(IN)SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 21 - June 2009

WINDOWS 7 SECURITY

WEB 2.0 EMERGING THREATS

IRONKEY REVIEW

MALICIOUS PDF

CERTIFICATION

+ MORE!

Reports

RSA CONFERENCE 2009

BLACK HAT EUROPE 2009

INFOSECURITY EUROPE 2009

TABLE OF CONTENTS

Welcome to (IN)SECURE 21
the digital security magazine

The magazine you're reading was put together during an extremely busy few months that saw us pile up frequent flier miles on the way to several conferences. You can read about some of them in the pages that follow, specifically RSA Conference 2009, Infosecurity Europe 2009 and Black Hat Europe 2009.

This issue brings forward many hot topics from respected security professionals located all over the world. There's an in-depth review of IronKey, and to round it all up, there are three interviews that you'll surely find stimulating.

This edition of (IN)SECURE should keep you busy during the summer, but keep in mind that we're coming back in September! Articles are already piling in so get in touch if you have something to share.

Mirko Zorz
Editor in Chief

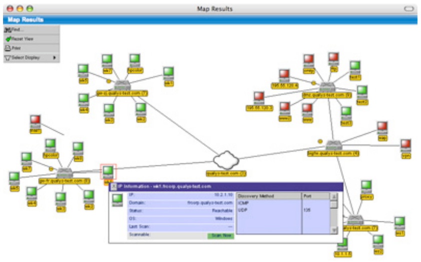
Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts
Feedback and contributions: Mirko Zorz, Editor in Chief - editor@insecuremag.com
Marketing: Berislav Kucan, Director of Marketing - marketing@insecuremag.com

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

Corporate security news

Qualys adds Web application scanning to QualysGuard



Qualys added QualysGuard Web Application Scanning (WAS) 1.0 to the QualysGuard Security and Compliance Software-as-a-Service (SaaS) Suite, the company's flagship solution for IT security risk and compliance management. Delivered through a SaaS model, QualysGuard WAS delivers automated crawling and testing for custom Web applications to identify most common vulnerabilities such as those in the OWASP Top 10 and WASC Threat Classification, including SQL injection and cross-site scripting. QualysGuard WAS scales to scan any number of Web applications, internal or external in production or development environments. (www.qualys.com)

Integrated protection for smartphones: Kaspersky Mobile Security 8.0

The new version of Kaspersky Mobile Security provides protection against the wide range of threats facing smartphone users. For instance, SMS Find can locate the exact whereabouts of a lost smartphone. After sending an SMS with a password to the lost device, the user receives a link to Google Maps containing its exact coordinates.

The Anti-theft module of Kaspersky Mobile Security 8.0 makes it possible for the owner of a lost or stolen smartphone to remotely block access to or completely wipe the memory of the device by simply sending a codeword via SMS to his/her number. (www.kaspersky.com)

NEW VERSION
Kaspersky
Mobile Security
World-class security for smartphones:
at home, at work, on the move
Kaspersky Mobile Security
KASPERSKY

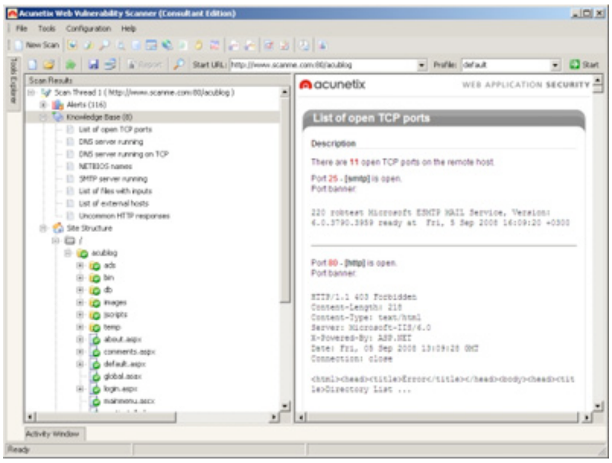
SSH solution for real-time inspection and audit of encrypted traffic

SSH Communications Security announced SSH Tectia Guardian, a new technology solution that enables real-time session and file transfer monitoring with IDS or DLP integration capabilities, as well as replay of sessions for post-session auditing of encrypted traffic.

This unique security solution enables both real-time inspection, and full replay of SSH, SFTP, Telnet, and RDP traffic and sessions to meet compliance, governance, auditing, and forensics requirements in enterprises and government entities. (www.ssh.com)

Acunetix Web Vulnerability Scanner 6.5 now available

Acunetix announced new "file upload forms vulnerability checks" in version 6.5 of the Acunetix Web Vulnerability Scanner (WVS). Other key features in the new versions are the new Login Sequence Recorder, Session Auto Recognition functionality and improved cookie and session handling. With the new Login Sequence Recorder and Session Auto Recognition module, WVS can automatically login to a wider range of authentication forms using different authentication mechanisms, while with the improved cookie and session handling. WVS is now able to scan a broader range of dynamic web applications effectively. (www.acunetix.com)



List of open TCP ports

Description

There are 11 open TCP ports on the remote host.

Port 25 - [smtp] is open.
Port banner:

```
220 robtest Microsoft ESMTP MAIL Service, Version:
6.0.3790.3959 ready at  Fri, 5 Sep 2008 16:09:20 +0300
```

Port 80 - [http] is open.
Port banner:

```
HTTP/1.1 403 Forbidden
Content-Length: 218
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Fri, 05 Sep 2008 13:09:20 GMT
Connection: close

<html><head><title>Error</title></head><body><head><tit
le>Directory List ...
```

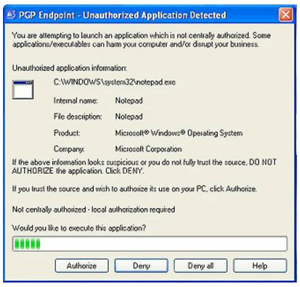
Wi-Fi kit for disaster response and temporary events

Xirrus announced a portable, pre-packaged kit designed for the rapid and simple deployment of Wi-Fi networks in temporary applications. Unlike other Wi-Fi networking solutions which require many different components, the Xirrus Wi-Fi Array integrates everything needed to deploy a large coverage, high density Wi-Fi network supporting up to hundreds of clients into a single device.

This makes the Wi-Fi Array the ideal fit for portable applications such as disaster response command posts; high-density events such as conferences and expositions; and short-term events such as festivals, markets, and fairs. (www.xirrus.com)

PGP launches Endpoint Application Control

PGP has announced PGP Endpoint Application Control, a product that blocks malicious and unauthorized software, including applications, scripts and macros, from executing on a user's system by automatically enforcing policies using whitelisting technology that explicitly allows only trusted and authorized software applications. By leveraging PGP Endpoint Application Control as another layer of data defense, customers can ensure business continuity with always-on protection and not have to worry about malicious software entering their networks. (www.pgp.com)



You are attempting to launch an application which is not centrally authorized. Some applications/executables can harm your computer and/or disrupt your business.

Unauthorized application information:

C:\WINDOWS\system32\notepad.exe

Internal name:	Notepad
File description:	Notepad
Product:	Microsoft® Windows® Operating System
Company:	Microsoft Corporation

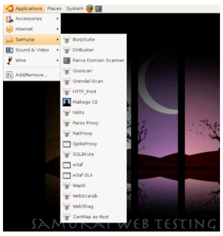
If the above information looks suspicious or you do not fully trust the source, DO NOT AUTHORIZE the application. Click DENY.

If you trust the source and wish to authorize its use on your PC, click Authorize.

Not centrally authorized - local authorization required

Would you like to execute this application?

Web penetration testing live CD



The Samurai Web Testing Framework is a live Linux environment that has been pre-configured to function as a web pen-testing environment.

