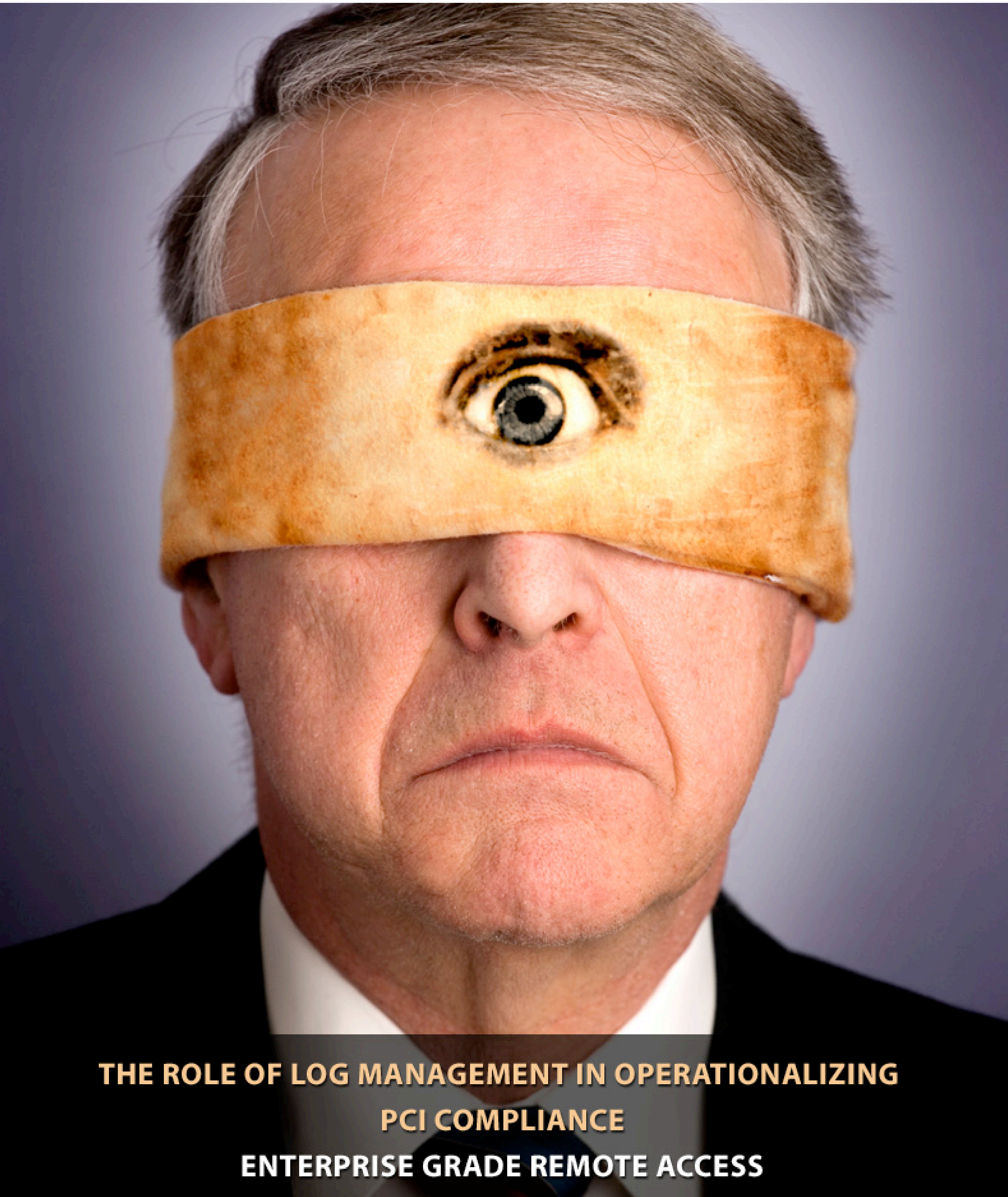
(IN)SECURE

OPEN. INFORMATIVE. TO THE POINT.

Issue 12 - July 2007



THE ROLE OF LOG MANAGEMENT IN OPERATIONALIZING PCI COMPLIANCE

ENTERPRISE GRADE REMOTE ACCESS

THERE IS A BETTER WAY

MYPW ONE-TIME PASSWORD SERVICE PUTS YOU IN CONTROL

SECURE. Powered by a revolutionary patent-pending, two-factor authentication technology, MyPW dramatically increases your site's security. No one will be able to access an account without possession of both the MyPW One-Time Password (OTP) and your local authentication information.

EASY TO USE. Available for any Internet connected service or device, such as a website or corporate Intranet. User-friendly web service protocols and technologies will have you up in hours, rather than days or weeks.

AFFORDABLE. No large upfront purchases or lengthy contracts. You can try MyPW with as many or as few users as it takes to see if the service works for you, and you only pay for the number of people who are actively using the system. We even offer a Direct Consumer model for companies that wish to make the MyPW service available for their security-minded customers but don't have the budget to foot the bill themselves.

ONE SOLUTION DOES IT ALL.
You only need to carry a MyPW token or your mobile phone. Everything you need to protect your valuable data can be accomplished via the MyPW API and website.

my pw

Strong Authentication Made Simple

To learn more visit us at **www.MyPW.com**

TABLE OF CONTENTS

Welcome to another issue of (IN)SECURE, packed with a variety of security articles for all levels of knowledge. With pressure related to PCI compliance growing as the year progresses, we offer some insight into the topic. We have an interview with Jeremiah Grossman from WhiteHat Security who will give you some interesting details when it comes to web application security. There's also material about keyloggers, Network Access Control, Windows security, and much more.

In collaboration with Addison-Wesley and Cisco Press, we have a book giveaway where 5 lucky readers will get some free knowledge. What are you waiting for?

Mirko Zorz
Chief Editor

Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts

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

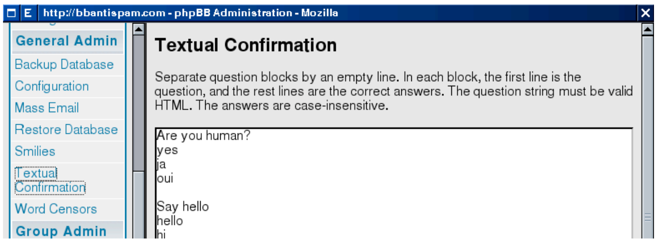
Marketing: Berislav Kucan, Director of Marketing - marketing@insecuremag.com

Distribution

(IN)SECURE Magazine can be freely distributed in the form of the original, non modified PDF document. Distribution of modified versions of (IN)SECURE Magazine content is prohibited without the explicit permission from the editor. For reprinting information please send an email to reprint@insecuremag.com or send a fax to 1-866-420-2598.

Corporate security news

Take care of spam on your phpBB forum with bbAntiSpam



Textual Confirmation

Separate question blocks by an empty line. In each block, the first line is the question, and the rest lines are the correct answers. The question string must be valid HTML. The answers are case-insensitive.

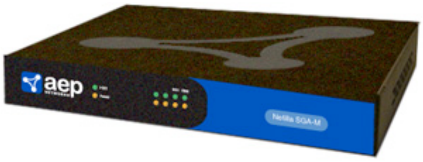
```
Are you human?
yes
ja
oui

Say hello
hello
hi
```

bbAntiSpam released bbAntiSpam Advanced Textual Confirmation 1.0.2. This PHP script will help users build rock-solid protection against spam messages for their phpBB, vBulletin, WordPress, Wiki, or a guestbook. The bbAntiSpam script works transparently between visitors and a PHP application. When some one attempts to submit data, the script comes to life and starts the confirmation process. It will select a random question from its database and wait for the visitor to give the correct answer. Once it's provided, the request of the visitor is forwarded to the web application. (www.bbantispam.com)

Requirements for the CISSP certificate will be raised

(ISC)2 announced its board of directors has approved new professional experience and endorsement requirements for the Certified Information Systems Security Professional (CISSP) certification. Effective 1 October 2007, the minimum experience requirement for certification will be five years of relevant work experience in two or more of the 10 domains of the CISSP CBK, a taxonomy of information security topics recognized by professionals worldwide, or four years of work experience with an applicable college degree or a credential from the (ISC)2-approved list. Currently, CISSP candidates are required to have four years of work experience or three years of experience with an applicable college degree or a credential from the (ISC)2-approved list, in one or more of the 10 domains of the CISSP CBK. (www.isc2.org)

First geographical load balancing SSL VPN



AEP Networks announced the AEP Netilla Security Platform (NSP) Release 5.6, in which the standard load-balancing configurations now enable geographical load balancing, providing load sharing and fail-over between independent NSP clusters in geographically diverse data centers. It is configurable by the enterprise as active-active for organizations self-insuring against a failure in their owned data centers or as active-passive for customers using a standby/backup disaster recovery facility service, such as those provided by IBM or Sungard. (www.aepnetworks.com)

SonicWALL Network Security Appliance E7500 unveiled

SonicWALL unveiled the SonicWALL Network Security Appliance (NSA) E7500, a new gateway security appliance that makes deep packet inspection security productive and easy to manage in larger network deployments. Designed to enable the highest level of UTM performance at its price point, the NSA E7500 is intended for campus networks, distributed environments and data centers. The NSA E7500 features SonicWALL's characteristic ease of management combined with low cost of ownership and a rich set of inbound and outbound network control capabilities. (www.sonicwall.com)

Nearly 40 percent of large organizations don't monitor databases for suspicious activity

Application Security announced the results of a Ponemon Institute survey underscoring the serious challenges organizations face in securing sensitive data. With more than 150 million data records exposed in the past two years, the survey also highlights an organizational disconnect between the realization of the threat and the urgency in addressing it. Forty percent said their organizations don't monitor their databases for suspicious activity, or don't know if such monitoring occurs. Notably, more than half of these organizations have 500 or more databases – and the number of databases is growing. (www.appsecinc.com)

New Digital Signature Services OASIS Standard

The members of the the international standards consortium OASIS have approved Digital Signature Services (DSS) version 1.0 as an OASIS Standard, a status that signifies the highest level of ratification. DSS defines an XML interface to process digital signatures for Web services and other applications, enabling the sharing of digital signature creation, verification and other associated services, without complex client software and configuration. DSS describes two XML-based request/response protocols, one for signatures and a second for verification. Using these protocols, a client can send documents to a server and receive back a signature on the documents; or send documents and a signature to a server and receive back an answer on whether the signature verifies the documents. (www.oasis-open.org)

GFI releases software suite for PCI DSS compliance

GFI Software announced the release of the GFI PCI Suite, a package aimed at helping companies meet the strict requirements and tight deadlines imposed by the Payment Card Industry Data Security Standards (PCI DSS) and comply with the majority of automated processes required for compliance. The GFI PCI Suite provides a centralized management console through which systems administrators can deploy the PCI DSS enhanced versions of GFI EventsManager and GFI LANguard N.S.S. – two solutions that are vital to network security and essential to meet the directives imposed by PCI DSS. GFI EventsManager boosts PCI DSS compliancy efforts by alerting administrators on key events occurring on the network while GFI LANguard N.S.S. allows IT professionals to proactively identify network security weaknesses and fix them before these are exploited. (www.gfi.com)

New Symantec Foundation IT Risk Assessment service

Symantec announced Symantec Foundation IT Risk Assessment, a comprehensive consulting service designed to provide customers with an overview of their current IT risk exposure and guidance on remediation. The service helps customers take the first step toward a comprehensive IT Risk Management program. The service identifies, categorizes and prioritizes current IT risks so investments can be made in projects that manage IT risk, cost, and performance for maximum business returns. (www.symantec.com)

One-time passcodes on mobile devices with SafeWord MobilePass

SafeWord
1
Activate MobilePass and generate a one-time passcode
2
Log on to application using the one-time passcode
Log On
3
Access application
Log On Successful.
Welcome!

Secure Computing released SafeWord MobilePass, a new software authenticator that allows a user access to Virtual Private Networks (VPN), Citrix, Outlook and a number of other applications through one-time passcodes generated on their personal mobile device or laptop PC. MobilePass provides convenience as well as enhanced security through proven, two-factor authentication, establishing proof-positive identity for all users accessing trusted corporate and consumer applications. Additionally, SafeWord MobilePass helps to increase productivity at a low total cost of ownership. (www.securecomputing.com)

New software programmer exams for application security certification

The SANS Institute launched the first GIAC Secure Software Programmer (GSSP) exams. The inaugural exams covering C and Java/Java EE will be held August 14, 2007, in Washington, D.C. “The lack of trustworthy standards and certifications has been a challenge for software buyers and software developers,” said Hartmut Raffler, head of Technology Division Information and Communication at Siemens Corporate Technology. “Secure programming skills are essential for building software that can be trusted. SANS’ willingness to offer this exam as part of a comprehensive secure coding improvement strategy is exciting and will help both buyers and sellers of software.” (www.sans.org)

Review: Centennial Software DeviceWall 4.6

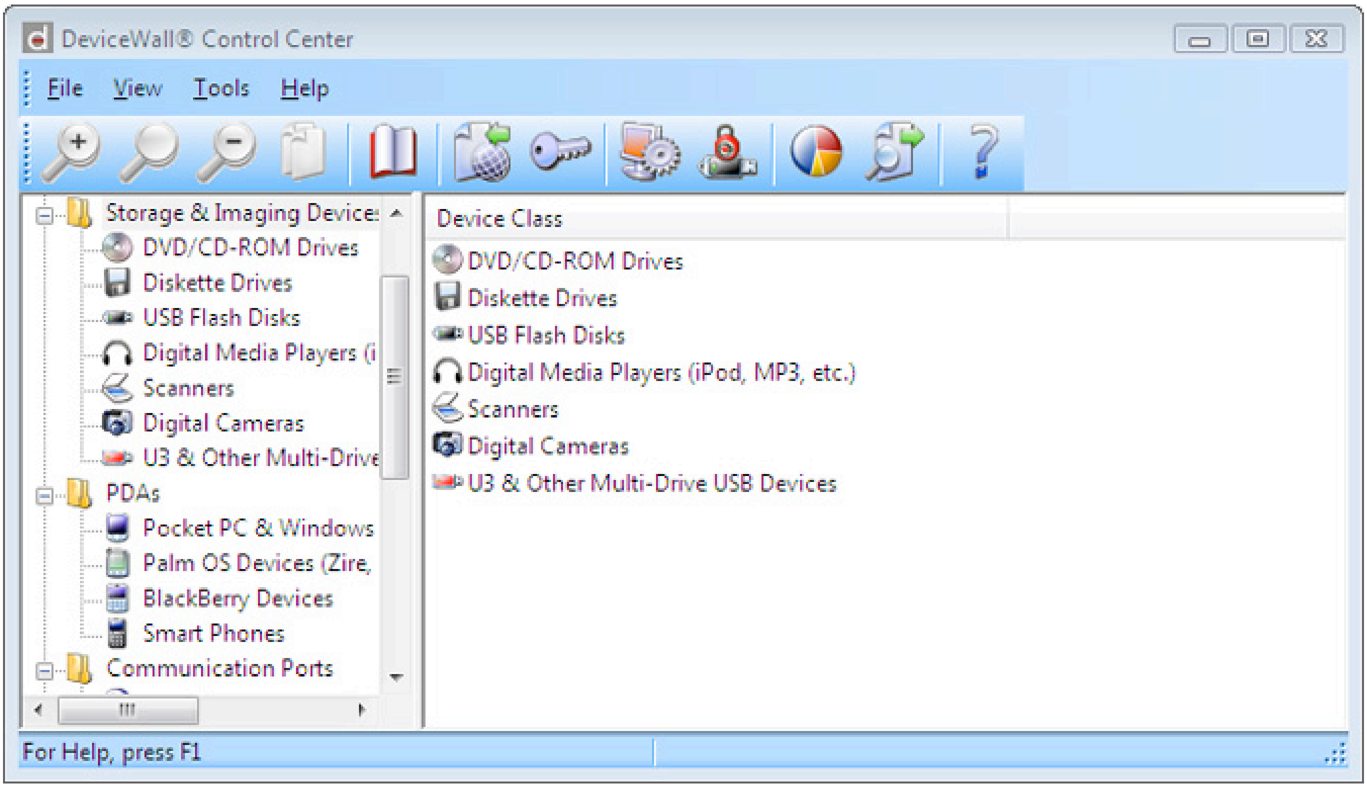
By Mark Woodstone

If you have been reading through (IN)SECURE Magazine or its sister web site Help Net Security, you have seen that endpoint security is one of the hottest information security topics. With all the new portable devices, ranging from 2 GB USB key chains, to U3 sticks or even the new Apple media darling iPhone, organizations are seeing more and more potential problems surrounding them.

You cannot strip search your employees for any eligible portable device, but you can enforce strict company policies with a tool like DeviceWall (www.devicewall.com). This application gives you an opportunity to centrally manage and control the usage of any kind of portable media on computers located on your network.

Installation

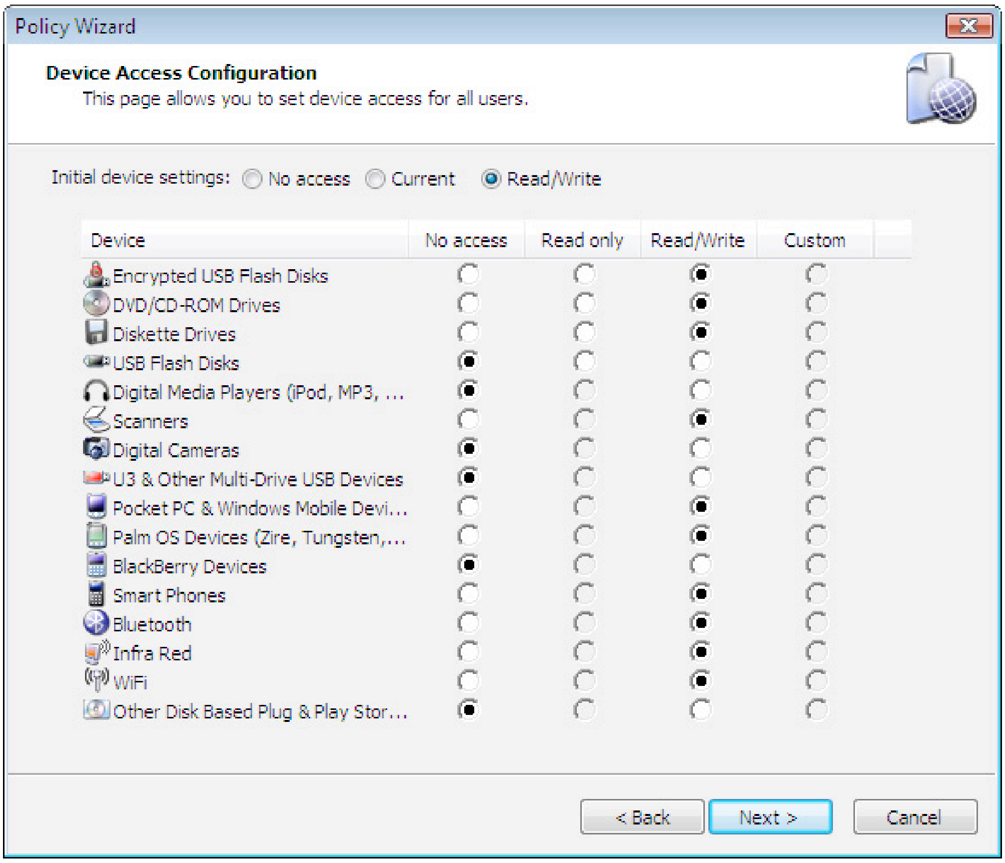
The DeviceWall installation process is a typical one. After setting up your registration details, you have the opportunity of choosing one of two setup options. The application needs an SQL installation, so if you don't have one active yet, just choose the "Typical" type of setup. This way, after DeviceWall is installed, the setup wizard will place on your computer a MSDE instance that will act as an SQL server. As you probably figured out, the SQL server will be used for centralized logging of events. If in the past you used some of the crypto products such as OpenSSL or PGP, the final act of the installation will be a familiar one - you will need to dynamically move the pointer of your mouse to generate a random key later used by the software.



Device Class
DVD/CD-ROM Drives
Diskette Drives
USB Flash Disks
Digital Media Players (iPod, MP3, etc.)
Scanners
Digital Cameras
U3 & Other Multi-Drive USB Devices

The DeviceWall control center interface

During the installation of the product on my computer running Windows Vista, I came across a warning message related to the MSDE SQL runtime. While at first I thought that this is some kind of a bug, DeviceWall promptly gave a message to consult with the Release.txt which came in the installation package. A warning message was about the file msxml2.dll, which was missing but was available as a Hot-fix from the Microsoft Knowledge Base Article 823490.



Device Access Configuration

This page allows you to set device access for all users.

Initial device settings: ○ No access ○ Current ● Read/Write

Device	No access	Read only	Read/Write	Custom
Encrypted USB Flash Disks	○	○	●	○
DVD/CD-ROM Drives	○	○	●	○
Diskette Drives	○	○	●	○
USB Flash Disks	●	○	○	○
Digital Media Players (iPod, MP3, ...	●	○	○	○
Scanners	○	○	●	○
Digital Cameras	●	○	○	○
U3 & Other Multi-Drive USB Devices	●	○	○	○
Pocket PC & Windows Mobile Devi...	○	○	●	○
Palm OS Devices (Zire, Tungsten,...	○	○	●	○
BlackBerry Devices	●	○	○	○
Smart Phones	○	○	●	○
Bluetooth	○	○	●	○
Infra Red	○	○	●	○
WiFi	○	○	●	○
Other Disk Based Plug & Play Stor...	●	○	○	○

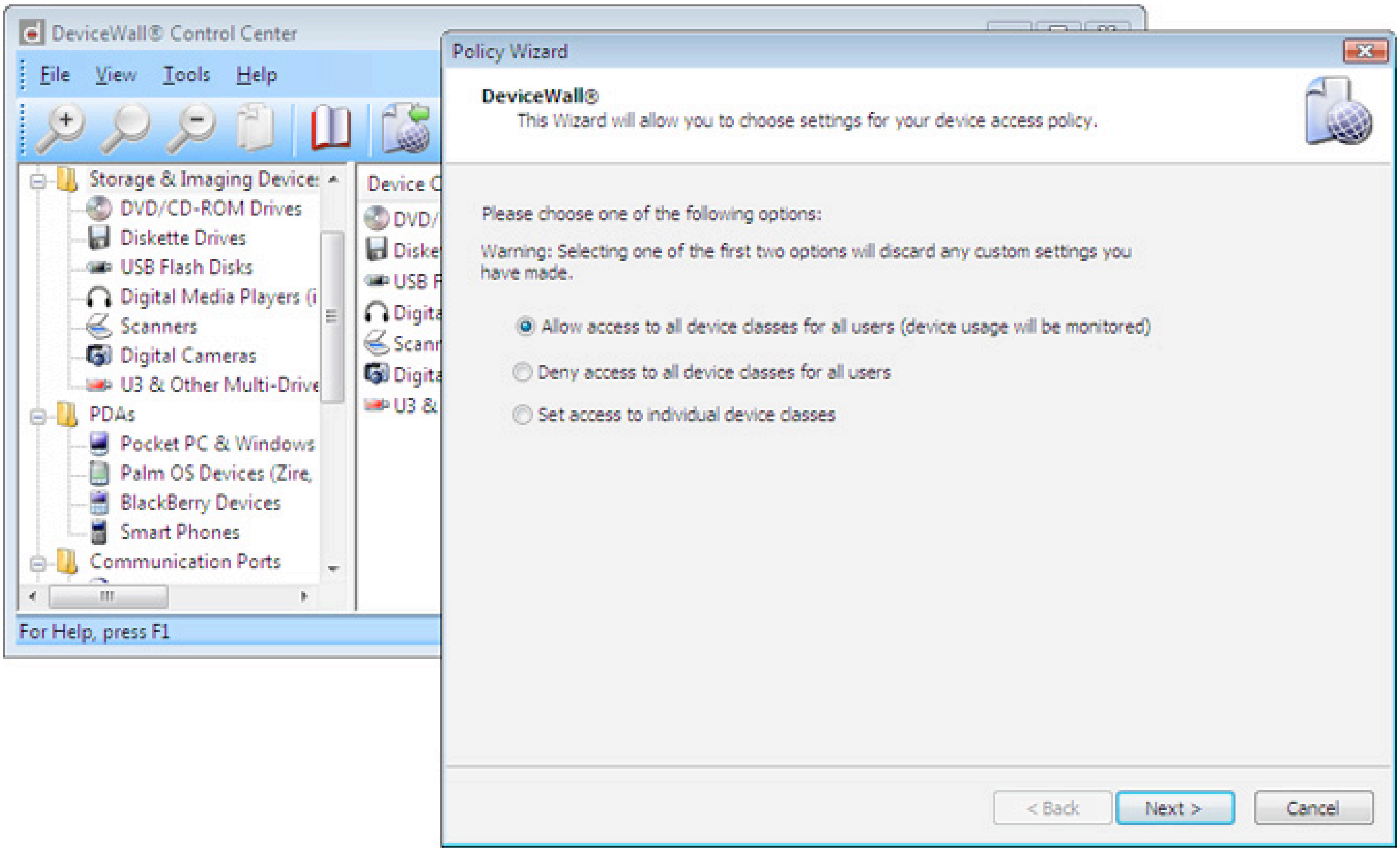
Customizing device access configuration

The link to the article is available in the mentioned text file and the good thing is that the installation doesn't fail because of this.

You will just need to install a Hot-fix before any device connection data can be successfully added to the Audit Log Database.

Usage and functionality

A couple of minutes after I started the installation, the setup was finalized and I must say that I found the graphical user interface very appealing. The application window is easy to apprehend and has a bit larger toolbar buttons than I usually stumble upon.



DeviceWall®

This Wizard will allow you to choose settings for your device access policy.

Please choose one of the following options:

Warning: Selecting one of the first two options will discard any custom settings you have made.

● Allow access to all device classes for all users (device usage will be monitored)

○ Deny access to all device classes for all users

○ Set access to individual device classes

Setting up a default policy

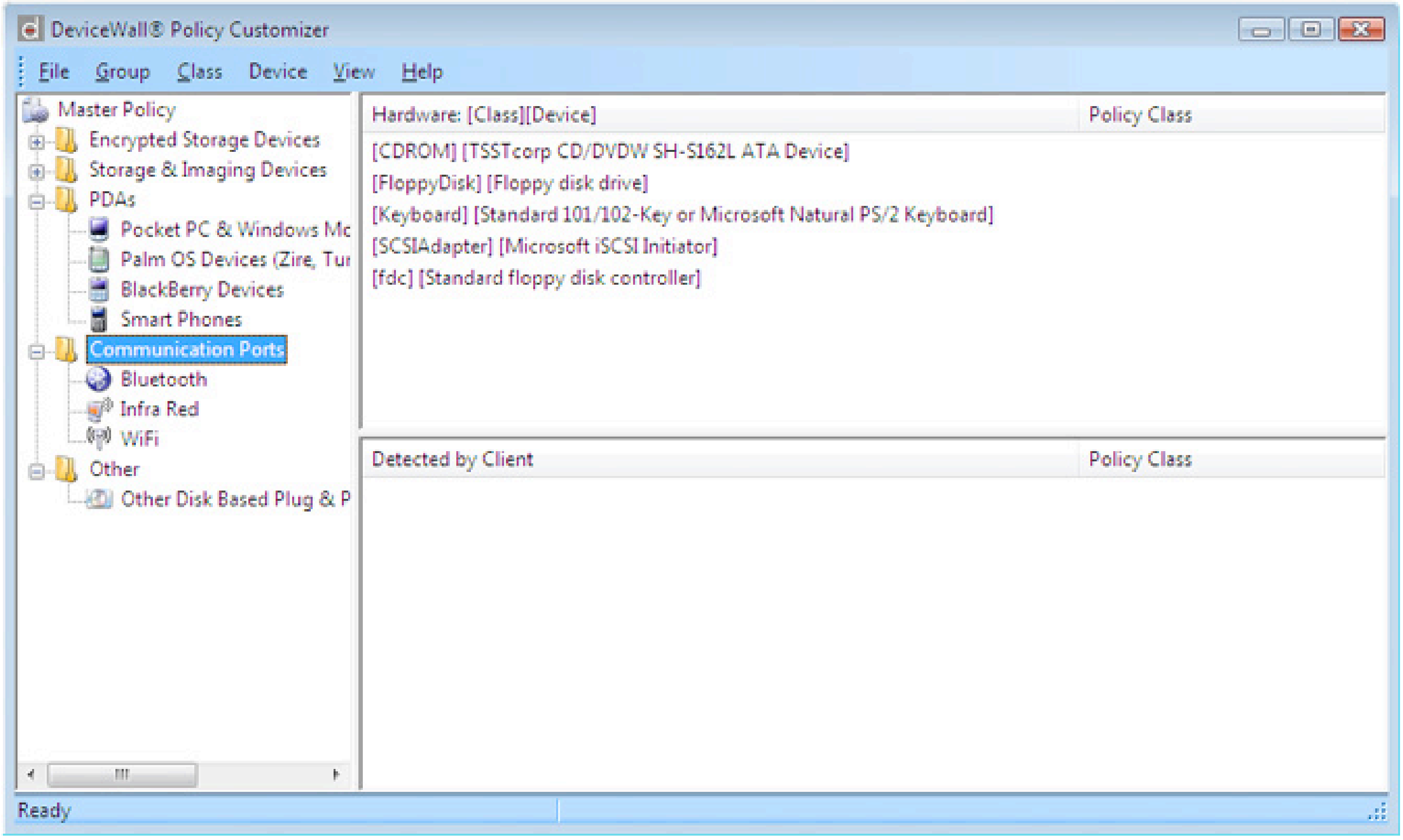
DeviceWall works on the client/server way. You install the application control center on the main computer and easily deploy clients all over the network.

