	•	•
Master Administrative Password		•
One Touch Data Eraser	•	•
Platform Independent	•	•
Driverless And Software Free	•	•
PC And Mac Compatible	•	•
USB Bus Powered	•	•
Hardware Based Malware Protection	•	•

CES Show - Jan 2009:

The Data Locker Pro was recognized by CES 2009 as a top computer peripheral innovation.

Visit: www.datalockerdrive.eu Call: +31 (0)467 111 201

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

@edskoudis
Handler at the Internet Storm Center, Microsoft MVP for Windows Server Security.
http://twitter.com/edskoudis

@Z3r0Point
Andrew Knapp, Analyst at CGI.
http://twitter.com/Z3r0Point

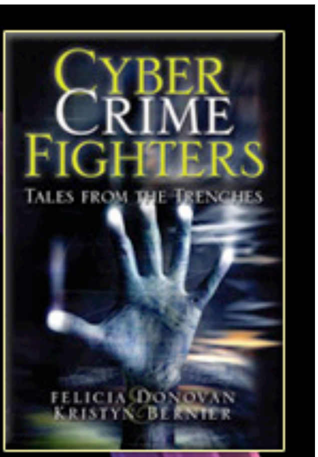
@agent0x0
Tom Eston, penetration tester, social media security researcher.
http://twitter.com/agent0x0

If you want to suggest an account to be added to this list, send a message to **@helpnetsecurity** on Twitter.

Book review

Cyber Crime Fighters: Tales from the Trenches

by Zeljka Zorz



Authors: Felicia Donovan, Kristyn Bernier | Pages: 336 | Publisher: Que | ISBN: 0789739224

Every new technology has the capacity to be used for good or for evil. And where is a new way to commit crimes, criminals will find it.

That being said, this book covers the great majority of criminal acts that can be done by using "new" technology and offers you tips on how to avoid being targeted or, if you already have been victimized, what steps to take and how to minimize the damage done to your life.

About the authors

Felicia Donovan is a law enforcement technology and cyber crime expert who spent ten years at a New England police department and received recognition from the FBI on her work related to cases.

Kristyn Bernier, a detective and 15-year veteran of a New England-based police department, currently specializes in undercover work fighting Internet crimes.

Inside the book

Every chapter deals with a specific type of crime and how it can be carried out. The authors additionally demonstrate, using real-life examples, cases that have been investigated and prosecuted. Unfortunately, the prosecution is not always successful.

To help you out in case you need them, the book also lists resources, addresses and telephone numbers of organizations that aid victims.

From this book you will learn about:

- Cyber stalking: how GPS, keylogging, identity assumption can become weapons in the hands of a stalker
- What kind of information can a malicious person gather about you and the place you live on the Internet, based on what you or different services put online (social networks, tax assessor's database, real-estate tools, online memorials and website registrations records - to name just a few)
- Identity theft: what's the difference between identity theft and identity fraud and how to prevent them both
- The perils of online dating
- How the Internet has become a means for sexual predators to reach their victims

- Smart use of social networks - tips on what type of information not to share with strangers
- Phishing, pharming, spam and scams.

Particularly interesting and useful is chapter 16 that presents an elaborate list of safety measures you should take to secure your computer and your network. Although the authors are focusing more on the technical aspect of these crimes, they don't forget to emphasize that common sense plays a great role in safeguarding oneself.

This book is a good mixture of technical knowledge, current laws, how-and-what-to-dos and actual cases. It's particularly these real-life experiences that help us translate all this information and make it easier for us to realize that some of these things can happen to us too, and that spending some time and effort on security is well worth it.

Final thoughts

In this fast paced world where the criminals seem always to be one step ahead of us and where, in most cases, our children know a lot more about the Internet and new emerging technologies than us, I think it's important to educate ourselves about how these technologies can be misused.

This book won't be an eye opener for advanced IT users, but it will provide a good overview for all new users. It's difficult to say if this is a book suitable for kids or teenagers - that is the kind of thing every parent should decide of him/herself after reading this book and weighing the pros and cons.

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

Top 5 myths about wireless protection

by Michael Raggo

In light of recent wireless breaches, I'm continuously amazed with the number of companies that have lackluster approaches to wireless security. It seems most companies with Wireless LANs are looking to meet PCI requirements by identifying Rogue Access points using free tools.

In order to help people stay on top of the latest vulnerabilities (and some old ones, too) I decided to put together a list of the Top 5 Myths about Wireless Protection. These top 5 myths were compiled from my own experiences in pen testing and fortifying customer wireless networks. If everyone who reads this article walks away with a least one "gold nugget" to help them protect their Wireless environment I will have accomplished my goal, so let's get to it.

Myth#1 - We have a firewall, we're from protected wireless break-ins

Most companies are building out wireless networks as an extension of their legacy wired network. Wireless is a physical medium, therefore you can no longer rely on your firewall to provide all of your protection. Obviously, rogue access points are a problem as they can provide a backdoor into the network, and it can be difficult to locate their physical proximity. More on that later…

Aside from rogue access points, there is also the threat of wireless laptops connected to your wired network. It's not uncommon to find laptops connected to the wired network that also have their wireless card enabled. In most cases, these wireless laptops are probing for previously accessed wireless networks by SSID. And if found, may automatically associate with a wireless network, whether that network is legitimate, neighboring, or malicious. In the case of malicious, once a laptop associates to the malicious wireless network, the hacker can target the laptop by scanning it for vulnerabilities, launching an exploit, and thus gain access to the laptop. In addition to the exposure of the information on the laptop, if bridging is enabled, the hacker could use the laptop as a launch pad into the wired network. In this scenario, the hacker has completely bypassed the firewall.

We've also been taught to evaluate security from a trusted and untrusted perspective. As a result, many companies configure their firewalls to protect themselves from Internet-based attacks, but fail to consider extrusions and leakage. Essentially with an extrusion, we're speaking about something going out of the network rather than coming in.

Many companies misconfigure their firewalls by not blocking outgoing traffic. This results in data leakage. For example, the most common thing we find during our wireless pen tests is traffic leaking from the wired network out through the wireless access point. With a simple wireless sniffer we capture a plethora of leaked traffic, including STP (Spanning Tree Protocol), IGRP, and other networking services and protocols, and in some cases even NetBIOS! This makes the network enumeration process child's play for a hacker. In fact, it doesn't even require any active scans or attacks. By simply sniffing the wireless network one can identify the wired-side network topology, critical network devices, and sometimes even account information.

Myth #2 - We have a policy that prohibits wireless, therefore we have no need to scan for rogue access points

I am just mystified when I hear this one. How do you know you have no wireless if you're not scanning for it?! In addition to rogue access points, the threat of ad-hoc networks, laptop accidental associations, and bridging are all potential wireless exposures present in environments with no wireless LAN.

For users with wireless laptops, accidental associations can be a risk. If a neighboring company has a wireless access point or ad-hoc network (client-to-client), it's not uncommon for a user's company laptop to accidentally associate with one of these wireless networks. This is one form of an extrusion. Hackers know this, and as a result can setup a SoftAP (software run from a laptop) that broadcasts common SSIDs to lure an innocent user into associating, thus giving them an IP. And as mentioned earlier, it can allow them to target the laptop and the wired network to which it is attached. It may also allow them to perform MITM (Man in the Middle) attacks or Identify Theft.

Many companies misconfigure their firewalls by not blocking outgoing traffic. This results in data leakage.

Myth #3 - We can rely on manual scanning to identify rogue access points

I respect the fact that in this case the customer is taking a proactive approach to identify rogue access points in their environment. Unfortunately the tools at their disposal are usually not well equipped to identify rogues.

For example, many customers use wired-side vulnerability management scanning tools to identify rogue access points connected to the network. My experience with both open source and commercial vulnerability scanners is that they normally only have a handful of operating system detections for access points, therefore when they run a scan the device normally shows up as a Linux device with a Web server. When running a scan against a Class C or larger, the device just blends in with the rest and you receive no real indication that you have a rogue access point.

Wireless scanning tools such as NetStumbler and Kismet are great, and I use them myself. But when it comes to tracking down Rogues they don't quite fit the bill. They don't really tell you if the identified access points are connected to your wired network. And it can be challenging to use the tools to locate the physical proximity of the questionable wireless device. If we're talking about a multi-floor high-rise building, good luck! Add to that high gain antennas and signal emissions, and your average network administrator is going to have a very difficult time trying to track down the wireless devices.

Myth #4 - We have upgraded all of our Access Points to eliminate WEP, therefore we're secure

WEP has been hacked for years. In addition, PCI has notified merchants that WEP should be decommissioned by June of 2010. Some companies have already made the move to stronger encryption and authentication options.

There are a number of options to choose from. Unfortunately, some of these stronger schemes are also vulnerable. For example, the PSK (pre-shared key) version of WPA suffers from an offline dictionary attack because of the broadcasting of information required to create and verify a session key. A number of tools exist to run these dictionary attacks, including coWPAtty and aircrack-ng. Most of the attacks involve collecting a bunch of packets, and then running the tool against the packet capture. Backtrack 3 will give you all of the tools necessary to successfully perform this attack.

Also, in November 2008, TKIP was also hacked in a proof of concept. To clarify, the attack affects all TKIP deployments, both WPA and WPA2, regardless of whether you use PSK or 802.1x authentication. But the TKIP keys are not compromised and it doesn't lead to decryption of all subsequent frames. Rather, the attack can reveal one byte per minute of a TKIP encrypted packet, and can lead to injection of up to 15 arbitrary frames for every decrypted packet. Sounds like a good candidate for ARP poisoning to me. It is important to note that WPA and WPA2 networks that use the more robust AES-CCMP encryption algorithm are immune to the attack, and is recommended as your best approach. If you have no choice but to run WPA-PSK, be sure to choose a very strong password and a bare minimum of 8 characters. A complex password consisting of 6 characters can be cracked well within 13 days.

Myth #5 - We use client VPN software to protect our mobile employees

Although client VPN software with a firewall is a great first step in protecting mobile employees, a plethora of other vulnerabilities exist. While your users are traveling they will inevitably attempt to obtain Wi-Fi access at hotels, coffee shops, airports, etc.

Tools such as hotspotter available on BackTrack can allow a hacker to setup a hotspot that looks almost identical to a legitimate hotspot. This includes setting up a fake access point with a common hotspot SSID (e.g. tmobile) and web pages that look like a real hotspot. The attacker then waits for innocent users to associate to the fake access point, and provides them an IP via DHCP, and a hotspot webpage. The user is fooled into logging in, thus providing their credentials to the hacker. In some cases, the hacker is even providing Internet access allowing the hacker to perform Man-in-the-Middle attacks to steal additional information such as logins, account numbers, etc.

Protecting mobile employees from these types of attacks is particularly challenging, but aside from your client VPN and firewall software, there are other steps you can take. None are a silver bullet, but can help minimize the risk. Windows administrators can enforce the wireless cards on wireless laptops to only connect to "Access point (infrastructure) networks only". This will help avoid users connecting to ad-hoc (computer-to-computer) networks. Many hacker tools that emulate access points are really fake ad-hoc networks. Disabling this feature in the Windows operating systems can help protect users from some of these attacks. Also, disabling the "any available network (access point preferred)" also protects against similar attacks. Finally, disabling "Automatically connect to non-preferred networks" will help protect against accidental associations.

Conclusion

A layered defense approach is key when it comes to wireless protection. Understanding the risks goes a long way toward minimizing the risks. The majority of wireless attacks are related to Layer 2, so it's important to review your existing firewalls to ensure that they provide Layer 2 filtering. Many firewalls only provide Layer 3 and above protection. And for those firewalls that provide Layer 2 protection, many operate as a packet filter rather than providing stateful inspection. Packet filters can be very tedious to configure, so Layer 2 and Layer 3 stateful inspection is the preferred approach for wireless security.

Upgrading and changing your Access Point configurations will also thwart attackers from targeting weak encryption and authentication schemes. In addition, they will also help you meet many of your current and future regulatory and industry compliance requirements.

Many wireless attacks are situational, and therefore require a Wireless IDS/IPS to model the environment and protect against exceptions to the approved wireless infrastructure. A mature Wireless IDS/IPS will provide detection of many of the aforementioned attacks, and protection against hacker tools that perform known attack sequences, something most firewalls simply cannot provide.

A Wireless IDS/IPS can also provide better means of detecting Rogue Access Points. A handheld scanner is simply a snapshot in time and provides no means of automatically protecting you against Rogue Access Points. Using a Wireless IDS/IPS for 24x7 monitoring and automatic termination of Rogue Access Points is a much better approach to minimizing the risks to your network. In addition, it will probably save you a lot of time and effort traveling to conduct manual wireless assessments.

Michael T. Raggo (CISSP, NSA-IAM, CCSI, SCSA, CSI) applies over 20 years of security technology experience and evangelism to the technical delivery of Wireless Security Solutions and Research. Mr. Raggo's technology experience includes penetration testing, wireless assessments, compliance assessments, firewall and IDS/IPS deployments, incident response and forensics, risk management, and security research, and he is a former security trainer. Mr. Raggo has presented on various security topics at numerous conferences (BlackHat, DefCon, SANS, InfoSec, etc.) around the world and has even briefed the Pentagon. He is currently authoring a book on steganography and steganalysis.

Securing the foundation of IT systems

by Jamie Adams

Recent studies show that securing the operating system is recognized as a necessary practice in an organization's overall security policy, but it is not being done on a regular, consistent basis across the enterprise. Operating systems control every function that the server on which it is installed, provides. The OS is responsible for the management and coordination of everything that happens on a computer, including how and where resources are shared. It serves as the foundation for every application running on a server.

With today's threat environment, security has become the focus of many system administrator jobs. Most system administrators agree that locking down (or hardening) operating systems to a prescribed level of compliancy, and maintaining that compliancy across the enterprise is a best practice to follow. On the flip side, studies reveal that the majority of organizations are not locking down all of their servers and many are not even locking down all Internet facing servers which are the most vulnerable. The vulnerability that organizations face when they do not lock down their operating systems, consistently and persistently, can be devastating.

Why the disconnect? Unfortunately, companies and government agencies are faced with limited resources and increasingly shrinking IT budgets, while at the same time, threats to data and other sensitive and classified information is on the rise. When faced with budget decisions, securing assets can become a costly afterthought.

In a constantly changing environment locking down operating systems across the enterprise and maintaining an identified level of compliancy is no easy task. On blogs frequented by system administrators, questions always arise regarding the lock down process, indicating the lack of straightforwardness. Regardless of which operating system a company or government agency is running, there are a variety of methods (such as free lock down scripts) that system administrators can implement to harden an operating system.

However, these scripts most often require modification in order to adhere to specific security policies. Modification has to be done manually which means that there is always the chance for error. What happens where errors are made? Applications don't run and users are very unhappy. Scripts can be reversed but then the OS configuration is back to its initial state and you find yourself starting over again. You cannot simply undo the one lock down that caused the problem.

Another option is to turn to a consulting organization that provides services, including scans of the operating system that show how the operating system fares against a set of security best practices. These organizations may also offer lock down services, but this can be costly over time, and once the consultants are gone, there is the issue of maintenance.

There are configuration management tools available that assess the security of operating systems and make recommendations as to what needs to be done to remediate vulnerabilities. But again, the configuration of the OS is done manually and therefore the same costs and risks remain.

The challenge comes in finding out which unnecessary services have been enabled and are not needed.

It would be ideal if new off-the-shelf operating systems were shipped with lock downs fully enabled. However, the vendors that provide these systems would soon be out of business. Installation of the OS would be cumbersome at best and once it was installed, there would be a high probability of some applications not running successfully.

Operating systems are shipped insecure for a reason, so that they can be easily installed and applications will run on them. Therefore, system administrators are tasked with locking down all new out-of-the-box OS before installing applications. Once the systems are up and running within an environment they must be constantly maintained to adhere to the organization's security and compliance standards.

When new software is installed on an OS, services needed for installation are enabled, but these services may not be needed beyond initial installation. Unused services are a prime target for attackers. They know that services are frequently turned on without the system administrator's knowledge, which make an operating system susceptible to widespread attacks. As part of the lock down process, system administrators should disable as many unused services as possible, including network, peer-to-peer, file sharing and general services.