The CD contains the best of the open source and free tools that focus on testing and attacking websites. The developers included the tools they use in their own security practice. (sourceforge.net/projects/samurai)

RIM launches BlackBerry Enterprise Server 5.0

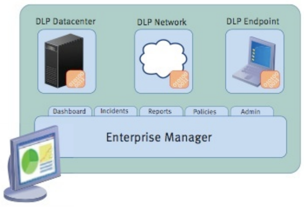
RIM launched BlackBerry Enterprise Server 5.0 which supports advanced IT administration features and smartphone controls that help improve the productivity of mobile workers and meet the demands of large-scale, mission critical enterprise deployments. It enables a secure, centrally managed link between BlackBerry smartphones and enterprise systems, applications, corporate phone environments and wireless networks. (www.blackberry.com)

New StoneGate FW-1030 appliance with firewall capabilities

Stonesoft introduced the StoneGate FW-1030 appliance with firewall capabilities. It provides data security for small enterprises and remote offices combined with StoneGate's built-in high availability features that guarantee always-on connectivity. With perimeter protection and internal network segmenting capabilities, the FW-1030 prevents computer worms from spreading and contaminating an organization's internal network. It provides built-in solid-state disk technologies that emphasize reliability and durability while using 50% less power compared to similar appliances. (www.stonesoft.com)

New release of RSA Data Loss Prevention Suite

RSA announced enhancements to the RSA Data Loss Prevention Suite, its suite of data security products that are engineered to discover, monitor and protect sensitive data from loss, leakage or misuse whether in a datacenter, on the network, or out at the endpoints. The allows organizations to secure sensitive content in a way that saves time and streamlines processes for data security personnel. Sensitive data at rest can now be moved or quarantined automatically and users can apply self-remediation for emails quarantined due to violations. (www.rsa.com)



New services to secure Web applications from TippingPoint

TippingPoint announced its Web Application Digital Vaccine (Web App DV) services, a two-part approach to address the security threat posed by Web applications. This set of services enables users to maximize their security investments, while reducing the risk of attacks through custom-built Web applications. (www.tippingpoint.com)

Malicious PDF: Get owned without opening

by Didier Stevens

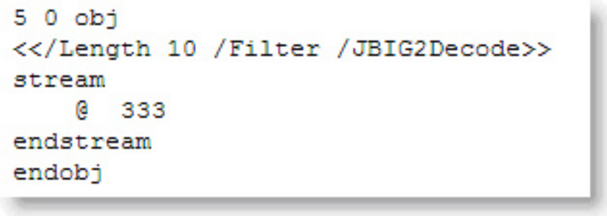
Malware researchers are very careful with the samples they analyze. They know several types of malicious files can execute their payload even without being opened. Up until now, the consensus was that malicious PDF documents were harmless as long as you didn't open them with a vulnerable version of a PDF reader, usually Adobe Reader. My research shows that this is no longer the case. Under the right circumstances, a malicious PDF document can trigger a vulnerability in Adobe Reader without getting opened.

The JBIG2 vulnerability

In March, Adobe released a new version of Adobe Reader to fix several bugs. One of the fixes is for the notorious JBIG2 vulnerability.

The PDF format supports several image compression algorithms; you're probably familiar with JPEG. JBIG2 is another compression algorithm. Adobe's implementation of the JBIG2 decompression algorithms contained bugs that could lead to arbitrary code execution: i.e, vulnerabilities. Malware authors started exploiting this JBIG2Decode vulnerability before Adobe was able to release a fix. They managed to create PDF documents that cause the buggy JBIG2 decompression code to malfunction in such a way that shellcode is executed, which ultimately downloads a Trojan.

I will use the following malformed JBIG2 data to trigger an error in the vulnerable JBIG2 decompression algorithm in Adobe Reader.



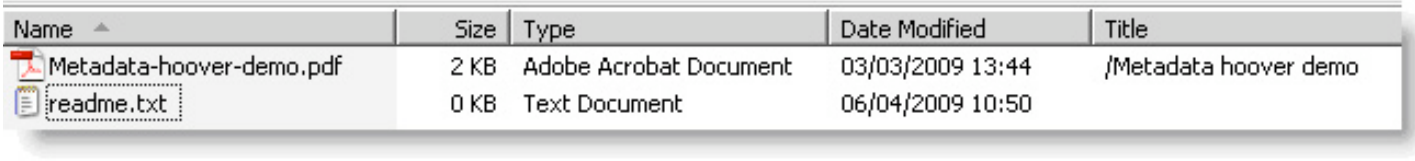
```
5 0 obj
<</Length 10 /Filter /JBIG2Decode>>
stream
    @  333
endstream
endobj
```

Some user interaction required

How is it possible to exploit this vulnerability in a PDF document without having the user opening this document? The answer lies in Windows Explorer Shell Extensions.

Have you noticed that when you install a program like WinZip, an entry is added to the right-click menu to help you compress and extract files? This is done with a special program (a shell extension) installed by the WinZip setup program.

When you install Adobe Reader, a Column Handler Shell Extension is installed. A column handler is a special program (a COM object) that will provide Windows Explorer with additional data to display (in extra columns) for the file types the column handler supports. The PDF column handler adds a few extra columns, like the Title. When a PDF document is listed in a Windows Explorer window, the PDF column handler shell extension will be called by Windows Explorer when it needs the additional column info. The PDF column handler will read the PDF document to extract the necessary info, like the Title, Author, etc.

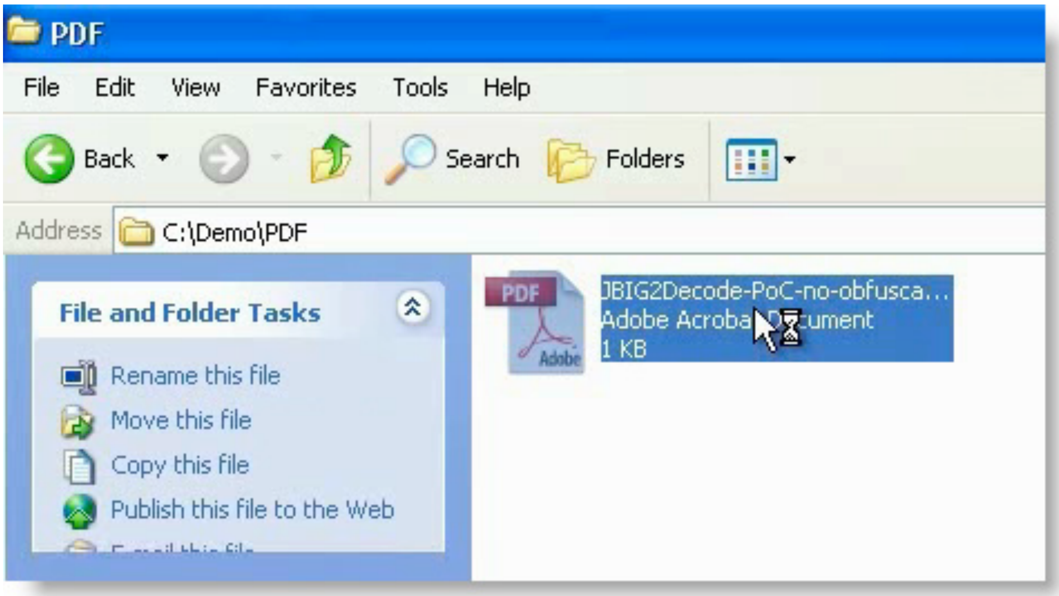


Name	Size	Type	Date Modified	Title
Metadata-hoover-demo.pdf	2 KB	Adobe Acrobat Document	03/03/2009 13:44	/Metadata hoover demo
readme.txt	0 KB	Text Document	06/04/2009 10:50	

This explains how the PDF vulnerability can be exploited without you opening the PDF document. Under the right circumstances, a Windows Explorer Shell Extension will read the PDF document to provide extra information, and in doing so, it will execute the buggy code and trigger the vulnerability. Just like it would when you would explicitly open the document. In fact, we could say that the document is opened implicitly, because of your actions with Windows Explorer.

You can find a movie on my website where I demonstrate three circumstances under which a PDF Shell Extension will act and thereby trigger the vulnerability. One important detail you have to know: when the exception occurs in the Adobe Acrobat code, it is trapped by Windows Explorer without any alert. That's why in the demos, I attached a debugger (ODBG) to Windows Explorer to intercept and visualize this exception. So each time the vulnerability triggers, the view switches to the debugger to display the exception.