Naturally, you don't need to manually go to every single computer (although strangely enough, not all companies switched from this "old school" way of doing things), as DeviceWall offers some typical remote installation possibilities.

In search for client computers, the administrator can browse a domain or Active Directory, import a list file, enter a computer name, but I found the "specify IP range" the best option for a larger network such as the one I tested at work.

DeviceWall's inner workings are based on a policy which can be setup on different ways. While installing the application you have an option to setup the default policy, but it is recommended than you do it directly from the application after the install.

DeviceWall doesn't log just the policy violations, so for the companies that don't have an already defined security policy related to portable devices, there is a neat way of setting up an "all open" policy to monitor your network.

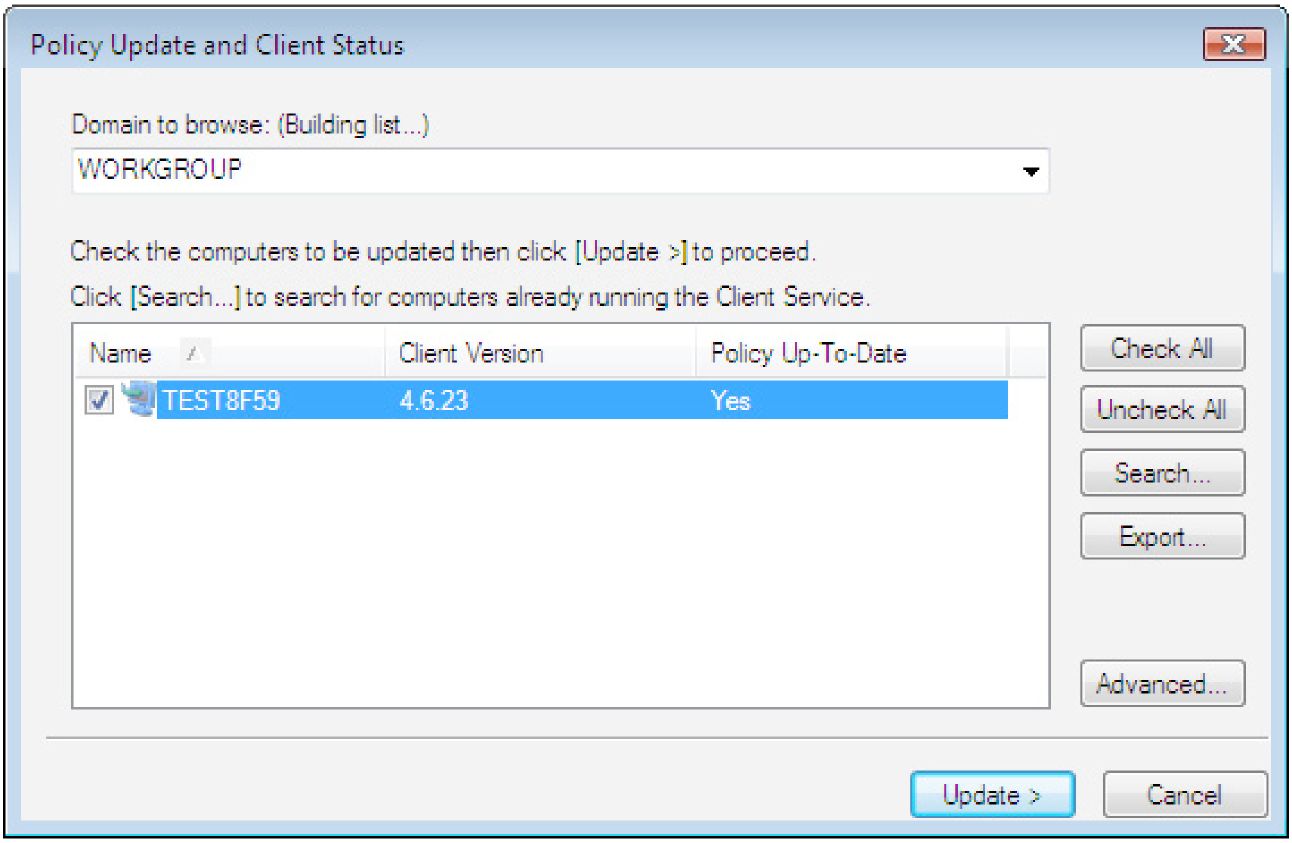


Hardware: [Class][Device]	Policy Class
[CDROM] [TSSTcorp CD/DVDW SH-S162L ATA Device]	
[FloppyDisk] [Floppy disk drive]	
[Keyboard] [Standard 101/102-Key or Microsoft Natural PS/2 Keyboard]	
[SCSIAdapter] [Microsoft iSCSI Initiator]	
[fdc] [Standard floppy disk controller]	

Detected by Client	Policy Class

Customizing the policy

> This way, in a week or so, you could see what actually happens with your users and their devices, and therefore can react to the actual happenings in your network.



Domain to browse: (Building list...)

WORKGROUP

Check the computers to be updated then click [Update >] to proceed.

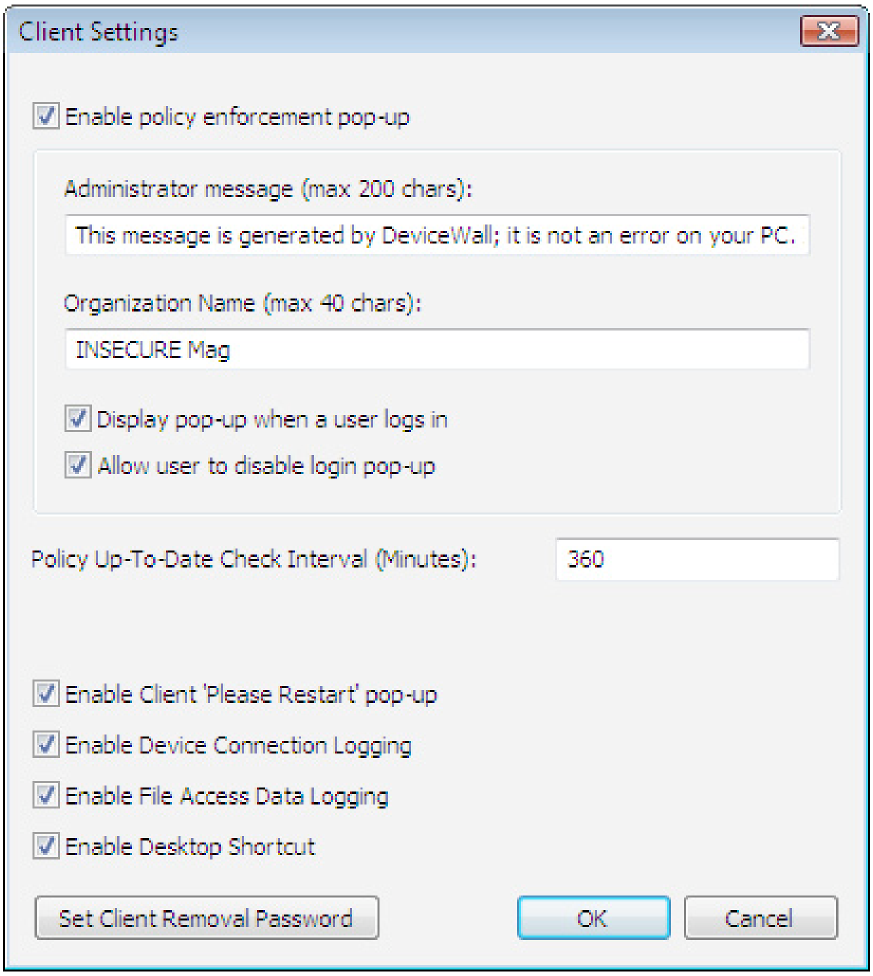
Click [Search...] to search for computers already running the Client Service.

Name	Client Version	Policy Up-To-Date
☑ TEST8F59	4.6.23	Yes

Updating policy on a test computer through the control center

The default policy provides you three different setups - deny all, allow all or to create a custom one.

The good thing is that the software comes with a list of grouped classes, such as storage and imaging devices, portable devices, communication ports etc, so you won't need much time to get into business and start DeviceWall's monitoring of your users. Each of these classes are divided into specific group of devices, so you can easily setup a custom allow/deny rules for each of them. Of course, you can also set permissions based on users and groups.



☑ Enable policy enforcement pop-up

Administrator message (max 200 chars): This message is generated by DeviceWall; it is not an error on your PC.

Organization Name (max 40 chars): INSECURE Mag

☑ Display pop-up when a user logs in

☑ Allow user to disable login pop-up

Policy Up-To-Date Check Interval (Minutes): 360

☑ Enable Client 'Please Restart' pop-up

☑ Enable Device Connection Logging

☑ Enable File Access Data Logging

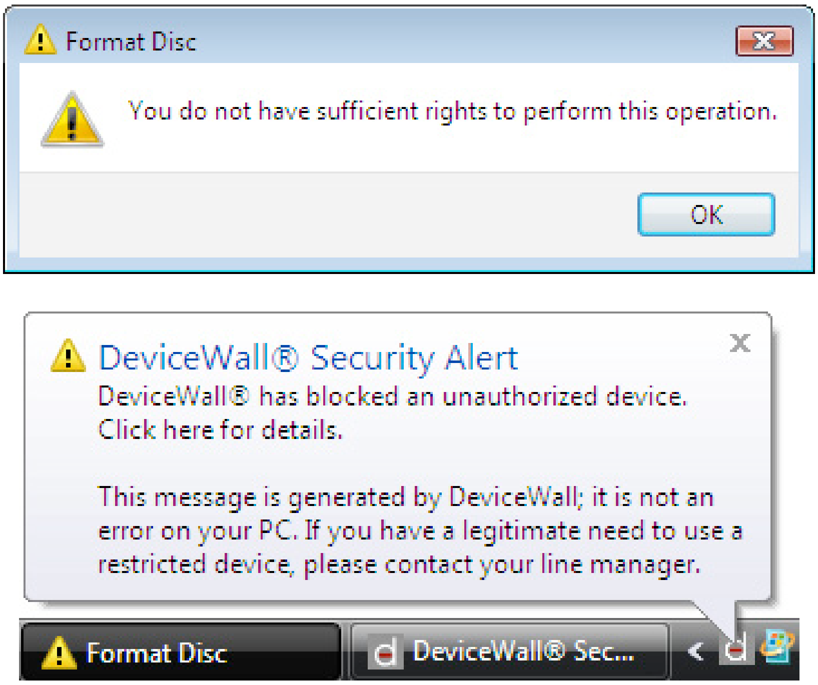
☑ Enable Desktop Shortcut

Creating custom client settings

While setting up the client you can describe the alert the user will get after trying something that is forbidden, as well as create a time interval in which the client will automatically contact the server for possibly updated policy. You can do this manually from the command center, but it is of course much better and flexible to do it automatically. As you would expect, the end users won't have any possibility of changing, editing or removing the client portion of DeviceWall on their computers.

One of the things I really liked was a piece of functionality that comes around while setting the custom policy. Let's say that your company has a standard equipment given to all the employees, such as a typical USB memory stick or a specific PDA device needed for the everyday work experience. For instance if you would block all USB storage devices, the one needed by the user would also get in the "black zone".

DeviceWall offers administrators the possibility to define and setup a specific device that can be identified as "safe" and therefore can be used even if the company policy denies the same type of hardware.


Format Disc

You do not have sufficient rights to perform this operation.

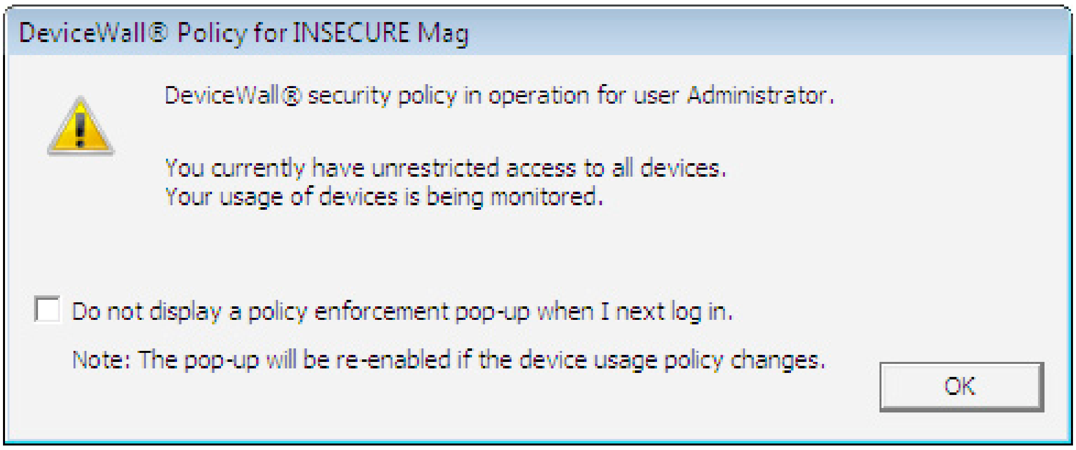
DeviceWall® Security Alert

DeviceWall® has blocked an unauthorized device.
Click here for details.

This message is generated by DeviceWall; it is not an error on your PC. If you have a legitimate need to use a restricted device, please contact your line manager.

Error and alert after starting a "forbidden" device

Besides the few nice additional tools I will mention afterwards, the last part of this software's functionality is related to auditing the logs generated by the device usage throughout the network computers. There is a separate portion of the product which offers different types of graphical reports, which you can redraw based on time frames, device classes, as well as different graphical presentation options.


DeviceWall® Policy for INSECURE Mag

DeviceWall® security policy in operation for user Administrator.

You currently have unrestricted access to all devices.
Your usage of devices is being monitored.

☐ Do not display a policy enforcement pop-up when I next log in.

Note: The pop-up will be re-enabled if the device usage policy changes.

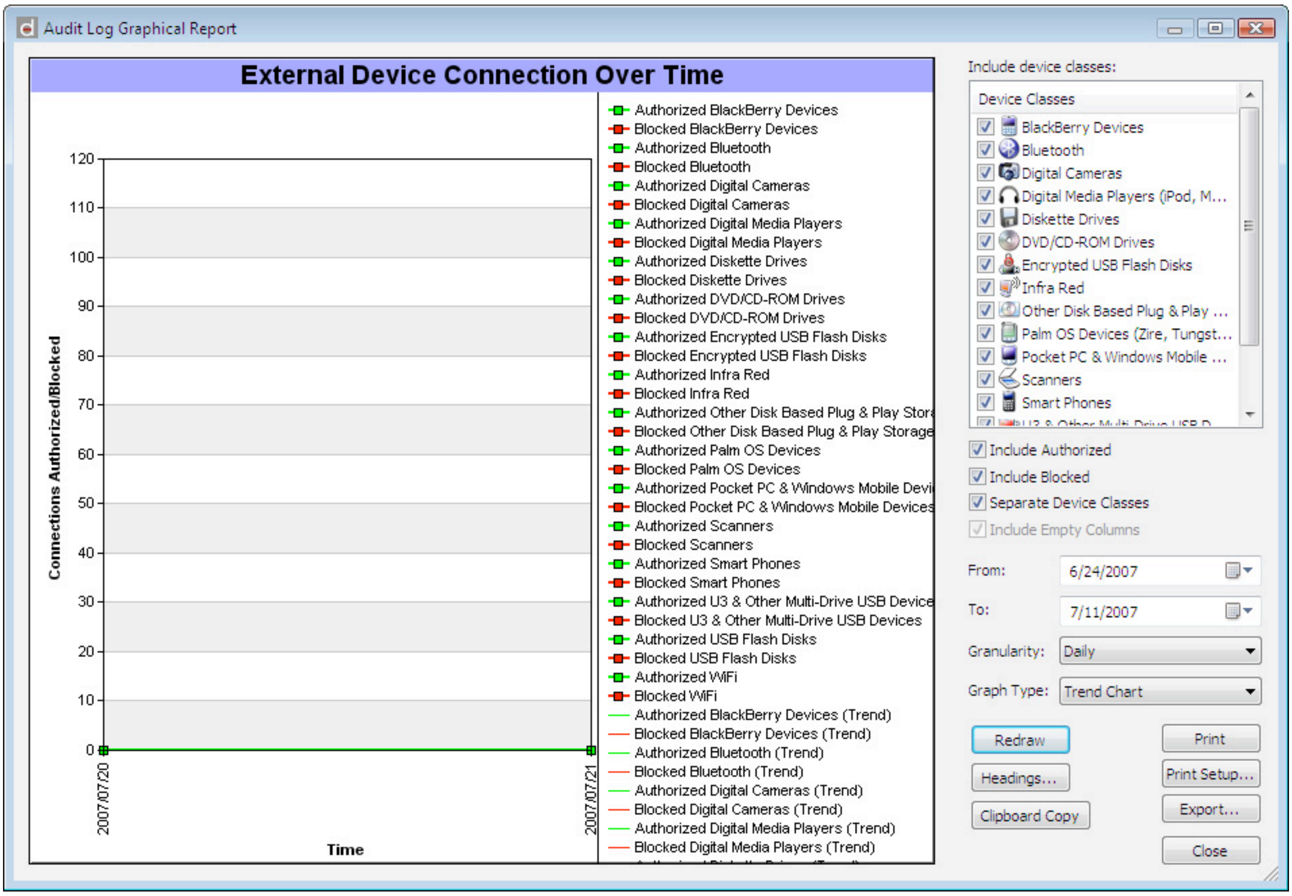
Alert that DeviceWall is present on the client computer

If you're running your control center on a computer with a screen resolution lower than 1024x768, the application will give you an error saying it needs at least 1024x768 to draw graphs.

I know that chances of installing this kind of a management platform on a system with a resolution such as 800x600 are slim, but this can also appear on some widescreen notebooks.

I found a quick workaround for this. Just go to your system settings and switch to a resolution needed by the application. Your display will look shoddy, but just use this new resolution until you click the Audit Log Graphical Display icon.

As soon as the Audit Log opens, switch back to your old resolution and the log presentation option will work just fine.


Audit Log Graphical Report
External Device Connection Over Time
Connections Authorized/Blocked
120
110
100
90
80
70
60
50
40
30
20
10
0
2007/07/20
2007/07/21
Time
Authorized BlackBerry Devices
Blocked BlackBerry Devices
Authorized Bluetooth
Blocked Bluetooth
Authorized Digital Cameras
Blocked Digital Cameras
Authorized Digital Media Players
Blocked Digital Media Players
Authorized Diskette Drives
Blocked Diskette Drives
Authorized DVD/CD-ROM Drives
Blocked DVD/CD-ROM Drives
Authorized Encrypted USB Flash Disks
Blocked Encrypted USB Flash Disks
Authorized Infra Red
Blocked Infra Red
Authorized Other Disk Based Plug & Play Stor
Blocked Other Disk Based Plug & Play Storage
Authorized Palm OS Devices
Blocked Palm OS Devices
Authorized Pocket PC & Windows Mobile Devi
Blocked Pocket PC & Windows Mobile Devices
Authorized Scanners
Blocked Scanners
Authorized Smart Phones
Blocked Smart Phones
Authorized U3 & Other Multi-Drive USB Device
Blocked U3 & Other Multi-Drive USB Devices
Authorized USB Flash Disks
Blocked USB Flash Disks
Authorized WiFi
Blocked WiFi
Authorized BlackBerry Devices (Trend)
Blocked BlackBerry Devices (Trend)
Authorized Bluetooth (Trend)
Blocked Bluetooth (Trend)
Authorized Digital Cameras (Trend)
Blocked Digital Cameras (Trend)
Authorized Digital Media Players (Trend)
Blocked Digital Media Players (Trend)
Redraw
Print
Headings...
Print Setup...
Clipboard Copy
Export...
Close

Include device classes:

Device Classes

- ☑ BlackBerry Devices
- ☑ Bluetooth
- ☑ Digital Cameras
- ☑ Digital Media Players (iPod, M...
- ☑ Diskette Drives
- ☑ DVD/CD-ROM Drives
- ☑ Encrypted USB Flash Disks
- ☑ Infra Red
- ☑ Other Disk Based Plug & Play ...
- ☑ Palm OS Devices (Zire, Tungst...
- ☑ Pocket PC & Windows Mobile ...
- ☑ Scanners
- ☑ Smart Phones

☑ Include Authorized

☑ Include Blocked

☑ Separate Device Classes

☑ Include Empty Columns

From: 6/24/2007

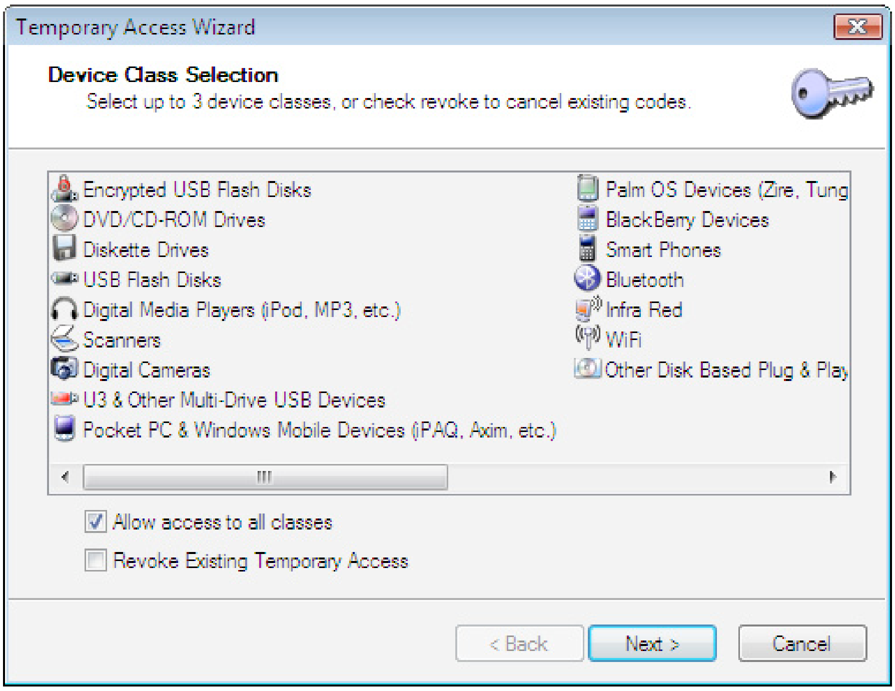
To: 7/11/2007

Granularity: Daily

Graph Type: Trend Chart

Options you can chose while drawing reports

The specific events can also be presented through the DeviceWall main interface, where a user can browse through per device or per user access details such as files and locations, as well as check out a file access summary with all the top file extensions. For example, the Dynamic Activity Monitor applet can be installed to client computers to dynamically check out all the events logged from this location. This allows you to check a specific (potentially problematic) computer without accessing the control center on the main server.



Device Class Selection

Select up to 3 device classes, or check revoke to cancel existing codes.

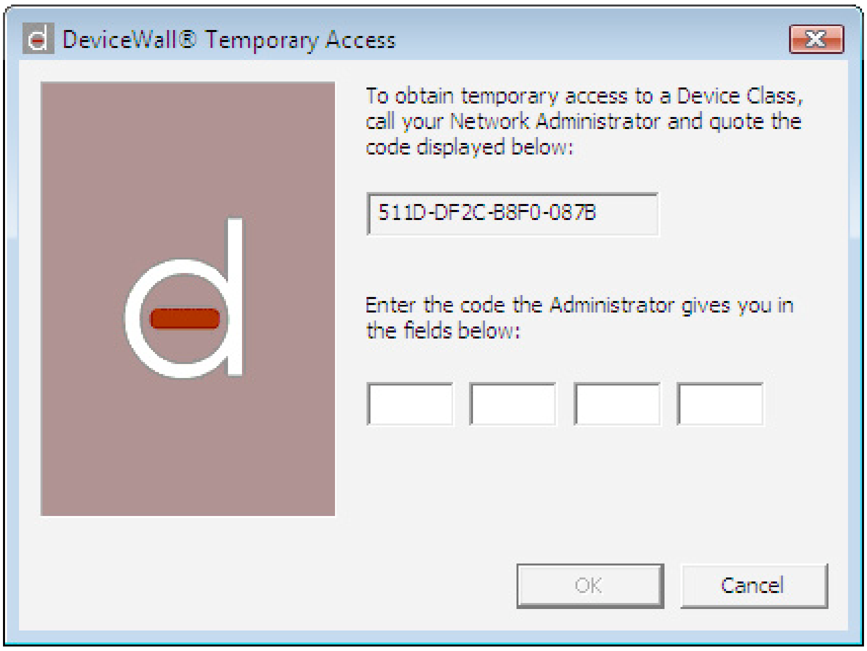
- Encrypted USB Flash Disks
- DVD/CD-ROM Drives
- Diskette Drives
- USB Flash Disks
- Digital Media Players (iPod, MP3, etc.)
- Scanners
- Digital Cameras
- U3 & Other Multi-Drive USB Devices
- Pocket PC & Windows Mobile Devices (iPAQ, Axim, etc.)
- Palm OS Devices (Zire, Tung
- BlackBerry Devices
- Smart Phones
- Bluetooth
- Infra Red
- WiFi
- Other Disk Based Plug & Play

☑ Allow access to all classes

☐ Revoke Existing Temporary Access

Using Temporary Access Wizard

The Temporary Access Tool is another interesting addition through which an administrator can temporarily give users access to specific devices. The time frame can be specified, or if needed, a 16-digit key can be dispatched to the user that can be used for unlocking some of the resources.

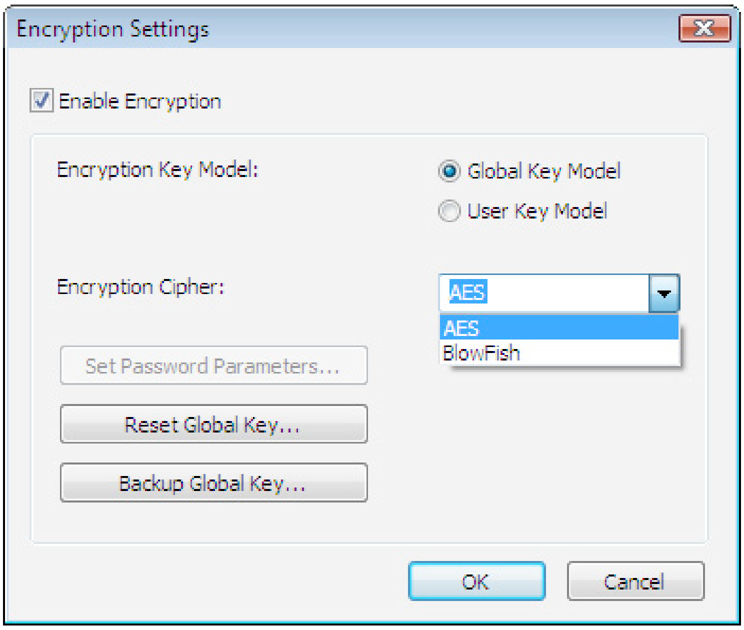


To obtain temporary access to a Device Class, call your Network Administrator and quote the code displayed below:

511D-DF2C-B8F0-087B

Enter the code the Administrator gives you in the fields below:

I will conclude this article on DeviceWall by mentioning a nice, but effectively not so important tool, that offers users possibility to encrypt data on recognized USB disks.



☑ Enable Encryption

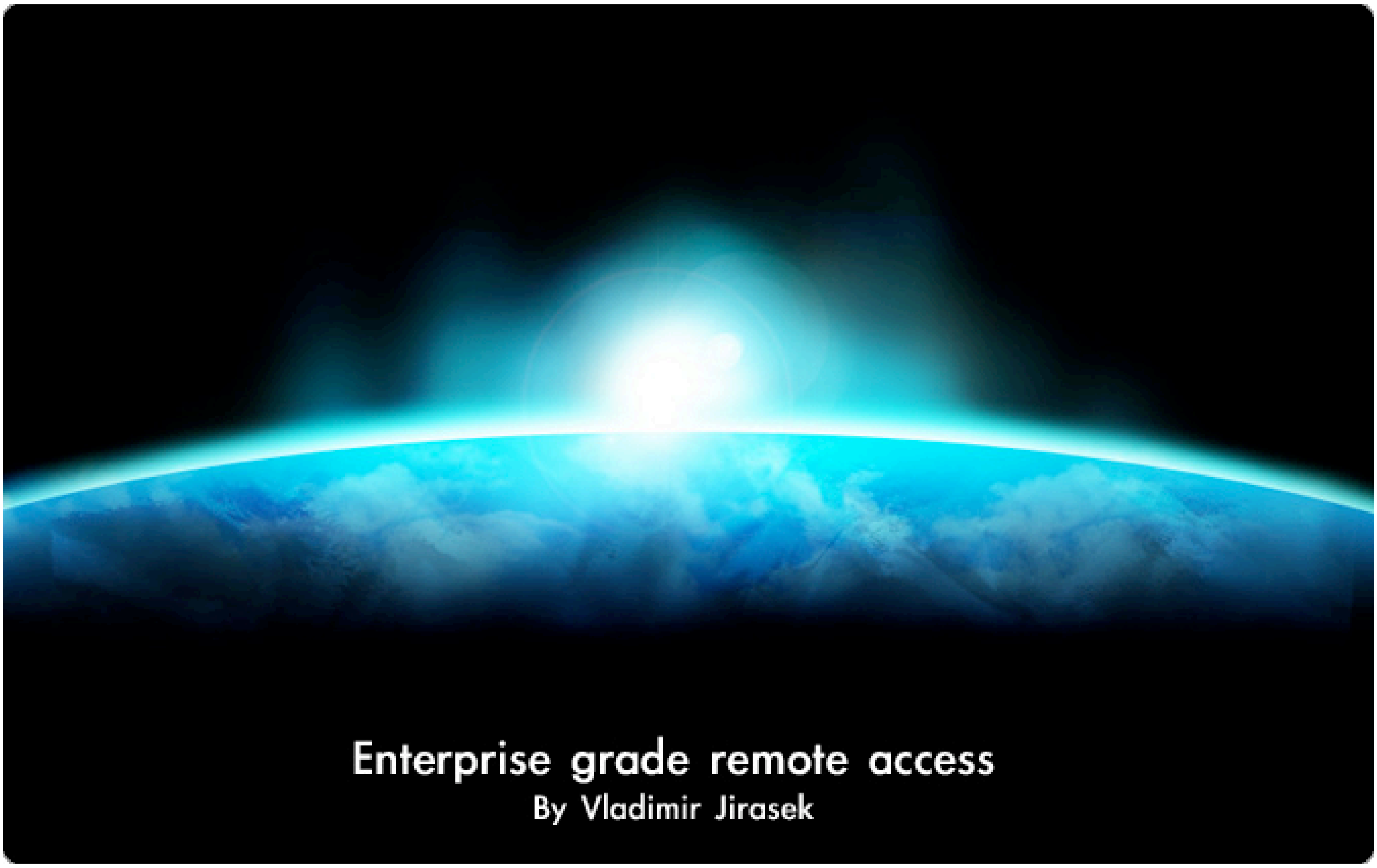
Encryption Key Model: ● Global Key Model ○ User Key Model

Encryption Cipher: AES

Final thoughts

DeviceWall is really an excellent application. In a nice looking GUI, it sports quality policy deployment methods, powerful event logging/analyzing options and strong policy enforcement and alerting actions. Bottom line - it works flawlessly and will definitely be an extensive endpoint security mechanism for your network.