The challenge comes in finding out which unnecessary services have been enabled and are not needed. Lastly, in the lock down process, system administrators should adjust the kernel's TCP/IP settings to help prevent denial-of-service attacks and packet spoofing.

These additional measures are often referred to as layered security or in-depth-defense. All of these things help minimize an organization's potential attack surface.

Administrative password misuse is another example of a potential vulnerability. According to the "20 Critical Security Controls," published by the SANS Institute, the misuse of administrator privileges is the number one method used by attackers to infiltrate an enterprise.

The second most common technique is the elevation of privileges by guessing or cracking a password for an administrative user to gain access to a targeted machine. As part of the operating system lock down practice, organizations need to ensure administrative passwords have a minimum of 12, somewhat random, characters and that all administrative accounts are configured to require password changes on a regular basis. Further enforcement of securing administrative accounts should ensure that machines cannot be accessed remotely.

Another best practice to protect an organization's systems from attackers is to maintain the highest possible degree of awareness. Logging is key. Without it, you don't always know that an attack has occurred. Even if you are aware without logging and analysis, there are no details provided about the attack.

The devil really is in the details. Having the details allows action to be taken to prevent the attacker from instigating broad-based damage to your enterprise vital information.

The devil really is in the details.

An organization's operating system lock down practices must include logging access control events when users try to gain access to something without having the appropriate permission. And lastly, extensive logging is worth little if potential attackers can gain access to log files. These files need to be maintained on separate machines from those that are generating the events.

While there is no single process to make any organization 100% secure, establishing a company-wide security policy based on industry standard best practices is a good place to start.

Many of these best practices can be implemented as part of the operating system assessment and lock down process. Securing the foundation on which your IT organization runs is not easy to do. It takes time, money, and resources, but the potential for an attack is too great and too costly to ignore. By implementing a consistent, enterprise-wide operating system assessment and lock down process, a company can hopefully thwart malicious attackers and keep them at bay.

Jamie Adams is the Senior Secure Systems Engineer Trusted Computer Solutions (TCS), a provider of security solutions for commercial and government organizations.

Subscribe to our YouTube channel.
www.youtube.com/helpnetsecurity

OCTOBER 24–30, 2009

NATIONAL HARBOR, MD
GAYLORD NATIONAL

CSI2009

ANNUAL CONFERENCE

REGISTER EARLY FOR BEST SAVINGS

SECURITY. STRATEGY. SUCCESS.

FOCUSED TOPICS:

- Attacks & Vulnerabilities
- Awareness
- Career
- Cloud Security
- Compliance
- Control Systems/ Physical Security
- Government
- Healthcare
- Identity & Access Management
- Incident Response & Forensics
- International
- Management
- Mobility
- Risk Management
- Secure Development
- Small Business
- Trusted Computing
- Virtualization
- Web 2.0

Featuring ISACA Workshops:

- Building an Effective Information Security Program: A Risk-Based Approach to Security Management and Governance
- Information Governance: An Executive View Then Framework Solution

" THIS IS THE FUTURE. THE IDEAS, CONCEPTS AND CONVERSATIONS THAT TAKE PLACE HERE WILL HELP CONTROL THE DESIGN AND SECURITY AS WE MOVE INTO THE FUTURE. IT IS A GOOD FEELING TO BE PART OF THIS. "

Dave Kuntz
Technical Analyst
SaskTel

GOLD SPONSOR

CISCO.

STERLING SPONSOR

LogRhythm

REGISTER NOW FOR BEST SAVINGS

CSIannual.com

A layered approach to making your Web application a safer environment

by Kyle Adams

Security has always been a serious problem with online Web sites and applications. As the technology available to developers evolves, the problems do as well. Traditionally, the mindset has been to lock down the application server and protect it from being exploited. In the last couple of years however, the threat has shifted. Malicious users are now starting to focus not on the server, but on the application's other users. This shift forces developers to consider another angle when creating and maintaining Web applications. Primarily, how do you protect your end users from being exploited from within the application environment?

As time progresses, many generalized security vulnerabilities are discovered and documented. These consist of techniques that can be employed on any number of websites and Web applications in a fairly generic manner. Cross-Site Scripting (XSS) for example is a technique used to execute malicious code in a target user's browser. Cross-Site Request Forgery (CSRF) is another technique used to temporarily hijack a user's session. Both of these are examples of attacks use the server as a vehicle to exploit the end user.

Because these vulnerabilities are so generic, it has become incredibly easy for less skilled malicious users to exploit them. Users can often find tutorials and software which help scan and identify vulnerabilities in a target website. The good news is that a generic threat usually has a generic solution. This article will discuss some of the generic vulnerabilities targeted at the end user, and how they are being addressed currently. It will also cover a few new technologies that have promise in addressing end user security.

Cross-Site Scripting (XSS)

An XSS exploit is usually achieved by persisting malicious code on the server, and waiting for the target user to view it. It can also be achieved by redirecting a user to a URL that directly outputs some of its input parameters. When an XSS exploit is loaded in the user's browser, it essentially has full access to do anything the user is capable of doing, as well as modifying the normal behavior of the application.

XSS is one of the biggest problems in many Web applications today, and it is arguably one of the most powerful techniques available to malicious users. Other attacks exist such as active man-in-the-middle, which can provide significantly more control over the end user. But, XSS is easy to employ and can impact a much larger population of users. The threat becomes even stronger when an application allows users to share data with each other.

The most common method of protection against XSS is to employ input validation on any untrusted data, such as data provided by the user. Presumably, if all data is checked for malicious content prior to being persisted on the server, it will not pose a threat when being served back to the user at a later point in time. There are several major flaws with this approach, which make it unsuitable as a single line of defense.

Primarily, validation filters are prone to vulnerabilities themselves. As the browsers introduce new technology, new methods for executing code are introduced. When Microsoft introduced CSS expressions for example, many filters were not prepared to block such content. As a result, many validation rules would approve unsafe content without hesitation, leaving users of the application vulnerable.

Furthermore, since validation filters create a barrier between the attacker and successfully employing a XSS attack, they have become a major focus of attention. There is now a published database of templates that can be used to test validation filters for common holes and finding a weakness in a validation filter has now been reduced to a copy and paste exercise.

Input validation also relies on the fact that all data is validated before it is persisted, without exception. If there are any inputs in the application that are not being sufficiently validated, then the data persisted on the server may become tainted. It is difficult to indentify unsafe data once is has been persisted with millions of other records, and adding additional input validation will not sanitize previously persisted data.

Output validation is an alternative that seems much more attractive than relying solely on strong input validation. Output validation essentially assumes that all data is unsafe and applies validation filters against the data being returned to the client. Of course this approach is also vulnerable to browser changes and new filter evasion techniques, but will protect against tainted database entries. However, output validation can't be used as the only protective measure because other threats still need to be addresses at the input phase, such as SQL injection.

Cross-Site Request Forgery (CSRF)

CSRF is a technique that exploits a weakness in the session management of a Web application. Malicious users are able to perform actions on behalf of another user by piggy backing on their existing session. A common approach to session management is to attach a token to an authenticated user. The token acts as a temporary credential to perform actions as the authenticated user without providing a username and password. CSRF exploits the fact that most sites store this token in a cookie. In a CSRF attack, code is written that attempts to execute a request on the target Web application in the background. It is assumed that the user is already logged into that website and has a valid session token stored in a cookie. If the user is in fact logged in, then the server will assume the request is legitimate and perform the associated action. All that is required for this attack to work is for the user to visit a site which contains the exploit code and to be already logged into the target website in the same browser.

For example, consider a web application that has a facility to change the user's password. Such a facility would usually consist of a form that is submitted to a known URL. By writing code that submits a new password to the known URL, anyone who visits a site containing the code, and who is already logged in, will have their password changed automatically and without their knowledge.

Because this attack does not attempt to obtain the session key, but instead just executes a single request under the authority of the session, it is not prevented by SSL. This attack has been used to achieve a variety of results, from changing passwords to transferring money in a bank account. Since this type of exploit is not the first to target the session token, there are already many common practices to help alleviate this threat. Mainly, sessions are usually configured to expire after a set amount of idle time. This countermeasure helps protect a session if the token is obtained long after the user stopped using the application. Enforcing session timeouts is always a good idea, but it only reduces the scope of the problem, it does not eliminate it.

A very strong protective measure against CSRF is to validate the referrer of any requests being made. This would prevent a request from being accepted from third party and potentially malicious Web pages. Unfortunately, it is quite easy to configure a browser to hide the referrer of all traffic as a privacy setting, so if accessibility is a key concern, then this protective measure may not be acceptable.

Alternately, if the session token were not stored in a cookie, but were provided on each request, either in the URL or as a POST parameter, then this vulnerability would not apply. This approach however, has its own accessibility challenges, as well as being difficult to retro fit into an existing cookie based session management solution.

Application firewalls

There are multiple products available which attempt to help resolve some of these generic vulnerabilities. Application firewalls are a relatively new technology that has emerged to address this type of protection. Application firewalls consist of special software packages that can be configured to inspect traffic between the client and server. They are designed to identify risk prone areas of data and apply validation and filtering, as well as inspect headers and identify potentially malicious network activity. If configured correctly, they can be used to combat a large variety of vulnerabilities, from SQL injection to XSS and CSRF.

This type of technology is a good example of an attempt to solve the generic vulnerabilities with a generic solution. Because an application firewall is a layer outside of the actual application logic, it does not understand context. This is usually overcome with complex and delicate configuration files that provide the necessary insight into the applications behavior. Without such configuration, the firewall would not be able to differentiate between legitimate data generated by the server and client, and malicious data. Similarly, configuration is necessary to allow the firewall to determine which URLs should allow third party submissions, and which should not.

One advantage of firewalls over other measures embedded directly in the application logic is that they isolate the security concern and make it a unified manageable entity. However, modularity aside, there are several major disadvantages to application firewalls as a comprehensive solution to generic Web vulnerabilities.

The complexity and the size of the configuration effort necessary to successfully protect an application are enormous. Even if correctly configured, the firewall will need constant maintenance to keep up with the evolution of the application. Furthermore, configuring an application firewall is a new skill that must be mastered by the implementing developers before any confidence in the protection can be rendered.

Scanners

Because these vulnerabilities are so generic, it is easy to write scripts and applications that automate their exploitation. This is a huge advantage for attackers, because it allows them to find vulnerable sites quickly and in a large scale.

Recently, developers have been empowered with the same capabilities. Code scanners and site scanners able to check code and site functionality have been created, searching for potentially unsafe operations and flagging them. These tools can help ensure that the application logic is protected from the most easily executed exploits.

Scanners are significantly more effective then the tools being used by malicious users because they are capable of reviewing the source code, rather than just the output. Because there are so many ways to accomplish the same thing in any programming language, scanners are not entirely perfect. There are some unsafe operations that a scanner will not pick up.

Web Application Frameworks

An ideal solution would understand the context of the application, while still extracting security concerns like output validation and CSRF protection. Such a solution could potentially eliminate these threats entirely, with minimal effort or configuration on the developer's part. The challenge is finding a way to provide the necessary insight without being embedded directly in the application logic.

A new direction in Web applications may help address this need. More and more applications are starting to adopt frameworks that help abstract many of the common and repetitive tasks involved in creating and deploying a Web application. The breadth of the feature set differs drastically depending on which type of framework and vendor is chosen, but the idea is the same - they encapsulate common concerns such as session management, persistence, logging, and user interface generation. Some frameworks can be used in combination to solve different aspects of web application development. For example, an application might use JBoss to serve the application, handle sessions and manage database connections. The same application might use the Dojo framework to create the user interface.

These frameworks are in a unique position to help address generic security vulnerabilities. They reside at a layer in the application where context is still available, but is completely abstracted from the actual application logic. If security measures are embedded at the framework layer, then there is an opportunity to achieve the same modularity provided by an application firewall. As long as the framework is updated to address new security vulnerabilities, the application can remain secure, and relatively untouched.

For example, if an application utilized a framework such as Dojo to fully replace their current user interface, then the Dojo framework would be the ideal place to implement output validation. This is because the framework knows the difference between the HTML that makes up a component such as Button, and the data being used in the component, such as the label. It could safely apply output validation to the label, while leaving the rest of the HTML alone.

Most frameworks are not taking advantage of the fact that they are in the perfect position to address the growing end user security problem. Many continue to focus on locking down the server and protecting Web services, but rarely attempt to handle problems such as XSS. As a result, developers must still carry the full burden of securing the client. This is likely to change in the future, as more and more Web applications built on these technologies suffer from costly attacks.

The solution

There is no perfect solution that will address every security concern. Strong programming practices and quality code is the fundamental core of security, but is not the complete answer. Each of the discussed solutions has advantages against some exploits, while disadvantages against others. The combine use of multiple solutions should achieve the highest degree of security, and provide multiple safety nets in case one of them is unable to stop a new threat. Code scanners can be used to catch vulnerabilities during active development, frameworks to protect against generic server and client vulnerabilities, and application firewalls to protect against protocol vulnerabilities.

This may seem like a lot of effort required to protect the application, but there are some good prospects on the horizon. Browser vendors are starting to consider adding extra protection mechanisms to the browser, allowing applications to more tightly control their environments. Such protection would include the ability to block all inline script, as well as blocking external script references. While this will not solve everyone's needs, it should go a long way in advancing the general security of many Web applications.

Kyle Adams is an undergraduate at the Rochester Institute of Technology, earning a Bachelor Degree in Computer Science with a minor in Criminal Justice. He started hacking at age 10, and was writing his own encryption software by age 14. As the lead software architect for Mykonos (www.mykonossoftware.com), Kyle has final responsibility for code quality and technical excellence.

BruCON 2009

18 September-19 September 2009

www.brucon.org

Gov IT Summit 2009

21 September-22 September 2009

www.endeavourevents.com

Gartner Information Security Summit 2009 UK

21 September-22 September 2009

www.gartner.com/it/page.jsp?id=787512

ICDF2C 2009: The 1st International ICST Conference on Digital Forensics & Cyber Crime

30 September-2 October 2009

www.d-forensics.org

InfoProtect Summit 2009

5 October-6 October 2009

www.endeavourevents.com

HITBSecConf2009 Malaysia

5 October-8 October 2009

conference.hitb.org/hitbsecconf2009kl

IT Showcase Asia 2009

6 October-7 October 2009

www.jfpsgroup.com.cn/itshowcaseasia

SC World Congress 2009

13 October-14 October 2009

www.scworldcongress.com

RSA Conference Europe 2009

20 October-22 October 2009

www.net-security.org/rsaconference2009

CSI 2009

24 October-30 October 2009

www.csiannual.com

23rd Large Installation System Administration Conference (LISA '09)