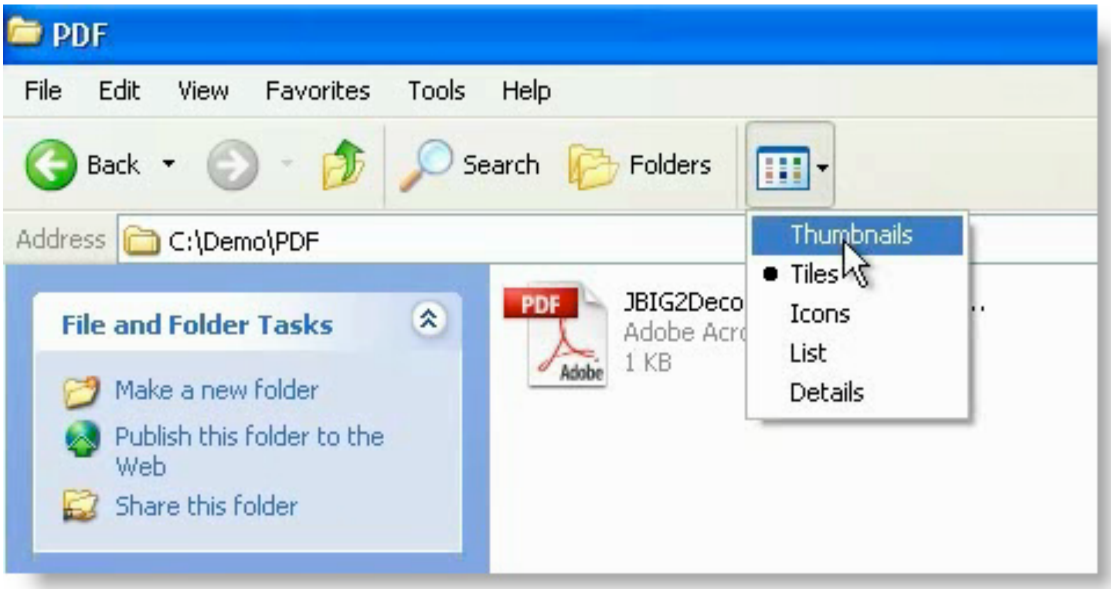
In the first demo, I just select the PDF document with one click. This is enough to exploit the vulnerability, because the PDF document is implicitly read to gather extra information.



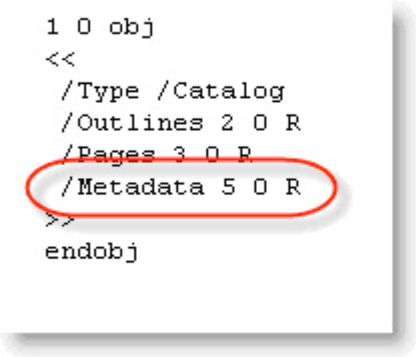
Address C:\Demo\PDF

JBIG2Decode-PoC-no-obfusca...
Adobe Acrobat Document
1 KB

In the second demo, I change the view to Thumbnails view. In a thumbnail view, the first page of a PDF document is rendered to be displayed in a thumbnail. Rendering the first page implies reading the PDF document, and hence triggering the vulnerability.

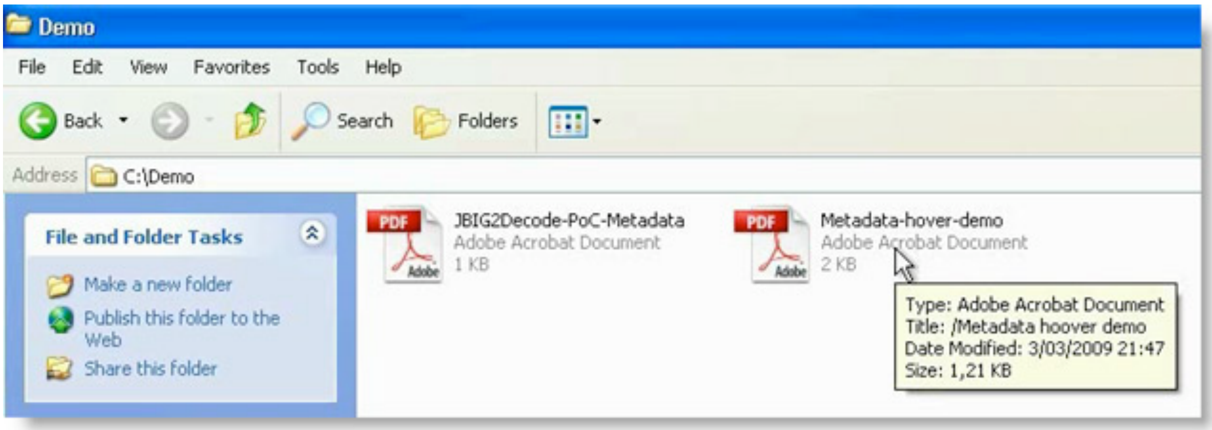


In the third demo, I use a special PDF document with the malformed stream object in the metadata.



```
1 0 obj
<<
 /Type /Catalog
 /Outlines 2 0 R
 /Pages 3 0 R
 /Metadata 5 0 R
>>
endobj
```

When I hover with the mouse cursor over the document (I don't click), a tooltip will appear with the file properties and metadata. But with my specially crafted PDF document, the vulnerability is triggered because the metadata is read to display the tooltip.



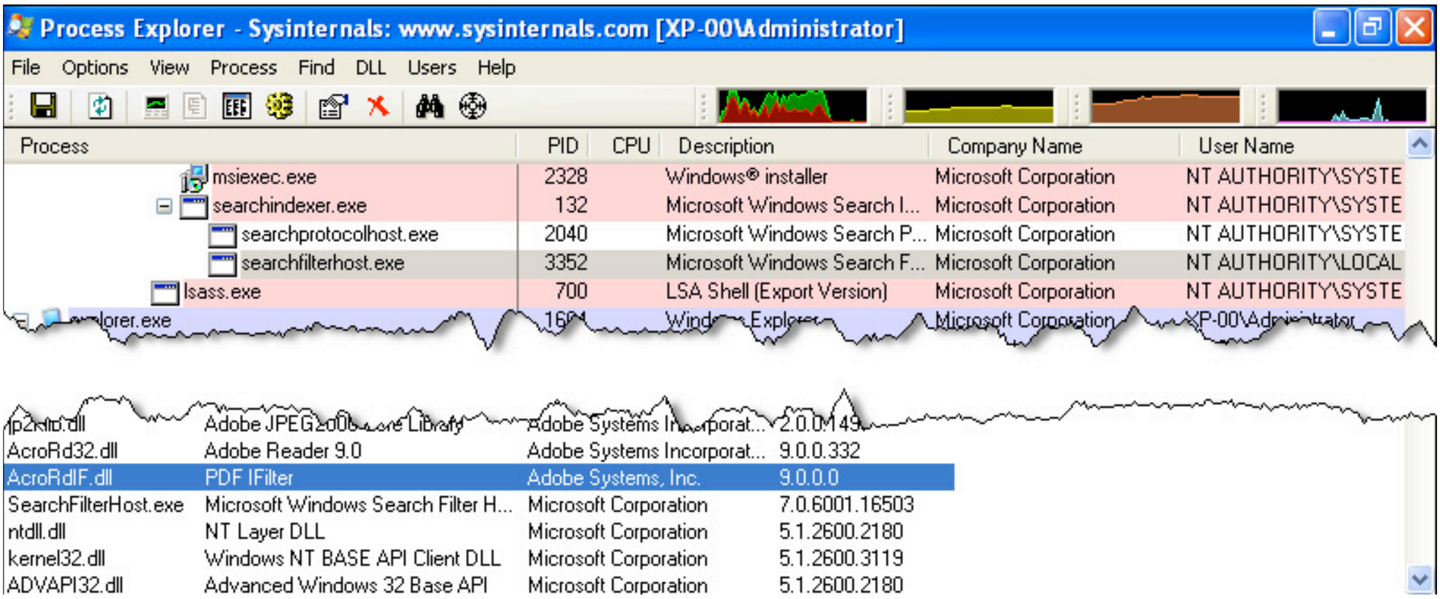
Type: Adobe Acrobat Document
Title: /Metadata hoover demo
Date Modified: 3/03/2009 21:47
Size: 1,21 KB

No user interaction required

There are also circumstances that require no user interaction at all to trigger the /JBIG2Decode bug. The bug occurs in a process running with Local System rights!