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



Enterprise grade remote access

By Vladimir Jirasek

I started with a basic solution for remote access to the network in my previous article published in (IN)SECURE volume 11. The solution was based on certificates and used two-factor authentication in its simplest mode – something you know (certificate pass-phrase) and something you have (a certificate).

However there was one big issue with the solution – manageability and scalability. We cannot really expect that an administrator, either security or network one, is going to manually generate certificates and then install them into hundreds or thousands of computers. That is why the solution was not really ready for enterprises with large number of computers and users. That is why we need to look for enterprise grade solutions and this article is going to show some of them, putting emphasis on authentication and authorization.

When choosing a solution for remote access, these questions should be answered:

- what is an acceptable level of security
- how many users will be enrolled for the service in total and using in peak times
- what applications need to be accessed by remote users.

The level of security is rather general term and should include authentication and authorization of users, access control, logging and monitoring of security events, enforcing end point security, level of encryption, resetting access, if a password is forgotten, etc.

Number of users will define the integration necessary with enterprise identity and access management system, scaling of the remote access platform and necessary bandwidth to serve users in peak times.

Application will define the type of the remote access system, such as full IP or SSL based systems. I will focus, obviously on security aspects covering different types of remote access systems.

Authentication and authorization

This is by far the first question anyone asks about the remote access system. We all hear about dual factor authentication, so what is it and, most importantly, do we actually need the dual factor authentication? And the answer is...YES

- it is more secure and
- it is possibly a regulatory requirement for your company! It is more secure by requiring users to present more than one piece of evidence to prove identity.

There are three factors of authentication:

- **knowledge** (something you know) – the most common and probably the most insecure method of all three. Knowledge can be easily transferred (would you not tell the password under the life threat?). Passwords and pass-phrases are typical examples and users have proven track of not selecting passwords strong enough. This can lead to dictionary or brute force attacks.
- **possession** (something you have) – you must have something to authenticate. This can be something like a certificate, a mobile phone (or better a SIM card), a RAS token, a smart card, etc. On its own, this is almost as (in)secure as the first one, purely because it can be easily transferred and lost. Although it provides better protection against brute force and dictionary attacks.
- **being** (someone you are) – the best method of all that uses your body (or parts of) to prove your identity to the system.

Several parts of body can be used like:

- iris – reading iris pattern, little more accepted than retina scan
- retina – some people might see this as little too intrusive
- palm – scans characteristics of the palm, there are some hygiene issues
- finger – old good finger print
- typing cadence – apparently everyone has its own unique typing cadence. (well I am not sure, after couple pints of beer...)
- voice – tricky one as your voice may sound different sometimes, also useless for disabled people
- DNA – the most accurate form of identification, the speed and collection of material might be an issue
- palm veins – reading blood veins in your palm; hygienic and spots a chopped palm.

Each of these biometric attributes has it own pros and cons, user acceptance, cross-over error rate, speed and the size of the template.

Interestingly enough, some say that dual factor is always more secure than single factor authentication. Please, allow me to disagree. I think that properly implemented biometrics (someone you are) is more secure than the combination of know and have methods. Why? Try to authenticate on a palm vein reader using a chopped (dead) palm. No luck! Remember that the primary objective of authentication is to establish the identity, i.e. verify it is me who is logging to the system, not someone who stole my password and RSA token/mobile phone. What do you think?

However, the most common combination of authentication methods is “something you know” and “something you have”. The reason is that they are, to date, the easiest ones to implement. You simply give something to users and let them to set the passwords/PIN/passphrase and that's it! Maybe this will change when biometric methods become more available, easier to use and accepted by us, humans.

Now, let's see the regulatory side. The most recent standard to mandate dual factor authentication for remote access to the network is the Payment Card Industry Data Security Standard (PCI DSS). This standard applies to all companies that accept credit cards and explicitly talks about how to authenticate remote users. The next close match is ISO27002 (previously ISO17999:2005) that loosely mentions HW tokens for authentication.

You company policy most likely mandates dual factor authentication as well.

Integration

Another important requirement for a remote access system is how it integrates with existing IT infrastructure and database of corporate users. Most organizations use Microsoft Active directory.

LDAP and Kerberos based authentication and authorization service capable of scaling into hundreds of thousands users with distributed database. Obviously these systems can also authorize users, i.e. is the user allowed to use RAS service at this time?

If your organization already has Active directory, or any other LDAP based user database, it makes business sense linking the remote access system to it. Obvious benefits are:

- up-to-date user database user creation, disabling and deletion take effect immediately. SOX auditors would call this “in timely manner”.
- user have just one set of credentials, i.e less chance they would write passwords on a piece of paper.

PCI DSS	8.3 Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens or VPN (based on SSL/TLS or IPSEC) with individual certificates.
ISO 27002	11.4.2 User authentication for external connections *Control* Appropriate authentication methods should be used to control access by remote users. *Implementation guidance* Authentication of remote users can be achieved using, for example, a cryptographic based technique, hardware tokens, or a challenge/response protocol. Possible implementations of such techniques can be found in various virtual private network (VPN) solutions. Dedicated private lines can also be used to provide assurance of the source of connections.

Logging and monitoring

The operational part is sometimes overlooked but it is important to get it right. It is easy to install a system and forget about it, virtually creating a channel into the enterprise network. Such system should send logs off to a remote logging
server where it is important to setup a monitoring and escalation system. This can be simple syslog based server with watchlog or alternatively an enterprise grade logging and monitoring system.

Is it important to watch logs 24/7 for possible incidents? I think so. Also, it is important to log appropriate level of detail. Cisco VPN GW, for example, does log username, time, IP address of the remote client, version of the Cisco VPN client. However, it does not log the hostname and the operating system of the client computer. So if you want to check that the user is using the company laptop to access the network, no chance. Perhaps, this should force you to purchase the end-point security add-on.

End-point security

This is currently the buzz-word. If you network and remote access systems do not provide endpoint security, you have a problem.

Do you know what is connected to your network? You might know if you have 802.1x and using non-exportable certificates. But do you know what is the level of compliance with your policies, patch levels and antivirus updates? If you do, you must have such system implemented. RAS is logically extension of the local area network and as such must have the same level of protection. Watch out for systems from Microsoft, Cisco, Symantec and others.

Level of encryption

This used to be the most discussed topic of all times in network security, don't you think? But with the arrival of public encryption algorithms and export restrictions lifted, it is easy to implement very strong encryption system. The most common is AES with various bit sizes. The encryption algorithm will determine the hardware requirements and the maximum numbers of users at one time. When configuring VNP gateways always aim for the most secure configuration that would be accepted by all clients. Fortunately, all enterprise computers should be configured the same way and eliminating incompatibilities. Following combinations of symmetric encryption and hash functions provide enterprise level of security:

Encryption	Key size (b)	Hash	Hash size (b)
AES-256	256	SHA-2	224, 256, 384, 512
AES-192	192	SHA-1	160
AES-128	128		

It is important to set the encryption key to provide adequate security without affecting performance. For example AES-256 is approx. 25% slower than AES-128 but provides double assurance (subject to random key material).

Resetting access

This is very interesting topic and each authentication technology uses different technique. The basic question is “How do I know you are, you are saying you are, over the phone?” This is the case if someone looses the password/ token and needs to connect to urgently finish the work.

I would suggest this is the area where great considerations and testing should be done. Remember that service desk, usually dealing with these request, have one task and one task only: the service for the user does not work and needs to be restored promptly. That is why so many social engineering attacks use service desks.

Types of remote access

The applications needed will determine the type of remote access system. There are two major type to look at:

1. SSL VPNs – Web based access to applications.

2. IP tunnel VPNs – full IP access to applications needed.

Let's go over them in little more detail.

SSL VPN - This type of remote access is on rise as more applications are web enabled. Effectively SSL VPN act as reverse proxies with SSL off-load. My small example of providing access to company Intranet was simple SSL VPN.

Some of possible solutions:

- Apache reverse proxy – discussed in my previous (IN)SECURE article
- MS ISA server
- Cisco VPN GW.

End point security can be assured using special Java applets which user's computer must run in order to get through the VPN box. Such Java applet can run the code on the local computer and send results to the VPN gateway and policy server for verification.

The advantage of SSL VPN systems is that it does not open IP tunnel to the network and can only reverse proxy Web based applications or some special applications using Java applet. This limits potential attack surface to minimum. Obviously SSL VPNs receive rather increasing attention and are favorite means of remote access, if the application allows it.

Users can also connect from anywhere on the Internet with just the https port open and even behind a proxy server.

One obvious disadvantage is that the client computer is connected to the Internet and company network at the same time. This is a threat to be included in the risk assessment. However, properly configured client personal firewall should minimize such risk.

IPSec VPN - Old good IPSec. If you need to give users full access to the network. IPSec in ESP/tunnel mode is used. This mode can traverse NAT. End point security is achieved with special software running on the client which communicates with VPN GW and Radius server in the back end. Both Cisco and Microsoft have their versions of Network Access Control systems. For obvious reasons IPSec VPNs do not work easily through the firewall and proxy server.

The best practice is to enable “default route mode” where all traffic is routed to the IPSec tunnel, effectively disconnecting computer from the internet. The computer retains specific routing to IPSec VPN GW though.

In both solutions there should always be firewall between VPN GW and the internal network to limit what systems users have access to. The reason is, without the firewall once the user is connected to VPN GW, it has unlimited access to the network (subject to routing and internal segregation). It is good practice to limit access to internal systems with classification INTERNAL, like Intranet site, email systems, proxy server for internet access, file server with non sensitive data.

Obviously the level of access the users get should correlate the classification of data and the used authentication technique.

Virtually everyone has a mobile phone (or two). Banks use it to deliver authentication text messages so why not use it for remote access.

Examples of interesting authentication systems for remote access

These are definitely the most widely used authentication systems for remote access. Please note that these can be used for all types of the remote access systems described above.

SecureID - I believe is by far the most widely used solution for remote access authentication. It is based on the time synchronization between a token with display and back-end RSA server. The number changes every minute and provides “something you have”. The user is required to combine this number with PIN (something you know) on login. The problem with this system us that the PIN is usually 4 numbers, it is difficult to change and the its randomness is questionable.

Text message - Virtually everyone has a mobile phone (or two). Banks use it to deliver authentication text messages so why not use it for remote access. The idea is rather simple: replace SecureID token with the phone. The system can generate new number on every login attempt (successful or not) or in the regular intervals and send it to pre-configured mobile phone number within the user's profile. I personally use it and I like it over SecureID:
a) I do not need yet another device to carry with me all the time and
b) I take care of my mobile phone, more than the RAS token. If the phone is lost I get the new SIM card with the same number, making the original one useless.

The SMS message delivers the “something you have” part but where is “something you know”? Well it turns out that the system can use your Active Directory password instead of PIN. I like this more than PIN as I can control password policies for users, unlike PIN. See references section for more details.

Certificate - I have covered the certificate usage in the previous article. Obviously for enterprise use it is important to make sure certificates can be enrolled and distributed automatically and must be locked down to the computer or the user. The certificates provide “something you have”. The other part is usually the user's password.

Office link (T-Mobile UK product name) - Little exception among the others in the list. This is the name of the service provided by T-Mobile UK. A company, a client of T-mobile, is provided with a special virtual VPN network. Then it can give its workforce SIM cards provisioned for the service which makes sure that only these SIM cards are allowed to be a part of the Virtual VPN for the company. Second factor authentication is implemented by requiring username and password when logging in. The secure link between the company and T-Mobile is established by using an IPSec tunnel.

This system is rather unique as it “outsources” remote access to a telecommunication company and an enterprise does not have to procure remote access hardware and software and operate it.

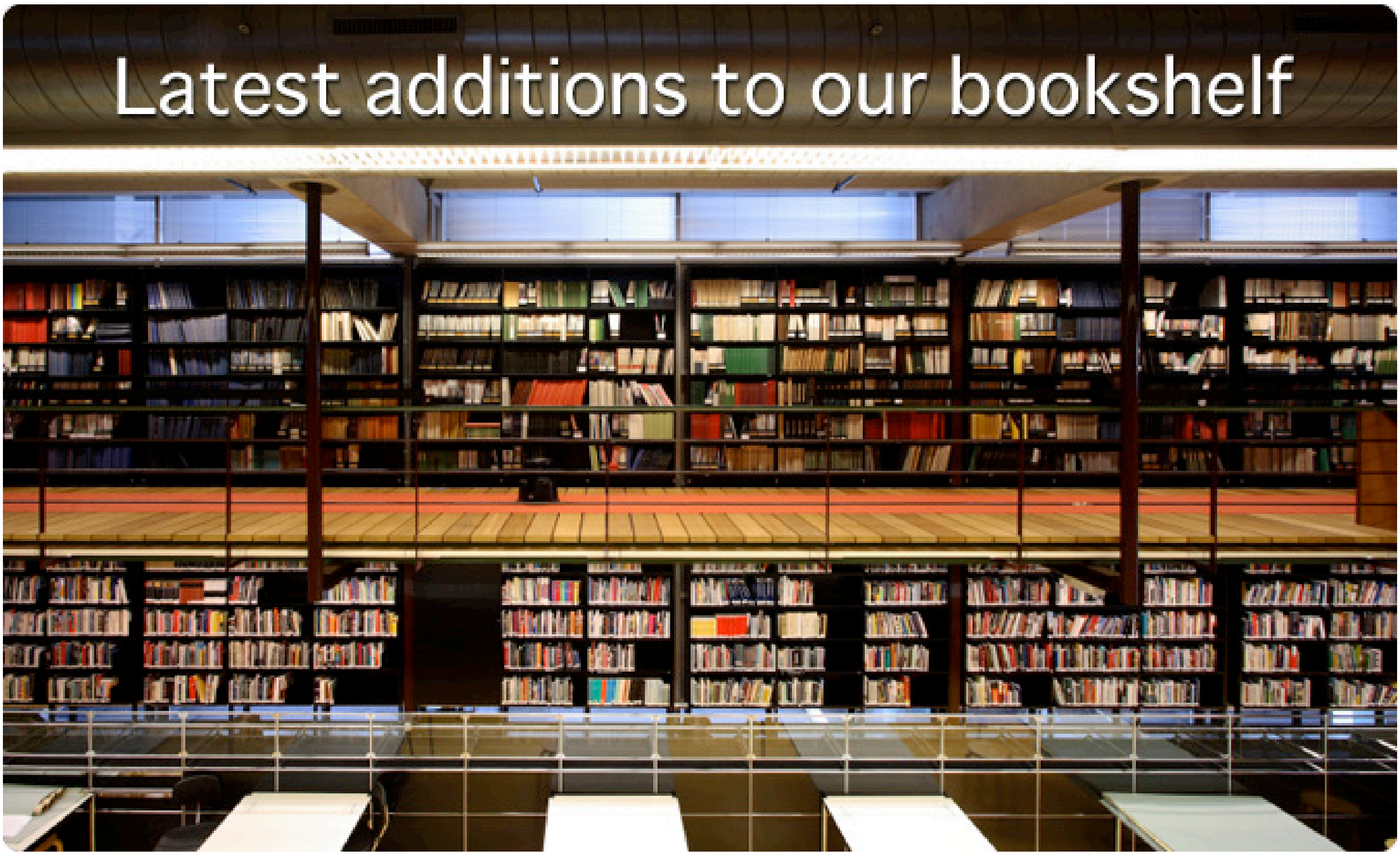
Conclusion

The way we access applications inside the networks is fascinating subject. The boundaries between inside and outside gradually diminish and we, as security professionals, face the new security threats. Having properly designed, secured and maintained remote access system is the key for the business to compete in fast moving world. It is no longer possible to fire an excuse “I am traveling, will login to my email and send it to you next week when I am back from my business trip.” There will be no-one to send it to then!

Let's design solutions that fit the purpose and help our businesses stay on a competitive edge.

Vladimir Jirasek is an experienced security professional currently working as the Head of System Security at T-Mobile UK. Recently migrated to Apple's Mac OS X operating system and is loving it. He holds CISSP-ISSAP, CISM and MCSE certifications and is the member of the ISSA UK chaper. He can be reached at vladimir.jirasek@googlemail.com and www.vjirasek.eu.

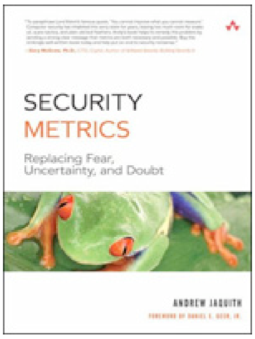
Latest additions to our bookshelf



Security Metrics: Replacing Fear, Uncertainty, and Doubt

By Andrew Jaquith

Addison-Wesley Professional, ISBN: 0321349989

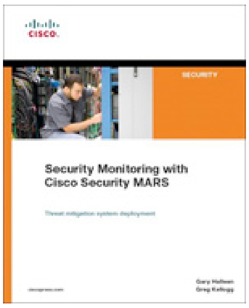


Security Metrics is the first comprehensive best-practice guide to defining, creating, and utilizing security metrics in the enterprise. Using sample charts, graphics, case studies, and war stories, Yankee Group Security Expert Andrew Jaquith demonstrates exactly how to establish effective metrics based on your organization's unique requirements. You'll discover how to quantify hard-to-measure security activities, compile and analyze all relevant data, identify strengths and weaknesses, set cost-effective priorities for improvement, and craft compelling messages for senior management.

Security Monitoring with Cisco Security MARS

By Gary Halleen and Greg Kellogg

Cisco Press, ISBN: 1587052709

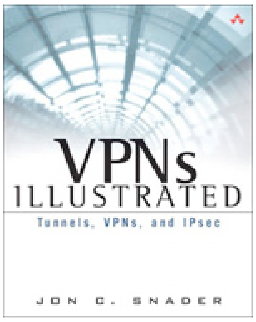


Cisco Security Monitoring, Analysis, and Response System (MARS) is a next-generation Security Threat Mitigation system. Cisco Security MARS receives raw network and security data and performs correlation and investigation of host and network information to provide you with actionable intelligence. Security Monitoring with Cisco Security MARS helps you plan a MARS deployment and learn the installation and administration tasks you can expect to face. Additionally, this book teaches you how to use the advanced features of the product, such as the custom parser, Network Admission Control (NAC), and global controller operations.

VPNs Illustrated: Tunnels, VPNs, and IPsec

By Jon C. Snader

Addison-Wesley Professional, ISBN: 032124544X

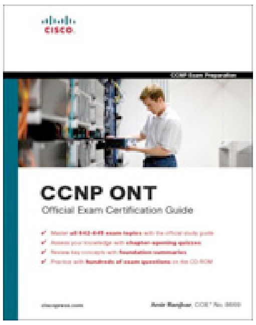


By explaining how VPNs actually work, networking expert Jon Snader shows software engineers and network administrators how to use tunneling, authentication, and encryption to create safe, effective VPNs for any environment. Using an example-driven approach, VPNs Illustrated explores how tunnels and VPNs function by observing their behavior “on the wire.” By learning to read and interpret various network traces, such as those produced by tcpdump, readers will be able to better understand and troubleshoot VPN and network behavior.

CCNP ONT Official Exam Certification Guide

By Amir Ranjbar

Cisco Press, ISBN: 1587201763



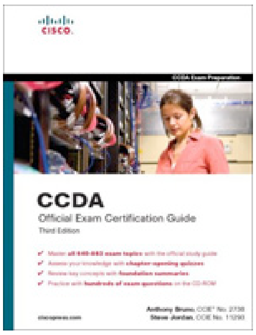
CCNP ONT Official Exam Certification Guide follows a logical organization of the CCNP ONT exam objectives. Material is presented in a concise manner, focusing on increasing your retention and recall of exam topics.

You can organize your exam preparation through the use of the consistent features in these chapters. “Do I Know This Already?” quizzes open each chapter and allow you to decide how much time you need to spend on each section.

CCDA Official Exam Certification Guide, Third Edition

By Anthony Bruno and Steve Jordan

Cisco Press, ISBN: 1587201771



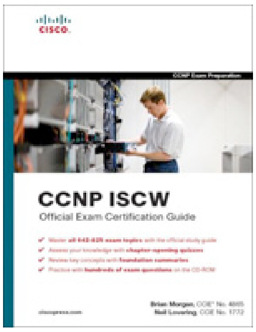
CDA Official Exam Certification Guide, Third Edition, is a best-of-breed Cisco exam study guide that focuses specifically on the topics for the DESGN exam.

CCDA Official Exam Certification Guide presents you with an organized test preparation routine through the use of proven series elements and techniques. Exam topic lists and concise Foundation Summary information make referencing easy and give you a quick refresher whenever you need it.

CCNP ISCW Official Exam Certification Guide

By Brian Morgan and Neil Lovering

Cisco Press, ISBN: 158720150X



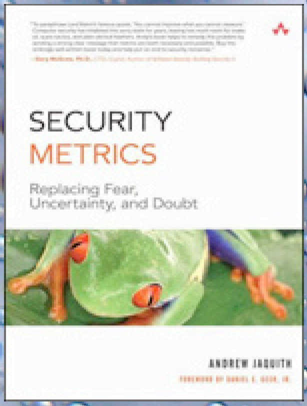
CCNP ISCW Official Exam Certification Guide is Cisco exam study guide that focuses specifically on the objectives for the Implementing Secure Converged Wide Area Networks exam (642-825 ISCW).

CNP ISCW Official Exam Certification Guide follows a logical organization of the CCNP ISCW exam objectives. Material is presented in a concise manner, focusing on increasing your retention and recall of exam topics. You can organize your exam preparation through the use of the consistent features in these chapters.

Want some knowledge?
Enter the (IN)SECURE book contest!

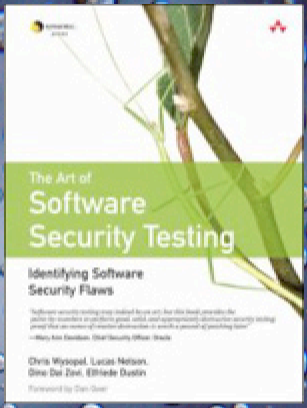
ADDISON-WESLEY

We are giving away a copy of the following titles:



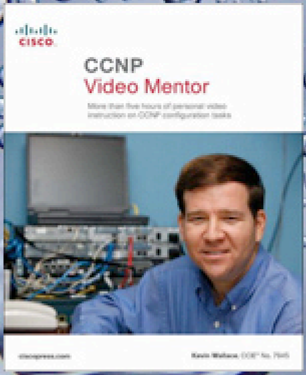
SECURITY
METRICS
Replacing Fear, Uncertainty, and Doubt

ANDREW JAQUITH
FOREWORD BY DANIEL E. GEER, JR.



The Art of
Software Security Testing
Identifying Software Security Flaws

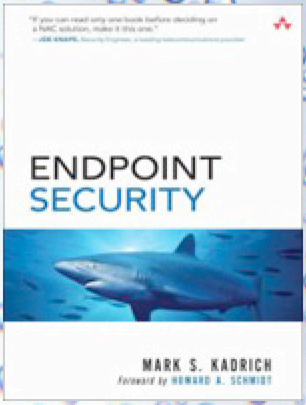
Chris Wysopal, Lucas Nelson, Dino Dai Zovi, Elfriede Dustin
Foreword by Dan Geer



CISCO

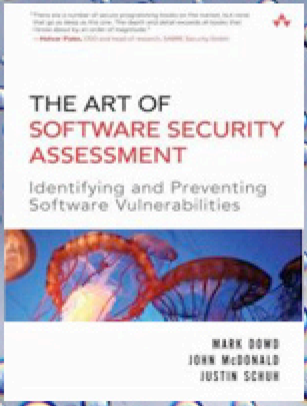
CCNP
Video Mentor
More than five hours of personal video instruction on CCNP configuration tasks

ciscopress.com
Kevin Wallace, CCIE® No. 7945



ENDPOINT
SECURITY

MARK S. KADRICH
Foreword by HOWARD A. SCHMIDT



THE ART OF
SOFTWARE SECURITY
ASSESSMENT
Identifying and Preventing Software Vulnerabilities

MARK DOWD
JOHN McDONALD
JUSTIN SCHUH

What do you have to do?

Go to www.insecuremag.com/contest to enter.

The contest ends August 21st 2007.

The role of log management in operationalizing PCI compliance

By Jason Chan

When people familiar with the Payment Card Industry Data Security Standard (PCI DSS) hear "logging" in conjunction with "PCI compliance," they naturally think of Requirement 10, entitled "Track and monitor all access to network resources and cardholder data." And it's true, Requirement 10 is quite explicit about the specific actions that must be logged, the details that must be tracked, and the length of time and manner in which logging data must be stored and retained. Similarly, when people discuss PCI compliance, there is an overemphasis and fixation on the yearly audit and submission of the Report on Compliance (ROC).

While the annual audit and ROC submission is an important requirement for many organizations subject to the PCI DSS, as the field of general compliance management matures and we learn more about how to successfully operate compliance programs, it has become apparent that a different manner of approaching compliance is required. Instead of scrambling to fill in checklists on a gap analysis and mounting a Herculean yearly effort to establish, prove, and document compliance, it is more effective to regularly and consistently monitor and evaluate the controls, processes and compliance key performance indicators associated with the regulations that influence and apply to your organization. In this vein, it is also useful to consider additional ways that PCI-related log management can be leveraged to regularly validate and evaluate compliance-related controls and processes.

This article will explore some of the ways that log management can bring efficiencies to PCI compliance and how organizations can use log management to transform their overall compliance strategy from reactive to proactive.

Operationalizing Compliance

First, let's review some definitions and background. Generally speaking, operationalizing compliance refers to moving away from a purely audit-focused perspective on compliance toward a more long-term, everyday, integrated and process-driven approach to compliance management. For PCI, this means obsessing less about the audit and ROC and instead focusing more attention on making the controls and processes required by the PCI DSS a core part of everyday IT and business operations.

Pragmatically, this involves a number of issues:

Comprehensive Understanding of Compliance Responsibilities

One of the ideals of general compliance management and operationalizing compliance is the development and implementation of a single set of policies, processes, and controls that will ensure compliance with all relevant requirements. Thus to begin in the quest for this ideal, the organization must be aware of and fully understand the entire scope of its relevant compliance responsibilities.

This includes internal and external compliance influences, such as:

- Industry mandates, including PCI.
- Legal regulations such as SOX (Sarbanes-Oxley).
- Governmental regulations such as California Senate Bill 1386 and FISMA (Federal Information Security Management Act).
- Regulations enforced by business partners (e.g. supply chain compliance requirements).
- Internal organizational requirements such as security policies, standards, and procedures.

Once the scope of compliance requirements has been documented, approved, and internalized organizationally, integrating compliance into everyday operations can move forward. Without this step, though, there is a danger of overlooking or misunderstanding compliance requirements, which can easily lead to implementing processes, policies, and controls that fail to address compliance needs.

Organizational Alignment for Successful Compliance Management

Creating a model that facilitates the efficient, bi-directional distribution of information on compliance-related activities; including gap analysis, remediation plans, control implementation, and status reports is the goal of compliance-specific organizational alignment. People with responsibility for compliance (no matter how small) must understand their obligations and how to work toward achieving ongoing compliance.

A PCI-specific example can be illustrated around requirement 12.7, which calls for employee screening (i.e. background checks) for personnel with access to cardholder data. With effective organizational alignment, the HR business unit will be fully aware of this requirement, how to bridge any gaps if the current screening process is insufficient, and the timelines and documentation required to demonstrate and maintain compliance.

Continuous and Automated Validation of Controls and Processes

To ensure effectiveness, it is important to be able to efficiently evaluate and validate the compliance-related controls that have been implemented. This concept is at the core of operationalizing PCI compliance– it is how the best practices espoused by the Data Security Standard are embodied, implemented, and evaluated in daily practice.

For example, PCI requirement 2.3 mandates the use of encrypted protocols and applications to administer systems over the network. A reasonable control to implement this requirement would be the use of SSH to remotely administer systems. Thus, this control would be specified in system configuration and administration standards (PCI requirement 2.2), and the installation of appropriate software would be included as a part of standard system builds. Of course, once systems are built and deployed, the controls must be validated to ensure continuous compliance.

To validate this control, logs can be examined to detect the use of unencrypted and insecure protocols (e.g. Telnet, r-services) to administer in-scope systems.