1 November-6 November 2009

www.usenix.org/events/lisa09/

Securitybyte & OWASP AppSec Asia Conference 2009

17 November-20 November 2009

www.securitybyte.org

Step by Step - Digital Forensics & Cyber Crime Masterclass

19 November 2009

bit.ly/PQOVk

SECUTEC 2009

19 November-21 November 2009

www.secutec.in

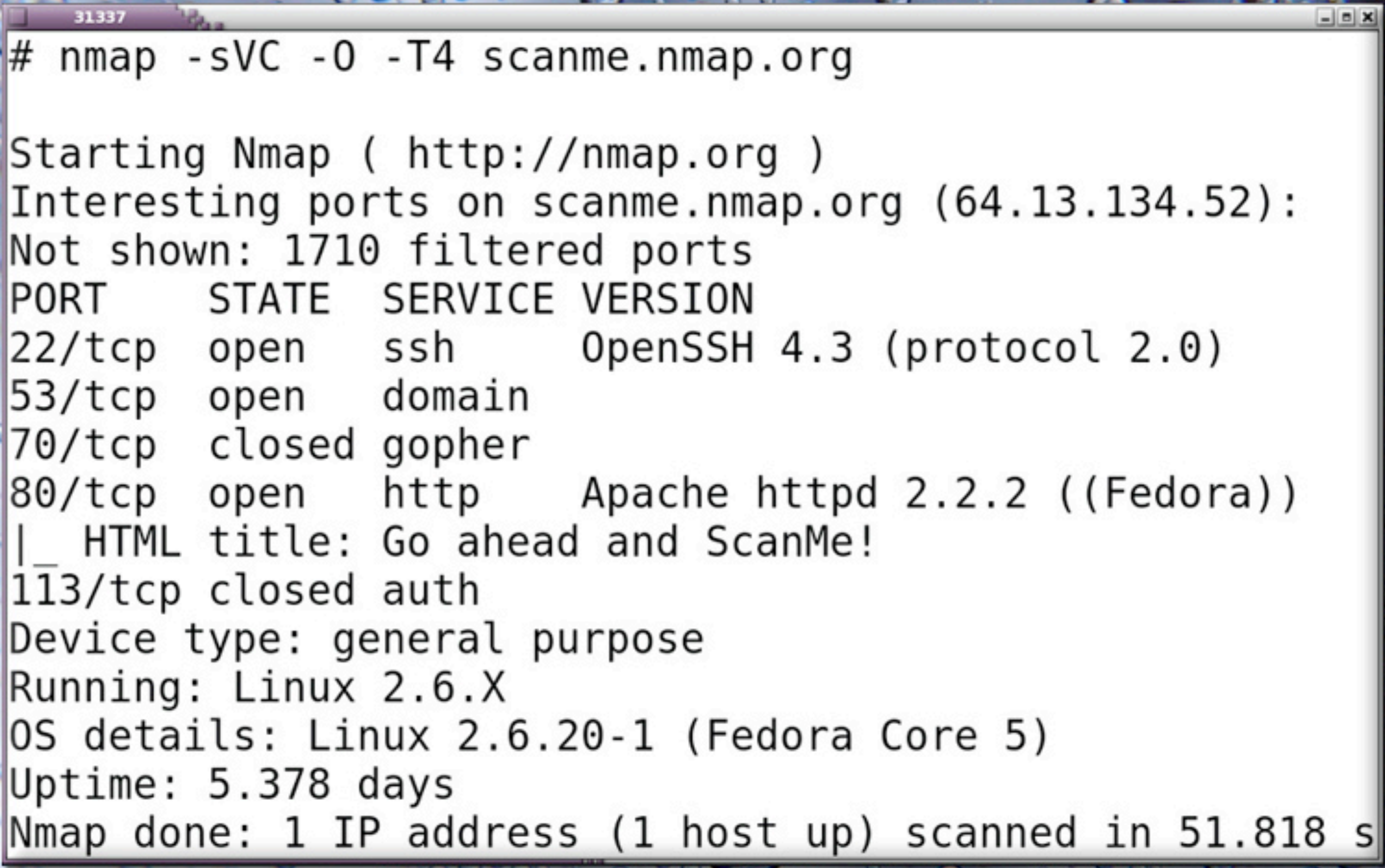
IBWAS09

iBWAS - 10 December-11 December 2009

www.ibwas.com

If you'd like us to feature your event on Help Net Security e-mail Berislav Kucan at bkucan@net-security.org for details.

Nmap is a free and open source utility for network exploration or security auditing.



```
# nmap -sVC -O -T4 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 1710 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 4.3 (protocol 2.0)
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Go ahead and ScanMe!
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 5.378 days
Nmap done: 1 IP address (1 host up) scanned in 51.818 s
```

Nmap was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are avalable for Linux, Windows, and Mac OS X.

Go to www.nmap.org to get your copy.

In mashups we trust?

by Erhan J. Kartaltepe

In art, a pastiche is a creative piece consisting entirely, or nearly entirely, of motifs or techniques from one or more sources. Many musical compositions, such as choral masses from the Baroque and Romantic era, were pastiches, comprised of movements of different composers. The postmodern art movement of the twentieth century employed pastiches in its paintings and sculptures, combining styles from previous works and other artists.

At its core, a mashup is a web application that combines data from two or more external sources to create a new service. Mashups are simply pastiches for the twenty-first century. A web application that displayed the coffee shops from an online directory on a map generated by a web mapping service is a definitely a mashup, albeit a trivial one.

However, unlike in art and literature, web application mashups must be secure. A coffee/map mashup like the above that also retrieved appointments from one's online calendar and suggested a close location to the person you were to meet is much more sophisticated, but also introduces security concerns such as authentication, authorization, and privacy.

While the map and coffee shops are publicly available data, one's calendar and contact details certainly are not. Imagine if the application could also suggest a coffee purchase based on your checking account balance! These issues of trust are something the artists of yore never had to deal with, but exist on the forefront of the minds of customers, businesses, and developers the world over.

The mashup consensus

Mashups are an incredibly popular programming paradigm. Gartner Group recently released a report (bit.ly/zYybX) that listed mashups as the web technology to watch: "By 2010, Web mashups will be the dominant model (80 percent) for the creation of composite enterprise applications. Mashup technologies will evolve significantly over the next five years, and application leaders must take this evolution into account when evaluating the impact of mashups and in formulating an enterprise mashup strategy." Its competitor Forrester Research notes in a similar study (bit.ly/MTixu) that mashups are growing and "will mature and eat into other major markets". Douglas Crockford, senior JavaScript architect at Yahoo and arguably the foremost expert on JavaScript and the writer of the JSON specification, stated in a recent talk (bit.ly/l3y1w) that "Mashups are the most interesting innovation in software development in twenty years."

With all this positive buzz, it seems wondrous that we are not as well versed in mashups as we are in any other web application. Alas, these selfsame experts are of two minds about mashups. After all, in the "The Creative and Secure World of Web 2.0" report, Gartner argued that "the potential for security risks increases as more business users morph into application developers by building mashups." A KPMG survey of 472 executives found that half of them viewed security problems as a limiting factor in the uptake of tools such as mashups and other web 2.0 tools in the enterprise. The same Douglas Crockford that was a fan of mashups as a powerful innovation, flatly states "Mashups are insecure. Mashups must not have access to any confidential information or any privileged connections to any servers. Until this is fixed, mashups are constrained to only trivial applications."

Thus, not only are experts in the field divided on the topic, but each group of experts is itself of two minds, conflicted with the power and flexibility of mashups on one hand and its lack of a fundamental security model on the other. Without a secure trust paradigm, mashups simply will not be deployed in the real world, and will be limited to toy applications only.

Business-to-business security

Servers across the Internet are littered with crossdomain.xml files to protect the user from malicious sites, SSL certificates identify the business the consumer is dealing with before any transaction is made, and the same-origin policy that prevented earlier incarnations of mashups also protected users from cross-site attacks. Business-to-business security in web applications is muddled by the fact that there is always a man-in-the-middle (MITM)—the user's browser.

In a consumer-to-business scenario, a consumer almost never requires an SSL authentication, but in business-to-business model, this is always required. Unfortunately, SSL was carefully designed to be a two-party protocol, but mashups involve at least three parties by their very nature—a browser, and two or more web applications. Moreover, SSL operates at the transport layer and thus is point-to-point and cannot go from one business to the other "through" the browser. Thus, mashups in all their incarnations, suffer from an authentication problem, but depending on the mashup type, attempt to mitigate this damage in different ways.

Classical server-side and client-side mashups

Consider one version of a mashup: All Politics Footage operates a site that provides video clips of politicians and candidates giving speeches. Its business model is to sell to other companies, such as news organizations and poll trackers. When Alice visits NewsNow and views a video that is served by All Politics Footage, her browser makes a request to the latter site. How does All Politics Footage decide whether to grant Alice access? That is, how does All Politics Footage know Alice came from NewsNow?

Keeping an access control list (ACL) of all partner sites and check the browser's origin header against it wouldn't work because it's so easy to spoof. Maintaining user identity and authenticating the user directly or through some federation protocol forces All Politics Footage to collect, maintain, and protect unnecessary user information and forces a user to create such an account. Implementing a proprietary cryptographic ticketing protocol with other companies to ensure Alice correctly arrives at the site requesting a service might work, but would rely on using a protocol that may not have been standardized and has not stood the test of time. Of course, this will require another set of credentials to manage.

This problem seems to scream for SSL, but the MITM that is the browser prevents its use, since SSL is point-to-point (and sadly, three points—business to user to business—do not make a line in this instance) and operates at the transport layer.

Worse, companies can become victims of their own popularity. If both companies' services are often used, it's likely that they are performing a similar mashup for many users. Thus, NewsNow must re-authenticate itself to All Politics Footage every time, and All Politics Footage would have to verify the credentials for each instance of the mashup. Depending on the authentication mechanism used, the performance overhead could be non-negligible for practical use.

The sandbox

Enterprise mashups have a different appeal and a different set of security issues. Their allure is the promise of faster development and deployment. To a security analyst working for that enterprise, a mashup is an entry point for external and unreviewed code into internal applications, an exit point for sensitive corporate information, and a new way to compromise the desktop.

The general response to this is to sandbox the mashup to mitigate the risk. The OpenAJAX hub specification augmented by IBM's SMash technology to police inter-widget communication does just that. This approach mirrors securing a computer from viruses or other malware, with the browser acting as the operating system. Microsoft's MashupOS hews to this metaphor more closely.

There are some issues with this method. The trade-off between functionality and security is a classic security problem, of course, and increasing one can lead to a decrease in the other.

THE TRADE-OFF BETWEEN FUNCTIONALITY AND SECURITY IS A CLASSIC SECURITY PROBLEM, OF COURSE, AND INCREASING ONE CAN LEAD TO A DECREASE IN THE OTHER

A broader limitation is that it is very hard to keep up with the Joneses, i.e., malicious code. To visit the operating system metaphor once more, Mark Bregman, CTO of Symantec, argues in an instructive article (bit.ly/4CCr8m) that whitelists may become essential and that "reputation based systems" may be in our future. Due to the dynamic nature of the code running within a widget, collecting signatures of all allowed widgets will be a difficult situation, although strongly authenticating the source from which the widget is being downloaded allows the enterprise to build more trust. Short of turning on client-side authentication and requiring users to purchase SSL certificates (the prospects of which are dubious, to say the least), the MITM that is the browser cannot be trusted and prevents one domain from authenticating another while in the sandbox.

Identity protocols

A third breed of mashups, the identity federation protocol such as OpenID or SAML, have a unique set of security concerns. They usually adhere to the following model: Alice attempts to access the relying party (RP); the RP redirects to the identity provider (IP) and asks if Alice is who she says she is; the IP authenticates Alice; and the IP redirects back to the RP, providing an assertion about Alice's identity.

Naturally, these protocols are vulnerable to phishing attacks precipitated by an active or passive MITM attack. If a MITM exists between the user and the IP or RP, then using SSL at least makes sure the browser "knows" who is at each end. Yet, the IP and RP are not able to "look behind the browser" (as the user cannot be trusted) and verify the identity of the server.

A key observation is that federation protocols like OpenID (or even OAuth to a degree) increase a user's comfort level in being asked for their IP credentials often or in being redirected from one domain to another, making these attacks more likely.

The case for authentication

The reader may have heard about the recent OAuth security hole (bit.ly/4jETsZ) that was susceptible to MITM attacks. To its credit, the OAuth specification is easy to read and simple to implement, and any cryptographic standard worth its salt (no pun intended) takes years and years to mature.

As an example, SSL was first developed in 1993, and cryptographers are still improving it a decade and a half later! Yet no one would argue that SSL is not a secure or well-thought-out spec. Having said that, the fundamental issue is that one organization cannot authenticate another behind the browser, a problem one often encounters when discussing non-trivial mashup applications.

The ideal solution might be to use some “multi-party” version of SSL running in the application layer. From an OAuth-centric standpoint, this version of SSL would run between the consumer and the service provider through the user's browser (using standard SSL certificates for each server; no certificate on the browser should be needed or expected) in the application layer. The OAuth credential type could then be set to "PLAINTEXT" since all the OAuth messages would be encrypted with the SSL "master secret" (the session key the two parties share at end of any SSL session).

This would be a very clean cryptographic solution because, except for the first go-round which involves public key operations, all subsequent sessions use the SSL abbreviated handshake, which is very efficient and only uses symmetric key crypto. The session fixation attack (bit.ly/BOj4I) would not work as the Service Provider won't operate with a site with which it cannot establish or share an SSL session. So when the "good" URL is moved to "bad" site (as in this OAuth vulnerability), the attack is detected and stopped.

EXPERTS AGREE: MASHUPS ARE TOO POWERFUL TO AVOID BUT TOO DANGEROUS TO USE

Everything old is new again

Experts agree: mashups are too powerful to avoid but too dangerous to use. This is a common proclamation in the world of innovation. Of course, the birth of the Internet itself was just as conflicted, yet now we think nothing of sending our credit card information over the wire. Just as a two-party transport layer security protocol made such an idea possible, a true multi-party trust protocol that provides for mutual authentication and key distribution is needed before mashups of any paradigm, whether they be server-side or client-side, identity federation or hub-and-widget, or something new entirely, become mainstream.

Erhan J. Kartaltepe is the associate director of the Institute for Cyber Security (blog.ics.utsa.edu) at the University of Texas at San Antonio, with nearly a decade’s experience in secure software engineering, applied cryptography, and technical leadership. While at the Institute for Cyber Security, Erhan served as chief architect on the Institute’s Incubator project, whose most recent idea was recognized as a “Most Innovative Company at RSA Conference 2009” finalist. He also architected a suite of software for multi-party, application-level SSL geared toward the facilitation of secure mashups.

Adopting the security best practice of least privilege

by John Moyer

Adopting the principle of least privilege is a critical objective for virtually every organization. This article provides a fundamental understanding of the concept and describes the different motivations organizations have for implementing least privilege. Whether driven by security concerns, business needs or mandated by compliance regulations, all organizations must also overcome similar hurdles before they can implement a least privilege environment. This article will also examine these challenges and recommend solutions to overcome them.

Introduction to the principle practice of least privilege

The principle of least privilege was first created by the Department of Defense in the 1970s as a security best practice to limit the damage that can result from a security breach or malicious user. According to the principle, people should only be granted the most restrictive set of privileges necessary for the performance of their authorized tasks. Even though its roots date back more than 30 years, the message is even more important in today's digital economy, and further in networks dominated by the Windows operating system. The Department of Defense defines the principle of least privilege in the Trusted Computer System Evaluation Criteria, frequently referred to as the Orange Book, as follows:

"Least privilege - This principle requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use."[1]

[1] Department of Defense. (1985). Department of Defense Trust Computer System Evaluation Criteria. DoD 5200.28-STD Library No. S225,711.

In a least privilege computing environment, users have the privileges necessary to perform their duties only when they need them.

Anytime a user is granted privileges that go beyond what is required for a specific task, that user's computing environment, and the network they are on, are put at risk. In a Microsoft Windows environment, many people log in to their computers with administrative privileges and run all software with the highest level of privileges. This is a clear violation of the principle.

The benefits of eliminating administrator rights

When users log into their computers with local administrator rights, there are two main classes of problems. First, when surfing the Internet or reading email with administrative privileges, users are much more vulnerable to malware infections. Another issue is that users are able to make unauthorized changes to the system configuration. By removing administrator rights and implementing the security best practice of least privilege, these issues can be avoided and network security increased.

This is not only a security issue, but a cost issue as well. In a least privilege computing environment, the costs of reconfiguring computers and supporting computers that are not configured correctly are reduced, since users do not have the power to install whatever they want on their computer, reconfigure security settings or turn off anti-virus software.

ANYTIME A USER IS GRANTED PRIVILEGES THAT GO BEYOND WHAT IS REQUIRED FOR A SPECIFIC TASK, THAT USER'S COMPUTING ENVIRONMENT, AND THE NETWORK THEY ARE ON, ARE PUT AT RISK

Fulfilling compliance mandates by implementing least privilege

In addition to the operational and security benefits, implementing least privilege assists with an organization's ability to maintain industry and regulatory compliance.

Virtually all organizations fall under some form of regulation—the Sarbanes-Oxley Act (SOX) for corporations, the Health Insurance Portability and Accountability Act (HIPAA) for medical organizations, the Gramm-Leach-Bliley Act (GLBA) for banking institutions, Payment Card Industry Data Security Standard (PCI DSS) for businesses that handle payment card information, and the Federal Desktop Core Configuration (FDCC) mandate for federal entities, among others.