On a Windows XP SP2 machine with Windows Indexing Services started and Adobe Reader 9.0 installed, there is absolutely no user interaction required to trigger the /JBIG2Decode vulnerability. When the PoC PDF file is on the disk, it will be indexed by Windows Indexing Services and the buggy /JBIG2Decode code will be executed.

When Adobe Reader 9.0 is installed, it also installs an IFilter (AcroRdIF.dll). This COM object extends the Windows Indexing Service with the capability to read and index PDF documents. When the Windows Indexing Service encounters a PDF file, it will index it. The content indexing daemon (cidaemon.exe) calls the Acrobat IFilter (AcroRdIF.dll) which loads the Acrobat PDF parser (AcroRD32.dll). If the PDF document contains a malformed /JBIG2Decode stream object, it will result in an access violation in the instruction at 0×01A7D89A.


Process Explorer - Sysinternals: www.sysinternals.com [XP-00\Administrator]
File
Options
View
Process
Find
DLL
Users
Help

Process	PID	CPU	Description	Company Name	User Name
msiexec.exe	2328		Windows® installer	Microsoft Corporation	NT AUTHORITY\SYSTE
searchindexer.exe	132		Microsoft Windows Search I...	Microsoft Corporation	NT AUTHORITY\SYSTE
searchprotocolhost.exe	2040		Microsoft Windows Search P...	Microsoft Corporation	NT AUTHORITY\SYSTE
searchfilterhost.exe	3352		Microsoft Windows Search F...	Microsoft Corporation	NT AUTHORITY\LOCAL
lsass.exe	700		LSA Shell (Export Version)	Microsoft Corporation	NT AUTHORITY\SYSTE
lorer.exe	16		Wind Explor	Microsoft Corporation	XP-00\Administrator

jp2klib.dll	Adobe JPEG2000 Core Library	Adobe Systems Incorporat...	2.0.0.149
AcroRd32.dll	Adobe Reader 9.0	Adobe Systems Incorporat...	9.0.0.332
AcroRdIF.dll	PDF IFilter	Adobe Systems, Inc.	9.0.0.0
SearchFilterHost.exe	Microsoft Windows Search Filter H...	Microsoft Corporation	7.0.6001.16503
ntdll.dll	NT Layer DLL	Microsoft Corporation	5.1.2600.2180
kernel32.dll	Windows NT BASE API Client DLL	Microsoft Corporation	5.1.2600.3119
ADVAPI32.dll	Advanced Windows 32 Base API	Microsoft Corporation	5.1.2600.2180

In other words, if you've a malicious PDF document on a machine with Windows Indexing Services, it can infect your machine. And you don't need a user to open or select the PDF document.

The good news is that Windows Indexing Services is not started on a default Windows XP SP2 install. But after you've executed a search as local admin, you'll be asked if you want "to make future searches faster". If you answer yes, Windows Indexing Services will be automatically started.

The bad news is that Windows Indexing Services runs under the local system account on Windows XP SP2. This results in a privilege escalation.

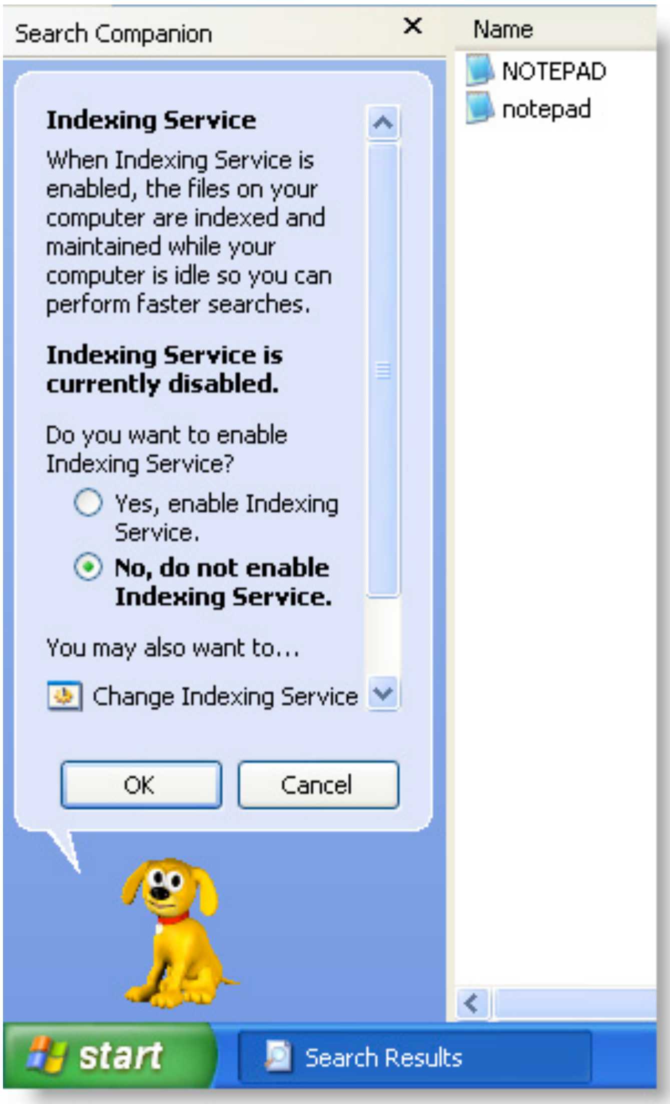
Consider a Windows machine with Windows Indexing Services running, Adobe Reader installed and a file sharing service (FTP/IIS/P2P/…). Uploading a specially crafted PDF document to this machine will give you a local system shell.

To disable Windows Indexing Services' capability to index PDF documents, unregister the IFilter: regsvr32 /u AcroRdIf.dll.

But IFilters are also used by other software:

- Microsoft Search Server 2008
- Windows Desktop Search
- SharePoint
- SQL Server (full-text search).

My PoC PDF file also triggers in /JBIG2Decode in Windows Desktop Search (I tested version 4.0). But Windows Desktop Search has a better security architecture than the Windows Indexing Service.



Search Companion

Indexing Service

When Indexing Service is enabled, the files on your computer are indexed and maintained while your computer is idle so you can perform faster searches.

Indexing Service is currently disabled.

Do you want to enable Indexing Service?

○ Yes, enable Indexing Service.

● No, do not enable Indexing Service.

You may also want to...

Change Indexing Service

Although the service runs under the Local System account, the actual calling of the IFilters is done in a separate process that runs under the Local Service account (this account has fewer privileges and can't take full control of the machine).

I've not analyzed other applications using IFilters. If you use SharePoint or another IFilter supporting application and you want to be safe, unregister the Acrobat IFilter.

And don't forget that, depending on your Windows version and CPU, you're also protected by technologies like DEP and ASLR.

Google Desktop Search doesn't use IFilters, unless you've installed a special plugin to add IFilter support to Google Desktop Search.

Conclusion

It's possible to design malicious PDF documents to infect your machine without you ever opening the PDF file. I've yet to see such a malicious PDF document in the wild.

Be very careful when you handle malicious files. You could execute it inadvertently, even without double-clicking the file. That's why I always change the extension of malware (trojan.exe becomes trojan.exe.virus) and handle them in an isolated virus lab. Outside of that lab, I encrypt the malware.

Didier Stevens (CISSP, GSSP-C, MCSD .NET, MCSE/Security, RHCT) is an IT Security Consultant currently working at a large Belgian financial corporation. He is employed by Contraste Europe NV, an IT Consulting Services company (www.contraste.com). You can find open source security tools on his IT security related blog at blog.DidierStevens.com.

Are Hackers
Finding a Way Into
Your Network?

Review: IronKey Personal

by Mark Woodstone

April was a busy month for those working in the information security industry. Two major events were held practically a couple of days apart - RSA Conference 2009 in San Francisco and Infosecurity Europe in London. My colleagues from Help Net Security were busy the entire month and did some fantastic coverage from these shows. As a result I am now swamped with software applications and hardware devices given to me for review purposes. Within this latest bunch of security goodies I first laid my eyes on the IronKey secure flash drive. I have been using and testing a number of similar devices, so I was eager to see what IronKey had to offer.