If your firewall logs show clear text protocols being used to access systems or your system logs show logins via Telnet, this control has been subverted or has otherwise failed. Log management can automate the validation of this control in a fairly straightforward manner; for example, a weekly report could be scheduled and executed to detail events that violate this control, and follow up and remediation can be planned as a result.

Thus, to fulfill this general goal of continuous and automated process and control validation, each implemented control will ideally have a clear and straightforward means by which both scheduled and ad hoc validation can be performed.

Using Log Management to Validate Compliance Controls

A real benefit associated with the use of log management for control validation is that no specific control instrumentation is required. The use (and misuse) of controls creates log messages that serve as permanent artifacts and evidence of the controls' efficacy.

By implementing log management to collect, store, analyze, and present this evidence, organizations are equipped with the data that allows them to:

- Ensure continuous compliance.
- Demonstrate control effectiveness.
- Identify gaps in control coverage.
- Fine-tune controls, operating procedures, and workflows.
- Facilitate audit-related data gathering and analysis.

To provide a better illustration of how this ideal is put into practice, this section offers an introduction to some of the specific PCI requirements and associated controls that can be validated through log management. A brief overview of each of the major PCI requirements is provided, and accompanying tables are used to enumerate the particular controls and processes related to each requirement and sample log messages that can be used to validate, evaluate, and demonstrate control effectiveness.

Build and Maintain a Secure Network (Requirements 1 and 2)

Requirement 1 describes the network traffic that is generally permitted in the PCI environment, and the policies and network-based access controls that must be in place to restrict traffic appropriately. Traffic must be limited to necessary data flows (1.1.5), and specific controls are required for DMZ and internal systems (1.3 and 1.4).

PCI Requirement	Related Controls and Processes	Relevant Log Messages
1.1.1 – Testing and approval of external network connections and firewall changes	• External connection policy • Change management process • Firewall and network management policies	• Firewall policy and configuration changes • Router configuration changes • Firewall and router reboots
1.1.5-1.1.7, 1.2 – 1.4 – Documentation and justification of ports and protocols used in the PCI environment; Control and restrict specific traffic flows within the PCI environment	• Authorized data flows and applications in the payment card environment • Network traffic whitelists/blacklists (i.e. explicitly allowed or denied services)	• Accepted firewall connections • Denied firewall connections

Requirement 2 outlines the configuration standards required for systems deployed in the payment card environment. Specific security configuration settings are mandated for systems (2.1 and 2.2), and encrypted applications and protocols are required for systems administration (2.3).

PCI Requirement	Related Controls and Processes	Relevant Log Messages
2.2.2 – Disable unnecessary and insecure services 2.3 – Encrypt administrative access to PCI systems	• System configuration and installation standards • System administration standards • Application whitelists/blacklists (i.e. explicitly allowed or denied services)	• Telnet, FTP, and r-service login messages • Firewall and router ACL accept messages for insecure or unencrypted services

Protect Cardholder Data (Requirements 3 and 4)

Requirement 3 spells out the specifics on how cardholder data can be stored. This data should be maintained for the minimum time required for business purposes (3.1), authentication data cannot be stored after card authorization (3.2) and the Primary Account Number must be appropriately protected during storage (3.4).

PCI Requirement	Related Controls and Processes	Relevant Log Messages
3.4 – Render PAN (Primary Account Number) unreadable when stored	• Data storage standards • Data classification policy • Confidential data processing and access policy	• Transaction and application logs containing unencrypted card numbers
3.5.1 – Restrict access to encryption keys	• Key management standards and procedures	• File and object access records for encryption keys

Requirement 4 mandates the use of appropriate controls (e.g. TLS or SSL, WPA2) when transmitting cardholder data over wireless and public networks.

PCI Requirement	Related Controls and Processes	Relevant Log Messages
4.1 – Use strong cryptography when transmitting cardholder data over open, public networks	• Data access, transmission, and distribution policies and standards • Application development and management policies	• Firewall and router ACL accept messages for insecure or unencrypted services

Maintain a Vulnerability Management Program (Requirements 5 and 6)

Requirement 5 describes the anti-virus controls that must be implemented on payment card systems, and includes requirements for deployment (5.1) and configuration (5.2).

PCI Requirement	Related Controls and Processes	Relevant Log Messages
5.1 – Deploy anti-virus software	• Anti-malware infrastructure • System protection policies • Desktop and server configuration standards • Patch and software installation policies and processes	• Anti-virus application installation messages • Virus detected, cleaned, quarantined • Virus signature file installed or updated
5.2 – Ensure anti-virus mechanisms are current, active, and capable of generating logs		

Requirement 6 enumerates the change management and systems development controls that must be implemented to ensure compliance. This requirement outlines standards for software development (6.3 and 6.5) and the required parameters for patch and update management (6.1) and change control (6.4).

PCI Requirement	Related Controls and Processes	Relevant Log Messages
6.1 – Ensure systems are patched with the latest vendor security updates	• Patch and software installation policies and processes • Incident response policy and process	• Patch installed • Software updated
6.4 – Follow change control procedures for all configuration changes	• Change management process • Enforcement of maintenance windows	• System reboots • Patch installed • Software updated

Implement Strong Access Control Measures (Requirements 7, 8, and 9)

Requirement 7 describes the access control restrictions needed for payment card systems, and states that access must be controlled based on job function (7.1) and be configured in a default deny manner.

PCI Requirement	Related Controls and Processes	Relevant Log Messages
7.1 – Limit access to systems and information based on job requirements	• Account management process and policy • Access control policy • Role-based access controls	• User account modifications • User group modifications • Database access (CRUD – Create, Read, Update, Delete audit records) • File access records • Login messages
7.2 – Establish a system to restrict user access based on need-to-know and default deny		

Requirement 8 sets forth the manner in which organizations must implement unique identifiers for users of payment card systems to ensure auditability and traceability of events. Authentication requirements are specified (8.2 and 8.3), and password standards are provided (8.4 and 8.5).

PCI Requirement	Related Controls and Processes	Relevant Log Messages
8.1, 8.5.8 - Identify all users with a unique ID before allowing access; do not use group, shared, or generic accounts	• User provisioning process • Separation of duties • Systems administration process and policy	• User logins (system, application, database) • Shared user logins (e.g. root, administrator, application and service accounts) • Accounts created
8.3 – Implement two-factor authentication for remote access	• Remote access policy	• VPN logins

PCI Requirement	Related Controls and Processes	Relevant Log Messages
8.5.1 – Control addition, deletion, and modification of user IDs and other identifiers	• User provisioning process • Account maintenance procedures	• Accounts created, deleted, modified • Groups created, deleted, modified
8.5.4 – Immediately revoke access for any terminated users	• Deprovisioning policy and procedures • Employee termination policy	• User deleted • User disabled
8.5.6 – Enable accounts for vendor remote access only when required	• Vendor remote access policy • Enforcement of maintenance windows • Change management process	• User logins (vendor user accounts) • VPN logins
8.5.13 – Lockout user accounts after six failed login attempts	• User account management policy	• Failed logins • Account lockouts
8.5.16 – Authenticate all access to any database containing cardholder data	• Data access policy • Access control policy	• Database logins

Physical security controls for payment card environments are described in Requirement 9. This includes physical access and visitor controls (9.1 through 9.4) and media (e.g. tapes, disks, paper) security, distribution and destruction (9.5 through 9.10).

PCI Requirement	Related Controls and Processes	Relevant Log Messages
9.1 – Use facility entry controls to limit and monitor physical access	• Physical security controls • Facility access policy	• Badge reader activity (e.g. entries, failures)

Regularly Monitor and Test Networks (Requirements 10 and 11)

Requirement 10 describes the foundational requirements for audit trails and log management within PCI environments. As such, every sub-requirement in this section is related directly to the collection, storage, protection, integrity and/or retention of logs.

This requires covers the core functions of log management, including:

- Enabling and configuring logging (10.1 and 10.2)
- Details required for audit trail events (10.3)
- Time synchronization (to support the integrity and usability of logs) (10.4)
- Centralization and protection of logs (10.5)
- Log review and analysis (10.6)
- Log retention (10.7)

Requirement 11 enumerates the testing and monitoring controls that must be implemented for payment card environments.

This includes regular control assessment, vulnerability assessments and penetration testing (11.1 through 11.3) and the use of IDS/IPS and file integrity monitoring software (11.4 and 11.5).

PCI Requirement	Related Controls and Processes	Relevant Log Messages
11.4 – Use IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems) to monitor traffic and alert personnel	• Network monitoring policy • Incident response program and procedures • Patch and software installation policies and processes	• IDS/IPS alerts • IDS/IPS signature updates
11.5 – Deploy file integrity monitoring systems (FIMS) to alert personnel to unauthorized modifications	• System monitoring processes • Change management process • Incident response program and procedures	• FIMS alerts

Maintain an Information Security Policy (Requirement 12)

Requirement 12 specifies the information security policies and procedures needed for PCI compliance, including operational procedures (12.2), usage policy (12.3), and incident response (12.9).

PCI Requirement	Related Controls and Processes	Relevant Log Messages
12.2 – Develop daily operational security procedures consistent with PCI requirements	• System monitoring processes • Incident response program and procedures • Security standard operating procedures	• Logins to security systems (to validate daily use and monitoring of controls) • Log review messages (to validate regular review of logs)
12.9, 12.95 – Implement an incident response plan – include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems		• IDS/IPS/FIMS alerts

Conclusion

As organizations become more familiar with the day to day requirements of managing PCI and other compliance initiatives, they are naturally looking for ways to both streamline their efforts and ensure the effectiveness of their controls. Log management dovetails well with this movement; satisfying log collection, retention, protection, and analysis requirements as well as providing the infrastructure for continuous compliance and control validation.

References

- Payment Card Industry Data Security Standard, version 1.1. September 2006.
- Payment Card Industry Data Security Standard: Security Audit Procedures, version 1.1. September 2006.

www.pcisecuritystandards.org

Jason Chan is LogLogic's Director of Product Management for Applications. Prior to joining LogLogic, he was Senior Manager for Symantec's Security Advisory Services office in San Francisco. Jason is a certified PCI auditor and has been involved with payment card security since 2002, when he began performing Visa CISP (Cardholder Information Security Program) assessments while at @stake, a security consultancy that was acquired by Symantec in 2004. He started working in the security field in the late 90s at the US Navy's Space and Naval Warfare Information Warfare Engineering Center. Jason received his undergraduate degree from the College of Charleston and his Master's degree from Boston University.

Interview with Jeremiah Grossman CTO of WhiteHat Security

By Mirko Zorz

Jeremiah Grossman founded WhiteHat Security in 2001. Prior to WhiteHat, he was an information security officer at Yahoo! responsible for performing security reviews on the company's hundreds of websites. Jeremiah is a world-renowned leader in web security and frequent speaker at the Blackhat Briefings, NASA, Air Force and Technology Conference, Washington Software Alliance, ISSA, ISACA and Defcon. He is a founder of the website Security Consortium (WASC) and the Open website Security Project (OWASP), as well as a contributing member of the Center for Internet Security Apache Benchmark Group.

Let's start with an easy one. How did you get interested in Web security?

Most of my technology background originates from Web development. I've created many websites, coded in several server-side (Perl, C, Java) and client-side (JavaScript, Flash, Java) languages, studied HTTP extensively, toyed with every major Web browser since Mosaic, and am very familiar with Apache and MySQL. But, it really wasn't until the summer of 1999 that I took an active interest in Web security. The mainstream media published several articles stating that the Web wasn't secure (nothing new here), but the big guys had (Yahoo, Amazon, eBay, etc.) fixed the problem (They did!? How!?).

To satisfy my curiosity, I proceeded to hack into my own Yahoo! Mail account and quietly reported my results back to them. A few emails later, Yahoo! offered me a position as "The Hacker Yahoo." And the rest, as they say, is history - tinyurl.com/2fmkwv

What are the most important lessons that you learned while working as the Information Security Officer at Yahoo? I'm sure many security professionals wonder what working at such a large company entails.

Yahoo! was/is big, really big. It's so big it's hard to wrap your mind around: at the time, my best count was roughly 600 websites, 17,000 publicly facing Web servers, and 120 million users.

Working for Yahoo!, or being responsible for the security of any popular website, is trial by fire. Think about the fact that there are more than 1 billion people across the globe with access to your website all the time, and a certain percentage (we thought 1%) is malicious. As demanding as this type of job is, the experience is also extremely rewarding and highly recommended for anyone in website security. Without having been in that role, it's difficult to appreciate which security strategies actually work, versus the ones that technically should, but don't.

Lessons learned:

- IDS says everyone is attacking you with everything they got all the time
- A hacker, who just has to find a single

vulnerability, has it easier than a security professional, who has to defend against all vulnerabilities all the time
- Everyone with a website gets a “vulnerability assessment,” probably several per day. Whether you pay for the results or not is another matter
- Use security obscurity to your advantage
- Security solutions that work for smaller websites don’t necessarily scale for the larger ones.

This year you've been selected as one of the Top 25 CTO's according to InfoWorld. How does it feel to have your work recognized and being put head to head with other well known industry giants?

It’s an honor. “Surreal” is the best word I can use to describe being listed next to names from top companies like VeriSign, 3Com, Motorola, and Credit Suisse. And while I’m receiving a lot of the credit recently, which I appreciate, it’s really the result of years of tireless effort from many amazing people at WhiteHat Security and around the webappsec community. I was always fond of the quote by Sir Isaac Newton, “If I have been able to see further, it was only because I stood on the shoulders of giants.”

Has the award put a spotlight on WhiteHat Security?

It’s funny, I was just getting used to seeing our name in the press about every week or so, then this happened. Now it’s almost every day we’re mentioned and it’s actually been difficult for us to keep up with all the inbound interest in WhiteHat Sentinel. Part of the build up is of course press generated. But, most of the increase is simply due to the complexity and difficulty of Web application security and the need for easy-to-use vulnerability management services. We’re really excited about the future and we seem to be at the right spot at the right time.

USE SECURITY OBSCURITY TO YOUR ADVANTAGE

With the constant evolution of threats, what kind of technology challenges does WhiteHat Security face?

It’s interesting. It’s not so much the new attacks or techniques that keep us on our toes, but the adoption of new Web development technologies such as Ajax, Flash, Java, etc. Websites using these technologies are really no more or less secure. But, what is more difficult is scanning for the vulnerabilities within them. Today’s Web pages share more similarities with running applications instead of traditional HTML documents. This makes “crawling” the website that much harder. By extension, the attack surface is more difficult to define, and as a result black box “fuzzing” is constantly challenged.

In your opinion, how has the Web security scene evolved in the last few years?

It might sound odd, but one big difference for me is that only a few years ago people barely knew that “Web application security” existed or that firewalls and SSL didn’t protect a website.

Today, almost everyone I talk to, from coast to coast and country to country, has that figured out. Now everyone wants to know what the latest trends and best practices are. The other big difference is the availability of knowledge. Before, the information people needed to secure a website really wasn’t documented. Now, people have access to websites with hundreds of white papers, presentations, and books right at their fingertips. If you want to secure a website, the information to do so is out there.

Have new development techniques brought more problems?

Some experts like to say that Ajax or Web 2.0 is the harbinger of new attacks. I’m not one of them. Fundamentally, we’re dealing with the same problems in the same locations.

The challenges that Ajax brings land more on the security vendor than on the enterprise. We have to find vulnerabilities in these custom Web applications and Ajax-enabled applications are much more difficult to do so. Read any of Network Computing's scanner product reviews and you'll see what I mean (tinyurl.com/2ypwo6).

What are the security tools/services that you use on a daily basis and couldn't live without?

I've blogged about the speed hack contests we hold at the office. This is where we race to find the first and the best vulnerability in a never-before-seen-website. For speed, nothing beats Firefox, the Web Developer Toolbar, and having the Paros or Burp proxy handy. If I happen to get stuck on an XSS filter, call up RSnake's XSS cheat sheet, use the encoders at the bottom, and that usually does the trick - ha.ckers.org/xss.html

If I woke up tomorrow back at Yahoo!, or was responsible for the security of any website, (I know I'm biased here) the honest answer is I'd get the Sentinel Service deployed immediately. The service is easy and complete, but most of all a security professional's time is precious. Sure they could do the vulnerability assessment work themselves with each site update, but it's a poor use of their time and expertise. Their time and expertise is better spent focusing on strategic solutions and big picture thinking, rather than trying to identify, prioritize and weeding through the next hundred Cross-Site Scripting, SQL Injection, or whatever other vulnerabilities there might be.

Are websites that you assess more insecure today in comparison to 3 years ago?

I'd say today's websites probably have less vulnerabilities, but they've also never been more at risk.

While SQL Injection seems to be on the decline and Cross-Site Scripting filters are far more common, the number of attackers and attack techniques has increased dramatically.

The bad guys go where the money is and right now that's the Web. To monetize, all they have to do is capitalize on one single vulnerability. So, if an organization is only going after the low hanging fruit, that isn't going to help much, since Web attacks are targeted. Websites that do better are the ones whose security posture makes is hard enough on the bad guy where it's in their best interest to try some place else.

TODAY'S WEBSITES PROBABLY HAVE LESS VULNERABILITIES, BUT THEY'VE ALSO NEVER BEEN MORE AT RISK.

A significant part in the process of developing a complex enterprise website is ensuring that the customer data being used on that website is secure.

What do you see as the biggest threats to that security? What are the most common mistakes you see your customers make?

With 125+ million websites, and most of them riddled with vulnerabilities, I think it's safe to say the mistakes have already been made. At this point, we're trying to stop the new holes in the dam and plug the existing ones. Here's the advice I give to everyone:

1) Asset Tracking – Find your websites, assign a responsible party, and rate their importance to the business. Because you can't secure what you don't know you own.
2) Measure Security – Perform rigorous and on-going vulnerability assessments, preferably every week. Because you can't secure what you can't measure.

3) Development Frameworks – Provide programmers with software development tools enabling them to write code rapidly that also happens to be secure. Because, you can't mandate secure code, only help it.
4) Defense-in-Depth – Throw up as many roadblocks to attackers as possible. This includes custom error messages, Web application firewalls, security with obscurity, and so on. Because 8 in 10 websites are already insecure, no need to make it any easier.

You are one of the authors of the recently released "Cross Site Scripting Attacks: XSS Exploits and Defense". How long did the writing process take? What was it like to cooperate with other authors?

The writing process took about six months. Generating hundreds of pages coherent and compelling content is challenging to say the least, even with five of the best subject matter experts working in parallel. It was great getting to review the work of the authors on the fly and see the project come together. And, people really seem to be excited about the book and enjoying the read.

For me, the feedback and reviews we've been receiving from the industry is what really made it all worthwhile. Knowing that your work is useful to so many is a great feeling.

Web security has been getting a lot of attention in the past 2 years and an increasing number of people is starting to pay attention. What resources would you recommend to those who want to learn more about Web security?

There are a lot of resources out there and the blogosphere has been one area that has exploded. Here are some good resources:

- Robert "RSnake" Hansen (ha.ckers.org),
- Planet Web Security (planet-websecurity.org)
- Mine :) (jeremiahgrossman.blogspot.com)
- Matasano (www.matasano.com/log)
- Web Application Security Consortium (www.webappsec.org)
- Open Web Application Security Project (www.owasp.org)
- Web Security Mailing List (www.webappsec.org/lists)

SOFTWARE VENDORS HAVE A RESPONSIBILITY FOR THE DATA THEY PROTECT AND THE PRODUCTS THEY SELL

In general, what is your take on the full disclosure of vulnerabilities? Should vendors have the final responsibility?

At the end of the day, website owners and software vendors have a responsibility for the data they protect and the products they sell. I've been on most sides of the full-disclosure debate (website owner, software developer, security researcher, and business owner) and can appreciate the concerns raised. I'm a pragmatist. When responsible for security, I have no expectation that anyone is going to share any vulnerability information with me ahead of time. I hope they would before going public, but it would be irresponsible to depend on it and hopeless to demand it. I also think describing the messenger as "unethical" or worse only gives the impression that company isn't taking full responsibility for the incident. Instead, try to be open, investigate what caused the problem, solve it, and move on.

What are your plans for the future? Any exciting new projects?

While specific projects I'm working on at WhiteHat must remain confidential, my "agenda" is twofold. Help organizations find the vulnerabilities in their websites, no matter how big or how often they change. If that means scaling big enough to scan the entire Internet every week, so be it. And, when we know where the vulnerabilities are, provide organizations with options to get them fixed, quickly and with the least amount of trouble. Once someone decides they want to improve the security of their website, I want to be able to provide them with a game plan to do so that makes sense.

Solving the keylogger conundrum

By Sacha Chahrvin

The geek shall inherit the earth! This is the slogan that has reverberated out from Silicon Valley from the mid-90s, as we all realized that technology was, actually, fun, interesting, essential. Geek chic took over the worlds of film, fashion – and even finance. Suddenly it was cool to be into computers.

But the rise of the geek didn't just confine itself to the light-hearted entertainment, start-ups that went stratospheric, or successful transformations of 'old economy' businesses. Computers and crime have come together. Mobsters are no longer the fast-talking, pin-striped, gun-toting caricatures of Hollywood legend. Criminal organizations are just as likely to be behind hacking and phishing networks as illegal gambling rackets and gun-running operations - with the same levels of profitability.

These days the weapons of choice are not sawn-off automatics, or revolvers fitted with silencers. It's much more likely to be illicitly gathered passwords, user-names and dates of birth. And of the armory at their disposal, keyloggers are an increasingly popular choice.

Available in either software or hardware form, keyloggers record every stroke made on a keyboard, and compile the data gathered to reconstruct login details, PINs, encryption codes, mothers' maiden names or any other form of security information. From there it is but a short journey to inviting vistas of identity theft, industrial espionage, blackmail, or simple credit card misappropriation.

Successful surveillance

In an age when CPUs are increasingly central to so many aspects of our lives, and the quality of information is a key differentiator between businesses, it is not surprising that keyloggers have proved to be so attractive to criminals.

Despite this, the keylogger/criminal connection has on occasion worked in the interests of the good guys.

In one of the earliest examples of cyber-crime fighting, Nicodemo Scarfo Jr, a well-connected member of the New York and Philadelphia mobs, was brought down by the Magic Lantern keylogger that the FBI installed on his computer via a Trojan. Certainly not be the typical bullets-and-bloodshed take-down of popular imagination, it was still enough to indict him for running an illegal gambling ring and loan sharking.

At the time the story raised a number of concerns about computer privacy. Now it serves as a useful reminder that there is a positive side to keylogging. As well as serving the interests of law enforcement agents, keyloggers can help employers maintain productivity by ensuring that staff are working on appropriate projects. They can protect valuable bandwidth, by spotting when unnecessary applications have been downloaded and ensure optimum use of networked resources by encouraging personal web or system use is kept to appropriate levels.

Keyloggers can even be used in the interests of child protection, enabling parents to check their children's computer activities, while giving those children a degree of independence and privacy.

Keyloggers and criminals

Nonetheless, it is still the darker side to these surveillance technologies that is more familiar to the majority of IT and security professionals. Using keyloggers gives thieves a veil of anonymity: they can plunder the treasure-trove of inter-connected corporate systems and storage devices at will, with very little chance of detection.

In the wrong hand therefore, keyloggers can damage business relationships, financial standing, and reputations. They can even cause an organization to breach major pieces of legislation such as European Data Protection and Human Rights Acts, or the Sarbanes Oxley Act in the States.

Using keyloggers gives thieves a veil of anonymity.

Nor is it just large corporates that experience keylogging attacks. They may well be the most attractive targets, but individuals' personal details are at risk from a carefully located keylogger – and far less likely to be adequately protected. In fact, any individual or organization that accesses, inputs or stores valuable information is at risk.

Software or hardware

Nicodemo Scarfo was caught out by a Magic Lantern, software keylogger that infected his machine through a Trojan, and this is the way that the majority of keyloggers work. The advantage of the software versions is that they are easy to install – despite the constant warnings, too many people lose the war between curiosity and caution and open up spyware, Trojan or virus-infected files and emails. Software also enables thieves to infect a huge number of machines and gather the data quickly, easily and remotely.

Fortunately, detection is becoming much easier. The attractions of the bigger corporates are tempered by the increasing awareness of IT security managers, who keep machines protected with the latest anti-virus software to prevent Trojans and spyware entering the system in the first place. Should a keylogger slip through the net, standard protection tools that monitor the status of a computer can detect and remove them.

Unfortunately, security managers are locked in a game of one-upmanship with criminals who have followed the lead of the most successful businesses and taken the maxim 'innovate or die' to heart. As security measures improve, so criminals find new ways to breach them. In this case that means hardware keyloggers. These devices are much harder to detect than software since they do not install any code onto the machine and cannot be spotted by traditional anti-virus or anti-spyware tools.

Installing the hardware

Hardware keyloggers take two main forms. The first, and probably the most common, is a small device installed at the back of a PC between the keyboard and its connection to the machine.

As with all hardware keyloggers, it requires the attacker to have physical access to the computer in question, both to install and later retrieve the device. With social engineering growing in sophistication, this doesn't pose a problem to the determined individual, particularly as it takes a matter of seconds to install, and requires no technical skill.

These kinds of keyloggers may only be approximately 1.5 inches long, but they have a memory capacity that allows up to two million key strokes to be recorded – which represents about five years' worth of typing for the average computer user.

Happily, this type of hardware keylogger is also the easiest to detect visually – provided you know what to look for.

More insidious forms of keyloggers are built into the keyboard. Thieves will either replace the keyboard completely or dismantle it, insert a keylogging device, and re-assemble it. Naturally this requires a greater degree of skill on the part of the criminal, and takes more time to complete. But the chances of visual or manual detection are almost zero.

Organizations can defend themselves against keyloggers.

Self-defense

The good news is that organizations can defend themselves against determined keyloggers. The first step, as with all effective security measures, is to educate and train users to raise awareness and create a culture of individual responsibility. The number of PCs in large companies makes it impractical for the IT security manager to check the back of every single box and every single keyboard manually. Users who carry out basic monitoring of their own equipment greatly increase the chances of detecting any rogue devices.

Secondly, organizations should look at alternatives to desktop PCs. Although still susceptible to hardware keyloggers, the inbuilt keyboards of laptop computers are far harder to tamper with. However, greater use of mobile devices brings new security challenges, which must be balanced against the reduced threat from keyloggers.

Then there are the secure tokens, smart cards or other devices that are used to provide a second layer of authentication after user names and passwords. These work by having a constantly changing passcode, meaning that any data gathered by a keylogger is immediately invalid, and cannot be used to sneak into the system.

Organizations should also consider increasing the use of drop down menus for gathering information. Instead of typing in information with trackable keystrokes, drop downs enable users to select characters or words with the mouse, which a keylogger cannot record.

However, in addition to these more general security tools, there are a number of applications, recently on the market, that can automatically identify hardware keyloggers. These software solutions disable the devices by intercepting and blocking communications between it and the targeted computer. The software also alerts the IT department to the presence of keyloggers.

The secure organization

Keyloggers are such a potent source of danger because they exploit the gap created by not one but two notoriously weak areas of IT security. The first is our ongoing reliance on passwords. Sophisticated intrusion prevention or segmented access authorization do add extra layers of protection to corporate networks, but they still cannot distinguish between a legitimate user with the right password and a malicious one.

The second is old-fashioned physical security, often forgotten when devising strategies to protect virtual assets. Since hardware keyloggers require physical access to the targeted machine the criminal must be in the presence of that computer, even if it's only for a matter of seconds. If they are to protect themselves against keyloggers, organizations have to give the broadest possible definition to IT security. That means policies to help employees recognize social engineering attacks, and even conducting thorough background checks on auxiliary staff who have access to the building.

After all, if you think your data is worth protecting, then someone else will think it is worth stealing.

Sacha Chahrvin has been the UK managing director of SmartLine for two years. He has a BA in Business Studies and has spent more than 10 years in the software industry. Before SmartLine, Sacha worked for a number of reseller organisations supplying software licensing to fortune 500 accounts, with his last role being global account manager at Reuters.

WINDOWS - WinSCP
http://www.net-security.org/software.php?id=6

WinSCP is an open source SFTP and SCP client for Windows using SSH. Its main function is safe copying of files between a local and a remote computer.

LINUX - Firewall Builder
http://www.net-security.org/software.php?id=230

Firewall Builder consists of an object-oriented GUI and a set of policy compilers for various firewall platforms. In Firewall Builder, a firewall policy is a set of rules; each rule consists of abstract objects that represent real network objects and services (hosts, routers, firewalls, networks, protocols).

MAC OS X - The DoorStop X Security Suite
http://www.net-security.org/software.php?id=674

The DoorStop X Security Suite is an integrated, comprehensive approach to securing your Macintosh on the Internet.

POCKET PC - Pocket Warrior
http://www.net-security.org/software.php?id=575

Pocket Warrior is a Pocket PC WiFi 802.11b Prism auditing software.

To submit a software for consideration e-mail software@net-security.org

Windows security: how to act against common attack vectors

By Rob Faber

The underlying goal of typical "hacker" sessions or seminars is to get attention and create awareness. They give you insight of what can be done to your network by those among us who have cruel intentions. With the release of Windows Vista a lot has changed. Microsoft tightened up user rights, introduces User Account Control, limited services and code execution, improved IE security and revamped the firewall. What's left for the good old hacker?

Technical vs. non technical aspects

While a lot has happened in the security field during the last few years, the (ethical) hacker still knows some tricks that work perfectly. Simply fire up a sniffer and you will know what I mean. As with all in life, things can end up in the wrong hands and can - in this case - be used to compromise security in many ways.