Though each regulation is unique in the text of its requirements, all require some form of technical control that ensure the safety and security of sensitive data in the environment.

Without going into the individual requirements of each regulation, the following benefits of least privilege relate to the fulfillment of each. By controlling and effectively logging user and administrator activities, the fulfillment of compliance regulation requirements can be assured. For example:

- ***Logging of user activities can be assured.*** The native logging systems within the Windows OS suffer from the limitation that any administrative user can clear the logs at will. This limitation means that a user with administrative access can clear any record of their activities, if desired. With the assurance of activity logging, a primary requirement of virtually all compliance regulations, preventing log erasure is a key necessity for the secure and compliant IT environment.

- ***Data access can be protected.*** Virtually all corporate data must be accessed through some form of application. When the access to that application has been elevated through the assignment of administrative privileges, the user may have the ability to leverage that access for other unauthorized purposes. Conversely, when granular privileges are assigned based on individual activities, the likelihood of data breech is reduced, due to a reduction in the count of potential activities that can be accomplished by the user.

Least privilege increases protection from malware and mitigates vulnerabilities

Due to the early success of antivirus products, many companies previously felt that antivirus products alone provided them with sufficient protection from malware. Only recently have people recognized the shortcomings of signature-based antivirus software and the need for better layered protection from malware. McAfee Avert Labs has published some interesting statistics, illustrating that there are over 500 new detections made per business day. As a result, it is made clear that it is virtually impossible for antivirus products to catch all viruses and their variants. Adopting a least privilege environment and removing administrator rights, however, will reduce the malware attack surface and prevent most installations of malware without identifying any signatures.

There is a clear difference between the level of risk of malware infection for a typical user versus a user with administrator rights. If you compare two identical machines, where only a user's group membership is varied, and the same Web sites are visited in an effort to install various types of viruses and spyware bundlers, the difference is staggering. On the machine with only standard user privileges, virtually none of the malware installs. And on the system that is operated by a user with administrative privileges, it is likely that you will find a tremendous amount of viruses and malware that have installed themselves.

In 2008, Microsoft published nearly 80 security bulletins documenting and providing patches for over 150 vulnerabilities. As every IT admin knows, vulnerabilities take time to identify and patches take time to apply. During this period, threats can damage a corporate network and it is important that companies reduce the severity or prevent the exploitation of undiscovered or unpatched vulnerabilities.

In fact, examination of all vulnerabilities documented by Microsoft in Security Bulletins issued in 2008, revealed that configuring users to operate without administrator rights enables organizations to mitigate the effects of 92% of critical Microsoft vulnerabilities. Furthermore, by removing administrator rights, companies will harden their endpoint security against the exploitation of 94% of Microsoft Office, 89% of Internet Explorer and 53% of Microsoft Windows vulnerabilities. Of the total published vulnerabilities, 69% are mitigated by removing administrator rights.

Application compatibility remains the greatest obstacle to least privilege adoption

While least privilege may seem like a simple model, organizations have struggled to remove administrator rights and implement it because of the number of activities users must do for their jobs that require elevated privileges. The greatest challenge organizations face is with applications that require administrative privileges to operate correctly. Some of these applications will be business critical applications and rebuilding the application or finding an alternative solution will not be feasible.

Additionally, there are other activities users need to perform that also require administrator rights, such as self-managing some system settings and installing authorized software and ActiveX controls.

In an effective and productive least privilege environment, an organization must be able to granularly define the privileges necessary for specific activities, such as running an authorized application that requires elevated privileges. When someone is not performing the authorized activity, the elevated privileges will not be available. Unfortunately, the Microsoft Windows OS alone does not natively provide the architecture to enable this granular control. Organizations should consider the use of third-party solutions that extend the granularity of privileges assignment. Such tools enable privileges to be assigned to applications based on user roles, adding that necessary granularity.

Windows User Account Control is not a solution to implementing least privilege

The inclusion of User Account Control (UAC) in Windows Vista and Windows 7 is helping to increase the adoption of least privilege. The goal of UAC is to allow all users to operate their PCs with non-administrative privileges when they are not required. This is an important move for Microsoft and validates the seriousness of the security threat posed by running with elevated privileges.

With UAC, there are only two types of users: protected administrators and standard users. The only difference is membership in the local administrators group. UAC takes effect when a user attempts to do something that requires elevated privileges. When a protected administrator attempts to perform a task that requires administrative privileges, he or she may be prompted to consent to running the application. When a standard user attempts to perform a task that requires elevation, a prompt asks for the local administrator username and password.

An important implication is that if standard users need to run applications or execute processes that require elevation, then the user must acquire and use an administrator account and password with its inherent administrative privileges. With the local administrator password, a standard user can perform any administrative function. This will allow a user to circumvent security policies inadvertently or maliciously, and run or install applications – including malware – as an administrator. There is also nothing to prevent a user from sharing the password with other coworkers.

With UAC, administrative credentials are assigned or given to an individual to allow them to perform activities that require elevated privileges. Once they are assigned, the individual has what amounts to full control over the entire computer. Privileges with UAC cannot be granularly assigned to enable usage for a specified activity or application. This limits its utility as a solution for enabling a least privilege environment.

PRIOR TO REMOVING ADMINISTRATOR RIGHTS AND IMPLEMENTING LEAST PRIVILEGE, AN ENTERPRISE MUST FIRST IDENTIFY THE ACTIVITIES EMPLOYEES NEED TO DO IN ORDER TO COMPLETE THEIR JOBS THAT REQUIRE ADMINISTRATIVE PRIVILEGES

Implementing least privilege in the real world

Prior to removing administrator rights and implementing least privilege, an enterprise must first identify the activities employees need to do in order to complete their jobs that require administrative privileges. As we've mentioned, these activities could include connecting to a local printer, running certain applications or installing software. A company needs to have a plan in place in order to address these user needs.

The second step for an enterprise is to create a pilot group composed of the first employees to no longer log in as administrators. This will allow the IT staff to confirm they have put the correct measures in place to ensure that user productivity will not be affected.

When a company eliminates administrator rights, it cannot simply tell an employee that they can no longer use an application that is critical for the job. If an enterprise has not properly planned for a mechanism to allow users to continue to do the work they need to do, there will be complaints and it will require the IT staff to spend a lot of time addressing the problems that arise. There is good news; third-party solutions currently exist that allow standard users to continue to run the applications, system tasks and ActiveX controls needed for their jobs.

The U.S. Federal Government adopts least privilege

The push to create standard desktop configurations is making more people aware of the value of least privilege. A standard desktop configuration enhances network security by establishing uniform security settings and facilitating faster application of security patches. It also reduces the cost of administrating desktops. Standard desktop configuration projects must restrict administrator rights on all computers to maintain the standard configurations because it's impossible to control how users will inadvertently or intentionally change the configuration of their computers when they are administrators. In other words, you can set a standard security configuration but if users log in as administrators, they or malicious software can change whatever they want.

As of February 2008, all Federal agencies must now comply with standard Windows XP and Vista security configurations, based on the Federal Desktop Core Configuration (FDCC) mandate from the U.S. Government, which requires agencies to restrict administrator rights on all PCs. Implementing the FDCC not only improves security, but also results in significant IT cost savings. It is much easier to support computers and test new patches if you have a standardized environment and do not need to investigate many different configurations. With the entire federal government adopting a least privilege security approach, the rest of corporate world won't be far behind.

Implementing least privilege is a prudent move for any organization

Whether driven by security concerns, business needs or mandated by compliance regulations, applying the principle of least privilege is a prudent move for organizations. Eliminating administrator rights protects against zero-day exploits, prevents unauthorized malicious use and will increase productivity and compliance when correctly implemented.

Unfortunately, organizations must often overcome hurdles before they can implement a least privilege environment. Companies must ensure that users can still run applications and perform tasks that their jobs require. Any implementation that results in a decrease in productivity will be quickly rejected.

A variety of solutions for implementing least privilege are now in common use. While some of these solutions are more secure and easier to implement than others, all of them are preferable to an environment with no attempt to adhere to the principle of least privilege.

John Moyer is the President and CEO of BeyondTrust (www.beyondtrust.com). Moyer holds a M.B.A. from Carnegie Mellon University and a B.S. in Engineering from Rensselaer Polytechnic Institute. His numerous accomplishments include the CMU award for "Entrepreneur of the Year" in 1998. Previously Moyer held management positions at General Electric and was an associate in Ernst & Young's business consulting unit.

Is your data recovery provider a data security problem?

by Michael Hall

Today's IT security professionals enforce aggressive enterprise-wide security programs to minimize the risk of data leakage and a security breach. But, what happens when a hard drive fails (and, at some point, they all do) and it must leave the confines of the company's secure environment for data recovery? Who monitors the security protocols of data recovery service providers?

The unfortunate truth is that security protocols used by third-party data recovery vendors are not on the radar of either the IT security team or the IT support organization. Location or low pricing typically trumps data security during the vendor selection process.

Data loss must be a consideration anywhere personal and confidential data can be accessed. If your data recovery service provider's network is hacked, and confidential customer data is accessed, your company could be liable. To close the gap in security when a hard drive is out for data recovery, data protection policies and systems used by third-party data recovery vendors should be scrutinized carefully.

Data recovery is an invaluable service to users who cannot afford to be without their digital data for any period of time. It is also an industry that has grown exponentially since the introduction of the world's first hard drive. Twenty years ago, there were only a handful of companies that could provide this service reliably. Today, a search on the Internet under the term "data recovery" generates over 50 million results. Who among the 50 million are truly qualified to handle confidential data appropriately?

Among the handful of companies that pioneered the Data Recovery Industry twenty years ago, a few underwent security audits that cleared them to offer High Security Service to government agencies and branches of the military. In recent years, greater demands for data security began to rise from the corporate market segment and only one company continued to adopt new data privacy and protection protocols to meet them.

Not all data recovery companies are created equal

A 2008 Ponemon Institute benchmark study on the costs of data breach revealed this disturbing fact: 44 percent of the breaches experienced by U.S. companies occurred when third-party vendors were in possession of their data. Incidents of third-party breaches have risen steadily over the past four years and cost more than breaches by the enterprise itself.

Security breaches involving electronic data have come to light largely as a result of the California Security Breach Notification Act, which went into effect in 2003. Since then, numerous data security bills have been introduced in the 109th Congress.

Regulations in 44 states, the District of Columbia, Puerto Rico and the Virgin Islands require that individuals be notified when a breach of protected personal information occurs and their confidential or personal data has been lost, stolen, or compromised. Both the U.S. Senate and House of Representatives continue to evaluate federal laws regarding data privacy and breach notification.

Considering the rise in third-party incidents of data breach, and increasing regulations that place the blame of data loss squarely on the enterprise, IT security professionals must put data recovery service providers on their radar when assessing potential security breach pitfalls. A single third-party security breach could diminish a company's business reputation, customer loyalty, and ultimately their profitability.

New security standards for data recovery service providers

In 2007, DriveSavers published data security standards for the Data Recovery Industry. Many InfoSec professionals from Fortune 100 companies have incorporated these protocols within their own supplier/contractor security standards, and use them as guidelines during the vendor selection process.

Ask if your data recovery service provider adheres to these new standards:

1. Service provider's information technology controls and processes have been audited by accounting, auditing and information security professionals, and verified to be operating effectively to provide maximum data security.

Demonstrates compliance with auditing standards, such as the Statement on Auditing Standards (SAS) 70. Assures that every aspect of the facility and network is secure and suitable to protect personal and confidential data from being compromised.

Certified, control-oriented professionals, who have experience in accounting, auditing and information security, conduct an audit of the service provider's data hosting control objectives, activities and related processes over a period of time (typically 6-12 months).

The audit focuses on identifying and validating control standards that are deemed most critical to existing and prospective clients of the service provider, and covers all aspects of security in the facility; both network and physical.

Since the introduction of the 2002 Sarbanes Oxley Act (Section 404) following the Enron debacle, the SAS 70 audit has become the Corporate Industry Standard for an overall control structure.

SAS 70 Type I audit verifies the "description" of controls and safeguards that a service organization claims to have in place. The SAS 70 Type II audit verifies that all data hosting controls and objectives are actually in place, suitably designed, enforced, and operating effectively to achieve all desired security control objectives.

2. Network security testing and monitoring are integrated into the service provider's security program. Critical systems, (e.g., firewalls, routers, servers) are configured, maintained, and certified to be operating according to the organization's security policy.

A professional data recovery provider temporarily archives recovered data on their network until the customer has received it and verified its integrity. The need for strong, verifiable security measures is necessary to protect network assets, employee endpoints, and sensitive customer data, such as e-mail servers, databases, and proprietary information. Every element of the provider's network should act as a point of defense. It must feature innovative behavioral methods that will automatically recognize and adapt to new types of threats as they arise.

Best in breed network security solutions allow for rapid response to emerging threats such as malware propagation spread by e-mail, SPAM, and botnets; phishing attacks hosted on websites; attacks targeting increasing extensible markup language (XML) traffic; service-oriented architecture (SOA); web services; and zero-day attacks that occur before antivirus companies have developed new virus signatures to combat them.

A comprehensive "defense-in-depth" approach to network security should, at minimum, include the following:

• Regular vulnerability assessments, penetration testing, and related reports
• Management of the network firewall, including monitoring, maintaining the firewall's traffic routing rules, and generating regular traffic and management reports
• Intrusion detection management, either at the network level or at the individual host level, intrusion alerts, keeping up-to-date with new defenses against intrusion, and regular reports on intrusion attempts and activity
• Mitigation support after an intrusion has occurred, including emergency response and forensic analysis
• Content filtering services, for electronic mail (i.e. email filtering) and other traffic
• Data archival.

3. Service provider is cleared to offer High Security Service that meets U.S. Government standards.

Government agencies, law enforcement bureaus, and other legal entities in the U.S. and abroad require third-party service providers to comply with the most stringent security standards and chain-of-custody protocols.

A professional data recovery service provider can provide documentation upon request that demonstrates how data is protected from point-of-receipt at the facility, to point-of-departure.

All of the data recovery service providers' employees have undergone background checks, a tamper proof/resistant-shipping container is provided to the customer to protect the damaged storage device during transport, and a government-approved courier is used to ship the device to the service provider.

Chain-of-custody protocols should include:
• Use of a government-approved courier service
• Barcode on storage device is scanned upon receipt by data recovery provider
• Serial number is checked against information in customer record
• Date/time and name of employee who received the device is logged into customer record
• Customer is provided with notification that the device has been received, and data recovery process has begun
• Dates/times/and personnel handling the device are logged into the customer record as the device moves through the data recovery process.

Certain data loss situations require extra security procedures. The protocols for High Security Service include all of the above procedures, in addition to the following:

• Chief Information Security Officer available on site to receive the drive and customize security levels beyond those routinely provided
• Non-disclosure agreements are signed and chain-of-custody documentation is provided
• The data recovery is given top priority throughout the entire process and performed in a secure area, on a stand-alone system running only when an authorized engineer is present and monitoring the job
• Only approved personnel with proper access cards are allowed access to the area where the recovery is performed
• Custom solutions for data recovery on encrypted drives can be provided
• Data set is always stored in a DOD-approved safe Class 5 Mosler Safe during non-working hours
• Two separate copies of recovered data are shipped to the customer via two different

courier services
- Secure, encrypted electronic data transfer service is available, if required
- No copy of the data is kept on site after the recovery is complete.

4. Data recovery engineers have been trained and certified by leading encryption software vendors to properly recover data from encrypted files and drives.

In June of 2006, a Presidential mandate required all federal agencies and departments to encrypt data stored on their mobile computers and devices to mitigate the impact of lost or stolen data that could be used to distinguish or trace an individual's identity. The U.S. General Services Administration (GSA) then awarded Data-at-Rest encryption contracts to leading encryption software companies who were contracted to protect sensitive, unclassified data residing on government laptops, mobile computing devices and removable storage media devices. Data-at-Rest refers to any data residing on hard drives, thumb drives, laptops, etc.