IronKey at a glance

The device I used as a basis of this article is the IronKey Personal with 1GB of storage. From the storage perspective this is the basic model, but for this review, storage is not an important factor.

IronKey drives come in three "flavors" - Basic, Personal and Enterprise. Basic, as the lower level offering, is to be used primarily as a secure storage device, while Personal has some advantages. These include Internet protection services, the identity manager and support for the Verisign Identity Protection (VIP) offering. I will talk about all these functions later in the review. Just in case you are curious, the Enterprise version provides the following additional performance: enforceable security policies, remote device termination, RSA SecureID support, as well as automatic antivirus scanning.

When the tagline of the product is "The world's most secure flash drive", you are definitely interested in hearing about the specs. IronKey sports a rather elegant and simple design with a rugged metal casing. The casing is waterproof and tamper resistant. Breaking into the device will only destroy it and you can automatically say goodbye to the data on board.

The Cryptochip operations follow industry's best practices, therefore the device uses only well-established and thoroughly tested cryptographic algorithms. All the data is encrypted in hardware using AES CBC-mode encryption. Everything stored, executed and saved to the disk is encrypted and, as hardware encryption is in place, everything works extremely fast. The encryption keys used to protect your data are generated in hardware by a FIPS 140-2 compliant True Random Number Generator on the IronKey Cryptochip. If you are a true hardware geek, you will also be interested in the fact that the memory used is the ultra fast dual-channel SLC Flash.

In short, what can I do with IronKey?

This will be a lengthy and detailed review of the device. If you are impatient to see if IronKey is of any use to you, let me tell you that it provides:

- Secure encrypted storage on the go
- Password management and elevated security in the online world
- A secure and anonymous Web browsing experience from any computer.

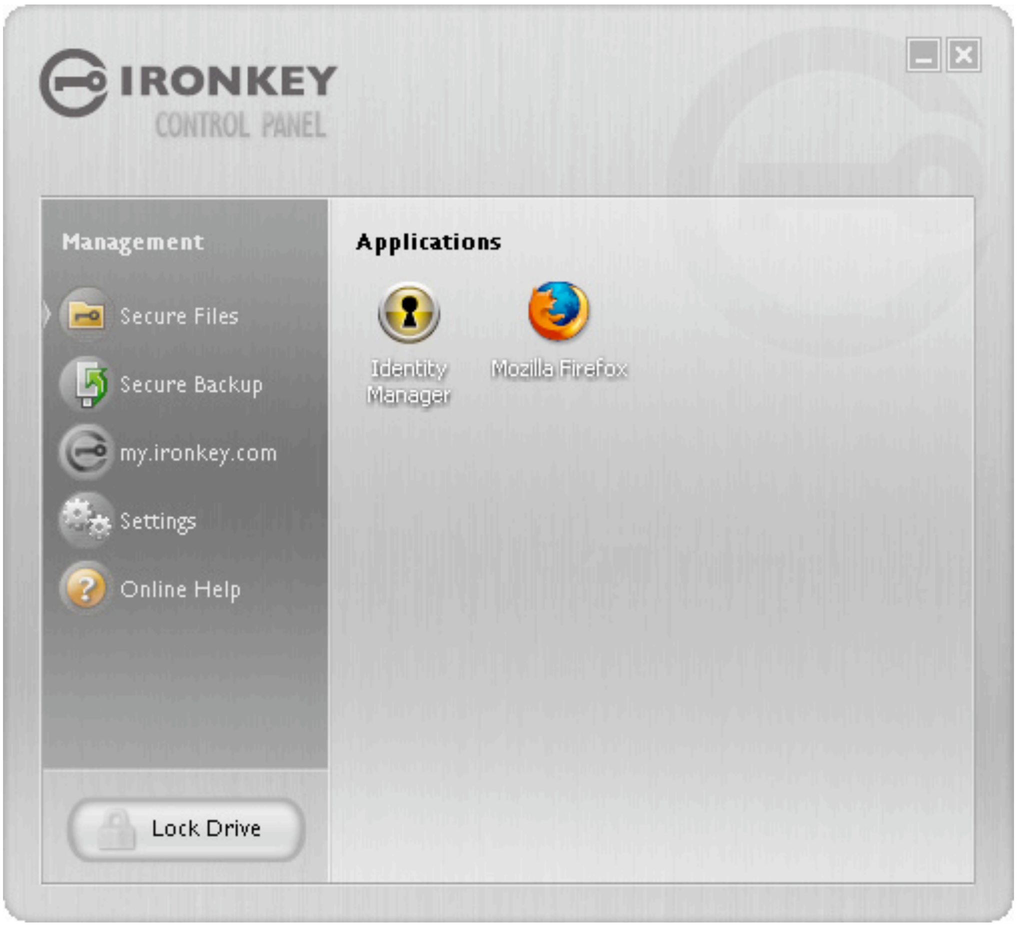
The secure browsing function alone would be enough for me to get this handy device.

Let's start: IronKey installation

IronKey's packaging reminds me of Apple's concept - a dark box with simple insides that contain a metal cased device. In addition to the device you get a folded instructions booklet and a lanyard. IronKey works on multiple operating systems - Microsoft Windows 2000, XP and Vista; Linux (2.6+) and Mac OS X (10.4+). The Windows usage offers the maximum from IronKey, while on Linux and Macs you will be able just to use it for secure storage. My operating system of choice for this review was Microsoft Windows XP.

The first stage of the installation process is done locally on your computer and you will need to initialize the device. The process is fairly straightforward - after entering the nickname for the device, you need to setup a password.

There aren't any special (positive) enforcement limitations like with some secure flash drives, the password just needs to be at least four characters long and you don't need to punch in any special characters or uppercase characters. If you are initializing the gadget from a non trusted computer, you can use the virtual keyboard icon located near the password input field and you won't need to worry about keyloggers. I would suggest selecting the "Backup my password online in case I forget it" checkbox, as it can prove to be invaluable when bad karma strikes.



IronKey control panel with two default applications

After punching in the initial data, the setup process will take a few minutes before you are prompted to go online. Activation is completed after successfully creating an online account located on https://my.IronKey.com. By the way, in the installation process you might come across an alert box saying your autorun.ing has been altered and that it is suggested to scan computer and IronKey for viruses. I looked into this in details and it proved to be a false alarm. Now, back to the online part of the activation process.

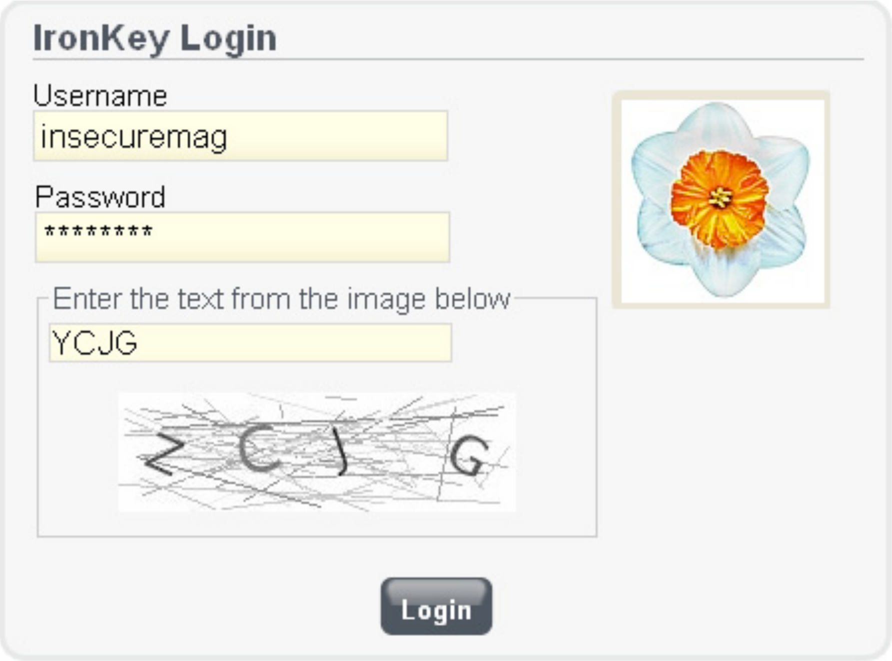
IronKey online activation stronghold

Activating IronKey's online account is not mandatory, but it is undoubtedly a good way to go. By creating an account and linking it to your device you can harness the full power of IronKey - backing up your passwords online, requesting the lost device authorization phrase, as well as doing a secure update with newly released software. The company updates the software from time to time. In late April they did a major update and it brought some changes mentioned later in the article.