Despite of it all, a lot of companies still don't see security as a complete set of measures that have to be taken to get a more secure environment. Security is definitely not a layer that can be pasted in after all the (infrastructure) implementation work is finished. "Oh yeah, we forgot that security thing! Just add some of it!" That won't simply work that way. Sometimes difficult but I think the only way is to create awareness, sometimes present the bare facts by - for example - giving a demo or to really show the vulnerabilities. The technical issues are not the only ones that play an important role, the human factor is also of great importance. It is highly important to have a good policy and follow strict procedures. I stress the fact that I mentioned "more secure" earlier because totally secure and 100 percent protection is out of the question. It's always a matter of calculating risk and a balanced investment in protecting your assets.

Be aware of certain risks

Why is it so easy to get access to a network? Well, because most of the times the proper countermeasures haven't been taken to limit the scope a potential attacker has. This goes from a security policy, knocking out rogue access points, implementing network segmentation and limiting user capabilities on an ordinary workstation towards patched and properly managed firewalls.

A system administrator doesn't have to be a hacker and he/she not even needs such skills to get proper network management in place. But being aware of the risks is a good thing. A basic understanding of what is possible on the network from an attacker's perspective and what can go wrong helps the IT (security) professional to better understand all of this and then be able to better secure the company network and protect the assets.

The starting point: disclose information

Ethical hackers can use many different methods during a simulated attack or penetration test. Really a whole range of tools and attack methods that can be chosen from. This can start from the remote network by for example launching an attack over the Internet. This way the ethical hacker tries to break or find vulnerabilities in the outside defenses of the network, such as firewall, proxy or web servers. One can be using remote dial-up possibilities (yes, they still exists) or the local network in order to launch the attack.

By using social engineering, it is possible to check the integrity of the organization's employees. Also, by gaining physical entry the attacker can attempt to compromise the organization's physical premises. You never will know how easy it is to tailgate and just walk into the entrance with double protected guards on the front door.

An attacker who gains physical access can plant viruses, Trojans, rootkits, install hardware keyloggers, copy information directly to a disk, install rogue access points or have access directly to systems in the target organization and network. He can also steal some unprotected hardware equipment with useful information on it.

The first step for any attacker is to get the information needed to start an attack. Hacks in general can be initiated from outside but can also launched from the inside. As you will know most of the attacks (around 75 - 80 percent) come from inside of the company.

These first steps can all be passive. A thorough search for information about the company on Google can disclose a lot of basic information. Information gathering is possible by querying the Whois database of, for example RIPE (www.ripe.net). The result is a range of IP addresses which can be the starting point for further steps in more active techniques used to get closer to the target.

Post scanning techniques and Nmap

It is very easy to start using the Nmap network mapping utility (insecure.org/nmap/) to scan networks and get crucial information about hosts on that network - what kind of hosts and how that host is configured, which ports are open or services are running.

The power behind Nmap is the huge number of scanning techniques and options available. Some Nmap scans can hide your own machine and in that way make it appear as if another computer is scanning the network, while other scans go directly for the targeted machine. Nmap's primary interface works from the command line of Windows. The command line is very strong and a lot of options and parameters can be added to do the work. There is a graphical utility available called NmapFE but in order to take advantage of the more advanced functionality you should stick to the command line.

With Nmap you can scan for TCP or UDP ports. TCP is a stateful or connection oriented protocol. Connection oriented means that, before any data can be transmitted, a reliable connection must be obtained and acknowledged by both parties involved in the communication. As you will know there is a specific set of control bits that can be set in a TCP packet also known as “flags”. Flags can be:

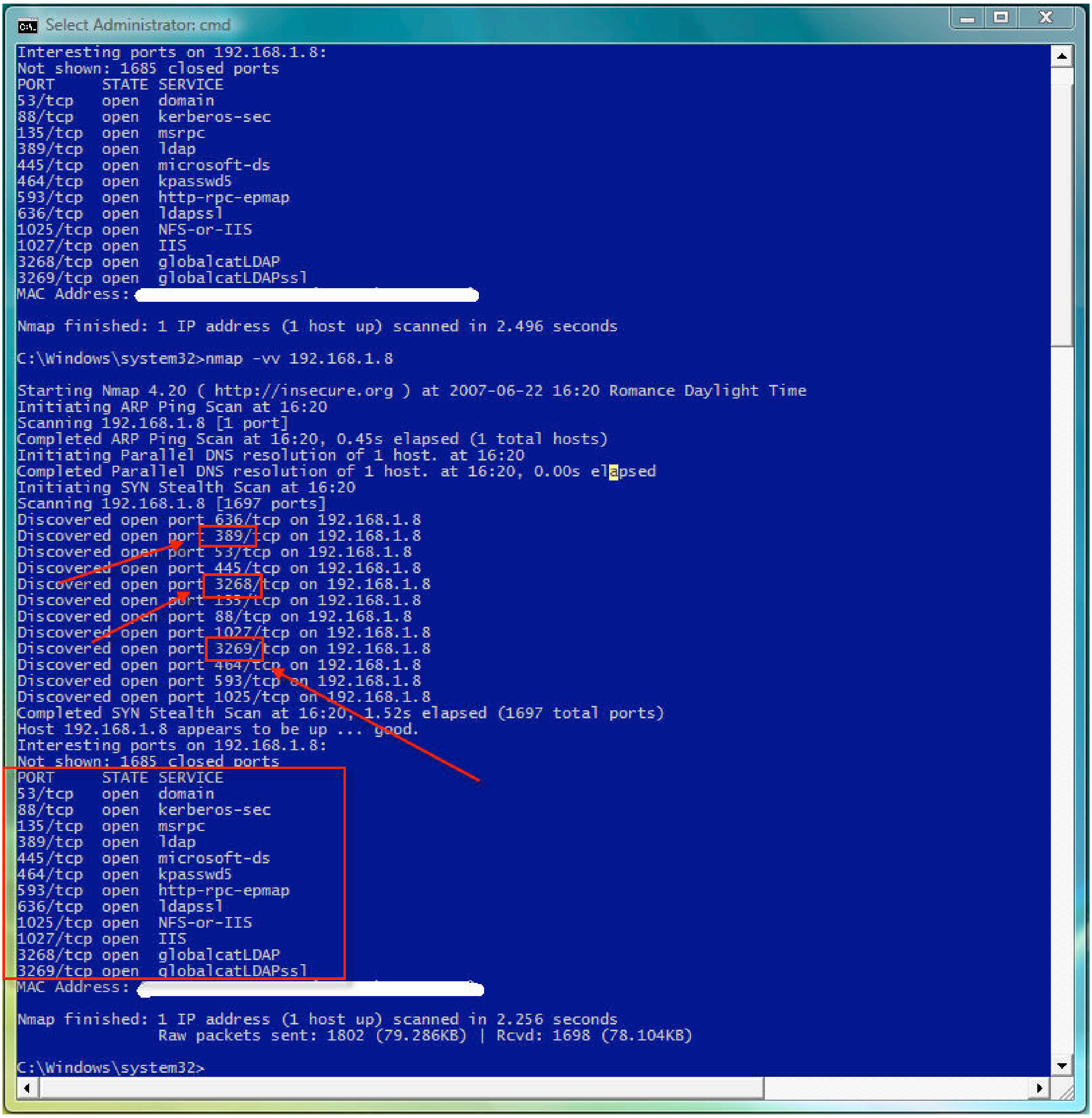
URG: Urgent Pointer
ACK: Acknowledgement
PSH: Push Function
RST: Reset the connection
SYN: Synchronize sequence numbers
FIN: No more data from sender

There are two scenarios where a three-way handshake will take place: First establish a connection (an active open) and second terminating a connection (an active close).

One problem with port scanning is that it is most of the times logged by the services listening at the scanned ports. This is because they detect an incoming connection, but do not receive any data, thereby generating an error in the log.

UDP is different as it is connection-less (fire and forget) traffic. UDP does not guarantee reliability or ordering in the way that TCP does. Datagrams may arrive out of order or go missing without notice. Missing the overhead of checking whether every packet actually arrived at the destination makes UDP faster and more efficient for applications or services that do not need guaranteed delivery such as messaging or streaming protocols. In order to scan for UDP ports with Nmap, you can generally send empty UDP datagrams at the port. If the port is listening, the service will send back an error message or ignore the incoming datagram. If the port is closed, then the operating system most of the times send back an "ICMP Port Unreachable" (type 3) message. This way the attacker can find open ports.

Port scanning techniques can be differentiated with Nmap and this way you can use open scan, half-open scan, stealth scan and a lot of other options to “dive under the radar”. Naturally, it is most preferable for the attacker to keep his actions undetected.



```
Interesting ports on 192.168.1.8:
Not shown: 1685 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1025/tcp open  NFS-or-IIS
1027/tcp open  IIS
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
MAC Address: [redacted]

Nmap finished: 1 IP address (1 host up) scanned in 2.496 seconds

C:\Windows\system32>nmap -vv 192.168.1.8

Starting Nmap 4.20 ( http://insecure.org ) at 2007-06-22 16:20 Romance Daylight Time
Initiating ARP Ping Scan at 16:20
Scanning 192.168.1.8 [1 port]
Completed ARP Ping Scan at 16:20, 0.45s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:20
Completed Parallel DNS resolution of 1 host. at 16:20, 0.00s elapsed
Initiating SYN Stealth Scan at 16:20
Scanning 192.168.1.8 [1697 ports]
Discovered open port 636/tcp on 192.168.1.8
Discovered open port 389/tcp on 192.168.1.8
Discovered open port 53/tcp on 192.168.1.8
Discovered open port 445/tcp on 192.168.1.8
Discovered open port 3268/tcp on 192.168.1.8
Discovered open port 135/tcp on 192.168.1.8
Discovered open port 88/tcp on 192.168.1.8
Discovered open port 1027/tcp on 192.168.1.8
Discovered open port 3269/tcp on 192.168.1.8
Discovered open port 464/tcp on 192.168.1.8
Discovered open port 593/tcp on 192.168.1.8
Discovered open port 1025/tcp on 192.168.1.8
Completed SYN Stealth Scan at 16:20, 1.52s elapsed (1697 total ports)
Host 192.168.1.8 appears to be up ... good.
Interesting ports on 192.168.1.8:
Not shown: 1685 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1025/tcp open  NFS-or-IIS
1027/tcp open  IIS
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
MAC Address: [redacted]

Nmap finished: 1 IP address (1 host up) scanned in 2.256 seconds
               Raw packets sent: 1802 (79.286KB) | Rcvd: 1698 (78.104KB)

C:\Windows\system32>
```

Scanned and open ports on a Windows Domain Controller

Different types of scanning

Open scans make use of a full connection opened to the target system by a three-way TCP/IP handshake. The downside of this is that these scans are easy to detect on the network. This is because the whole tree-step handshake process will finish and most of the times will be logged by the contacted machine or IDS. However, the information gathered with an open scan is the best in determining the actual (port) state of the target machine.

In the handshake process the client sends a SYN flag, which is replied by a SYN+ACK flag by the server and which in turn is acknowledged back with an ACK flag by the client to complete the connection. If a port is closed or 'not listening' the server responds with a RST-ACK flag, to which the client responds with a RST flag, closing the connection. This allows the user to see if a particular port is open or closed.

Another disadvantage of this scan technique to an attacker is that it is impossible to spoof his identity as spoofing would require sending a correct number sequence as well as setting the appropriate return flags to set up a data connection. Spoofing an IP-address in this case will never complete the process of the three way handshake and responses go to the spoofed IP-address. Besides that, most intrusion detection systems and firewalls detect and log this scan, because the IP address is known and so the attacker's IP address can be logged, filtered or easily blocked.

Half open scan

One way to circumvent logging and detection this is to perform a half open scan in which a complete TCP connection is never established. Instead, as soon as the server acknowledges with a SYN-ACK response, the client tears down the connection by sending a RST. This way, the attacker detects an open port listening/running a service from the ACK response. Intelligent intrusion detection systems and firewalls are also capable of detecting a scan like this and will prevent this from taking place.

Stealth scanning

Half open scans were considered stealth for a long time, but as intrusion detection systems evolved, these scans became easily logged. Now, there are other ways to stealthy scan a network. Scans where the packets are flagged with a particular set of flags other than SYN, using a combination of flags, with no flags set, with all flags set, just appearing as normal traffic, by using fragmented packets and like this tricking filtering devices.

Discover systems

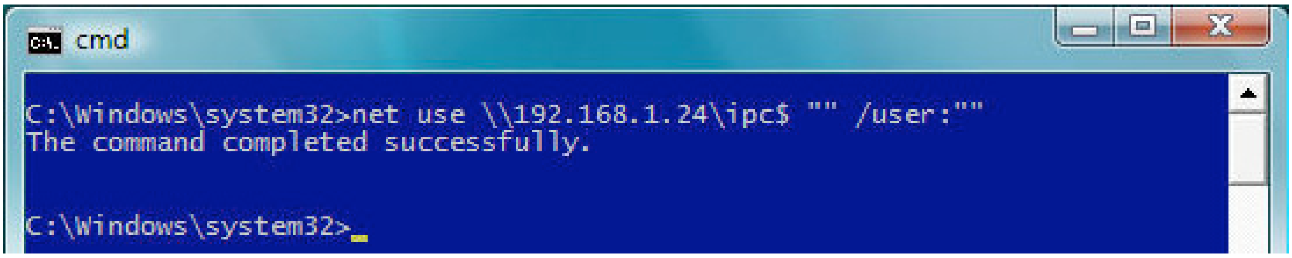
Now we can scan a network for specific systems. It’s beyond the scope of this article to discuss this all but assume the attacker is on the internal network. A system presents most of the times a fingerprint of services running on that box by - for example - specific opened ports. This makes it in one or another way unique. Linux, Unix and Windows systems all have some unique characteristics. This makes it possible to get a picture of the workstations and servers on the network segment and the type of systems. A domain controller presents some specific ports open like the port for Kerberos and LDAP traffic. Active Directory does its job by transmitting traffic over this type of ports and to have this opened up give a good indication of the possible role of the machine scanned.

Once the attacker finds an interesting system, he can use several exploits in the field that can be used to compromise a system. For ethical reasons I’m not presenting the whole story here. However, there are many vulnerabilities, not only Microsoft Windows orientated but also on Linux, Firefox, specific routers and applications. Just pretend I now want to get control over a specific machine in the network, either remote or physical. You gain that control. Next I’m presenting a very old trick that most of you will know from the past, this just as an example. The point is that it is still working on older or unpatched systems.

The famous and notorious Null Session

A so called “null session” occurs when you log on to a Windows system with no username or password at all. NetBIOS null sessions are vulnerabilities found in SMB, Server Message

Block protocol. SMB is a protocol for sharing files, printers, and communications such as named pipes between Windows computers.



```
C:\Windows\system32>net use \\192.168.1.24\ipc$ "" /user:""
The command completed successfully.

C:\Windows\system32>_
```

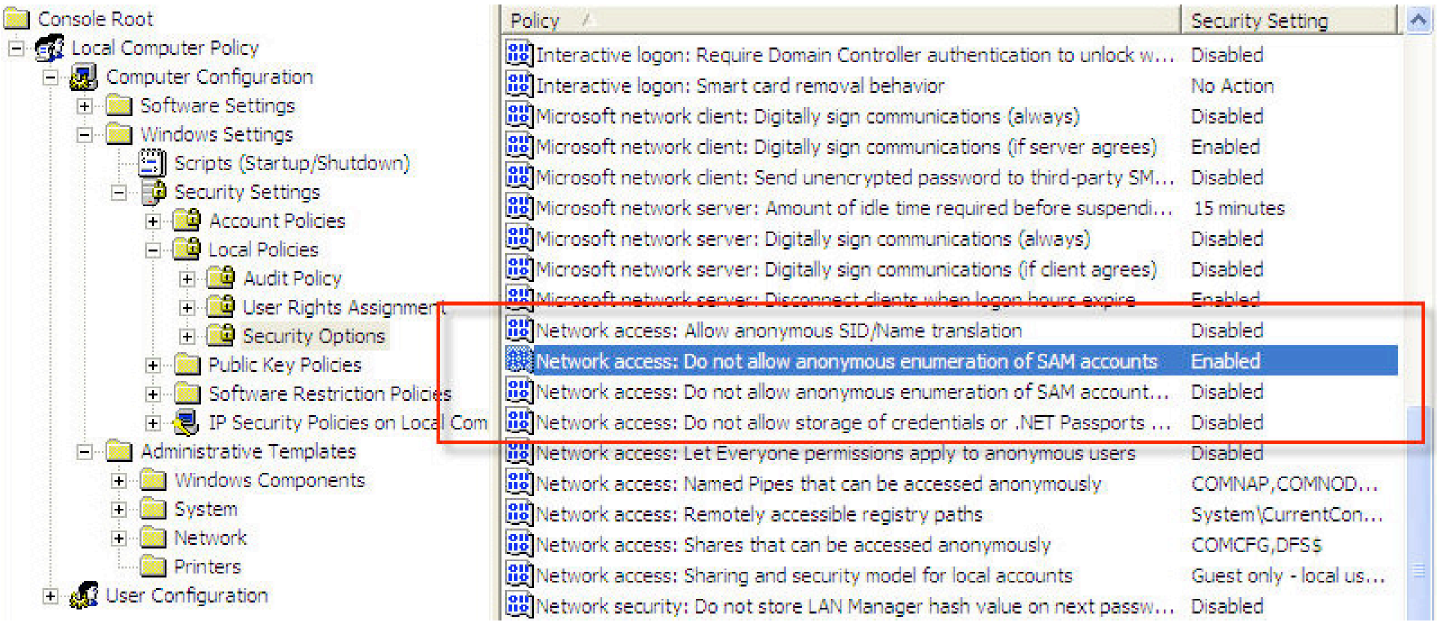
Setting up a Null session

One method of connecting a NetBIOS null session to a Windows system is to use the hidden Inter Process Communication share (IPC$). This hidden share is accessible using the net use command. The empty quotation marks ("") indicate that you want to connect with no username and no password. The syntax is as follows:

```
C: \> net use \\192.168.1.71 \IPC$ "" /u:
""
```

Once the net use command has been successfully completed, the hacker has a channel over which to use other hacking tools and techniques. Its relative easy to get a full dump of all usernames, groups, shares, permissions, policies, services and more using the Null user session possibility.

At this moment there are some options to protect against this kind of null sessions by setting a specific policy. In Windows (XP, Vista) there is a handful of policies that can be used and activated or are there by default to protect you against this type of attack. You can get some additional things in place to protect against this, I'll return on that later.



Console Root
- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Public Key Policies
        - Software Restriction Policies
        - IP Security Policies on Local Com
    - Administrative Templates
      - Windows Components
      - System
      - Network
      - Printers
  - User Configuration

Policy	Security Setting
Interactive logon: Require Domain Controller authentication to unlock w...	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SM...	Disabled
Microsoft network server: Amount of idle time required before suspendi...	15 minutes
Microsoft network server: Digitally sign communications (always)	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM account...	Disabled
Network access: Do not allow storage of credentials or .NET Passports ...	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	COMNAP,COMNOD...
Network access: Remotely accessible registry paths	System\CurrentCon...
Network access: Shares that can be accessed anonymously	COMCFG,DFS$
Network access: Sharing and security model for local accounts	Guest only - local us...
Network security: Do not store LAN Manager hash value on next passw...	Disabled

Policies in Windows

Take over accounts

If an attacker can get on a Windows computer (either a server or client computer), it is possible to choose from a wide variety of tools to get access to the password database (NTLM hashes) on that machine.

After that, the attacker can start a brute force attack on the hashes and before you know it, the worst has happened. More accounts will be compromised and can be used to further elevate privileges, empty logs and create backdoors.

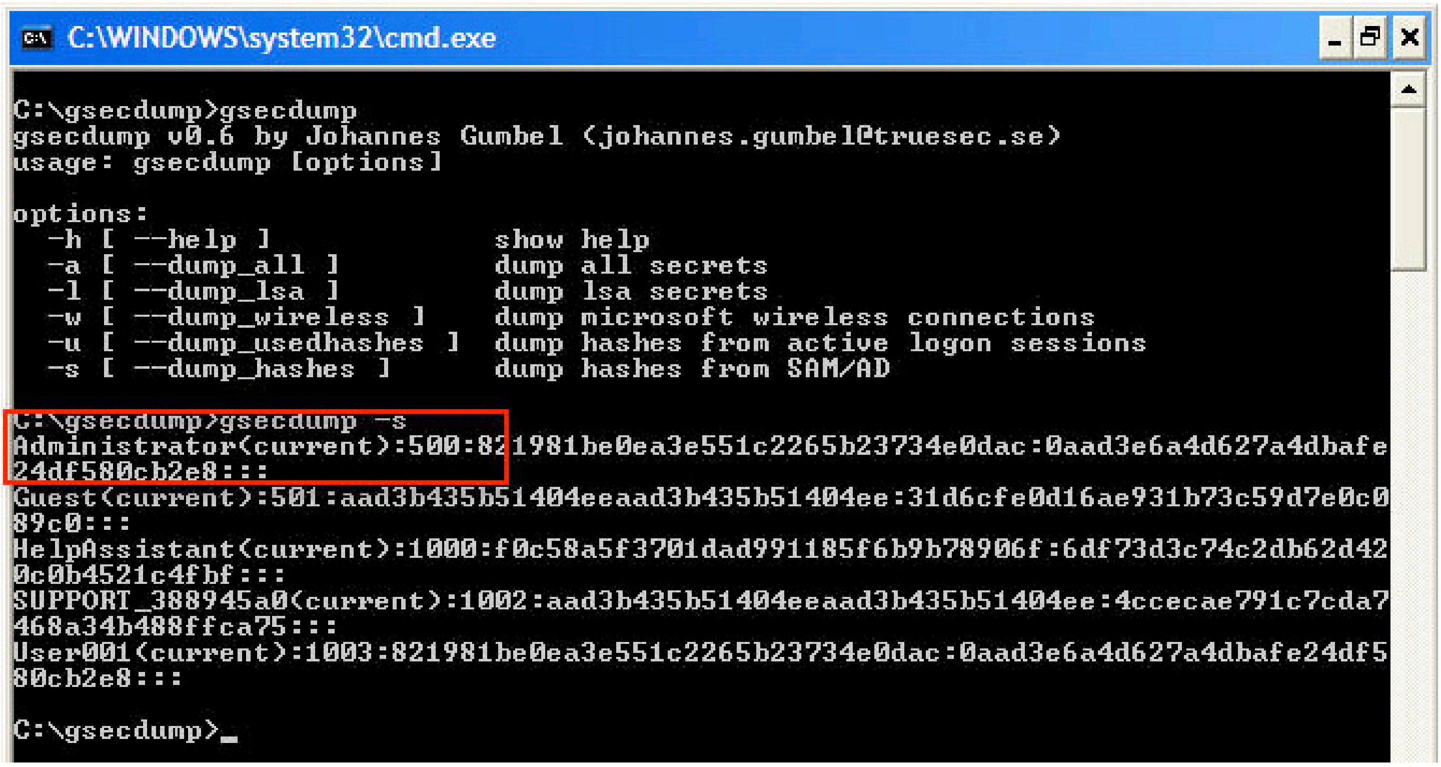
On the Windows computer it’s possible to use the gsecdump tool. This tool dumps all the hashes from the accounts on that machine. Possibilities from the command prompt are:

```
-h [ --help ] show help
-a [ --dump_all ] dump all secrets
-l [ --dump_lsa ] dump lsa secrets
-w [ --dump_wireless ] dump Microsoft
wireless connections
-u [ --dump_usedhashes ] dump hashes from
active logon sessions
-s [ --dump_hashes ] dump hashes from
SAM/AD
```

However, this tool needs to be running under a SYSTEM context on that computer while the logged on user will not be running in that context. Services however will be running under the credentials of SYSTEM. The solution is to create a service that is running the command line shell in SYSTEM context. To do this;

```
C: \> sc create shellcmdline binpath=
"cmd /K start" type= own type= interact
C: \> sc start shellcmdline
C: \> sc delete shellcmdline
```

Now the command line window is running under the right credentials. Even under Vista this can be done. Now the gsecdump tool can be started and get some data. In the next screenshot you can find the result of such an action.



```
C:\gsecdump>gsecdump
gsecdump v0.6 by Johannes Gumbel (johannes.gumbel@truesec.se)
usage: gsecdump [options]

options:
  -h [ --help ]             show help
  -a [ --dump_all ]         dump all secrets
  -l [ --dump_lsa ]         dump lsa secrets
  -w [ --dump_wireless ]    dump microsoft wireless connections
  -u [ --dump_usedhashes ]  dump hashes from active logon sessions
  -s [ --dump_hashes ]      dump hashes from SAM/AD

C:\gsecdump>gsecdump -s
Administrator(current):500:821981be0ea3e551c2265b23734e0dac:0aad3e6a4d627a4dbafe
24df580cb2e8:::
Guest(current):501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
HelpAssistant(current):1000:f0c58a5f3701dad991185f6b9b78906f:6df73d3c74c2db62d42
0c0b4521c4fbf:::
SUPPORT_388945a0(current):1002:aad3b435b51404eeaad3b435b51404ee:4ccecae791c7cda7
468a34b488ffca75:::
User001(current):1003:821981be0ea3e551c2265b23734e0dac:0aad3e6a4d627a4dbafe24df5
80cb2e8:::

C:\gsecdump>_
```

A gsecdump result

The next thing to do is to attack the hashes by using a good password crack utility. Another possibility would be to fire up a sniffer and to get the hashes sniffed off the network. Since most of us don’t use SMB signing the SMB traffic is simple to intercept.

Counter measures

How can you take some precautions without having to spend that much of money on special hardware, software and consultants?

First and foremost, get a decent security policy and baseline in place, hand out proper procedures and manage and control them, let users sign a non-disclosure agreement or a disclaimer document. If you don’t have it, all the other will be a waste of time. Then think about segmenting your network. Servers on a server segment and clients separately on another part. Even in the DMZ you can use segmentation. In case one server is attacked and compromised, the other isn’t necessarily affected. Create some strict paths between these segments and ensure monitoring is in place.

Implement server isolation. In such a scenario, specific servers or applications are configured to require IPSec policies to accept authenticated communications from other computers. For example, you might configure the domain controller to accept connections only from another domain controller in the Active Directory domain for certain services. Besides that, you can also implement domain isolation in a Windows environment. To isolate a domain, you can use Active Directory and the domain membership to ensure that only domain-member computers accept authenticated and secured communications from other domain-member computers. The isolated network holds only computers that are part of this domain.

Protect your workstations (laptops) by using encryption and lower the cache for logged on users (be able to log on even the domain is not there). On laptops, this setting can probably be set to 1. Get good password policies with more strong passwords or better and use passphrases or get the smart card in with pin code.

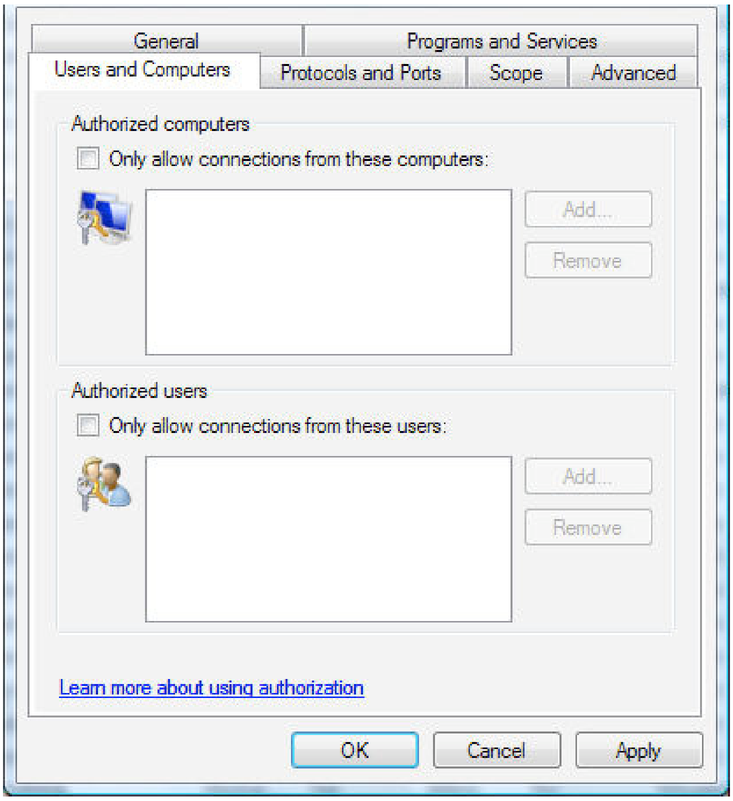
Next, harden servers as much as possible. Microsoft understands this problem and in Longhorn server or Server 2008 the started services will be minimized. You can download some pre-defined (policy) templates to implement this for Windows Servers.

When there is no need to get Internet access from workstations in your environment, just don't provide it Most malware and rootkits come in by simply clicking or browsing on a website. Block unwanted devices using device control on your workstations so you have much more control over this kind of behavior.

Use logging to actively monitor servers, clients and users and care about the central and safe storage of this all so logs can't be destroyed by non-authoritative persons or personnel. Server 2008 and Windows Vista do have the option to write or upload log data to a central server to analyze this when needed. Use encryption techniques to protect data and get decent patch management in place.

Then, use host firewalls and IPSec for the creation of tunnels or use only the authentication part of IPSec to let systems strong authentication.

I will go in a little more detail on the Vista firewall in combination with IPSec and the possible solutions it can offer for you. All the attack vectors I mentioned earlier in this article can be broken down by implementing one or more of the things I just mentioned.



Authorized computers

□ Only allow connections from these computers:

Authorized users

□ Only allow connections from these users:

Vista firewall: allow only specific connections

Using Host based firewall and IPSec

The Windows Vista Firewall comes enabled for both inbound and outbound connections. The default policy is to block most inbound connections and allow outbound connections. You can use it with the Advanced Security interface to configure specific custom made rules for both inbound and outbound connections.