There are hundreds of encryption tools out there and each one is unique. The professional recovery service provider has documentation that technicians have been trained by leading encryption software vendors, and are certified experts in multiple encryption recovery techniques. The provider can offer customized data recovery solutions that will meet stringent data security requirements when handling encrypted files and drives:

- Data is restored in an image-only format. Drive is returned with original encryption still intact
- Data is restored and decrypted at recovery facility to verify integrity of data. Data is returned encrypted or fully decrypted. Encryption username, password and/or key must be provided if this method is chosen
- Engineers are trained in proper handling of encryption keys
- A secure, encrypted electronic data transfer service is available upon request.

5. The service provider offers secure and permanent erasure of sensitive data, when requested.

Deleting files, emptying the recycle bin, or quick formatting a hard drive does not permanently delete data, it simply removes the information the hard drive needs to find the data, allowing it to be recovered. A wiping or erasing utility can be used to overwrite every sector of the hard drive with a pattern of binary 1's and 0's. A degausser approved by the National Security Agency, Department of Defense, the Central Security Service, and meets HIPAA and GLB Act privacy requirements is the best method to permanently erase classified or sensitive digital data stored on magnetic media.

Choose a data recovery service provider that is compliant with data security regulations

Government regulations and industry compliance statutes for security controls and data privacy, such as the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley Act (GLBA) were created to protect personal and confidential data from unwanted breach and inappropriate use.

Leading enterprise IT managers and industry analysts are reinforcing the message that corporations must closely evaluate the data protection policies used with by third-party vendors. When a hard drive has crashed and professional data recovery is required, IT security and support professionals should choose a third-party service provider that can quickly and cost-effectively restore business critical data, and is verified to be in compliance with data protection and privacy regulations. Doing so will help them protect critical data from being compromised during the recovery process—and avoid the penalties, financial losses, and customer loyalty risks associated with a breach in data security.

Michael Hall is the Chief Information Security Officer for High Security Programs and Director of PC Engineering at DriveSavers Data Recovery (www.drivesaversdatarecovery.com). With over 13 years experience in data recovery technology focusing on high-end RAID arrays, he has successfully recovered data from over 12,000 failed storage devices. Hall supports DriveSavers corporate and government accounts with security protocols designed to meet their criteria.

New strategies for establishing a comprehensive lifetime data protection program

by Kyle Parris

Whether driven by data security mandates and consumer privacy laws or trading partner requirements, IT directors across industries are investigating ways to protect confidential information from theft and misuse, wherever it resides and travels. As a result of the exponential growth in electronic information sharing, it's no surprise that as higher volumes of sensitive data are being exchanged there are many more opportunities for cyber criminals to steal it.

With data theft now happening even at the application level, there is no place inside or outside the enterprise where information is safe. The numerous criminal breaches—in addition to accidental losses—illustrate the importance of protecting information during its entire lifespan.

While most companies have established secure methods of using secure FTP or another secure protocol for exchanging business documents with trading partners, there is more that can and should be done to protect these files and other customer, employee and company confidential information. Today most enterprises use a jumble of file transfer options—FTP servers supporting isolated departmental activities, point-to-point connections such as AS2, email and more. End users struggle with ad hoc large file transfers and clog IT helpdesks. Every trading partner connection is a fire drill. As a result, many transfers are not secure - much less the data as it moves around internally or sits at rest. Fortunately, CSOs can develop a comprehensive data security program that protects the sensitive information entrusted to their organization from the time it's created or received until it's archived or deleted.

This article presents the key elements of a lifetime data protection program that provides 100 percent security during internal and external transmissions as well as for data at rest. If constructed properly, the program can also reduce overhead and costs, and make it much easier to manage B2B communities and comply with data security mandates and laws.

Step 1: Protect files in transit between trading partners and your enterprise

Simply put, there's more to protecting business files being sent between companies than establishing a secure pipe for transport (e.g. SFTP, FTP, AS2, HTTPS, secure portal) and/ or file encryption (e.g. PGP, PKCS8, 12, AES). A widely used and necessary practice, it ranges from simply encrypting a file for transport, sending an unencrypted file through a secure pipe, or both; or, even better, using a Managed File Transfer (MFT) solution to establish a B2B gateway.

But what happens once the file reaches your enterprise? In many cases, it hits the receiving server in the DMZ and is written to disk where it sits, susceptible to compromise. What's more, the enterprise is left vulnerable during the time the data is being moved from the DMZ to within the enterprise because an inbound hole has to be opened in the firewall momentarily.

A more secure approach is using an MFT solution that puts trading partner verification and authorization in the DMZ and prevents a company from needing to have inbound holes in their firewall, which can expose the network. In this case, the portion of the MFT solution behind the firewall opens an outbound hole in the inner firewall to receive incoming files into your enterprise. The MFT solution then receives the data and manages the movement between your business partners and your internal end points.

In addition to separating these responsibilities, another data security truth is that no data in motion should ever exist in clear text. This requires all communication channels to be encrypted. As soon as incoming files are written to a disk in the DMZ, they become data at rest and are no longer protected by the transfer protocols. This problem is easily solved by using a MFT solution that provides secure streaming so that no data ever touches the iron in the DMZ. Under this scenario, when files are streamed through the DMZ they continue to be protected using the same secure file transfer protocols and/or encryption they were sent with. Streaming files through the DMZ also has the added benefit of moving large files faster, since they are never "set down" and "picked back up." This is also beneficial for helping your company adapt to handle escalating file transfer volumes.

A final note on securing external file transfers: it is always wise to select an MFT solution that supports all secure protocols and encryption methods in order to maximize ease of interoperability with new trading partners.

Step 2: Protect files moving within your enterprise

If your friend wants to send you a snail mail letter, she would drop it in her mailbox. From there, the post office is responsible for picking it up, delivering it to a mail distribution center and then sending out to be delivered directly into your mailbox. You would simply walk out and retrieve the letter. But what if there were no home mailboxes? Your friend would have to drive to the nearest post office to mail the letter. The post office would then send the letter to the post office nearest your house. You would then have to drive to the post office to pick up the letter.

The second scenario is, in fact, how many MFT solutions handle file transport, while the more advanced MFT solutions treat file transfers like we're accustomed to with home mail delivery. This "intelligent routing" of transactions ensures that documents coming in from your trading partners are delivered directly to the intended end point, bypassing intermediate servers and remaining in their secure wrappers all the way to their final destination or multiple destinations. In order to be truly secure for the entire lifecycle of the file, they must stay protected from the time they leave your trading partner until they hit the designated application server.

Another benefit of intelligent routing is that application servers do not have to request files from an intermediate server where they may be sitting unprotected in clear text, unless you are using data protection application that automatically encrypts the files when they are writing to disk. This eliminates another layer of security management as well as the need for those servers to have an FTP client installed, scripts written to request and direct files, to be managed separately.

Intelligent routing also includes a way to chain these transactions together based on file characteristics allowing you to change the security methods such as from PGP to SSH, route a file to multiple application destinations, or even route the file based on the metadata of the file itself. For example, you can send a file to ADP and the finance department on two separate application servers. This means fewer places to manage it and fewer users to grant access to it, further reducing security risks.

Another capability that factors into internal file transfer security is the ability to handle secure ad hoc transfers. While MFT solutions should inherently handle scheduled and event-driven transfers securely, some fall short when it comes to ad hoc transfers—those that happen when an employee needs to send a file outside the parameters set for scheduled and event-driven transactions.

It's not unusual for an ad hoc file transfer to be unprotected simply because the employee doesn't know it needs to be secured, forgets to secure it or simply doesn't want to take the time to figure out how to send a file securely. Making it easy for employees to send files securely themselves between departments or to trading partners closes another security loophole while reducing IT helpdesk requests.

While MFT solutions should inherently handle scheduled and event-driven transfers securely, some fall short when it comes to ad hoc transfers—those that happen when an employee needs to send a file outside the parameters set for scheduled and event-driven transactions.

In addition to being interrupted by coworkers who need help with ad hoc transfers, IT can also spend an inordinate amount of time managing other types file transfers. This happens when organizations use multiple solutions from different vendors to send and receive files all of which require a certain amount of support effort.

Using a managed file transfer solution that handles both internal and external file transfers securely and provides visibility to the entire enterprise from a central management console reduces helpdesk and IT involvement.

Step 3: Protect files at rest in your enterprise

Once your MFT solution delivers files securely to the prescribed end point, they sit at rest unprotected until they're needed. This is another point where they become vulnerable —a target for cyber criminals. Installing a data security solution to protect data at rest is the final step for putting into place a comprehensive data protection program.

Strong encryption is traditionally used to protect data at rest and it works well. In addition, a new data security model is gaining traction: tokenization. Unlike traditional encryption methods where the encrypted data or "cipher text" is stored in databases and applications throughout the enterprise, tokenization substitutes a token—or surrogate value—in place of the original data. Tokens can then be passed around the network between applications, databases and business processes safely while leaving the encrypted data it represents securely stored in a central data vault.

Tokenization is effective in protecting entire document files as well as payment card information, all types of personally identifiable information (PII) and business information stored in databases.

What's more, because it takes systems and applications out of scope for PCI DSS audits (because tokens are substituting for clear text or cipher text data); it simplifies compliance management for data security standards and privacy laws.

For some companies, either traditional strong encryption or tokenization is the answer; for others a combination of the two is the best solution. Whichever is right for your organization, you'll want to protect data at rest the moment your MFT solution delivers it to one of your application servers where it waits to be used and until it is safely archived or destroyed.

Finally, make sure that both your MFT solution and your data security software provide cross-platform protection to secure your entire enterprise; not just part of it. It doesn't make sense to only protect data on Windows systems and not the Linux systems in your enterprise.

Implementing a comprehensive lifetime data protection program using a Managed File Transfer solution with advanced security capability in conjunction with strong encryption and/or tokenization is an obtainable objective well worth investigating.

Protecting all of the sensitive and confidential information your company sends, receives, holds and stores until you no longer need it is the ultimate offensive move. It establishes the best defense against data theft and accidental loss while easing data security and privacy compliance. All of the software tools to do this are easily obtainable and field proven.

Kyle Parris is Director of Product Management for data protection software and managed services vendor nuBridges (www.nubridges.com). Kyle can be reached at kparris@nubridges.com.

Want to reach a large audience of
security professionals by writing for (IN)SECURE?
STOP
Send your idea to editor@insecuremag.com

Securitybyte
Securing the information DNA

OWASP
AppSec Asia

Securitybyte & OWASP AppSec Asia

Conferences & Trainings 2009

Nov 17th - Nov 20th in Delhi & NCR, India.

Asia's biggest Information Security Event

Multiple tracks, 30 Conference Sessions Spread Over 2 Days
Twelve Training Sessions Covering all aspects of Information Security
Network with over 700 Delegates from around the world
Interact with over 40 Security Experts, Researchers, Ethical Hackers and World Renowned Speakers

CAPTURE THE FLAG

A live hacking competition where hacker teams are challenged to prove their skills.

The themes for this live event include:

- **Wireless Hacking**
- **Packet Wars**

CXO EVENING

The evening will have the theme of "Security Concerns for Off-shoring" and CXOs (CEO, CIO, & CISO) of select Fortune 500 companies will be invited to share their experiences and vision through Panel discussions. Guests for the evening will also include special invitees from the government agencies, Information security bodies and Industry leaders with distinguished InfoSec, Off-shoring and research background.

PACKETWARS™ THE EXPERIENCE

ATTACK. DEFEND. SURVIVE.

IF BUSINESS IS WAR, THEN THE INTERNET IS A

BATTLE FIELD

For Registrations, visit us at: www.securitybyte.org, www.owasp.org | Email: regsitrations@securitybyte.org

Software spotlight

PE Explorer (www.net-security.org/software.php?id=589)

PE Explorer is the most feature-packed tool for inspecting the inner workings of PE files (EXE, DLL, ActiveX controls, and several other Windows executable formats). It comes with a PE file viewer, disassembler, exported/imported API function viewer, API function syntax lookup, resource editor and dependency scanner.

SILC Toolkit (www.net-security.org/software.php?id=189)

SILC (Secure Internet Live Conferencing) is a protocol which provides secure conferencing services on the Internet over insecure channel. SILC superficially resembles IRC, although they are very different internally. They both provide conferencing services and have almost the same set of commands. Other than that, they are nothing alike. The SILC is secure and the network model is entirely different compared to IRC.

fe3d (www.net-security.org/software.php?id=590)

fe3d is a 3D visualization tool for network (security) information, it currently supports insecure.org's nmap and languard XML log files.

Keychain (www.net-security.org/software.php?id=239)

Keychain helps you to manage RSA and DSA keys in a convenient and secure manner. It acts as a frontend to SSH-agent, but allows you to easily have one long running SSH-agent process per system, rather than the norm of one SSH-agent per login session. This dramatically reduces the number of times you need to enter your passphrase - with keychain, you only need to enter a passphrase once every time your local machine is rebooted.

Security for multi-enterprise applications

by Dr. Taher Elgamal

When I heard about the recent creation of the White House cyber security czar role, I was genuinely impressed. It stands as positive proof that our nation's leaders, now well aware of the economy's truly global nature, seem to recognize what so many of us security folks have believed for so long: that the Internet has completely transformed the way we do business, that the potency of cyber threats increases by the minute, and that mere boundary protection is by no means the only necessary countermeasure we must employ.

While the impact of the cyber security czar will not be felt until other measures, such as financial incentives, are put in place, I believe that nothing so completely benefits from this level of recognition as the multi-enterprise application—a single application that sustains multiple networks, authentication systems, and policies, and the security of which offers itself as rich fodder for this security professional to explore.

The multi-enterprise application

Exchanging business information is the multi-enterprise application's life's work, and the dissemination of business information must be controlled, especially when intentionally shipping information outside of the organization. This could be easy when you're scanning small files and checking for account numbers, but more challenging when you're scanning 50GB files, an operation that could take a veritable eternity to finish.

This is to say nothing about the challenges created by the wide variety of methods for the multi-enterprise exchange of business information. Systems exchange information automatically, but people exchange information with systems, too, as well as with other people, and to further complicate things, multi-enterprise exchanges can happen over any mode (e.g., mobile-to-mobile, application-to-application, etc.). A policy must be either embedded in the multi-enterprise application or inherited so that an organization can manage this complex interaction.

Policy

Policy is an overused word, but for our purposes, "policy" applies to data being exchanged. "If your job is X, then you're allowed to do Y with this kind of information." But what if your job is not X? Tracing processes across enterprise boundaries, then, is a supreme challenge because there's no unique and/or standard way of expressing policies when it comes to content.

When Enterprises A and B want to talk to each other and they have their own notions of policy, they can't match their notions correctly. For example, one policy may be "broken" simply because Enterprise A sent the data to Enterprise B, which has a different kind of policy. Yet nobody is at fault! This paradox demands that we think of policy as something that the industry needs to standardize—and what a challenge that is, especially when it comes to dealing with confidential data! This is a challenge precisely because the Internet was built in a way that makes it very easy for two entities to send packets back and forth through whatever mechanism they choose. This creates weaknesses, and because hackers can exploit weaknesses, we must take security into consideration when we build multi-enterprise applications with Internet connectivity.

Sixteen years ago, when the Web started, viruses and malware were created by teens who wanted to be famous, not criminals. But today, most of the malware that gets routed over the Internet is done with the intent of making money. The hackers who wrote bad software colluded with organized criminals, and all of a sudden we faced a situation that called for robust security.

Five aspects of security for business content

In a multi-enterprise application, robust security is achieved when transactions happen correctly—when the right party always gets the right information on time and sensitive information never lands in the wrong hands. But people judge the quality of security in different ways (e.g., "How does your security deal with exception cases?", "How do you deal with the wrong behaviors?", "How do you deal with failures?"). This brings me to the five aspects of security for business content.

1. Confidentiality. What does it mean to secure content? Most people think of confidentiality in the sense that if you expose account information, that's a breach of security. However, there are many aspects that are far more important (see #2).

2. Integrity. It's annoying when a third party sees that you've done a $100,000 transaction, but it's devastating when that third party actually changes something in that transaction on the fly. Making sure the data integrity is satisfied is more important than confidentiality.

3. Authenticity. Authenticity is part of confidentiality. How you apply authentication basically determines whether confidential information can get in the wrong hands.

4. Authorization and access control. People in the security domain think of access control as the most important thing in security. The reality is that applying the correct access control measures helps us achieve all the other aspects around the security of information.