The online step-by-step activation guide is one of the most impressive of its kind. I was positively surprised with the layers of extra security developers were thinking of when creating this web application.

The process starts with a typical input scheme where you setup your username and passwords. Afterwards you need to tie in one of your e-mail addresses and setup a secret question/answer phrase. I always hated applications relying solely on this Q&A scheme to make someone retrieve a lost password. In the era where people are sharing practically everything over social networking profiles and when Google is indexing almost everything that appears online - this password retrieving scheme can only create more security problems. Well, IronKey's developers thought of that and are asking at least three questions.

Some questions are given by default, but you can easily refresh them and get a new set of data. If you are still paranoid, why not use additional questions? You can add as much as you want.



IronKey Login

Username: insecuremag

Password: *********

Enter the text from the image below: YCJG

Logging in to the IronKey online account

You thought that was it? Wrong, there is another layer of security just waiting to be introduced. Phishing can be a drag and IronKey is not intended only for those well familiar with the basic security principles. Therefore, before finalizing your activation you need to setup a secret phrase and a photo image.
The secret image will be displayed every time you log in to help assure you that you are at the real my.IronKey.com website.

In order to secure you login into the online account and enter your username, the system automatically fetches your selected image and if it's the same one you selected, you can enter the password knowing that you are inside the real IronKey web user interface. The chances of someone mimicking the IronKey web site and targeting you might be slim, but it’s better to be safe than sorry.

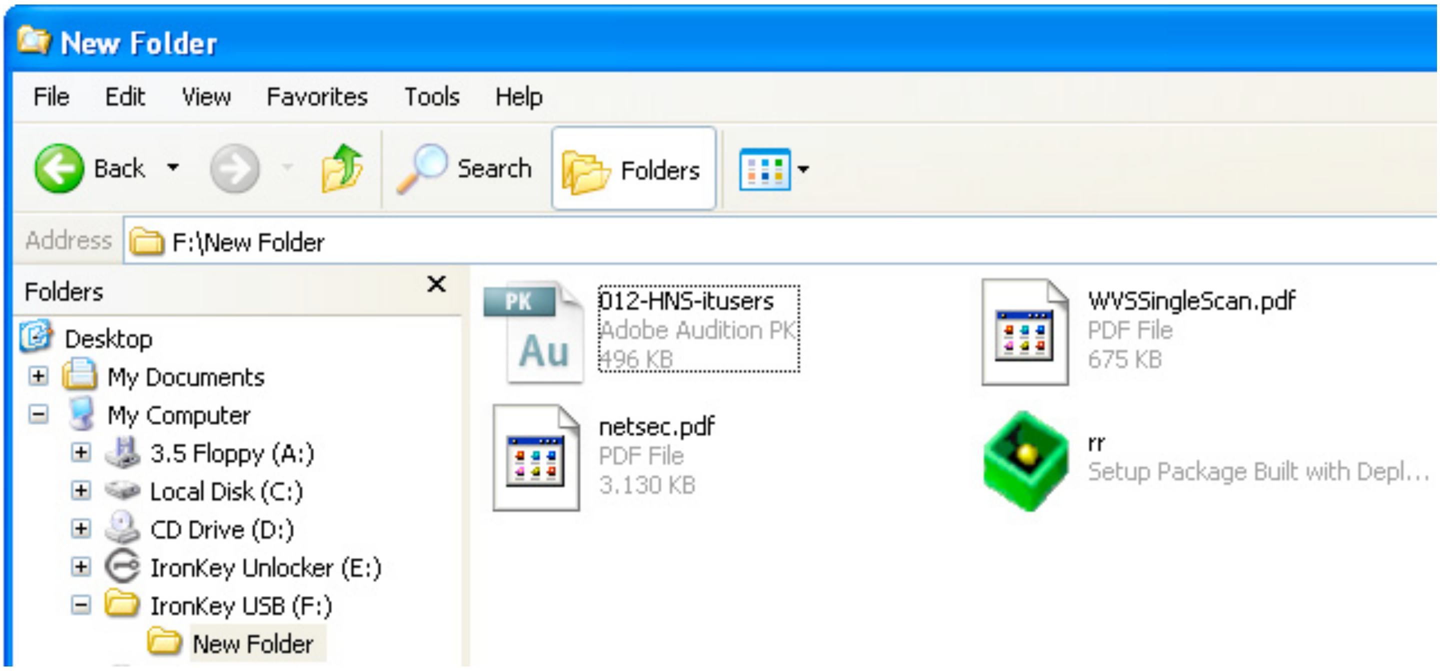
The Secret Phrase that you need to type in will be presented to you in the subject line of every email you receive from IronKey regarding your account. With this, IronKey just shows that they are really passionate about stringent security methods surrounding their little USB device.

Secure Files - basic usage

The adoption rate of USB flash drives, especially the encrypted ones, is on the rise. They are not so expensive, especially when you compare them with standard drives of the same size. Almost every security flash drive on the market is mainly concentrated on being a secure vault for private data. IronKey is definitely not principally focused on this role, but fully supports it by default. The Control Panel application that gets called off from the device is user friendly. Its first management role is "Secure Files". When selecting this option, the Windows Explorer window will open, and you can drag and drop files to it. Everything inside the folder is automatically encrypted, and as soon as you plug off the device the data goes with it. The only thing that bothered me a bit is that I couldn't delete the autorun file from this location.

Secure backup

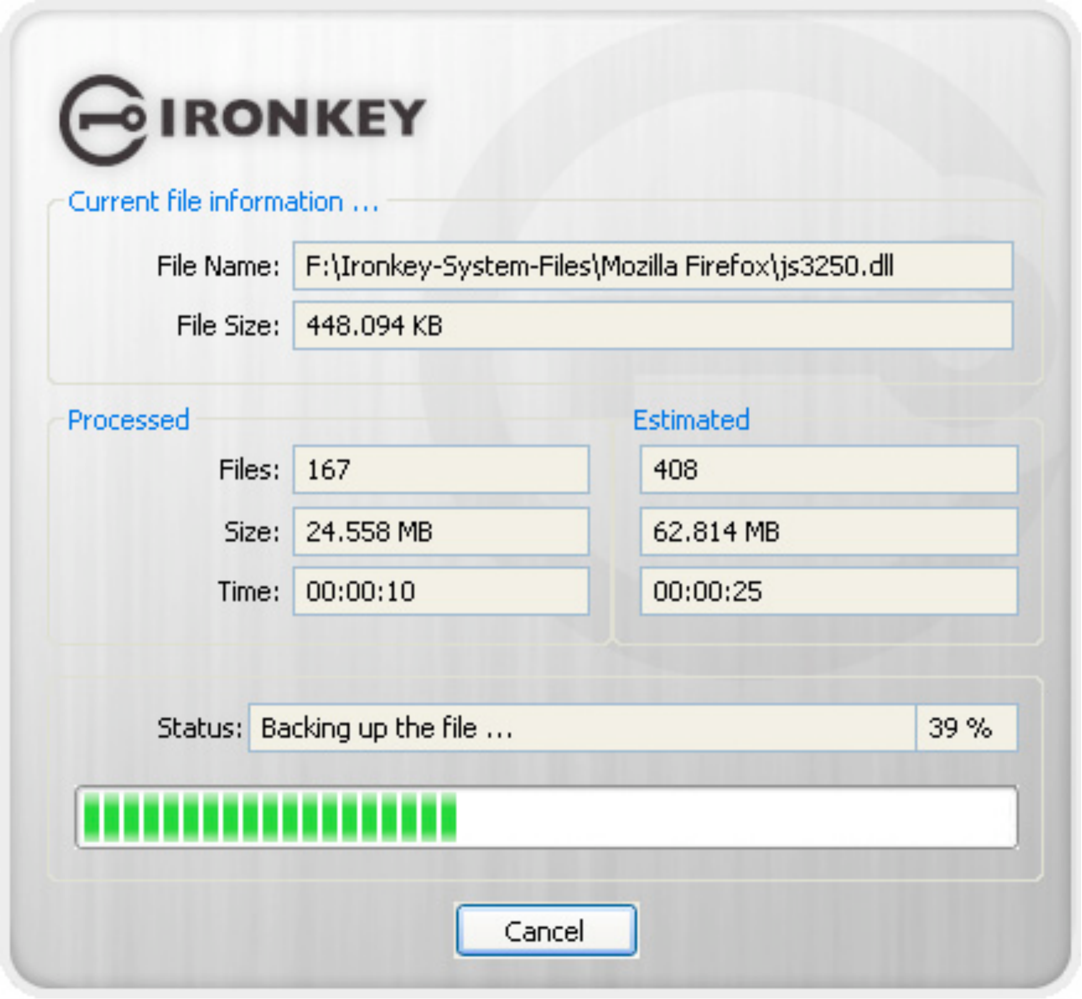
When working with sensitive information, especially relying on one device to hold a collection of important data, you always need to think about backup. IronKey's secure backup option will dump data from your flash drive to an encrypted archive located on a local computer or a network share. It automatically copies all the secure files as well as private data that is marked as hidden on Windows computers.