You can configure different rules and settings for the following firewall profiles:
- domain. Used when a computer is connected to an Active Directory domain of which the computer is a member.
- private. Used when a computer is connected to a private network behind a private gateway or router.
- public. Used when a computer is connected directly to the Internet or any network that has not been selected as Private or Domain.

When a user connects to a network that is not part of the domain, Vista pulls up that wall and asks the user to identify the network as either Public or Private. In combination with IPSec authentication, you can configure rules for specific computers so that connections from those computers bypass other rules set up in the Windows Firewall. This allows you to block a particular type of traffic, but allow authenticated computers to bypass this.

The great thing about this is that a certain port is not even open if the criteria are not met. So if a non-authorized computer is trying to contact, the port is not available. This authentication goes all the way - specific computer, users, membership of Active Directory groups and so on. If you do have a PKI in place, it's possible to combine this with the presentation of a client computer certificate and a user certificate that is stored on a smart card. In that way a user can be restricted to log on from a specific network segment, computer or a combination.

You can even restrict an administrator to do some work from specific computers or network segments by implementing the appropriate rules. If an administrator is trying to log on from home, this can be made impossible because of certain rules. As you can see, very granular and easy to manage because you will already be familiar with other management tasks within Active Directory.

With Windows Vista, the firewall can allow more granular authenticated bypass rules, allowing the administrator to specify which ports or programs can have access, as well as which computer or group of computers can have access.

Windows Service Hardening helps prevent critical Windows services from being used for potentially malicious activity in the file system, registry or network. If the firewall detects specific behavior as defined by the network rules, the firewall will block its traffic at once. If a service is exploited and gets to run malicious code, it is prevented from sending or receiving traffic over non-authorized network ports. This reduces the effect the malicious code has on the system itself and spreading of that to other hosts in the network greatly reducing the attack vector.

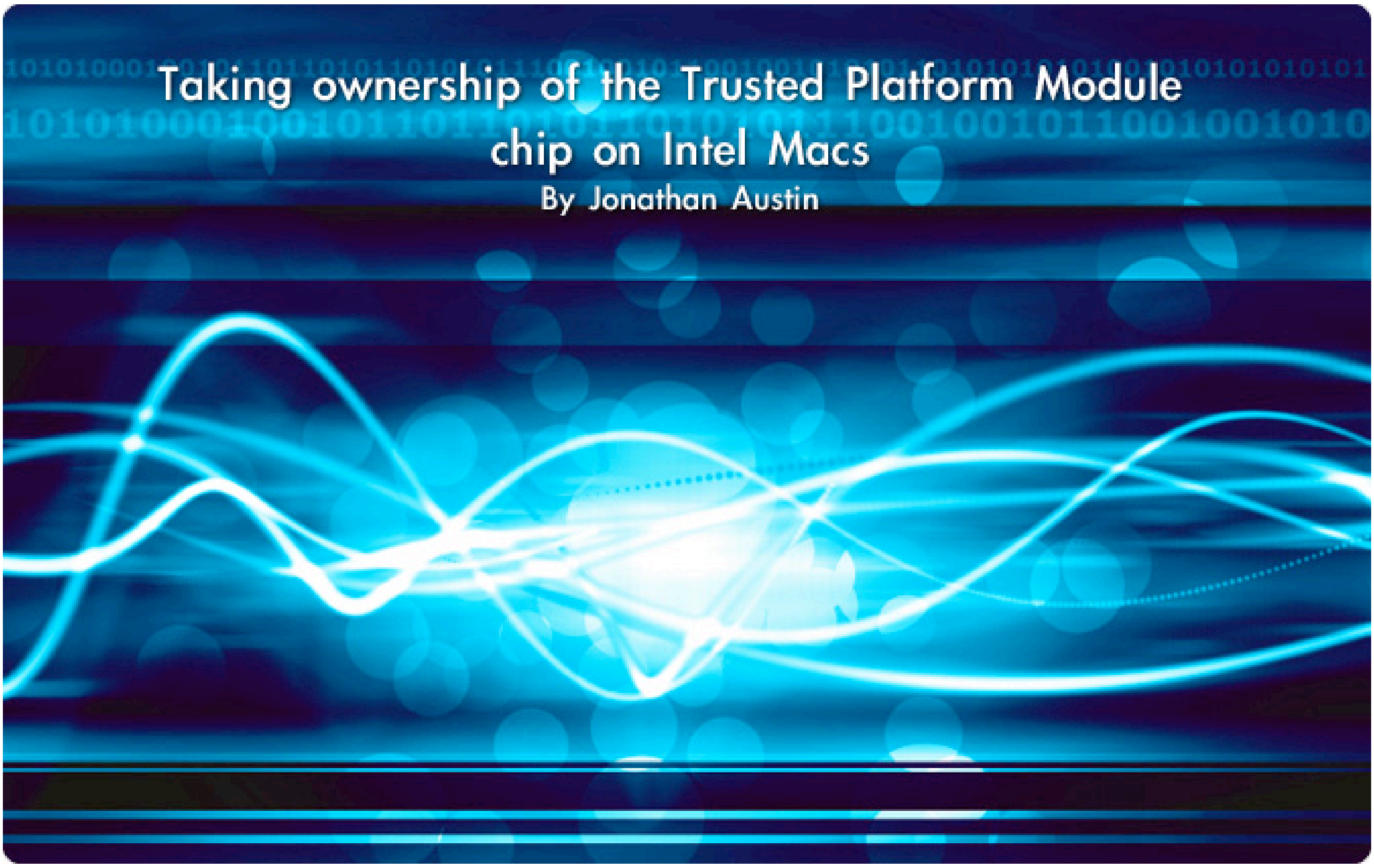
I believe there are several possibilities within Windows XP, Server 2003, Vista and the not yet released Server 2008 to act against the more traditional attacks. With a good plan and up to date technology, there is a lot that can be done to make it much harder for the determined attacker to gain access and control over your environment.

Malware, rootkits and other types of sophisticated technology play an important part in our networked and more open world today than ever before. 70 percent of Windows computers today are infected by some kind of malware. It is a new and different threat and not stopped by traditional solutions. We certainly need to create awareness in our end-users to make sure this doesn't happen as often.

Rob P. Faber (CISSP, CEH, MCSE) is an infrastructure architect, consultant and senior engineer. He is currently working for an insurance company (22.000 client computers) in The Netherlands. His main working area is (Windows Platform) Security, Active Directory and Identity Management. You can reach him at rob.faber@icranium.com or find him on the LinkedIn network.

Taking ownership of the Trusted Platform Module chip on Intel Macs

By Jonathan Austin



I have been following the works of Trusted Computing Group (TCG) since their inception. The body, successor to the Trusted Computing Platform Alliance started by such giants as Hewlett-Packard, IBM, Intel and Microsoft, has a goal to develop vendor-neutral standard specifications for trusted computing. TCG is quite present on all the major information security conferences around the globe, so I had an opportunity to attend to some of their lectures and check out the actual trusted platforms (hardware devices with TPM chips) in test environments.

What is a TPM chip

The TPM is a microcontroller that stores keys, passwords and digital certificates. It's typically affixed to the motherboard of a PC. The nature of this silicon ensures that the information stored there is made more secure from external software attack and physical theft. Security processes, such as digital signature and key exchange, are protected through the secure TCG subsystem.

Access to data and secrets in a platform could be denied if the boot sequence is not as expected. Critical applications and capabilities such as secure email, secure web access and local protection of data are thereby made much more secure. TPM capabilities also can be integrated into other components in a system.

Apple and TPM

If you bought your Mac between May and October of 2006, you most probably have a TPM chip. The chip in question was Infineon TPM, module SLB 9635 TT 1. It looks like Apple had plans to use the trusted platform possibilities, but while the chip was present, Apple did not use it at all. Therefore, computers released after October 2006 do not contain an onboard Infineon TPM. As Trusted Computing Group is seeing an upscale adoption rate of their technology, TPM will most probably be back inside Apple hardware in the future.

Benefits for the users

Amit Singh, author of the "Mac OS X Internals: A Systems Approach" wrote a whole chapter about trusted computing for

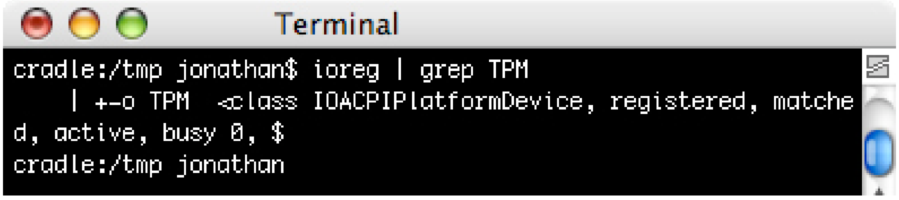
Mac OS X. Besides this, he released Mac driver and daemon that will be used later in this article.

While the TPM chip is not used by any of the Apple software products, that doesn't mean that developers cannot use it for the specific purposes of their applications. While it is not the best idea to target just the computers that have TPM chips, this "perfect" customizations can be used in some organizations for instance running just the TPM-enabled Macs. Singh notes that developers could use the TPM from within their own applications to:

- Create private/public key pairs such that the private key never leaves the TPM in clear form and because of it the private key cannot be stolen.
- Sign data without the private key ever leaving the chip.
- Encrypt data such that it can only be decrypted on the physical machine it was encrypted on.
- In protocols such as SSL that use key exchange, employ the TPM for a much better guarantee regarding the identities involved.

Testing the existence of TPM chip

For the purpose of testing your computer for existence of the TPM chip we will need to use a command line utility ioreg which displays the I/O Kit registry. Starting the utility without any particular switches, we can just filter the output while grepping for TPM. The result shows that TPM is present on my MacBook notebook:



```
cradle:/tmp jonathan$ ioreg | grep TPM
    | +-o TPM  <class IOACPIPlatformDevice, registered, matche
d, active, busy 0, $
cradle:/tmp jonathan
```

Tools of the trade

For the purpose of mangling with the TPM chip, we need to use the following:

TPM Setup

Mac application released in mid June 2007 that can be used to setup and take ownership of your TPM. The software package is provided by the fine folks at Comet Way, which recently noted their plans to release a simple file encryption utility for your TPM Mac.

Important: TPM Setup is an Intel binary, therefor can be used just on Intel Macs.

TPM Setup can be downloaded from:
1) Comet Way: darkside.cometway.com
2) Help Net Security:
net-security.org/software.php?id=675

OSXBookTPM.kext and tcsd

These are Amit Singh's kernel extension and the daemon needed for the whole TPM experience. These files were released under GPLv2, so the guys at Comet Way are redistributing them within the TPM Setup package. Bottom line, all the applications you will need are located in the same archive linked in the previous paragraph.

There are is a disclaimers the developers provided with the TPM Setup application. The software is provided as a demo and should be used on your own risk. From the technical perspective the only troublesome thing you can create is to setup and then forget the TPM password which could be a bad thing. You will also need to be at least a bit familiar with the UNIX Shell, but following the graphics from this article should be just enough.

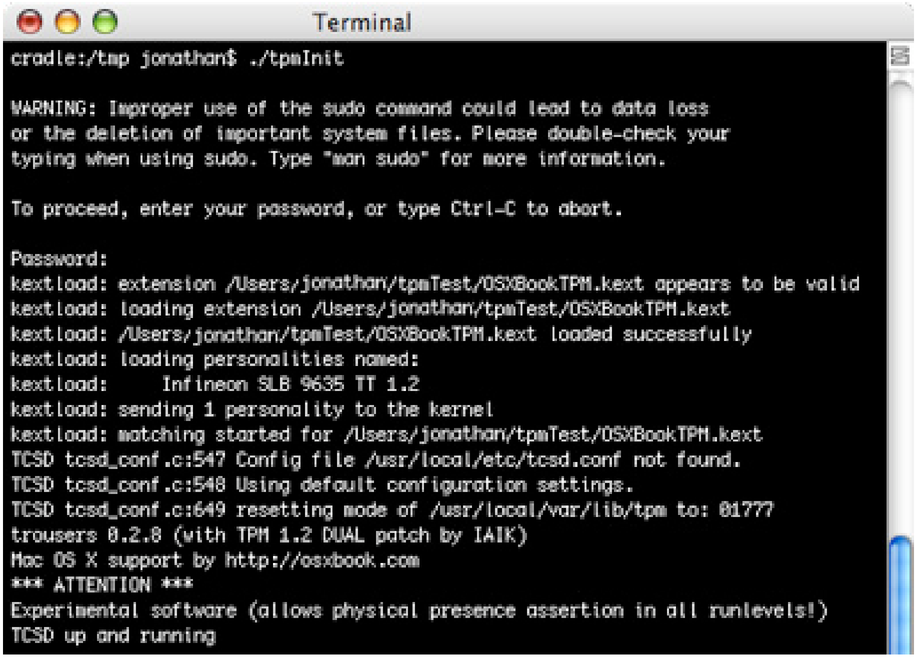
Let's take the ownership of the TPM chip

As you could see from the first screenshot, TPM is enabled and activated. The only thing still needed is to take the ownership of it. This means that we need to setup two passwords: one for the TPM chip itself and the other one for the Storage Root Key (SRK).

TPM Setup can also reset a TPM by clearing it, enabling and activating it, and allowing the user to take ownership of the TPM. In this case two reboots will be required, once after clearing the TPM, and once again after enabling and activating it.

In our case of a "clean TPM", we won't need any reboots and the only interaction is entering two sets of passwords (can be identical). Before this, we need to use the Terminal and start the Amit Singh's tcsd daemon and load the TPM kernel extension:

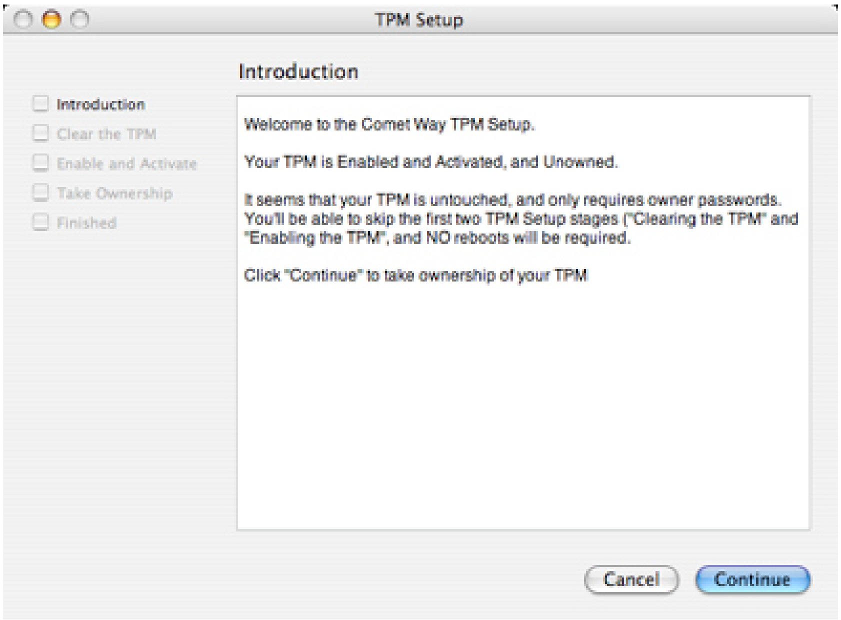
As mentioned earlier, the support directory of the TPM Setup contains all the needed scripts, kernel extension and the daemon. Let's start the daemon with the tpmInit script:



```
cradle:/tmp jonathan$ ./tpmInit

WARNING: Improper use of the sudo command could lead to data loss
or the deletion of important system files. Please double-check your
typing when using sudo. Type "man sudo" for more information.

To proceed, enter your password, or type Ctrl-C to abort.

Password:
kextload: extension /Users/jonathan/tpmTest/OSXBookTPM.kext appears to be valid
kextload: loading extension /Users/jonathan/tpmTest/OSXBookTPM.kext
kextload: /Users/jonathan/tpmTest/OSXBookTPM.kext loaded successfully
kextload: loading personalities named:
kextload:     Infineon SLB 9635 TT 1.2
kextload: sending 1 personality to the kernel
kextload: matching started for /Users/jonathan/tpmTest/OSXBookTPM.kext
TCSD tcsd_conf.c:547 Config file /usr/local/etc/tcsd.conf not found.
TCSD tcsd_conf.c:548 Using default configuration settings.
TCSD tcsd_conf.c:649 resetting mode of /usr/local/var/lib/tpm to: 01777
trousers 0.2.8 (with TPM 1.2 DUAL patch by IAIK)
Mac OS X support by http://osxbook.com
*** ATTENTION ***
Experimental software (allows physical presence assertion in all runlevels!)
TCSD up and running
```

The script needs administrative privileges so the appropriate password needs to be entered. As you can see from the screenshot, kernel extension is successfully loaded and the daemon is started. Do leave this terminal window open and if you want to kill the daemon hit the Ctrl+C key combination.

Now when the daemon is started, we can open the TPM Setup application and take the ownership of the TPM chip. If because of some reason you didn't start the daemon or the start was unsuccessful, the following window will say that you should start the process again. In our case, everything is just fine:



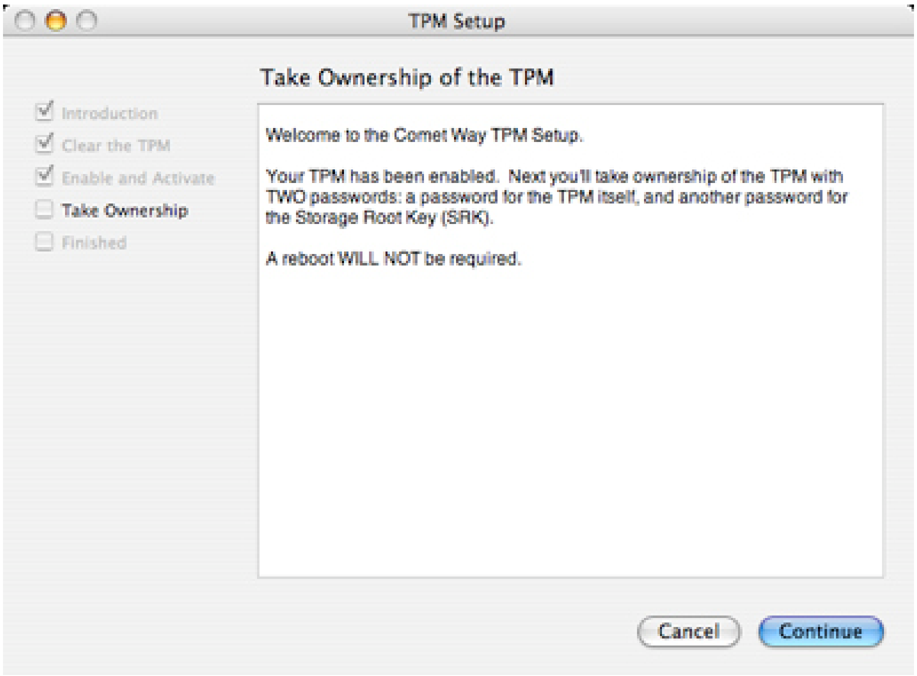
Welcome to the Comet Way TPM Setup.

Your TPM is Enabled and Activated, and Unowned.

It seems that your TPM is untouched, and only requires owner passwords. You'll be able to skip the first two TPM Setup stages ("Clearing the TPM" and "Enabling the TPM", and NO reboots will be required.

Click "Continue" to take ownership of your TPM

Time to enter the user and SRK passwords:



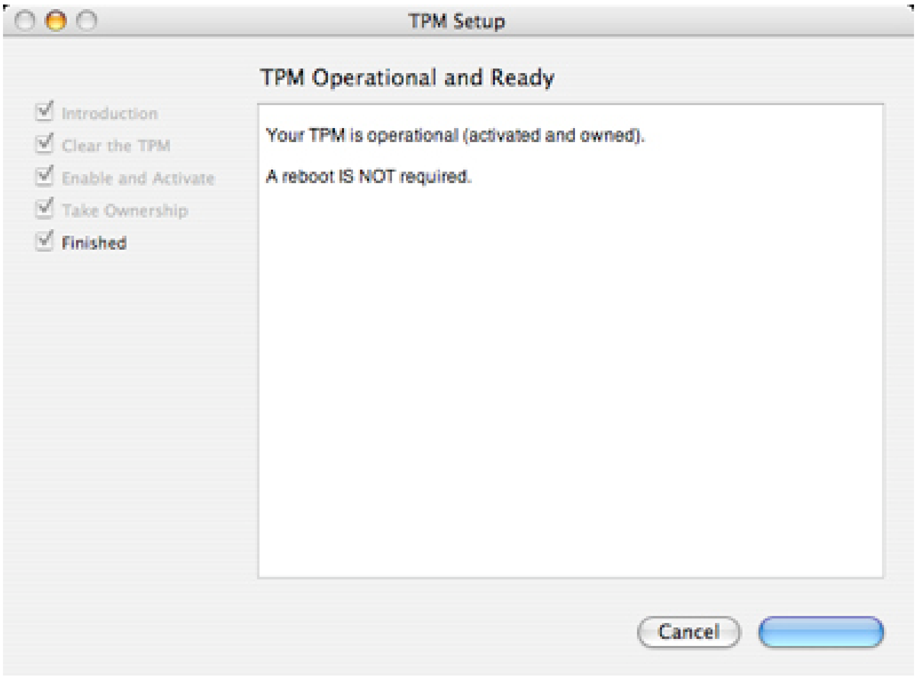
Take Ownership of the TPM

Welcome to the Comet Way TPM Setup.

Your TPM has been enabled. Next you'll take ownership of the TPM with TWO passwords: a password for the TPM itself, and another password for the Storage Root Key (SRK).

A reboot WILL NOT be required.

Final phase - TPM is operational, activated, enabled and owned:



TPM Operational and Ready

Your TPM is operational (activated and owned).

A reboot IS NOT required.

Conclusion

The whole procedure covered throughout this article is not at all "mainstream", so TPM will currently be of use to an extremely limited number of users. Soon Comet Way will release the mentioned file encryption utility and there is always a need for enhancing the state of security on your Mac.

References

- TPM Setup (tinyurl.com/2ytlar)
- Trusted Computing for Mac OS X (tinyurl.com/yqvydz)
- Trusted Computing Group (trustedcomputinggroup.org)
- TPM Work Group (trustedcomputinggroup.org/groups/tpm/)

Jonathan Austin is a security manager at a healthcare provider with over 10 years of IT experience. His passions include Mac OS X security, Linux clustering and PHP code auditing.

Compliance, IT security and a clear conscience

By Calum MacLeod

Never has the need to prove compliance with external regulations and internal policies been more acute than it is today. The likely consequences of failing to prove that your organization is compliant and that you are strictly adhering to your own policies can be significant, up to and including possible criminal penalties for top corporate executives. And the buck doesn't stop there. Anyone who is familiar with the Enron story may also remember that it resulted in the once grand Arthur Andersen being brought to its knees, illustrating the thoroughness that external auditors will apply to ensure that they are not implicated.

Organizations today must prove beyond a shadow of a doubt that not only do they have a security program in place, but that it is enforced and is consistent across your organization. Information technology departments play a key role in this endeavor. Shortcomings in IT policies can have potentially serious consequences.

Research by Gartner has shown that 65 percent of all successful computer attacks take advantage of badly configured systems such as use of out-of-the-box default conditions, configuration of user accounts that have privileged rights, simple configuration errors or unscrupulous system administrators. If that's not bad enough another in a recently published survey conducted by the U.S. Secret Service together with Carnegie Mellon University's Software Engineering Institute CERT Program found that eighty-six percent of people who carried out insider sabotage held technical positions and ninety percent had system administrator or privileged system access – which meant they held the passwords to override the system and access the network.

No matter how secure a system may be, if the controls to access that system are not adequate, eventually this will be exposed.

A recent Audit Commission report in the UK highlighted that problems are frequently a result of poor access controls that inevitably increase the risk of accidental damage and deliberate abuse. Instances such as the failure of management to escort disgruntled employees from buildings and remove all IT system access facilities have resulted in such staff having the time and opportunity to vent their anger on the organization and cause major disruptions.

Interestingly, the report found the main reasons for breaches were ineffective policies, and the failure to enforce policies.

There are also many misconceptions about regulatory compliance for outsourcing. For example, if your company has outsourced management of its IT infrastructure, the responsibility of compliance still rests with your company, not its outsourcing partner. Additionally, companies providing outsourcing services need to ensure that they are not implicated in the event that issues arise. In other words, select a good outsource partner and you could be a winner. Select a bad one and you could be out of business. It is not the brand name that should convince you but the quality and experience of the staff that will be responsible for your highly sensitive data.

THE IMPORTANCE OF AUTOMATION IN TRACKING AND REPORTING IT CONTROLS CANNOT BE OVERSTATED.

Compliance and regulatory requirements

Being compliant has become a major focal point for most large organizations, but this for all practical purposes should be a goal for risk management and security in every organization. Regardless of external factors, those responsible for the integrity of the IT environment should be actively involved in ensuring that permanent staff, business partners and contracted staff, who may have privileged user rights, comply with company policies when it comes to handling company assets.

For those organizations that also need to meet public standards, the level of media exposure that has resulted from high-profile cases in the United States means that most people in the IT security arena are familiar with Sarbanes-Oxley, Basel II, 21 CFR Part 11, PCI, Gramm-Leach-Bliley and HIPAA.

However, it is not simply these much publicized standards. Today most countries have regulations in place that are very similar, such as France's "Loi de Securité Financière", Germany's "KonTraG", the UK's "Combined Code" and the Netherlands "Tabaksblat Code", which require a similar level of due diligence when it comes to IT security practices, although there are variations related to the compulsory nature in different countries.

Additionally, many organizations are adopting best practices by implementing standards such as ITIL, and ISO 27001 in order to ensure consistency across their enterprises. From an IT perspective, what all of these regulations have in common is that they require the strengthening of internal controls related to the use of IT systems.

The controls that are specified in most standards are very similar. All deal with the primary threats that exist in the IT environment, focusing on the misuse of privileged accounts, mistakes by privileged users and malfunctions within the IT infrastructure itself, particularly when it comes to the security of highly sensitive information. The IT security group needs to be able to prove which privileged user accessed what system, demonstrate that confidential systems and data could not have been accessed by those who had no rights and that those who have the right are tracked.

The importance of automation in tracking and reporting IT controls cannot be overstated. These tools are important in providing timely alerts by continuously collecting and alerting on events for any critical component within the IT infrastructure. Additionally, they are an important factor in reducing the costs associated with collating the information. For any organization that must comply with these regulations, it is mandatory that the IT departments comply, and that the IT security department in an organization must be able to demonstrate to the rest of the organization, and to those external parties that monitor the activities, that the effectiveness of IT controls are adequate.

Anyone who has been faced with an audit, either internal or external, can attest to the resource demands that are placed on the IT organization. This can be especially challenging when an organization is present in different geographical locations. The effectiveness of the controls and reporting tools within the IT security departments are critical both to achieving a successful audit, and limiting the amount of resource that is required to deliver the necessary information.

Ultimately, you are answering the questions, do you have the important controls in place, have you implemented effective change management and if your access controls are effective – and of course can you prove it.

A major challenge facing organizations today is that regulations do not make allowances for unintentional errors, and human error is one of the biggest risks faced by companies, especially as pressure to reduce costs means that more and more tasks are being carried out by less staff. Today almost all risk results from internal threats and because many organizations focus their investment in protecting against the external threat, they are often not adequately prepared to protect the internal risks. Today any organization that has an IT infrastructure relies heavily on databases, and database security practices, including everyone and every process that accesses the database, will always be scrutinized very closely by auditors.

So what should you do?

Whether or not you are compelled to apply policies to comply with the various standards, you should familiarize yourself with what is required. My recommendation would be to start by taking the time to study the ISO 27001 standard to gain an overall view of what is required to have an effective information security policy and in conjunction look at the requirements of the Payment Card Industry (PCI) standard. Although the PCI standard is intended for organizations that deal with credit card transactions it offers a very practical guide to what should be done on a practical level in many areas, and will ensure that you have taken adequate precautions to protect yourself and your business.

Calum MacLeod has over 30 years of expertise in secure networking technologies, and is responsible for developing the Cyber-Ark business in Europe and Africa.

Before joining Cyber-Ark, MacLeod served as Europe, Middle East and Africa Business Development Director for Netilla Networks, and was responsible for leading some of the early SSL VPN projects in Europe. MacLeod has also served as an independent consultant to corporate and government clients on IT security strategy for various European market segments, including the European Commission.

Events around the world

Black Hat USA 2007 Briefings & Training
28 July-2 August 2007 – Las Vegas, USA
http://www.blackhat.com/

HITBSecConf2007
3 September-6 September 2007 – Kuala Lumpur, Malaysia
http://conference.hitb.org/hitbsecconf2007kl/

Security ‘07 – 16th USENIX Security Symposium
6 August-10 August 2007 – Boston, USA
http://www.usenix.org/events/sec07/

Chaos Communication Camp 2007
8 August-12 August 2007 – Finowfurt, Germany
http://events.ccc.de/camp/2007/Home

InfowarCon 2007
9 September-21 September 2007 – Bethesda, USA
http://www.infowarcon.com/

RSA Conference Europe 2007
22 October-24 October 2007 – London, United Kingdom
http://www.rsaconference.com/2007/Europe

3rd Annual Techno Forensics Conference
29 October-31 October 2007 – Gaithersburg, USA
http://www.Techno2007.com/

Key management for enterprise data encryption

By Ulf Mattsson

Best practices dictate that we must protect sensitive data at the point of capture, as it's transferred over the network (including internal networks) and when it is at rest. Protecting data only sometimes - such as sending sensitive information over wireless devices over the Internet or within your corporate network as clear text - defeats the point of encrypting information in the database.