5. Auditability and tracking. How do we audit and track information so that we can produce either reports, receipts, or evidence that the transaction happened correctly? If somebody says "I never got that," dispute is difficult unless you have a secure way of purveying audits for all the transactions. You must be able to prove when the information left your location and arrived at theirs, and when they opened it. That's one of the reasons I like to refer to the "multi-enterprise application" rather than "a bunch of applications talking to each other," because it's a lot easier to audit things within a single application even if the single application spans enterprise boundaries.

Network layers

Then there's the other way of looking at security—the network layers. The Internet's data itself exists in multiple layers, far differently from how we think of things existing in the physical world.

This multi-layer design means you can have an application that is very secure, creates data, and stores and encrypts information, but once you leave the data for a system administrator (or another application with a different security model) to handle, you break the security model. But system administrators must have access because they maintain the machines, upload patches, and read logs. At the end of the day, you can't just take a single security mechanism, apply it to data, and think it will work. If I give you $10,000 to secure your four-door building, the best strategy would be to invest the cash equally in each door. But in reality, there are those who would buy a $10,000 lock for the most-trafficked door. In the electronic world, this mistake is even more serious, as the back door is just as easily accessed as the front door.

What do we do about this?

We apply multiple technologies and security controls to address all exploitable weaknesses at the different layers and create a reasonable approach to security. You need to protect the network and the application, understand user access, and secure the content separately. Malware scours the Internet 24 hours a day trying to find a weakness to exploit, so we must foil this with automated programs that allow honest people to conduct their business safely.

One of the biggest problems with security is that people are looking for a silver bullet.

Metadata

If your team is tasked with designing an application that secures data transmission from one place to another, your security guy, charged with finding a way for the application to encrypt the data, will inevitably say, “The actual communication link beneath the encryption already has encryption. Why are we encrypting again?”

Whoever is doing the encryption at the network layer is working on a completely different system, so in some deployments encryption will work, and in others, it will not. Whoever designed the network may forget to apply encryption at the IT layer, for example. Then you've lost all your protection at the network layer, so you still have to do the encryption at the application layer.

Plus, it's very difficult for an application to actually tell what's happening under it. There is no protocol between network layers that can tell the application layer that the network layer is actually using encryption. This demands that we secure every one of these layers and the content on its own.

Content needs to be secured on its own because of the multi-enterprise application scenario. It's difficult for one application to tell another application what to do with the data unless that communication is actually embedded inside the content itself. Perhaps Application A secures a document because it has sensitive information and puts enough metadata inside the document to tell Application B what to do with it. Otherwise, the second application will open and distribute the document, the first application will have no knowledge of this, and no one will know what the overall security model looks like.

That is what I call securing the content itself: embedding policies—metadata—inside the content that tell users what they can do with it. And that metadata stays with the content at all times. If somebody leaks something out, the content will “know” that it's in the wrong place.

Six key areas

One of the biggest problems with security is that people are looking for a silver bullet. “Just secure this for me, and leave me alone,” they say. If you follow that thread, that attitude guarantees failure, because there is no such thing. And the reason? Things change constantly. Each year brings new applications, patches, configurations, and firewalls. To do this right, we must embed the policy *inside the content itself.*

The media likes to talk about worms and malware, but security breaches generally start with insiders. With malware, at least you have the ability to determine whether it is coming from outside, whether it looks different, whether there's a different piece of code that's trying to do something malicious. But when an insider does something, the insider already has authorized access, and if he accidentally does the wrong thing, he'll cause a lot of financial loss unintentionally. If he intentionally does the wrong thing, it may be an extremely difficult thing to actually remediate. But a proper security profile, while not the fabled silver bullet, renders both unintentionality and intentionality in a multi-enterprise application meaningless.

It may be instructive to discuss now the six key areas that, in my opinion, best characterize this profile.

1. Secure the connection and the content. The connection between the two enterprises is the most obvious weakness.

2. Embed security seamlessly. The more you make security visible to normal end users, the less likely they will actually follow guidelines. The successful security technologies in the last 20 years were, in general, hidden from end users. When you ask end users to manage encryption keys and certificates, they end up not using the facility, and all of the security that comes with it is lost.

3. Prevent unauthorized access. It's the essence of what we're trying to do. It's not always easy to tell who's authorized unless you write a very specific policy that spells that out.

4. Interface between the different security policies of the different enterprises. A company you're exchanging data with may have a completely different set up for their active directory, no groups like you do, no levels of access, and a different system of access control. This is a problem in the industry that is unsolved, and one that I challenge all of us to address!

5. Content-based security. Content will truly be secure when enough metadata itself, inside the content, restricts access.

6. Build specific security offerings only when it comes to visibility and reporting. If you don't report what happened, how will you prove that the correct events actually occurred?

Secure the connection and the content. The connection between the two enterprises is the most obvious weakness.

How can we manage all of this? Who is responsible?

It is wrong to say that the Chief Security Officer or even the CIO is responsible for security? The entire company must take ownership. It's a business issue, not a technology issue. It's about "Is the business running correctly?" and "Are we protecting our assets?"

As for managing the security of multi-enterprise applications, there are three main processes that must be established.

1. Governance. Communicating with important partners or conducting important business transactions is part of your business. The fact that you're using security technology to accomplish some of the tasks is actually all good, but the owner of the issue is actually the management of the company at large.

2. Risk management. We have to agree that there is no such thing as 100 percent security, which suggests a degree of tolerance. Take the credit card industry. Pre-Internet, fraud accounted for 0.1 percent of all credit card transactions. Post-Internet, the number jumped to four or five percent. A tenth of a percent risk was acceptable, part of the cost of business. But five percent was not acceptable, and PCI compliance was born: a prime example of an industry recognizing that the risk had exceeded a reasonable limit, and a lesson all industries can learn from.

3. Compliance. If you try to put a measure into security, you always fail. What does it mean that you had only two events this week versus seven the week before that? Is that really an improvement? What's the value of each one of these threats? Compliance is the only way to measure whether a company is secure. But the problem with compliance is that it draws focus on becoming compliant, often at the expense of security. When we are compliant, we declare success, and this is a fallacy. It's very important to be compliant, but not just to be compliant. We must actually implement the correct business policies.

Should the White House cyber security czar inaugurate the office with security for multi-enterprise applications firmly in mind, and deeply reflect upon all the critical issues discussed here, we may be standing at the threshold of a significant moment. Could it be that the perennial challenges surrounding confidentiality, authenticity, and integrity are in their twilight days, about to be demoted from "serious" to "quaint"?

Probably not.

Dr. Taher Elgamal is the Chief Security Officer at Axway (www.axway.com), a provider of multi-enterprise solutions and infrastructure. Dr. Elgamal is an expert in computer, network and information security. Also, recognized in the industry as the "inventor of SSL," Dr. Elgamal led the SSL efforts at Netscape and throughout the industry. He also wrote the SSL patent and promoted SSL as the Internet Security standard within standard committees and the industry. Dr. Elgamal invented several industry and government standards in data security and digital signatures area, including the DSS government standard for digital signatures. Elgamal has public company board experience with RSA Security, hi/fn, Phoenix Technology and Tumbleweed Communications. He holds a Ph.D. and M.S. in Computer Science from Stanford University and a B.S. in Computer Science from Cairo University.

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

EU data breach notification proposals: How will your business be affected?

by Richard Moulds

This article discusses the impact of recent proposals for EU data breach regulation that have the potential to affect the majority of European organizations.

The impact of data breaches is one of the main security headaches for CEOs and IT specialists alike. Keeping tabs on your data has become a growing concern as organizations become more fragmented and store ever increasing volumes of data. This data is often scattered across the enterprise in huge data centers and thousands of high capacity laptops, iPhones and USB sticks, providing more opportunities for criminals to steal this data and for good old-fashioned human error to lose it. With increasingly sophisticated technologies to access this information and spyware or malware, such as Trojans, the likelihood that a company will fall foul of a data breach is greater than ever before.

The consequences for businesses of leaving data vulnerable to attack or loss are significant. Recent research by the Ponemon Institute found that the average UK data breach costs a total of £1.7 million; the equivalent of £60 for every record compromised. The study also found that 70 per cent of UK organizations have been hit by at least one data breach incident within the last year, up from 60 per cent in the previous year. The number of firms experiencing multiple breaches has also increased, with 12 per cent of respondents admitting to more than five data loss incidents in the twelve-month period (up from 3 per cent). Costs aside, the associated loss of customer loyalty and trust is equally damaging to business operating in today's highly competitive environment.

For a number of industries, regulation is already playing a role in terms of tightening data security and providing a better service to customers once a data breach has occurred. The financial services sector has been heavily regulated for some time, but more recently, the European Parliament has proposed amendments to the e-Privacy Directive that regulates the telecoms industry.

For the first time in EU law, the amendments introduce a definition of "personal data breach"; i.e. defining what constitutes sensitive data. The regulation also introduces the concept of a data breach notification requirement. The amendments provide that, in the event of a breach, the provider must, without undue delay, notify the breach to the competent national authority. In cases where the breach is likely to adversely affect the personal data and privacy of a subscriber or an individual, the provider must also notify the subscriber or individual of the breach without delay in order for all of them to take the necessary precautions. (bit.ly/D5uYB)

Even more significantly, there are now growing calls for data breach notification legislation to be extended to incorporate almost all types of businesses.

Data breach notification laws are not new in Japan, as well as most States in the US putting such laws in place since 2003. The proposed EU telecommunications bill targets the end of 2010 for adoption of the notification requirements by telecommunications operators and Internet Service Providers.

In May this year, the European Commission's (EC) Viviane Reding stated that this law should be extended to the majority of business and that the EC would seek approval for the mandate by the end of 2012.

SOME OBSERVERS BELIEVE THAT REGULATORS SIMPLY SHOULD NOT HAVE THE AUTHORITY TO DECIDE WHAT CONSTITUTES "SENSITIVE DATA" AND WHAT DOES NOT, AND THEREFORE WHICH DATA BREACHES SHOULD BE DISCLOSED AND WHICH NOT

There are strong arguments for and against such mandates. Those against the regulation suggest that it would increase costs and bureaucracy for businesses. Another often-cited argument is that the regular announcements of data breaches will desensitize the public and that the notifications will therefore lose their impact over time. Many concede that data loss has now become a fact of life and that by broadcasting such losses the 'news' only serves to damage consumer confidence in e-commerce and electronic record keeping hurting the economy and slowing technological progress in general. Furthermore, some observers believe that regulators simply should not have the authority to decide what constitutes "sensitive data" and what does not, and therefore which data breaches should be disclosed and which not.

Conversely, supporters of the proposed law argue that it will provide greater visibility into the scale of the data breach problem, which will prove invaluable to law enforcers and help encourage implementation of enhanced security measures to protect customer data. It is argued that the only way to motivate organizations to proactively protect data is to make the consequences of data loss or breach more tangible by hitting their bottom line or public reputation, things that shareholders really care about.

At present, the UK seems to be sitting on the fence with the UK's data protection watchdog, the Information Commissioner's Office, stating that they should decide on a case-by-case basis whether an individual organization should be forced to disclose a data breach. Whether selective disclosure or an all-encompassing proposal becomes law, it is clear that a large number of UK organizations will be impacted in some way if these proposals move forward.

What could this proposed law look like?

The trouble with defining any data breach disclosure law is in defining what each of the four words actually mean. What classes of data are covered, what constitutes a breach, what form of disclosure is required (i.e. what role does encryption play) and what are the penalties if the law is broken? These are four questions that are not easily answered when you consider all industries, all consumers, all forms of data and all countries in the EU.

It is possible that an EU law could be similar to the California Security Breach Information Act (SB-1386). This California state law requires organisations that hold personal information about Californians to inform those individuals if it is suspected that their privacy has been compromised as a result of a data breach.

According to the Californian law, personal information includes "an individual's first name or first initial and last name in combination with one or more of the following: a social security number, drivers license number or California Identification Card number, account number, and/or credit or debit card information including numbers and passwords, PINs and access codes.”

Not all of these examples of data are typically regarded as being secrets, particularly when they exist in isolation. For instance, a name and address is accessible to anyone, however the combination of name, address and account number should be less easy to find. Equally, a credit card number is not often a particularly well kept secret, most people being happy to expose it to shop assistants and restaurant waiters. However, a credit card number in combination with a PIN number or online password becomes a real concern. Of course, it’s perfectly possible that a future EU law could go much wider than this relatively narrow definition and encompass other forms of personal data including healthcare details, employment information and criminal records.

The question of what constitutes a “breach” also needs to be asked. For example, under Californian law, even suspected breaches must be reported. Since it is not always possible to establish whether a breach has occurred, this is a matter of some debate. There are also question marks about whether a lower limit on the number of records lost should be set, above which disclosure would be made mandatory. Generally speaking, regulators don’t like grey areas like these and in an effort to motivate the right sort of behavior they often try to narrow the issue by providing an exemption for all data that has been rendered unreadable.

There are quite a few methods for making data unreadable but most only work in one direction, they can make data unreadable, but they can’t make unreadable data readable again. That can be a problem if data is being stored for a reason, for example to resolve a dispute that may arise in the future. Encryption is one of the few reversible methods for protecting data and is increasingly being favored by regulators and policy makers because of the black and white nature of the technology. Data is either encrypted or not, which in theory means it is either secure or insecure, even following a breach. That starts to sound like security you can measure – something you can mandate. The Californian law doesn’t quite go that far but it does provide immunity from disclosure requirements if organizations can prove that their data was encrypted.

There is likely to be much debate among EU regulators as to what should be protected and what should not. Experts must decide whether EU law will only come into effect once there is evidence of a breach or whether the mere suspicion of one will be enough to mandate notification. No matter what they conclude and what rules are put in place, there will still be those that actually do nothing more to protect data than they do today. These organizations will take a calculated risk, trusting either to luck, assuming that it won’t happen to them, or actually believing that they have adequate protections in place already and that they are safe. Some may be right to take this approach, others will wish they hadn’t.

The impact of SB 1386

Regardless of the subtle parameters of any future EU law, there is some evidence that disclosure laws are just the tip of the data protection iceberg. When data breach notification was implemented in California and other US states, the number of reported data breaches increased significantly which in turn served to increase consumer awareness of the problem and triggered data protection initiatives that actually required increased security rather than just publicize security failures.

For example, although not directly related, the arrival of disclosure laws in California and other states is viewed as a major driver for the Payment Card Industry Data Security Standard (PCI DSS). As news stories of millions of credit card numbers being lost or stolen piled up, public confidence in the ability of organizations to adequately protect their personal data decreased and pressure for legal action to address perceived security weaknesses increased. Even though limits on financial liability for cardholders were already in place ($25 or so), consumers still suffered high levels of inconvenience with cards frequently being reissued, leading to increased costs across the payments industry. The leading card brands have been refining security recommendations for a number of years and these were brought together as a converged standard and most importantly, a standard that had teeth.

Unlike most standards, PCI DSS compliance is audited by default and in the extreme, non-compliance can cause a merchant to be struck off the list of trusted providers. While, PCI DSS is not a law and does not carry a legal penalty, financial penalties can be incurred as recent examples have shown. Currently, PCI DSS only applies to credit card data and is limited to retailers and the payments industry. However, it is based around 12 core technology areas the vast majority of which apply just as well to any industry. In fact, it would be hard to argue that they do not already represent well-established best practices in those industries – the difference is that today they are not hard requirements. Should the EU data breach regulation become law, then it is possible that PCI DSS or a mandate very much like it will be extended across all sectors.

Should this occur, it is likely that within the next five years the majority of companies will need to employ encryption based security in order to protect themselves from the business costs associated with data breaches and ensure that they are able to compete effectively with their peers by complying with industry security regulations.

SHOULD THE EU DATA BREACH REGULATION BECOME LAW, THEN IT IS POSSIBLE THAT PCI DSS OR A MANDATE VERY MUCH LIKE IT WILL BE EXTENDED ACROSS ALL SECTORS

Encryption – the key to security?