Secure documents located on the device

Before testing I thought the software creates some kind of an encrypted archive, but as it turns out it just mirrors the existing folders. It looked like this didn't work, as the backed up files had the same extensions and icons, but the mismatched file sizes and the always handy `diff` application have clearly shown that the files are fundamentally different.

From my perspective, I would rather like my data to be in one archive, as in this way accessing the backup folder on a PC would reveal the names and types of my private data. No one could do anything with it, but I am just looking at this from the information disclosure point of view.



File Name: F:\Ironkey-System-Files\Mozilla Firefox\js3250.dll

File Size: 448.094 KB

	Processed	Estimated
Files:	167	408
Size:	24.558 MB	62.814 MB
Time:	00:00:10	00:00:25

Status: Backing up the file ... 39 %

Process of backing up to a local disk

Secure online surfing and shopping

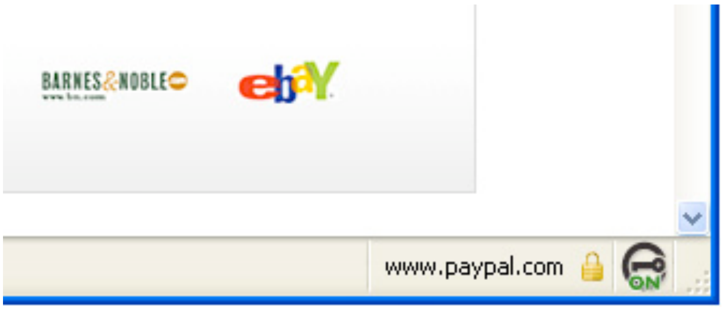
As I previously noted, this feature of IronKey is the selling point. Let's identify a couple of common problems.

When it comes to important data that we transmit online, we mostly use some kind of Secure Sockets Layer implementation. However, secure transmission is not always available.

The second problem is logging in to different sites or even shopping from computers that aren't yours. Working from a conference, checking the latest emails from an Internet kiosk on an airport, paying bills from your parents' computer - am I the only one that always has potential keyloggers in mind?

Maybe this will sound like a marketing pitch, but IronKey indeed tackles all of these situation through one fine concept - a customized Mozilla Firefox browser, sitting installed directly on the device and leveraging the powerful Tor network that provides security and anonymity.

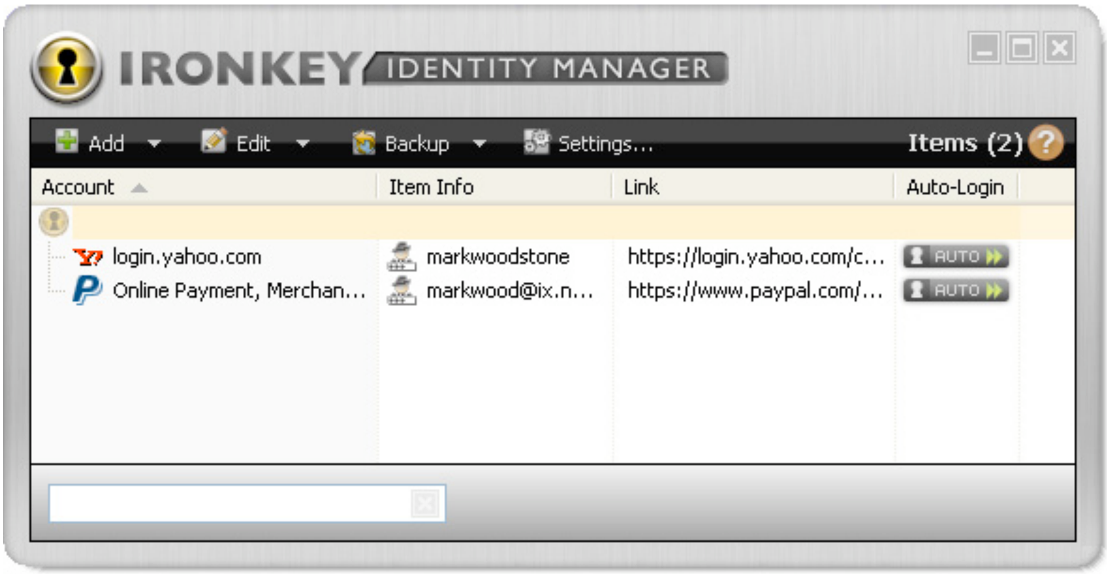
They named this security mechanism Smart Surfing. It is directly built into the browser and you can switch it on and off with a click.



Smart Surfing toggle on/off

If you are not familiar with the concept of Tor, by using this Secure Sessions service your data goes from a secure encrypted tunnel to IronKey's servers and then it is rerouted to its final destination. When packets are coming into their data centers, the actual destination is tested against a local DNS database so pharming and phishing ploys are automatically intercepted. As Tor is using multiple network routing servers, your online surfing habits will automatically be made anonymous. Surfing this way will be secure but naturally a bit slower because of the multiple routings.

Keyloggers won't be a threat if you deploy a built-in virtual keyboard which can be opened through a keyhole icon in the top right corner of Mozilla Firefox. Input works as a charm, perfectly fitted when you need to use shared computers.



Account	Item Info	Link	Auto-Login
login.yahoo.com	markwoodstone	https://login.yahoo.com/c...	AUTO
Online Payment, Merchan...	markwood@ix.n...	https://www.paypal.com/...	AUTO

Newly released Identity Manager application

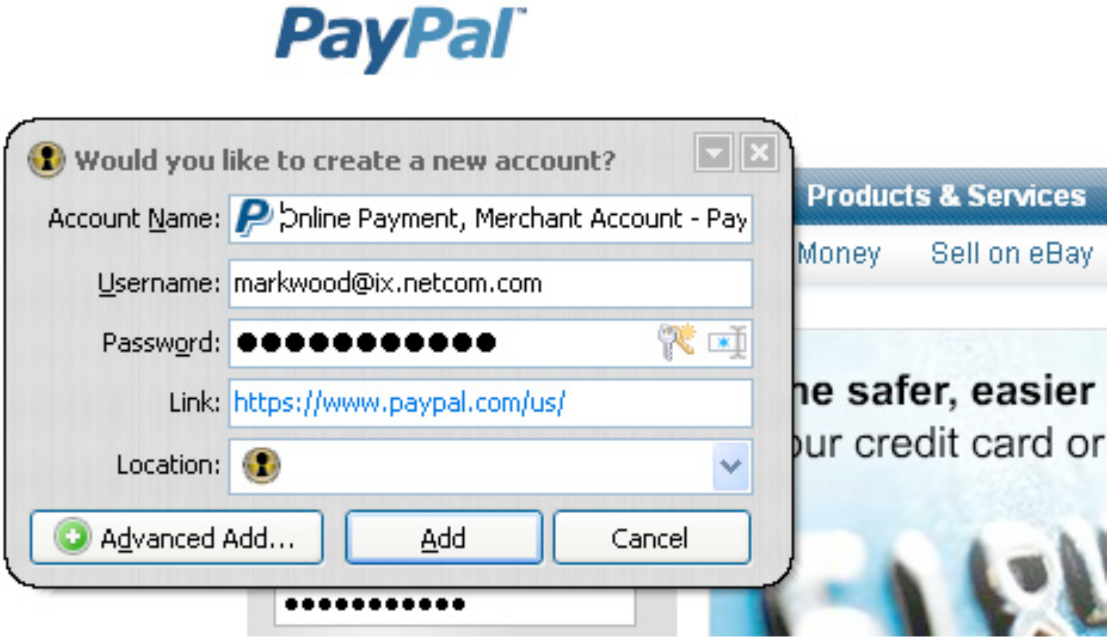
Identity Manager, a place for secure passwords