It’s far too easy for information to be intercepted in its travels so the sooner the encryption of data occurs, the more secure the environment will be. A comprehensive encryption solution doesn’t complicate authorized access to the protected information - decryption of the data can occur at any point throughout the data flow wherever there is a need for access.

Decryption can usually be done in an application-transparent way with minimum impact to the operational environment. Due to distributed business logic in application and database environments, organizations must be able to encrypt and decrypt data at different points in the network and at different system layers, including the database layer.

Encryption performed by the database management system can protect data at rest, but more security oriented corporations will also require protection for data while it’s moving between applications, databases and data stores. One option for accomplishing this protection is to selectively parse data after the secure communication is terminated and encrypt sensitive data elements at a very granular level (usernames, passwords, and so on). Application-layer encryption and mature database-layer encryption solutions allow enterprises to selectively encrypt granular data into a format that can easily be passed between applications and databases without changing the data.

Key Management is often overlooked

One of the essential components of encryption that is often overlooked is key management - the way cryptographic keys are generated and managed throughout their life.

Since cryptography is based on keys which encrypt and decrypt data, your database protection solution is only as good as the protection of those keys. Security depends on several factors including where the keys are stored and who has access to them. When evaluating a data privacy solution, it is essential to include the ability to securely generate and manage keys. This can be achieved by centralizing all key management tasks on a single platform, and effectively automating administrative key management tasks, providing both operational efficiency and reduced management costs.

Data privacy solutions should also include an automated and secure mechanism for key rotation, replication, and backup. The difficulty of key distribution, storage, and disposal has limited the wide-scale usability of many cryptographic products in the past. Automated key distribution is challenging because it is difficult to keep the keys secure while they are distributed, but this approach is finally becoming secure and more widely used. Standards for key-management have been developed by the government and by organizations such as ISO, ANSI, and the American Banking Organization (ABA). The key management process should be based on a policy. This article will exemplify different elements of a suggested policy for a Key Management System used for managing the encryption keys that protect secret and confidential data in an organization.

A major problem with encryption as a security method is that the distribution, storage, and eventual disposal of keys introduce an expensive and onerous administrative burden.

Issues with native point solutions

A major problem with encryption as a security method is that the distribution, storage, and eventual disposal of keys introduce an expensive and onerous administrative burden. Historically, cryptographic keys were delivered by escorted couriers carrying keys or key books in secure boxes.

An organization must follow strictly enforced procedures for protecting and monitoring the use of the key, and there must be a way to change keys. Even with all of these restrictions, there is always a chance that the key will be compromised or stolen. Even if there are standards developed for key-management it is still the most difficult part of an encryption solution. This is one of the greater challenges to overcome when you decide to create your own solution based on encryption toolkits from database vendors and security vendors. These toolkits provide the basic functionality for encrypting and decrypting information but typically do not provide a secure key-management system.

Many companies have tried to develop their own encryption functionality, but few have succeeded in creating a system that performs not only by doing the obvious encryption, but doing so in a secure and reliable manner that does not prohibit you from keeping your systems operational. A mature data protection system should be based on a sophisticated key management system that is transparent, automated, secure and reliable for the environments where it operates.

A distributed approach with a central point of control

A mature data protection system should provide a central point of control for data protection systems at the application, database and file levels. The encryption solution has a combined hardware and software key management architecture which combine the benefits of each technology. This will address the central security requirements while providing the flexibility to allow security professionals to deploy encryption at the appropriate place in their infrastructure. It provides advanced security and usability smooth and efficient implementation into today’s complex data storage infrastructures.

If your human resources department locks employee records in filing cabinets where one person is ultimately responsible for the keys, shouldn't similar precautions be taken to protect this same information in its electronic format? One easy solution is to store the keys in a restricted database table or file. But, all administrators with privileged access could also access these keys, decrypt any data within your system, and then cover their tracks. Your database security in such a situation is based not on industry best practice, but on trusting your employees. When securing the sensitive data within your organization trust is not a policy. The key custodian should be a role in the IT organization.

The key custodian

The key custodian is responsible for managing the multi-layer key management infrastructure, including the creation of keys, distribution of replacement keys and the deletion of keys that have been compromised. The custodian should be appointed by the Compliance Review Committee. Access to central key management functions should require a separate and optional strong authentication and management of encryption keys should be logged in an evidence-quality audit system. Keys stored in the Hardware Security Module are protected from physical attacks and cannot be compromised even by stealing the Hardware Security Module itself. Any attempt to tamper with or probe the Hardware Security Module will result in the immediate destruction of all private key data, making it virtually impossible for either external or internal hackers to access this vital information.

Encryption of the application data should be performed by an Enforcement Agent that should be implemented as a Dedicated Encryption Service (Please see my articles in (IN)SECURE issue 8 - insecuremag.com and tinyurl.com/23bhz7) that is separated from the administration of the data that it protects. This service may run in different environments including in a separate process, a separate server or in a Hardware Security Module depending on the security class of the data and the operational requirements for performance and availability.

When securing the sensitive data within your organization trust is not a policy.

Key domains for protection and easier management

A mature data encryption solution should support the concept of key domains which can isolate different systems for security reasons or operational needs. Each key domain may have different security exposures and can have a different policy for how keys should be managed including key generation, key rotation and protection of key material. It should support transparent re-encryption of the data when it flows between systems that are using different encryption keys or different algorithms.

The Key Management System must support multiple levels of keys to ensure that the encryption keys that protect secret and confidential data cannot be compromised. This enables the use of different encryption keys for different columns, tables and files. When setting policy, it is important to configure the use of different encryption keys and initialization vectors across different columns, tables and files to maintain compartmentalization and a diverse front against attack. The Keys should be stored in an Enforcement Agent that supports dual control (requiring more than a single administrator/operator) for key recovery. It may be implemented in hardware or software, but it must support both the encryption and integrity of the key backup format.

Annual review of algorithms and key lengths

The Key Management System must support key length or strength of 128-bits or greater for symmetric keys. Such keys are deemed "strong encryption" and are not susceptible to a brute force attack using current technology. Public or asymmetric keys must be of equivalent strength. That is, a 128-bit symmetric key and 3072-bit public key are considered to be equivalent in terms of strength, while a

15,360-bit public key is equivalent to a 256-bit symmetric key. The data encryption should be performed with strong standard algorithms including 3DES, AES 128 or AES 256. Data requiring protection for longer periods of time should use the longer key lengths. Note that adequate CPU power today may not be enough tomorrow as you incorporate more secure communications. It is wise to establish a key-length policy early and review it annually.

Secure generation and distribution of keys

The Key Management System must generate a unique key for each file, tape, or other data element that needs to be encrypted. Private keys must be generated within the secure confines of the Key Management System and never be transferred outside the Key Management System unless encrypted with a Key Encryption Key. All keys should be centrally generated in software or hardware based on the security class for the type of data they protect.

The key management system must be able to electronically transfer private keys to other trusted key repositories throughout the enterprise. This may also be implemented via Smart Cards. The security policy should define where different keys should be stored and cached. The master keys are used to encrypt all operational keys that should be stored in cipher text in separated databases.

Security metadata and operational encryption keys should be kept in cipher text (even when stored in memory) until needed for use by crypto-services routines. All communication both external and internal is encrypted. All Data Protection System services should be using X.509 certificates and SSL for secure distribution of encryption keys. Unique keys should be generated for each Enforcement Agent, and should be used when sending information between system components.

The data encryption method should be based on different encryption keys for different columns, tables, files and directories. An optimal design for Hardware Security Module support can be based on an optimal combination of hardware and software keys. The supported Hardware Security Module should be tamper evident and compliant with FIPS PUB 140-2 Level 3 Security Requirements for Cryptographic Modules, and keys are randomly generated in compliance with ANS X9.24 Section 7.4.

Key validation, access control and logging

Key validation is performed by integrity checking the security metadata that is kept in ciphered text (even in memory). Key access control is performed by role-based authorization of users, allowing for specific authorized actions by user (select/insert/update/delete). Users can be authenticated by any accepted means of the native database.

Any encrypt/decrypt operation requested by the user is verified against the policy by the Enforcement Agent after authorization and authentication checks have been completed by the database. Under the control of the authenticated Security Administrator, the system should generate a Master Key used to encrypt all operational keys.

Security data remains ciphered until needed for use by crypto-services routines. The master keys and data encryption keys should be secured, and their integrity checked. All communication, external and internal, should be encrypted. The system may use public key cryptography to exchange the symmetric encryption keys. The Key Management System must support tracking of; when keys are created and deleted; who created and deleted them; who used what keys; and what was done with the key.

Key protection and aging

Encryption keys should be protected and encrypted when stored in memory or databases, and during transport between systems and system processes. The use of a combination of software cryptography and specialized cryptographic chipsets, called a Hardware Security Module, can provide a selective added level of protection, and help to balance security, cost, and performance needs.

Certain fields in a database require a stronger level of encryption, and a higher level of protection for associated encryption keys.

Encryption keys and security metadata should continuously be encrypted and integrity validated – even when communicated between processes, stored or cached in memory. Security data should remain ciphered until needed for use by crypto-services routines.

Key Rotation, or more accurately Key Aging, is best security practices and required in some governmental regulations and industry initiatives. More sensitive data and data more exposed systems should be re-encrypted with fresh encryption keys more frequently than the rest of the data. A well designed automated key rotation solution can provide zero downtime by attaching key labels to each record or data field in the operation databases and file systems. The Automated key rotation process can run in background and utilize spare cycles on each available processor on your data servers. The background processing can be assigned a priority level that will complete the key rotation according to the policy that is defined.

Encryption keys and security metadata should continuously be encrypted and integrity validated.

Secure key storage

To maintain a high level of security the endpoint server platform should provide the choice to only temporarily cache encrypted lower level data encryption keys. Key encryption keys should always be stored encrypted on separated platforms. A central server with a hardened standard computing platform to store the keys can provide a cost effective solution. Keys should be kept in an encrypted format in memory (cached) until they are to be used.

Data encryption keys should be stored in encrypted format in a separate data server along with other policy information, optionally on the Security Administration System repository or on the local database where the Enforcement Agent is installed, depending on the operational requirements and security level of the data that is protected. All keys except the Master Key should be stored (encrypted) under the Key Encryption Keys. The Master Key should also be protected while in transient storage or be kept inside the Hardware Security Module storage, depending on the operational requirements and security level of the data that is protected by the keys.

Effective protection of memory cached keys

Memory attacks may be theoretical, but cryptographic keys, unlike most other data in a computer memory, are random. Looking through memory structures for random data is very likely to reveal key material. Well made libraries for use as Native Encryption Services go to great efforts to protect keys even in memory. Key-encryption keys are used to encrypt the key while it is in memory and then the encrypted key is split into several parts and spread throughout the memory space. Decoy structures may be created to mimic valid key material. Memory holding the key is quickly zeroed as soon as the cryptographic operation is finished. These techniques reduce the risk of memory attacks.

Separate encryption keys should be used for different data. These encryption keys can be automatically rotated based on the sensitivity of the protected data. A Dedicated Encryption Systems can provide separation between processes or servers dedicated to encryption operations but they are also vulnerable to memory attacks. However, a well made Dedicated Encryption System runs only the minimal number of services. Since web servers, application servers, and databases have no place on a dedicated cryptographic engine, these common attack points are not a threat. This severely constrained attack surface makes it much more difficult to gain the access needed to launch a memory attack. The security classification of the protected data will help in deciding a topology that will give the right balance between security, performance and scalability for each type of environment within an organization.

Key backup and recovery

A weak link in the security of many networks is the backup process. Often, private keys and certificates are archived unprotected along with configuration data from the backend servers. The backup key file may be stored in clear text or protected only by an administrative password. This password is often chosen poorly and/or shared between operators. To take advantage of this weak protection mechanism, hackers can simply launch a dictionary attack (a series of educated guesses based on dictionary words) to obtain private keys.

To maintain a high level of security and separation the application data backup files should be separated from the backup of encrypted lower level data encryption keys. After keys are created, they must be archived to a secure storage environment where they can be kept for long periods of time. Master keys should be backed up separately. During installation, the master key should be generated and stored on removable media for recovery purposes.

Maintaining this media in escrow and/or at your disaster recovery site is best practice. Backup of keys on the Security Administration System should be performed on a regular basis, usually before and after major policy changes are realized.

Backup of the encrypted data encryption keys should be automated and performed at the same time as business data backup, using standard database backup and restore procedures. Even if policies or keys have changed, or if the Security Administration System is unavailable, any Enforcement Agent and its protected database may be restored successfully as long as access to the Master Key is provided via proper user authentication. The Key Management System must be able to survive multiple hardware and site failures and still be able to retrieve the archived keys to unlock encrypted data. The Key Management System must support creation and management of “split keys,” so that the ability to decrypt data requires cooperation of multiple persons, each knowing only their part of the key, to reconstruct the whole key.

Conclusion

We have reviewed crucial guidelines and best practices for a Key Management System for data encryption based on the approach of a central point of control for key management and distributed encryption and policy enforcement across applications, databases and file systems.

The solution provides great flexibility by combining the benefits from hardware and software based encryption and key management. This approach addresses the requirements for central security control while providing the flexibility to allow security professionals to deploy encryption at the appropriate place in their infrastructure. It provides the needed balance between advanced security, availability, and performance for the combined solution.

The concept of separate key domains across a data flow can isolate different systems from a risk perspective and it can also accommodate for differences in the operational requirements. Best practices dictate that we must protect sensitive data at the point of capture, as it's transferred also over internal networks and when it is at rest.

A mature solution for encryption and key management can provide this higher level of protection of information.

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

For more of his work download earlier issues of (IN)SECURE Magazine.

DEEP KNOWLEDGE SECURITY CONFERENCE

HITBSecConf2007 – Malaysia

3rd – 6th September 2007

Day 1 Keynote

Mark 'Phiber Optik' Abene

Former member of LOD / MOD

Emmanuel Goldstein

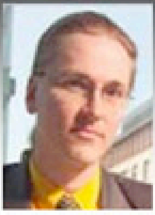
Founder, 2600 Magazine

Day 2 Keynote

Lance Spitzner

Founder, Honeynet Project

Mikko Hypponen



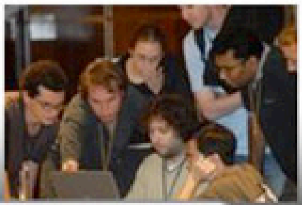
Chief Research Officer, F-Secure Corp.

3rd – 4th September : 7 Hands-On Technical Training Tracks

- Advanced Web Application & Services Hacking
- Practical Malcode Threat Analysis
- The Exploit Laboratory
- Telecommunication Fraud
- Structured Network Threat Analysis & Forensics
- Wardriving Kuala Lumpur
- Hacking & Hardening Oracle

5th – 6th September : Conference Topics

- Dual Track Security Conference
- Capture The Flag (CTF)
- Zone-H / HITB Hacking Challenge
- Lock Picking Village
- BZFlag Competition
- Charity Auction
- HITB Cinema (Freedom Downtime, Urchin)



Invited Speakers

- **Anthony Zboralski**
  Founder of HERT & PT Bellua
- **Carlos Lowie**
  Unit Mgr, investigations, Belgacom
- **Deviant Ollam, Eric Michaud & Q**
  Members Of The Open Organization of Lockpickers
- **Dino Covotsos**
  Founder & CEO, Telspace Systems
- **Frank Yuan Fan**
  Founder & CTO, DBAPPSecurity
- **Felix 'FX' Lindner**
  Security consultant, SABRE Labs
- **Jim Geovedi**
  HERT member & Security Consultant, PT Bellua
- **Dr. Jose Nazario**
  Senior Software Engineer, Arbor Networks
- **Shreeraj Shah**
  Director, Net-Square
- **Dr. Stefano Zanero**
  CTO, Secure Network, Milan
- **Raffael Marty**
  Manager, Strategic Application Solutions, ArcSight Inc.
- **Roberto Preatoni**
  Founder, Zone-H Defacement Mirror
- **The Grugq**
  Independent Network Security Researcher

The menace within

By David Beesley

Handheld USB devices have been a godsend to anyone who wants to take information from one PC to another, but their ease of use also has created a new type of security headache for companies.

The recent explosion in sales of devices such as USB sticks, iPods and PDAs mean they are a common sight in most offices.

Where's the harm in an iPod, you might ask. Surely the most offensive thing about an iPod is the often dodgy choice of music coming from it? When you consider that these tiny portable media devices can just as easily be used to remove confidential customer files, there is a clear menace behind the shiny chrome exterior.

So what steps should businesses take to protect themselves against the risks associated with such devices?

Keep your enemies close. Keep your workforce closer.

The biggest threat to the integrity of a company's IT security is not some sinister hacker trying to break into the corporate network, but employees and partners with easy access to business information.

With removable media devices such as MP3 players, digital cameras, and PDAs commonplace in companies, uncontrolled use of them carries a number of risks, from the simple nuisance factor of the network being used to store personal files and the risks associated with software theft, to the consequences of a deliberate attack on the network.

The storage device is also a simple way for malware to propagate within your network; a user can unwittingly infect the network with a virus that has been transferred from his home PC by such a device.

The right security strategy

It’s a worrying fact that around 80% of IT security incidents occur inside an organization, and yet an estimated 80% of security spend still goes outside on perimeter defenses such as firewalls, anti-virus, intrusions detection and content filtering.

Businesses need a formalized control mechanism in place in order to protect critical business systems and databases for data and IP theft.

If you decide to outlaw USB devices, good luck. This is a difficult proposition, and there's no foolproof method. Windows 2003 will block USB port access, but critically, will also stop USB keyboards, mice and other legitimate USB devices being used – a move that will not be popular with employees. Simply disabling USB ports is therefore not the answer, as it inevitably has an adverse effect on business productivity and flexibility

Striking the right balance

It’s important to have an Acceptable Usage Policy (AUP) in place, so that employees are aware of what they may and may not use in the workplace. However, relying on AUPs alone is insufficient – organizations need to back up any policy with robust enforcement capabilities.

A wholesale ban on portable media devices is not the answer. Certain employees across an organization will have a perfectly legitimate need to use removable media, be it a USB stick to transfer data or a PDA to synchronize diaries.

Not all employees will need such access, so a flexible solution is needed for permissible usage and blocking unauthorized connections.

David Beesley is managing director of IT security consultancy Network Defence (www.networkdefence.com), which he co-founded in 1996. David has been involved in the IT industry since 1985, responsible for the design and delivery of a number of large LANs and WANs over the past 15 years. David is recognized as a leading IT security expert in the UK and has over 12 years technical experience designing and implementing IT security solutions.

Subscribe to our YouTube channel: youtube.com/helpnetsecurity
Security videos

Stephen Northcutt on Security Certification and the SANS Top 20
http://www.net-security.org/article.php?id=1007

Stephen Northcutt, the CEO of the SANS Institute, provides us with an overview of SANS activities, the Internet Storm Center, the SANS Top 20 and the evolution of the IT security market in terms of the growing need for certification. This is a video that anyone wanting to get certified will be interested in.

Anomaly-Based Unsupervised Intrusion Detection
http://www.net-security.org/article.php?id=1013

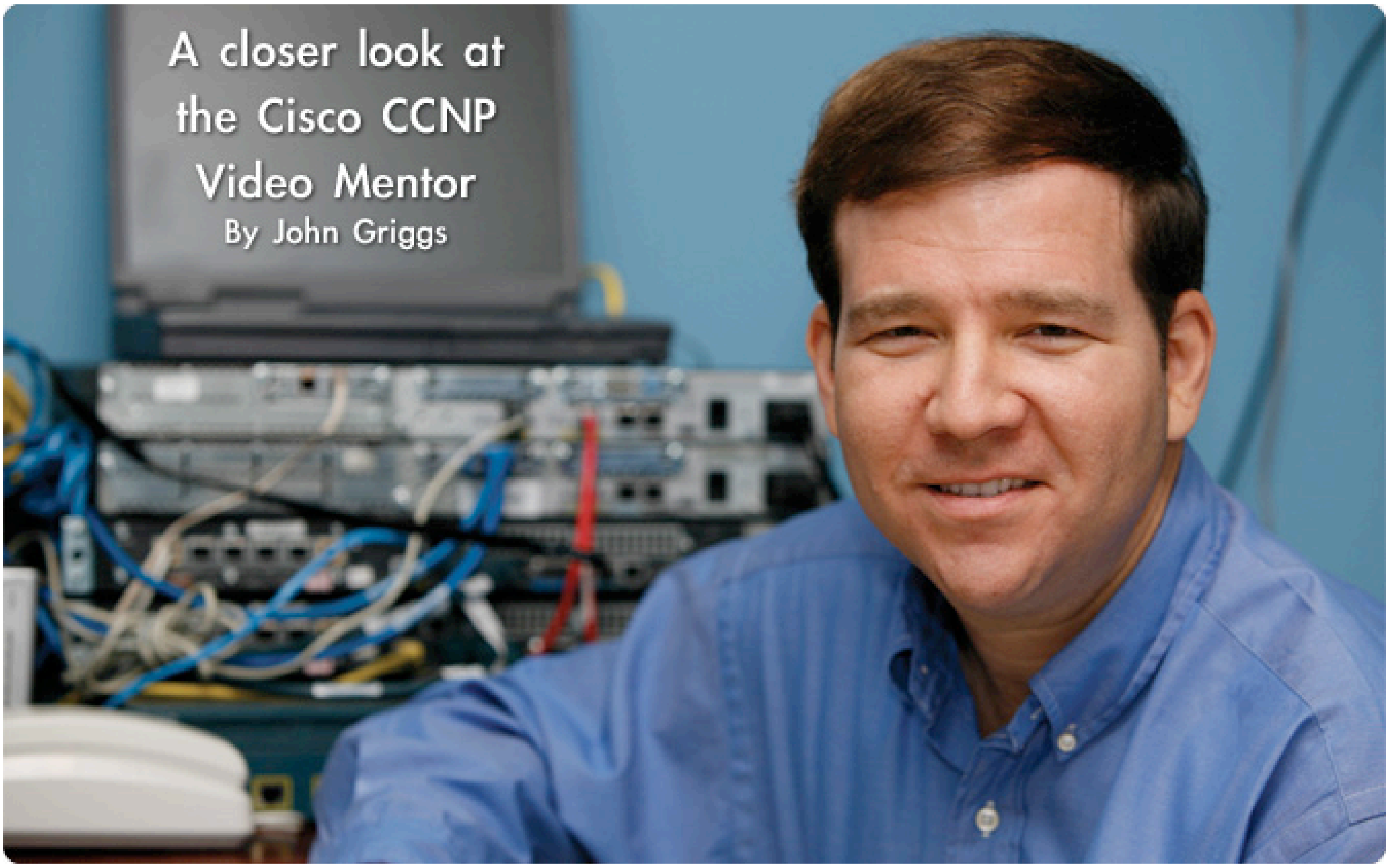
Stefano Zanero talks about anomaly-based unsupervised intrusion detection. In this video he provides an overview of his research into the subject by illustrating how he worked trying to find ways to detect intruders without relying on signatures.

Data Seepage: How to Give Attackers a Roadmap to Your Network
http://www.net-security.org/article.php?id=1015

In this video, Robert Graham and David Maynor, the CEO and CTO of Errata Security, talk about how the days of widespread internet attacks are long gone. What's more popular now are more directed or targeted attacks using a variety of different methods. This is where data seepage comes in. Unbeknownst to a lot of mobile professional's laptops, PDAs, even cell phones can be literally bleeding information about a company's internal network.

The Exploit Development Process
http://www.net-security.org/article.php?id=1020

Alexander Sotirov is a Vulnerability Researcher at Determina Inc. In this video, made at Black Hat Europe, he discusses on a general note how exploit writers develop exploits.



A closer look at the Cisco CCNP Video Mentor

By John Griggs

On a regular basis, Cisco Press releases a number of books that are of a great help for both Cisco practitioners, as well as those learning for one of the certifications that this networking leader offers. Over the past couple of years I had access to a vast collection of their titles and while the quality is almost always astounding, there was a clear need for this kind of a "video mentor". Reading through extremely technical topics, understanding diagrams, snooping through the command line interface commands was never this easy.

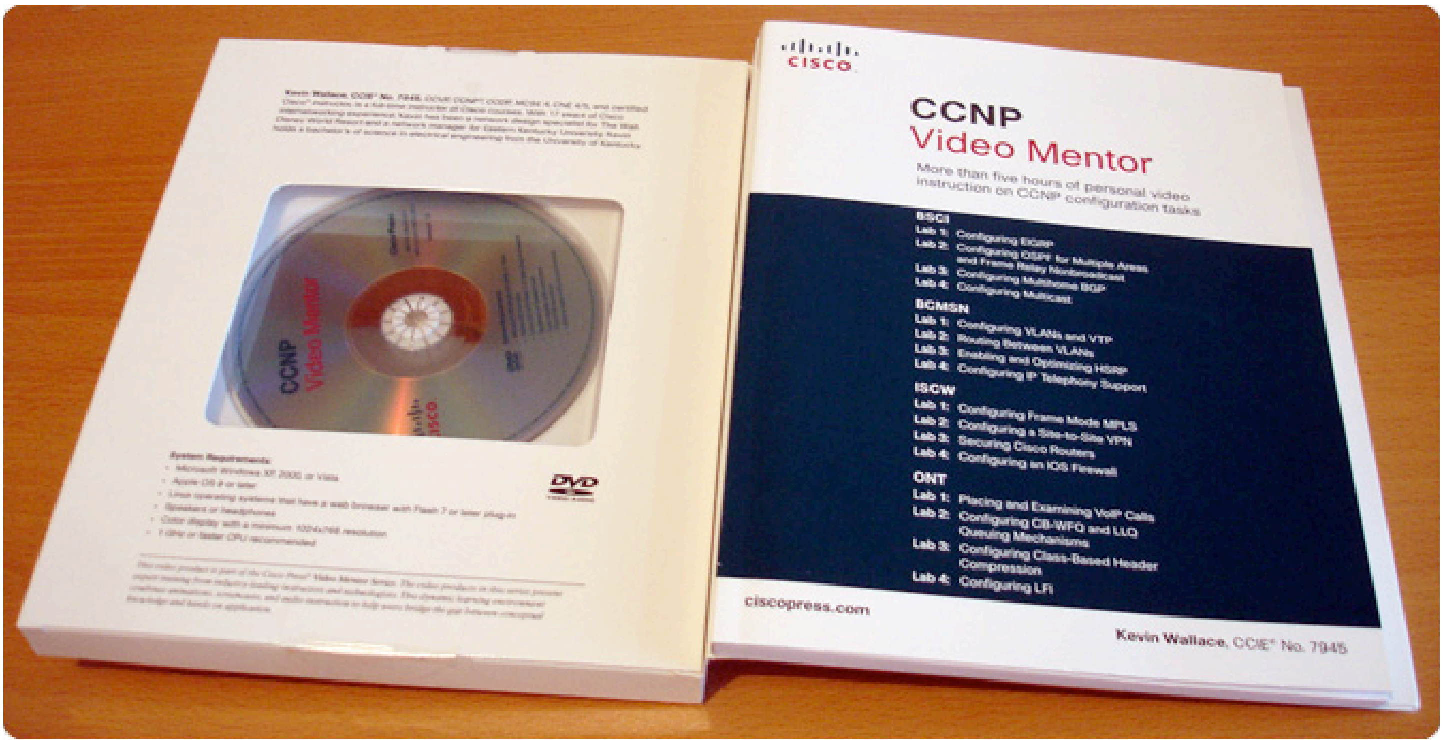
The author Kevin Wallace, CCIE No. 7945, is a full-time instructor of Cisco courses. With 17 years of Cisco internet-working experience, Kevin holds a bachelor of science degree in electrical engineering from the University of Kentucky.

The CCNP Video Mentor helps CCNP candidates prepare to pass the series of CCNP exams by supplying 16 instructional videos. Each video presents a unique lab scenario, with both visual references and audio explanations of what you should expect to happen in a particular lab.