Encryption is already on the enterprise agenda with 44 percent of enterprises planning to encrypt more than 75 percent of their data by the end of 2009, according to IDC, although I expect these plans to slip considerably as a result of the current economic situation. However, the proposed EU legislation is something to be kept in mind and could significantly impact the business community by imposing a hard timescale, forcing industry to consider how encryption can be implemented in a way that minimizes cost and disruption, as well as the risk to business continuity.

Unfortunately, encryption has had a reputation for being costly, complex, disruptive to implement and something only banks and governments need to worry about. This is no longer the case. The good news is that encryption is now significantly easier to implement and manage than in the past. The security industry and standards bodies have reacted quickly to the increased demand for encryption technologies over the last few years and today there are numerous examples of IT products and systems that include embedded or native encryption capabilities, sometimes even included for free.

Tens of thousands of companies are deploying encryption technologies in order to protect their customer data. Encryption is proving to be one of the most effective ways of securing data on the market. The very nature of encryption means that data is secure even if many of the other enterprise security mechanisms fail. Encryption is fail-safe security, and that’s why regulators will grow to depend on it. Given that a data breach notification law is likely to be on its way, companies will see encryption as a key way to get them off the hook.

Of course, things are rarely so black and white. While encryption as a mathematical process is clear cut, there are many deployment choices that result in good or bad encryption – good security or a false sense of security – and these choices often come down to key management. The PCI standard has done a good job in identifying this and has been steadily updated with specifics about key management. Future EU legislation should also be concerned with this detail and learn from the industry’s experience.

As the use of encryption grows, companies need to be able to manage (or control) a growing number of encryption keys securely. This is crucial not only to prevent keys from being lost or stolen, but also for important operational reasons such as on-demand recovery of encrypted data, automated updates and compliance reporting.

Companies have previously struggled with key management and a 2008 Trust Catalyst survey found that organizations see key management as the biggest challenge when deploying encryption.

Below are some issues to consider for good key management when implementing encryption:

Going the extra mile to protect your keys: Good encryption algorithms are effectively impossible to break and, as a result, criminals or corrupt insiders are increasingly targeting encryption keys and the management systems that control them. While awareness regarding this issue has increased and the horror stories of keys stored in spreadsheets or written on sticky notes are nowadays rare, most organizations still rely on software-based key management tools and manual processes. These approaches can be inherently insecure and often scale very poorly, driving up operational costs. To ensure the security of encryption keys, it is essential that keys are stored in hardware, for example by using hardware security modules (HSMs) and taking advantage of security certifications such as FIPS and Common Criteria.

WHILE DATA NOTIFICATION REGULATION IS STILL A FEW YEARS AWAY, THE LANDSCAPE IS ALREADY CHANGING

Controlling access and authorization: Physically secure key management systems can still be undermined by weak access controls. Many have argued that the current economic environment has triggered a rise in insider fraud and it is important that an organization's key management systems can guard against this significant risk. Adding strong authentication techniques for administrators is an obvious first step and this can often be bolstered by the concept of separation of duties to establish mutual supervision and help to remove the threat of all powerful 'super-user' roles.

Audit and reporting: Audit trails are required for companies to prove that their data is secure, particularly if this is a means to avoid disclosure. Once data is encrypted, an auditor's attention will quite rightly turn to the systems that manage the keys. It is essential that companies can demonstrate that every copy of every key is under control.

While data notification regulation is still a few years away, the landscape is already changing. Increased calls for such laws mean that CIOs of organizations must begin to consider how best to protect themselves against the consequences of a publicly reported data breach.

Encryption is likely to be the best, most comprehensive way to go about this and, given the increased maturity of this technology over the last decade, it has become simpler and less expensive to deploy and manage.

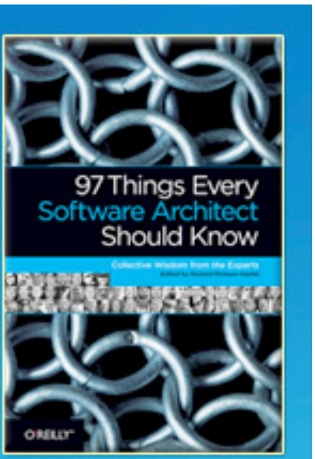
With such a rapidly changing environment, the EU must look to support organizations with the right information prior rolling out any new data protection regulation. Equally, companies must prepare themselves for these changes in order to ensure that they are not negatively impacted by the data breach notification proposal if and when it becomes law.

Richard Moulds is the EVP of product strategy for the information systems security activities of Thales (www.thalesgroup.com).

Book review

97 Things Every Software Architect Should Know

by Zeljka Zorz



Author: Richard Monson-Haefel | Pages: 200 | Publisher: O'Reilly | ISBN: 059652269X

Don't we all sometimes wish we could just TAKE good advice, instead of thinking we have found a better way and make the mistakes we've been warned about? This book is a collection of really sound, tried and tested guidelines from hardened experts that have done the work for us, so why not listen to their wisdom?

About the author

Richard Monson-Haefel is a software architect specializing in multi-touch interfaces and a leading expert on enterprise computing.

Inside the book

Every experienced software architect will tell you that the key to being successful in this line of work is to find a balance between the business and the technology aspect of their job, and to extract and combine the best of these two completely different worlds. How to do that? Read the advice and think about it. What do you already do right, and what things you should think about changing? There are 97 pieces of advice in this book, coming from professionals around the world.

As you already know, software architects have a unique position in the IT world. They work with software developers and the project sponsors. Their job is to make sure that the customer is satisfied with the end result and that the application is finalized on schedule and within budget restrictions. To do all this, they also have to be good leaders, know when to give the developers autonomy and when to step in, be knowledgeable in the technology and methods used, know how to listen, communicate and motivate.

This books offers new perspectives on old problems that will probably make you reevaluate some of your methods. It also offers some simple tips and psychological tricks to increase the effectiveness of your communication, to return the project on the right path when it has veered off course, to make you a better negotiator, and many more.

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

ICDF2C 2009

International Conference on Digital Forensics & Cyber Crime

30 September - 2 October 2009, Albany, NY, USA

www.d-forensics.org

ICDF2C a unique conference encompassing not only technical, but also the social, legal, and business aspects of forensics. The forensics field is set to explode and the Capital Region is in a prime position to take advantage of it. By bringing together both practitioners and researchers, we hope to benefit from understandings of current practice and the innovations that research has to offer.

TRACKS

Financial Crimes
Accounting Fraud / Forensic Accounting
Continuous Assurance and Crime Detection / Deterrence
Forensics Training & Education
Forensics and Law
Cyber Crime Investigations
Network Forensics and Data Analysis
Computer/Handheld Device & Multimedia Forensics
Forensics Standardization and Accreditation
Data Recovery & Business Continuity
Intellectual Property Theft and Watermarking
Cyber Warfare and Terrorism

CALL FOR PAPERS

Paper submission deadline is on 15 June 2009. For the details visit http://d-forensics.org/callforpapers.shtml

CALL FOR PRESENTERS

As opposed to research papers, the presentations will be focused on more applied topics. For further details visit http://www.d-forensics.org/callforpresenters.shtml

ICST

HELP NET SECURITY
WWW.NET-SECURITY.ORG

New York State Division of Criminal Justice Services DCJS

CREATE-NET

UNIVERSITY AT ALBANY
State University of New York

Safety in the cloud: How CIOs can ensure the safety of their data as they migrate to cloud applications

by Yaron Sinai

It's a common scenario right now, played out in executive suites across the country. A company is looking to cut back on expenses and overhead. IT, with its myriad of projects, expensive equipment and maintenance costs, is targeted for budget cuts. As CIOs and IT Directors search for an alternative to layoffs, Software-as-a-Service (SaaS) solutions are frequently emerging as a cost effective way to reduce overhead, without the trauma of slashing projects or staff.

SaaS providers typically offer subscription options for different software products, which are hosted on the providers' servers. While allowing companies to reduce their spending on developing in-house solutions and maintaining the hardware to host such solutions (particularly for large companies), SaaS services also operate in such a framework as to allow for frequent and effortless (on the part of the user) updates to the service.

This way, companies are able to outsource much of their peripheral work, and reduce the costs associated with this work, in order to concentrate on development of their product and their business needs. This might seem like a no-brainer at first – but take a minute to approach it from a CIO's perspective. Much of the data that these services store or manage is of a sensitive nature: billing and receipts, customer feedback, proprietary code, sensitive email and documents, etc. It's not unexpected for security concerns to be a primary issue holding back widespread adoption of SaaS services.

As the CEO of a company that develops SaaS project management tools, aimed specifically at software developers, this is an issue that I've encountered on many occasions. Furthermore, this is something that I deal with myself. Not only in ensuring that the services we provide our customers and users are secure and reliable, but also in protecting our own data against system failures and outages, security threats and software malfunctions.

As a SaaS provider with customers to service and a reputation to protect, ensuring the integrity of our products is of utmost concern, and the same holds true for most companies in the business of providing a service. A hosted solution will have more checks and balances in place in order to avoid, or if unavoidable, deal with any situation quickly.

That being said, although reliable SaaS providers are outfitted with a variety of security measures such as failure protection systems and backup servers, ultimately it is up to the CIO to do his or her due diligence both in selecting a SaaS provider, and being an active participant in maintaining operations and security within their own company.

What's out there?

These days, there are many Software-as-a-Service providers in operation, both large scale operations and smaller, more nimble, outfits. As a business model in tough economic times, SaaS offers a cost effective alternative to homegrown and user maintained software. Additionally, in most cases, SaaS applications are business and project management tools of some sort, which aim to streamline business functions. As the SaaS business model becomes more popular, software companies from Oracle to Microsoft are joining the party, along with more established and niche players such as Netsuite, Salesforce, and Elementool, among others.

Since many of the smaller newcomers have limited budgets, in order to offer hosted services they use shared servers or servers that are hosted by small operations in different locations across the globe. Shared hosting means that the SaaS system is located on a server that is being used by other, often undisclosed, companies.

In situations where there is a dedicated server, the SaaS provider will usually have many different standard security and IP protection measures in place such as firewalls, antivirus software, and often times a failure protection system and backup as well.

In these instances, the security of the SaaS system is questionable at best, and the possibility exists that an application executed by other companies which are sharing the server can cause the entire operation to crash.

On the other hand, larger or more entrenched operations will have dedicated servers that are reserved for the use of the provider exclusively. In situations where there is a dedicated server, the SaaS provider will usually have many different standard security and IP protection measures in place such as firewalls, antivirus software, and often times a failure protection system and backup as well.

Choosing a SaaS provider

CIOs or decision makers should be actively involved in the process of evaluating SaaS or cloud computing providers. The following questions are a good guideline of what to ask potential vendors, in order to ensure the safety of data in the cloud:

1. Does the SaaS provider have direct control over their servers, and can they respond quickly to any security breaches or system failures?

While no company representative in their right mind would respond to the second part of that question with the answer NO, it's often a simple matter to ask a few probing questions in order to determine a provider's flexibility and access to security measures such as backup servers, and other fail-safes.

2. Will the SaaS provider offer up testimonials from existing clients for reference?

As it is with choosing any type of service provider, existing users of the company's SaaS tools should be able to offer a clear picture of how reliable the provider is and how secure they feel entrusting their business operations, or pieces of it, to the providers' systems.

3. How quickly can you and your IT staff become familiar with the services in question and how they operate?

This one is a question that implies a bit more than the standard, “is it user friendly?” For the software developer or IT worker who is using the tool, familiarity means the ability to see where possible security threats may occur and then proceed accordingly.

Additionally, becoming familiar with the protection measures built into the software, such as password protection and session management, allow users to take full advantage of them from the start. For companies planning on using SaaS applications for particularly sensitive data, this deceivingly simple question carries extra weight.

4. Can your company consolidate its SaaS services and needs under the umbrella of one provider?

As more and more companies are jumping into the cloud, software companies that used to offer their products for purchase and installation are moving to web based business models. As more services become available, companies will find that they have a need for more than one hosted application – a time tracker, email and a help desk application, for example. Common sense tells you that the more your data is spread around, the more susceptible it is to a threat. Finding one SaaS provider who offers a range of business tools not only minimizes the hassle of integrating multiple tools from several vendors, but also reduces the vulnerability of your data.

5. Does the SaaS provider offer an option to download your company’s database(s) for self backup?

Providers that offer this option understand that despite backup servers, multiple fail-safes and other protection, nothing is ever 100% guaranteed. Self backup lets the user download their database so that it can be backed up on their company’s system. In the event that the SaaS system becomes unavailable one day, for whatever reason, all information isn’t lost.

Becoming familiar with the protection measures built into the software, such as password protection and session management, allow users to take full advantage of them from the start.

Maintaining data safety

The marketplace has been assessed and you’ve chosen a vendor based, among other things, on your faith in their security measures. Once your IT team has begun using the SaaS applications in their daily roles, there are still measures and precautions that can be taken to ensure a safer work environment when using SaaS applications.

Most web-based services offer strong password protection features. Don’t take these safeties lightly, or share passwords. Have all users change their passwords on a regular basis. Lastly, obvious passwords such as names and birthdays may be easy to remember, but they’re also easy for others to guess, so avoid using these for sensitive data and accounts.

While the initial idea of hosting your data elsewhere may be tough to come to terms with, in the end, the savings in time and money offered by Software-as-a-Service applications more than make up for the effort expended to ensure the safety of your data.

Yaron Sinai is the Founder and CEO of Elementool, the developer of Web-based project management tools, which was established in 2000. Prior to founding Elementool, Sinai worked for the Federal Bank of Israel, BDO accounting Firm, and several software startup companies including Chart.co.il, the online advertising company which he founded in 2005, and sold to the Israeli branch of Leo Burnett advertising firm in 2007.

For Assistance / Details Contact
SECUTEC 2009 SECRETARIAT
C/o Winmedia Communications Private Limited
120, Hoodi Apts, Cunningham Road, Bangalore - 52 INDIA
Tel : +91 80 2234 2611 | 2612 **Fax :** +91 80 2234 2613
Email : info@secutec.in www.secutec.in

SECUTEC

19th - 21st November 2009
Kanteerava Indoor Stadium
Bangalore - INDIA

South India's Premier Exhibition & Conference on Security Products & Services

SecuTec will be a one stop solution for all those looking at security solutions. SecuTec is all set to house the latest in home, office and industrial security systems, which compromises of over 150 exhibitors and a conference covering the latest of topics in the security industry. The event will house exclusive pavilions dedicated to different kinds of security systems, thus providing a specialized platform for various kinds of exhibitors. SecuTec will be held at the Kanteerva Stadium- Bangalore, India from Nov 19th 2009 to Nov 21st 2009.

The Safest Security Market in the World Beckons...

With the Indian security industry anticipating to achieve a growth rate of 125 per cent by 2012, SecuTec gives businesses an unparalleled platform in 2009 to reach out and build relationships with desired audience, get exposure amongst your counterparts and as well as buyers, to create and expand your market, and meet prospective agents and distributors for your products

www.secutec.in

EXHIBITOR PROFILE

- Access Control
- Biometrics
- CCTV
- Home Systems
- Alarms
- Fire pumps
- Rescue Vehicles
- Fire Control Tools
- Disaster Management Tools
- Fire Vehicles
- Signaling burglary
- Protection of mass events
- Security firms
- Anti-Terrorist Equipment
- Automatic fire fighting systems
- Identification device & system
- Gas leak prevention devices
- Night vision equipment
- Detection device & system
- Entrance control device & system
- Fire resistant garments
- Fire proof wires & cables
- Perimeter security
- Telecommunications systems
- Article Surveillance System
- Emergency response centers
- IT-Based Security
- Smoke Detectors

Supported by

CAPSI CSPIA SECURITY PARK.NET Security Solutions Today HELP NET SECURITY WWW.NET-SECURITY.ORG WINMEDIA

Vulnerability management

by Rajender Singh

Vulnerability management is the process of identifying the presence of vulnerabilities and minimizing the security risk to assets to an acceptable level by keeping the priority of assets for the organization. Necessary security controls are put in place to protect the asset from any residual risk.

Methodology

Vulnerability management follows an evolving methodology to combat threats trying to exploit vulnerabilities. It's not all about scanning your network, but a structured process that aims to minimize or zero down vulnerabilities in your network.