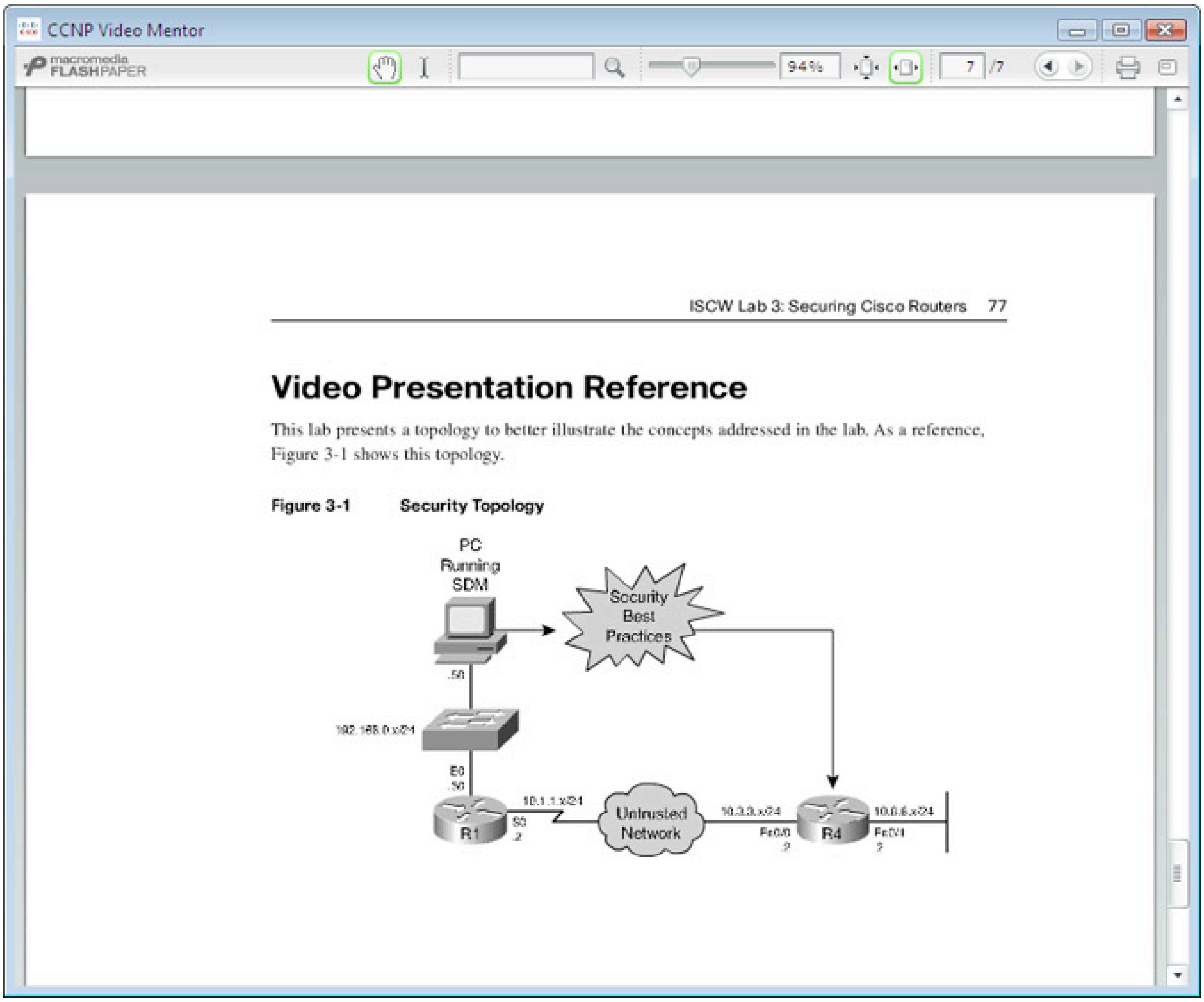
The videos also show how details of the command-line interface commands are used to implement the features described in each lab video, along with running commentary. The result is a set of videos that explain some of the most important CCNP topics from the BSCI, BCMSN, ISCW, and ONT courses, with thorough explanations from a trusted mentor.

As you can see from the images accompanying this preview, the packaging includes a DVD-ROM with the video course bundled together with a booklet covering all the labs contained in the video presentations.

The DVD-ROM sports a spartan but easy to use interface that starts of the video course with a personal introduction by the author. After this short video, you can chose one of the CCNP labs including "Building Scalable Cisco Internetworks", Building Cisco Multilayer Switched Networks", "Implementing Secure Converged Wide Area Networks" and "Optimizing Converged Cisco Networks".


cisco
CCNP
Video Mentor
More than five hours of personal video instruction on CCNP configuration tasks
BSCI
Lab 1: Configuring EIGRP
Lab 2: Configuring OSPF for Multiple Areas and Frame Relay Nonbroadcast
Lab 3: Configuring Multihome BGP
Lab 4: Configuring Multicast
BCMSN
Lab 1: Configuring VLANs and VTP
Lab 2: Routing Between VLANs
Lab 3: Enabling and Optimizing HSRP
Lab 4: Configuring IP Telephony Support
ISCW
Lab 1: Configuring Frame Mode MPLS
Lab 2: Configuring a Site-to-Site VPN
Lab 3: Securing Cisco Routers
Lab 4: Configuring an IOS Firewall
ONT
Lab 1: Placing and Examining VoIP Calls
Lab 2: Configuring CB-WFQ and LLQ Queuing Mechanisms
Lab 3: Configuring Class-Based Header Compression
Lab 4: Configuring LFI
ciscopress.com
Kevin Wallace, CCIE® No. 7945
DVD

All of the separate labs are also personally introduced by the author and afterwards split on four specific chapters. While all of the videos combine the author's audio with product screenshots, usage videos, diagrams and code, you can also complement your experience by viewing the accompanying PDF files to further understand the topology diagrams and the code.



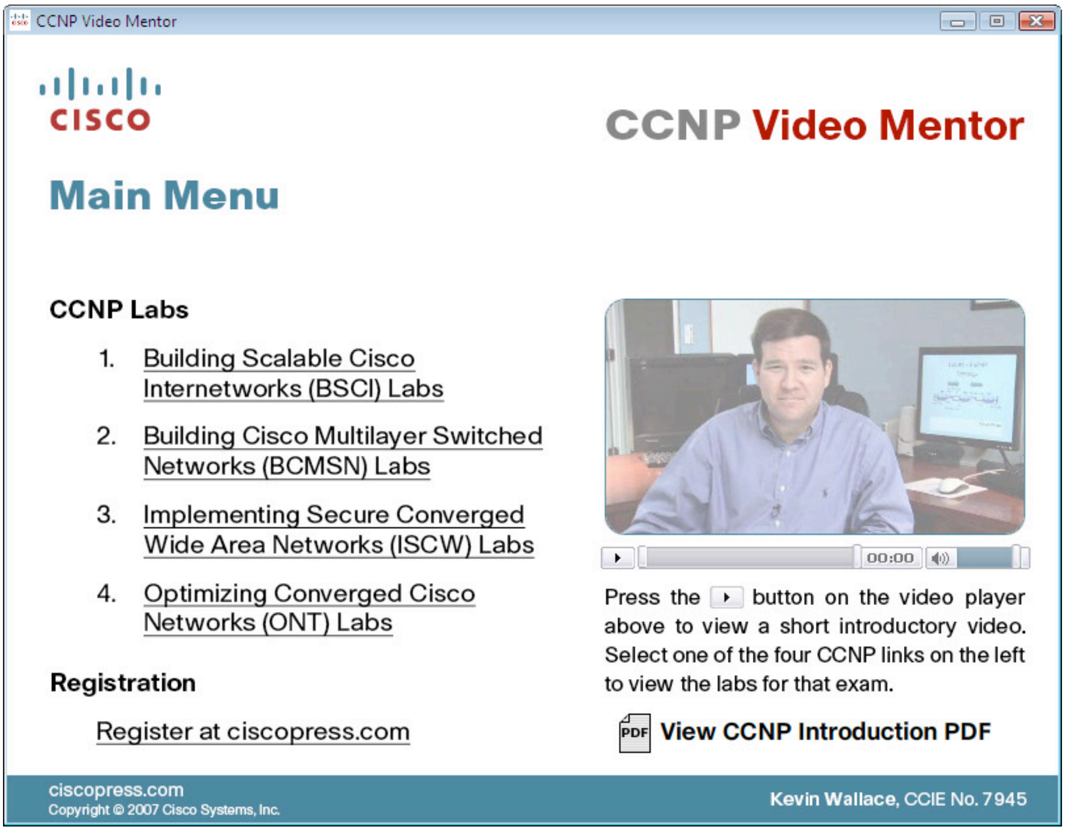
ISCW Lab 3: Securing Cisco Routers 77

Video Presentation Reference

This lab presents a topology to better illustrate the concepts addressed in the lab. As a reference, Figure 3-1 shows this topology.

Figure 3-1 Security Topology

The Cisco Press people really made this video mentor available for multiple platforms, as the DVD-ROM root contains auto start applications for both Microsoft Windows and Apple Mac OS X. There is also a HTML+Flash version of the whole class, which targets additional operating systems.



CCNP Video Mentor
cisco
CCNP Video Mentor
00:00
ciscopress.com
Copyright © 2007 Cisco Systems, Inc.
Kevin Wallace, CCIE No. 7945

Main Menu

CCNP Labs

1. Building Scalable Cisco Internetworks (BSCI) Labs
2. Building Cisco Multilayer Switched Networks (BCMSN) Labs
3. Implementing Secure Converged Wide Area Networks (ISCW) Labs
4. Optimizing Converged Cisco Networks (ONT) Labs

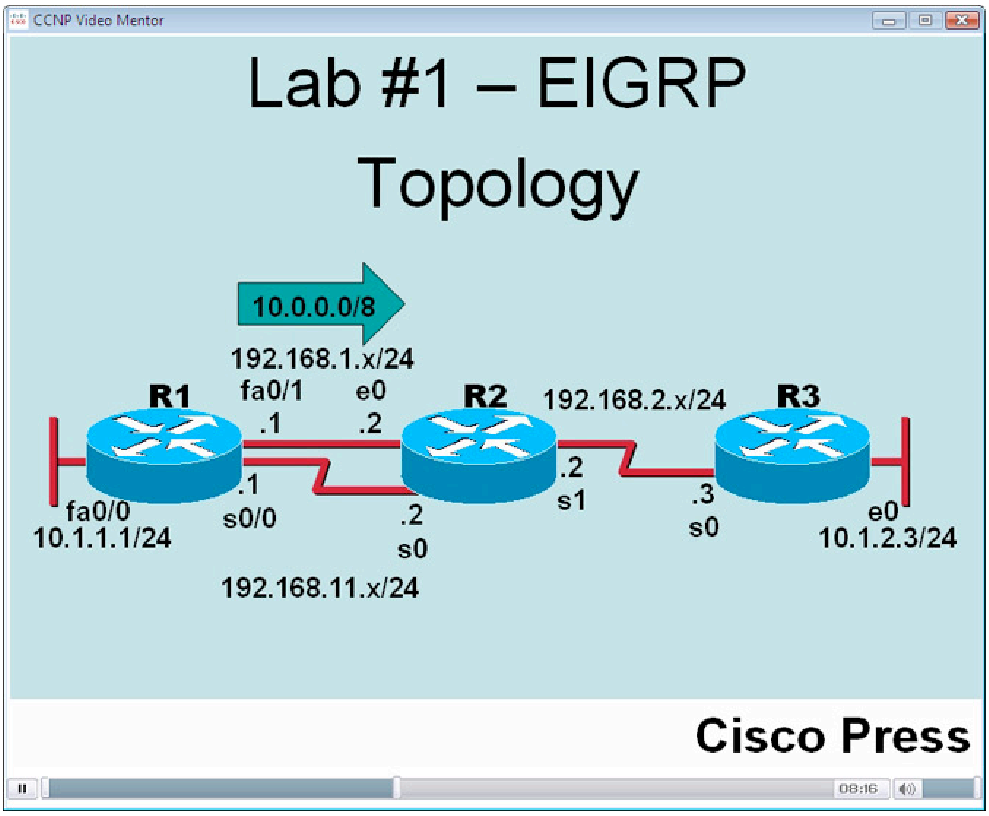
Registration

Register at ciscopress.com

Press the ▶ button on the video player above to view a short introductory video. Select one of the four CCNP links on the left to view the labs for that exam.

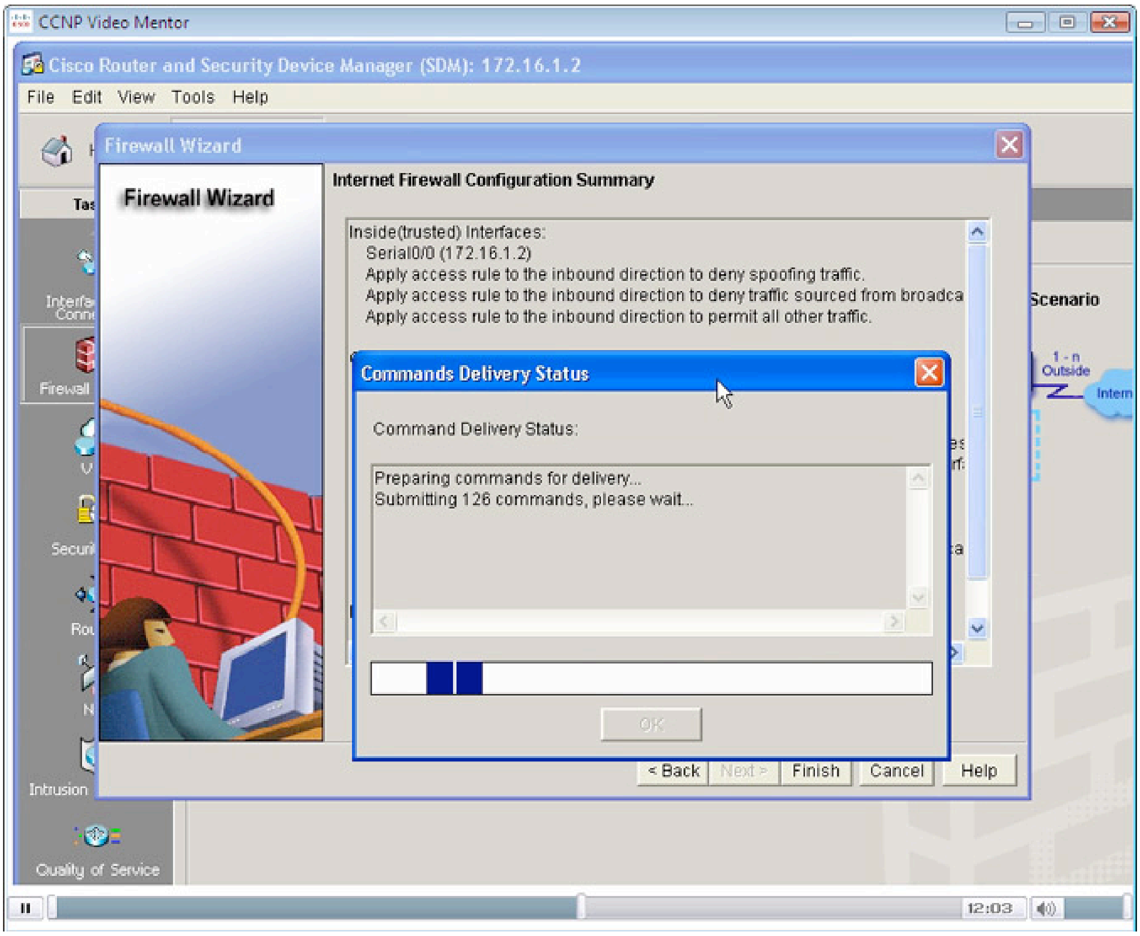
View CCNP Introduction PDF

Overall, "CCNP Video Mentor" will definitely present itself as the next big step for Cisco Press. The videos contain quite a lot of in-depth content provided in an easy to follow way.



All the videos takes the same basic approach:

1. The video begins with a description of its goals.
2. The lab scenario steps are listed, giving an outline of what you should expect to see and hear during the video.
3. The network topology used in the video is detailed.
4. Then, for each scenario step:
a. The video shows what you should expect from each part of the lab exercise.
b. The video shows the CLI details of how to configure and verify that the routers and switches are working properly.

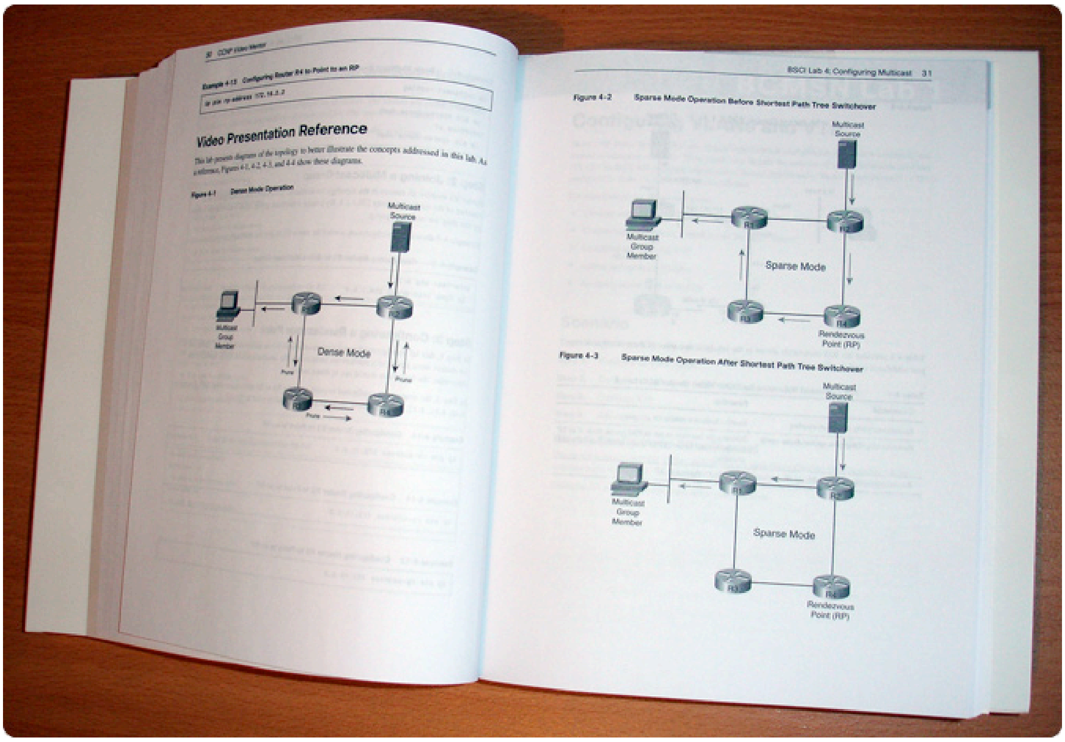


Internet Firewall Configuration Summary

Inside(trusted) Interfaces:
Serial0/0 (172.16.1.2)
Apply access rule to the inbound direction to deny spoofing traffic.
Apply access rule to the inbound direction to deny traffic sourced from broadca
Apply access rule to the inbound direction to permit all other traffic.

Command Delivery Status:

Preparing commands for delivery...
Submitting 126 commands, please wait...


Video Presentation Reference
Figure 4-1 Dense Mode Operation
Multicast Source
Multicast Group Member
Dense Mode
Figure 4-2 Sparse Mode Operation Before Shortest Path Tree Switchover
Multicast Source
Multicast Group Member
Sparse Mode
Rendezvous Point (RP)
Figure 4-3 Sparse Mode Operation After Shortest Path Tree Switchover
Multicast Source
Multicast Group Member
Sparse Mode
Rendezvous Point (RP)

Network Access Control

by Naveen Sharma

According to Aberdeen Group's "Endpoint Security Strategies Part-1" benchmark report published in November 2006 "Only 22% of the respondents agree that they had visibility for the end point compliance to the security policy, 80% had no idea of the end point compliance". These findings make the situation look pretty dire, and urgent action is demanded of those belonging to 80% in the unprotected category. The new technology on the block is Network Access Control or simply NAC (Cisco's NAC offering is called Network Admission Control). NAC can help in determining the end point security compliance status and providing for the remediation of these end points which fail compliance checks.

The three cardinal questions for security compliance, which every network administrator and owner endeavor to answer are:

1. How do I stop unauthorized users and endpoints from accessing resources on my network, whether through wired or wireless means?

2. How do I validate the user's and endpoint's health status? For example: assess the level of operating system patches installed, the status of the anti-virus application and its currency, and other malware detection engines and definitions.

3. How do I remediate the endpoints and users if they fail the above, and present a layered "defense in depth" with security technologies in a cooperative environment?

Often these questions remain unanswered, and the results are visible in the news and reports, as evident from analysis by Aberdeen Group. NAC or the end point security solution can provide the answer to all the above questions - and more - if designed and configured properly. This article will provide a clear overview of the Network Access Control or End point security technologies. I'll present the NAC architecture with the details of major components and their functionality, along with considerations in implementation in real production environments. You'll get a clear view of the present day NAC techniques in the wild from major vendors, which will assist them in arriving at an optimal NAC based solution for their own environment.

Vendors have promoted NAC solutions leveraging their own product offerings. For example Cisco's NAC uses the Cisco PIX firewall, ASA Appliances, Routers and Switches to perform NAC functions. On the other hand Microsoft, being the dominant provider of operating systems, has offered NAC (by the name of NAP, or Network Access Protection) built on the product line offerings such as Windows server, Windows XP and recently Microsoft Vista.

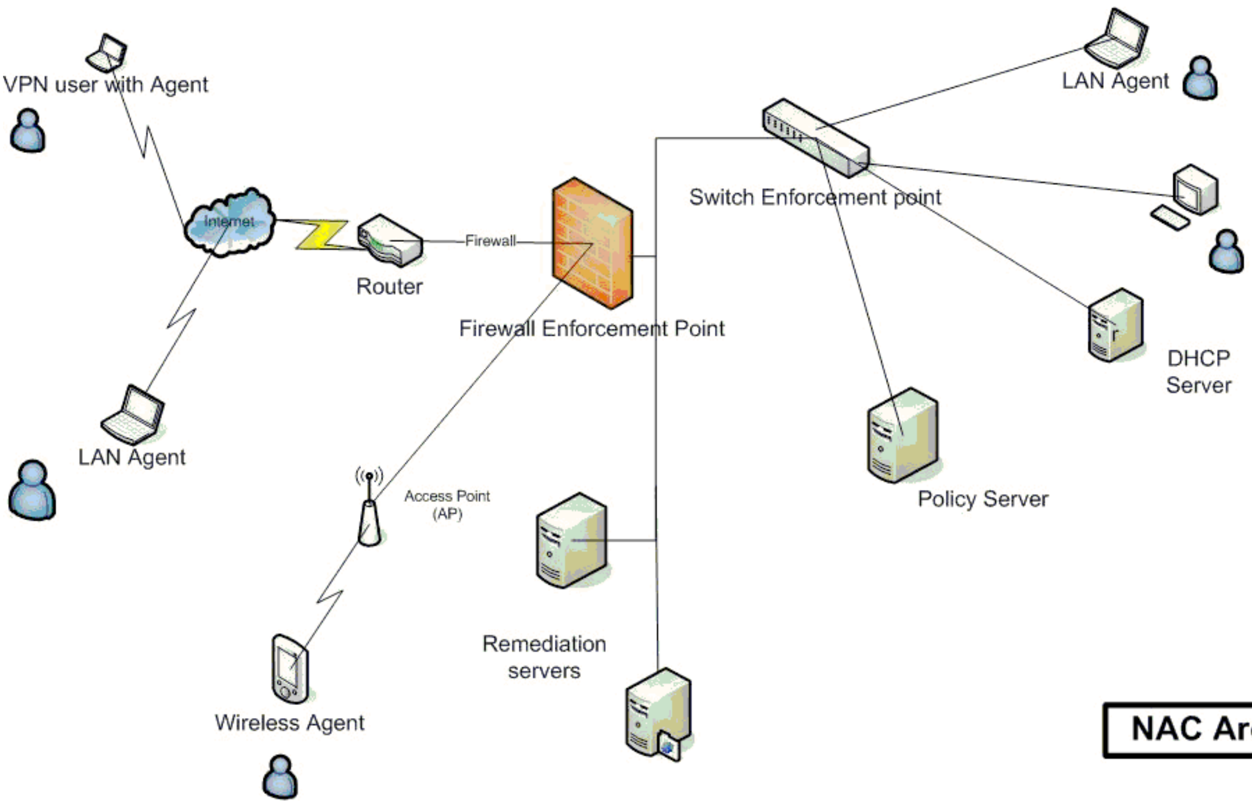
I'll use the terms NAC and endpoint security interchangeably for your ease.

NAC solutions provide the following:

1. Determines the Security posture of clients.
2. Grants access to various parts of the network, depending upon the outcome of first step.
3. Remediate compliance failures, and distributes policy to endpoints.

For example, if a policy says to deny access to endpoints whose patch level is older than 30 days, then NAC will restrict the access of those clients which are non compliant for this policy, and optionally a remediation process will be invoked to make that client compliant by downloading and installing required patches.

The three keywords in the NAC process are: Identify, Assess and Remediate.



NAC Architecture

The figure above shows a high level NAC architecture where the end users access enterprise resources by wireless, VPN and LAN. We have the option of enforcing the policies at the firewall, or at other access device such as a Layer2/3 switch or DHCP server.

The fundamental components of a NAC solution are:

1. Endpoints
2. Enforcement points
3. Policy and remediation services

The vendor offerings may comprise of a combination of the above components of NAC. Understanding of these components will allow the reader to differentiate vendor offering from one another in a pragmatic manner.

Endpoints

First, there must be a mechanism to determine the security posture of the endpoint machine before taking any decision for identity and access management. The endpoint assessment technologies currently available include:

1. Agent-less: Nothing is downloaded or installed on the endpoint host.
2. Agent: An application is pre-installed or downloaded at the first connection.
3. ActiveX or browser plug-in: This is downloaded to the endpoint when connection is attempted.
4. Scanner: performs an IP based vulnerability scan to determine the installed patches, services etc on the endpoint.

The agent-less approach uses an end point's administrative account to connect (via Windows RPC) to central user management systems for all the end points. The administrative overhead is considerable, adding to the cost of this approach. In the agent base approach an agent application is pre-installed or NAC prompts for the installation of agent at the first logon of the user to the network. Agents not only assist in determining the posture of the endpoint, but can also do access control and reporting to the NAC server on the end user machine, with the built-in firewall. One of the disadvantages of the agent-based approach is that it works on the assumption that the agent will be pre-installed or will be installed at the first attempt of access to the network, which can be potential source of risk.

In the scanning method the NAC scans the end machine and, based on the scan result, the posture is determined for the next step of identity and access to network resources. This approach may or may not test the endpoint's patch levels, anti-virus definition files status, or file/registry value. Another issue is that of the time required to scan an endpoint, which may be exacerbated at peak endpoint activity due to simultaneous endpoint scans. With the ActiveX or browser plug-in technology, the plug-in is downloaded on the end point for posture determination and to report the compliance status of the end point. The advantages of this are comparatively less memory and CPU overhead.

Enforcement points

Enforcement is the pivotal element of the whole NAC architecture, as all the access decisions are implemented here. NAC offerings from vendors tend to favor their own product lines: for example some traditional network companies implement access control on their layer2/3 switch (which may be a difficulty for users who have different brand switches).

Here are the possible enforcement options currently available in the market:

1. Inline: includes firewalls, layer 2/3 switches and purpose built appliances
2. 802.1X: IEEE standard for port based access control
3. DHCP: IP assignment restrictions

Inline based enforcement options include firewalls, layer2/3 switches or purpose built dedicated inline appliances. Some NAC solutions offer support for other vendors firewalls and switches for enforcement, which is welcome news for users who have a multi-vendor networking infrastructure.

Some considerations for inline devices are:

1. Bandwidth requirements: must support the traffic and provide future scalability, or else the inline device will become the choke point.
2. High availability: Some sort of redundancy is expected, in case the primary inline device fails (and the time associated with fail over).
3. The degree of separation provided between the endpoints and the business critical systems inside the network.
4. Reporting from the enforcement device: for both compliant and non complaint endpoints.

802.1X or port based network access control is a protocol based on Extensible Access Protocol (EAP), an IEEE standard. New generation layer 2/3 switches offer the possibility of segregating specific IP's onto a separate VLAN, and imposing various access control lists on VLAN traffic. 802.1X has three major components: the Supplicant, which is the person or endpoint attempting access, the Authenticator, which is the device that the Supplicant is attempting to connect to, and the Authentication server, which holds credentials.

The process of gaining access is:
• The end user machine connects to the Authenticator, which can be a WLAN access point or a LAN switch.
• The Authenticator sets the port to 'unauthorized', which will only permit 802.1X traffic, and requests authentication data from the endpoint. The endpoint returns it's authentication data to the Authenticator.
• The Authenticator knows the Authentication server, and forward to the request to authentication server (typically a RADIUS server). The radius server returns a pass/fail.
• Once the authentication is successful, the Authenticator opens the port for the supplicant to join the network.

DHCP based access restriction works on the premise that the endpoint user will play by the rules of the game. Purely DHCP based restriction may not prove to be effective as it is possible to bypass. DHCP assigns quarantined or unknown end points to an IP address that is restricted by ACL's on switches/routers.

Some of the considerations for the DHCP method of enforcement are:
1. Is this secure enough for the environment? Requires a risk analysis.
2. Is the existing environment's architecture suitable for this enforcement? Possibilities here include placing a NAC server inline with DHCP.
3. Does it require a significant additional outlay for the equipment?

Policy and remediation service

Policy and remediation services are the last part of NAC picture, though the endpoint assessment is done against the policy set by administrator at the very start of NAC process. Once the assessment is carried out on the endpoint, and matched against the policy for compliance, the decision to restrict or allow the endpoint is taken. If the endpoint is restricted due to a failure to comply with one or more policies, the endpoint is quarantined.

The next logical step is to seek to remediate the endpoint. The task of a remediation service is to make the endpoint compliant to the policy, thus restoring the access to join the network for services in a healthy state.

The remediation process may be single or consist of multiple steps. For example, if an endpoint does not have current anti-virus definition and lacks critical Microsoft patches, then the remediation process directs the endpoint to the current anti-virus definition and required Microsoft patches.

The endpoint security posture should also be regularly re-tested, so as to remain proactive. The results of this continuous monitoring of the endpoint posture and status of compliance must be reported promptly. Another point to consider here is the execution and delivery of policy, either to the endpoint or enforcement point. The frequency and protocol for delivery are equally important in this whole NAC framework. Needless to say the policy has to be regularly backed-up, and the facility to restore from backed-up policies should be regularly tested.

Some considerations for the remediation and policy service are:
1. Placement and capacity of remediation servers, for example the patch distribution mechanism, etc.
2. Will remediation be self-service, or will be performed by help desk?
3. How does the remediation server obtain the third-party details such as the anti-virus and other malware definition currency, MS patches levels, and more.
4. What mechanism is in place for communication between the remediation servers and the policy server?

Conclusion

NAC is a rapidly evolving field and holds immense promise for the future of endpoint security. NAC can deliver lower costs and tools for the compliance checking and managing the security posture of endpoints. More mature NAC products can be expected in the future with the entry of innovative players into the market.

Naveen Sharma, CISSP, is working in the Information Security space with a leading IT service provider in Australia. He has previously worked in networking and telecommunication industry for more than 8 years. He is presently pursuing Masters in Systems Security from Macquarie University in Sydney. His other passions include Linux and table tennis.