To put in place an effective vulnerability management process for your organization, you need to look at the common targets and channels that an attacker follows to exploit various vulnerabilities. The targeted systems are friendly to an attacker only when they are vulnerable at network or host level.

Today, even after a hardening at host and network level, attackers are able to break into systems using vulnerable Web applications.

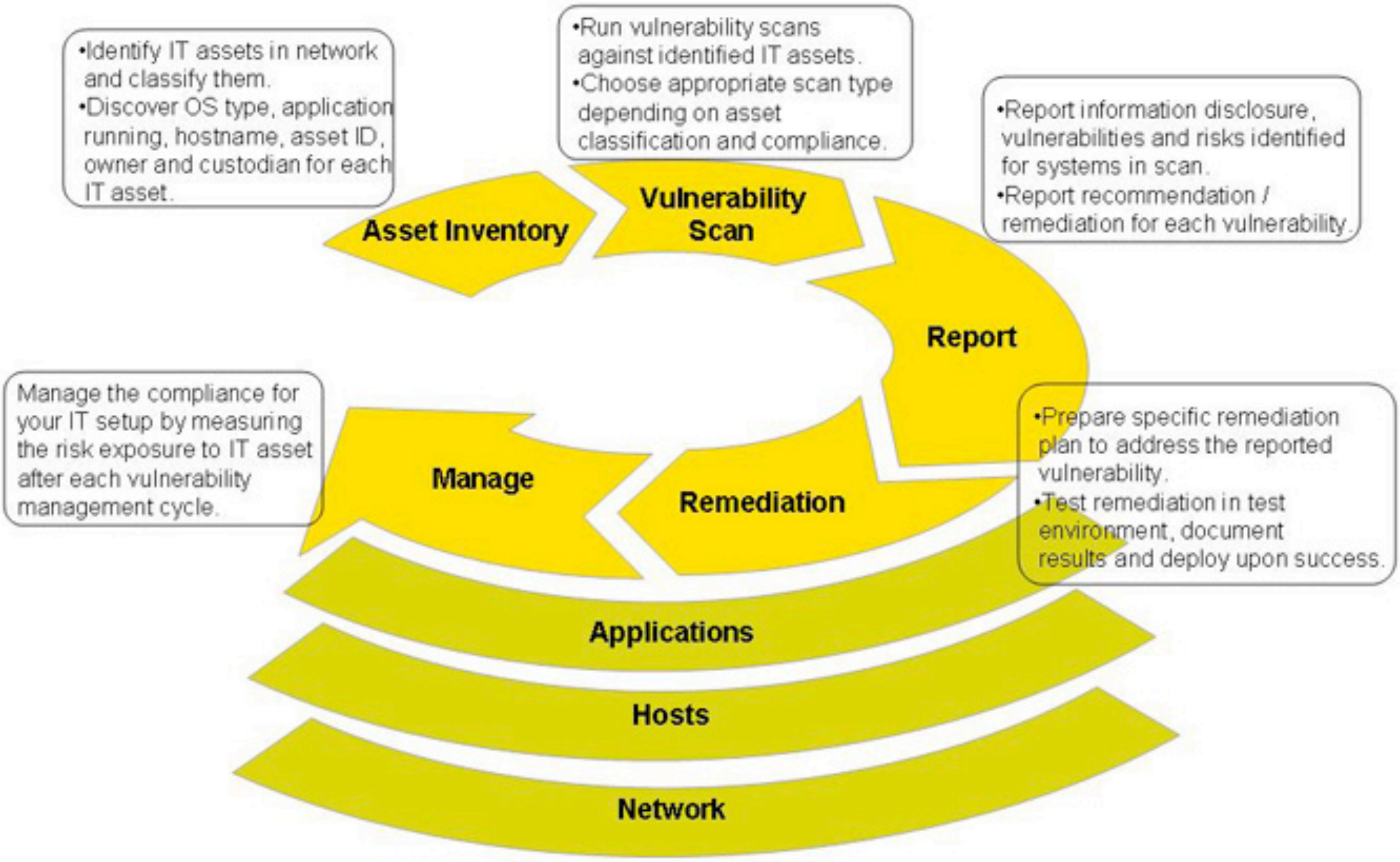

•Identify IT assets in network and classify them.
•Discover OS type, application running, hostname, asset ID, owner and custodian for each IT asset.
•Run vulnerability scans against identified IT assets.
•Choose appropriate scan type depending on asset classification and compliance.
•Report information disclosure, vulnerabilities and risks identified for systems in scan.
•Report recommendation / remediation for each vulnerability.
Asset Inventory
Vulnerability Scan
Report
Manage the compliance for your IT setup by measuring the risk exposure to IT asset after each vulnerability management cycle.
Manage
Remediation
•Prepare specific remediation plan to address the reported vulnerability.
•Test remediation in test environment, document results and deploy upon success.
Applications
Hosts
Network

Figure 1: Vulnerability management lifecycle.

Manage network security

Attacks on a network could be either external, internal or both. In case of an external attack, an attacker can breach the network by sending malicious code through border or gateway devices and bypassing the existing security controls. Vulnerability detection along with closure at the network and perimeter layer needs to be put on higher priority. They are your first line of defense. A regular process needs to be in place for scanning the networked systems and validating the presence of vulnerabilities against them. Networked systems are not limited to routers, switches, firewalls, VPNs, DNS, DHCP, Print server, Web servers, Proxies, database servers but should include desktops and laptops connected on you network.

Design a secure network architecture

1. Make sure hosts are not permitted to access the Internet directly. They should access it through content filtering proxies capable of scanning the packets for malicious code. If they need to be connected by a NAT rule on the firewall, ensure that the necessary network and security controls (such as desktop firewall, antivirus and antispyware tools) are present on the host.
2. All emails should pass through a secure mail gateway that is capable of filtering email threats.
3. Implement strong authentication for accessing networked resources.
4. Host hardening lowers the chances of system compromise or exploitation. Stick to best practices of system installation, followed by hardening and conducting of regular vulnerability scans. Hardening hosts and network devices directly after installation considerably reduces the attack surface.
5. If your organization uses wireless as a network connectivity option, ensure that proper security controls are placed to safeguard the flowing of data through a wireless network. Some of the security measures to be taken are:

a) Secure the wireless access via VPN tunnels or strong encryptions like WPA2.

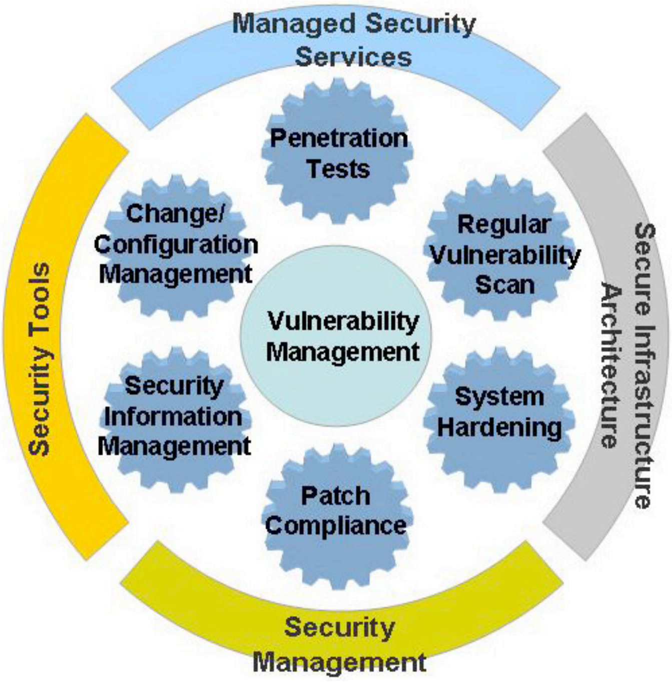
b) Wireless access points should be hardened and endpoint security measures should be taken.

c) Implement wireless IPS and rogue device detection techniques.

6. Implement a strong password policy in your organization to safeguard online accounts against password attacks such as brute force, dictionary or hybrid password attacks.
7. Use automated tools to gather network information on a regular basis and analyze them. Create the latest network map based on the information and a list of assets belonging to your organization. This assists in the detection of rogue devices on wired or wireless networks. Maintain and update the switch port, router port configuration document. Keep unused ports disabled on all network points.
8. Use a Security Information and Event Management tool to obtain meaningful security logs and events correlations. SIEM/SIM tools assist in infrastructure security by providing important logs to centralized security server and correlate them at that point. It helps IT security operations personnel be more effective in responding to external and internal threats.

Establish network, wireless and application penetration testing

Evaluate the security posture of your network and applications on a periodic basis, as a defined security policy. Penetration tests involve activities such as simulations of attacks and exploitation of the target systems, analyzing the target for any potential vulnerability.



Managed Security Services
Penetration Tests
Change/ Configuration Management
Regular Vulnerability Scan
Vulnerability Management
Security Tools
Secure Infrastructure Architecture
Security Information Management
System Hardening
Patch Compliance
Security Management

Figure 2: Vulnerability management architecture.

Manage Host Security

Implement an automated host / endpoint vulnerability scan

Regular host based vulnerability scanning via agent based software and a centralized policy push can help achieving automated host scan. It can be conducted to discover all the problems or vulnerabilities in the running operating system, like registry values, password complexity, account integrity, startup details, hardening settings, kernel parameters, etc. Such reports provide a peek into the system security posture.

After detecting a vulnerability, it must be closed as per defined by the remediation process.

Implement configuration management for server and network domain

Configuration management tools assist in monitoring, detecting and reporting any unauthorized change in the setup. Taking a step forward from the traditional vulnerability management solutions, configuration management tools aid administrators and information security groups in keeping an eye on changes at the configuration level.

Endpoint or host security is critical for vulnerability management

Vulnerabilities can spread through systems across networks. They can enter your systems via Internet or via compromised systems in your network, through a malicious user connecting to your network just outside your office premises or through gadgets/disks to get access into the most secure zones. Deploy antivirus along with anti-spyware kits to combat malicious software codes entering your systems and network. Today the most popular antivirus vendors are coming up with endpoint security solutions. They include capabilities to detect viruses, spyware, adware, combat against network threats with the help of inbuilt personal firewalls, zero day attack prevention by pre-configured the settings for threat or attack prevention. Ensure that the antivirus product is updated daily and keeps the pace with current virus definitions. Activity logs of antivirus clients must be sent to a centralized server and reviewed for any possible attack or scan failures.

Attacks on your machines generally originate from external machines, but are not limited to them

They can come from internal (trusted) systems as well. If you have a compromised system on your internal network, malicious packets and code can spread through your network to affect other machines as well. Installing a personal firewall on individual machines will add an extra layer of security and protect systems from those attacks. The logs generated by personal firewalls that are forwarded to the centralized system and analyzed by administrators and SIM tools, assist in reporting incidents and their remediation.

Address Web application threats

A vulnerable web application hosted on a secure environment can also present a risk. Default web accounts, weak session management, privilege escalation, cross-site scripting, buffer overflow - these are some of the common web application vulnerabilities which differ in risk rating but need to be closed as soon as possible. Web application vulnerabilities along with system level weaknesses can result in significant damage to IT systems and the organization profile. Appropriate actions must be taken to close vulnerabilities before they can be exploited.

Install a web application firewall and make it mandatory for all the Internet facing servers. Undergo periodic web application penetration testing, at least for Internet facing servers and newly hosting applications. Internal applications penetration testing will also mitigate the risks arising from insiders.

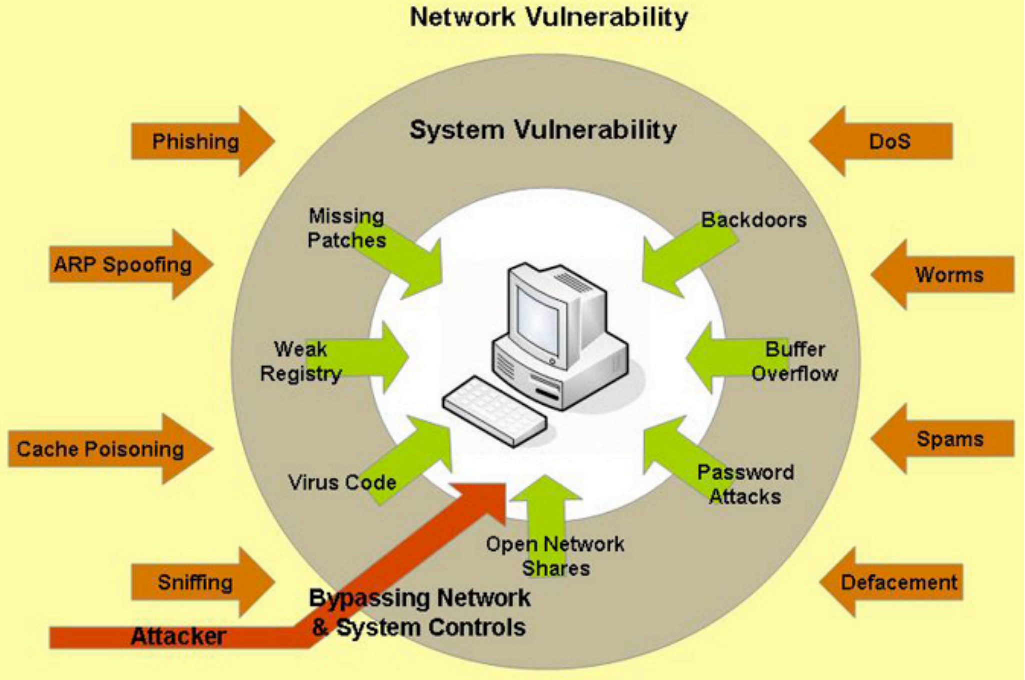


Figure 3: Systems and network attack points.

Enterprise patch management

Running a vulnerability scan against a fresh network would probably deliver a report presenting a large number of medium to high vulnerabilities. A large chunk of that report would consist of events such as missing patches. Why did they come up in the first place? How do I close them? Will it show in the next scan report?

Many organizations are still struggling with the implementation of patch management policies and procedures. An automated patch management system shields you against vulnerabilities arising due to missing patches. The problem of patches is not limited to operating systems but has reached applications and 3rd party software. An unpatched application running on top of an unpatched operating system is risking getting compromised by malicious user. Patching applications is equally important when it comes to building a secure infrastructure.

Patch management must undergo a change management cycle and testing procedures to test these patches prior to implementation. Tested patches with positive results must be deployed on all systems within timelines defined by the security policy.

Patches are classified by risk exposure. Generally, patches are released with vendor default classifications. If your organization has a separate classification policy, you must change the same according to it. Patch management policy shall guide administrators in handling and deploying patches on hosts depending on category and tagged timelines. This overcomes the problem of irregular patch deployment.

Security professionals must also address the problem of failed patch installation on some miscellaneous hosts. Patch server logs must be pulled and reviewed after every patching activity. Such missing patches should be installed manually within the defined timeframe to fix the problem.

Change control process

Manage changes to your IT environment by implementing a robust change control process. A good change control process ensures implementation of a standard process to raise, manage, document and implement the changes by minimizing the risk to IT environment. Such a process involves various entities who need to approve the changes based on the requirement, implementation risk level and feasibility. Change control needs to document the change area, summary, exact change details, validity and approvers. A typical change management implementation to a development environment would involve documentation, approval and implementation of change. A project manager will estimate if there is a need to change the development environment, an infrastructure manager will estimate the feasibility and actual implementation method and the security manager will evaluate the proposed solution for any potential or inherent risk. If any security risk is discovered in the proposed or existing solution, it must be modified to meet the enterprise security standard.

Automated vulnerability management

Network vulnerability scanners are capable of scanning network assets for vulnerabilities. Hackers look for such a weakness on a network to help them infect large number of systems on a corporate network. These tools assist with security management by automating the vulnerability management program. These tools can be scheduled to run during the off-peak hours of your network to save bandwidth and system resources. Scans must be scheduled at standard frequency as defined by the security policy. Any discovered vulnerability or weakness must be reported to a security group through an established channel of incident management. The incident response group, asset owner and application owner of the respective system shall also be kept informed regarding the same.

Rajender Singh is an IT security consultant with experience in network and application security assessments, network security architecture review, implementing and managing ISO27001 and PCI DSS. He is a penetration tester and avid sailor.