The original version of the IronKey I got was created prior the RSA Conference 2009, so besides an older Firefox (2.0*) the only other application was Password Manager. During testing it appeared a bit spartan. With the new update, Password Manager was decommissioned and its functionality evolved into the newly released Identity Manager.

Since the mid 90s I always tried to remember all my passwords. As the Internet evolved, lots of new web services appeared and with increased use, it became practically impossible to track all the password phrases.

Combining this with the mindset change that now all passwords need to contain at least 10 characters of garbled text made me start using password management applications. That was five years ago, and now I am very satisfied with 1Password - a top solution that works solely on Macs and iPhones. Identity Manager is practically the same type of application, it sits in the background and tries to "sniff" web pages for login forms. If the form is not in the database it will ask if you would like to save it. If the form is found in the database, you will have an option to automatically fill username and password for the specified page. This is a rather straightforward concept that works perfectly on IronKey.

The new Identity Manager looks much better than the now obsolete Password Manager, it has a better GUI and it is much easier to work with. If in any case you wouldn't like to run it in the background, you can always manually start it via the mentioned keyhole icon in Mozilla Firefox. When your passwords database pumps up, don't forget to back it up locally or directly to your associated online account.



Would you like to create a new account?

Account Name: Online Payment, Merchant Account - Pay

Username: markwood@ix.netcom.com

Password: ●●●●●●●●●●●●

Link: https://www.paypal.com/us/

Location:

Automatically scouting the PayPal login page for data

Further benefits of an online account

Here's some insight on the actual interconnection between IronKey and your my.IronKey.com account. When the device is in place in one of your USB slots and you have successfully authorized to it, you will be able to access your full online account. Only in this situation everything will be available for you to use. In case you want to login online, but you don't have the device with you, the two-factor authentication cannot be done and you will enter the account in Safe mode.

Safe mode is used mostly in the case you lose your key and while residing in it, you might just work around some activities such as recover your device's password, report the device as lost and delete your online backups (both the password, as well as data from Identity Manager). By the way, even when logging in to the Safe mode, there is a security twist. Before successfully logging in with just your username and password, an Account Login Code will be sent to your e-mail and you will need to write it in.

Final thoughts

If you had the willpower to read this extensive review, or better say a guide on IronKey usage, you won't be shocked to learn that I really liked the product. It works great and there were no issues during my thorough tests. The functions I described in detail would take care of multiple situations I usually come across and the additional reliability with the paired online account is surely a significant plus.

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

Windows 7 security features: Building on Vista

by Rob Faber

In November 2007, Windows Vista first saw the light of day with all of its heralded improvements. After a mixture of both criticism and positive reactions from end-users, there will soon be a new member of the Windows family available. Following Microsoft's announcement, Windows 7 will be released this year and will make us forget its predecessor. As a consequence, it's about time to have a look at the enhanced security features that have been added to Vista's fundamentals.

Windows 7 (formerly code-named Blackcomb and Vienna) will be the next version of Microsoft's Windows platform. In 2007, the company revealed that it was planning to develop this software over a three-year time period which would follow on from the release of Vista. The latest announcement is that the new OS will be made available in the last quarter of 2009, while the RC is out right now.

Unlike Vista, Windows 7 is intended to be an incremental upgrade. With updated features, a new task bar, improved performance and a revamped shell, it will certainly be ready to take the place of its predecessor. Nevertheless, there will be no major changes on the security part, Microsoft will instead be concentrating on scalability and stability. As well as the touch, look and feel of Windows 7 there will also be security improvements, so let's have a look at these particular features and see what they will mean for your business.

Overall, Windows 7 has been built upon the security foundations of Windows Vista, although improvements have been made in a number of areas such as the auditing of group policies, the User Account Control (UAC) experience and BitLocker. As well as these changes there are also some new features such as AppLocker, which enables you to control which software can run in the environment, and BitLocker To Go, which makes it possible to secure removable storage devices.

Secure Windows 7: Secure Start-up

Like Vista, there is Secure Start-up in Windows 7, which means that the entire hard drive can be encrypted prior to boot and the encryption key will be safely stored inside a Trusted Platform Module (TPM) chip on the motherboard. This can be achieved with BitLocker. Many of the methods currently used to circumvent permissions will no longer work by way of the simple reading of data from the NTFS partition.

Although Windows Vista Service Pack 1 did later add the ability to encrypt multiple fixed disks, within the initial release of the OS the BitLocker encryption mechanism could only be used to encrypt the volume upon which the system was installed, even though a volume can, of course, span one or more disks. In fact, it was only by using the command line that more options were available. Both the improved BitLocker Drive Encryption and the new “BitLocker to Go” will be discussed next.

There has been much improvement to BitLocker in Windows 7, although the first activation or use of it is slightly different to Vista because the BitLocker partition is already available and will be 200 MB in size. Since the partition is hidden and there is no drive letter attached to it, its utilization is only possible by disk management (MMC). It can be found and activated by searching under System and Security in the Control Panel.

If you want to upgrade from Windows Vista to Windows 7, this will be possible without having to decrypt the whole partition. This saves time and solves a bunch of other issues and minimizes additional problems (as you can sometimes see happen with other products for disk encryption where you have to decrypt the disk first).

To encrypt the drive, BitLocker uses either the Trusted Platform Module (TPM) chip from the computer (version 1.2 or higher) or a removable USB memory device, such as a flash drive. If your machine doesn’t have the TPM chip available, BitLocker will store its encryption and decryption key on the flash drive so that it is separate from your hard disk.

BitLocker Drive Encryption seals the symmetric encryption key in the Trusted Platform Module (TPM) 1.2 chip. This is the so-called SRK (or Storage Root Key), which encrypts the FVEK (or, Full Volume Encryption Key). The FVEK is then stored on the hard drive in the operating systems' volume. Every time you boot, the TPM conducts an integrity check to ensure that specific components haven't been changed. What’s more, there is also the option to save a Recovery Key, which is necessary in the event that the USB flash drive is lost, because it otherwise wouldn’t be possible to access your data! Overall, BitLocker has three modes of operation:

- **Transparent operation mode:** To provide a solution that is enterprise ready, the Trusted Platform Module (TPM) 1.2 chip is used and required to store the keys which encrypt and decrypt sectors on the hard drive.

- **User authentication mode:** To be able to load the OS, this mode requires the user to provide some authentication to the pre-boot environment. Two such methods are supported: a pre-boot PIN entered by the user, or the insertion of a USB device that contains the required start up key.

- **USB-Key:** To be able to boot the protected OS, the user must insert a USB device that contains a start up key into the computer. In this mode, the BIOS on the protected machine must support the reading of such tools in the pre-OS phase.

Preparing for BitLocker

Since it is user-friendlier than Vista, and because the Preparation Tool does the work for you behind the scenes, you only have to fire the wizard up to turn BitLocker on in Windows 7. BitLocker Drive Encryption supports 128-bit and 256-bit encryption, although the former will be most commonly used. As you already know, the longer the encryption keys, the more enhanced the level of security. Be aware, however, that longer keys demand more calculation power and can slow your machine down when it's in the process of encryption and decryption.

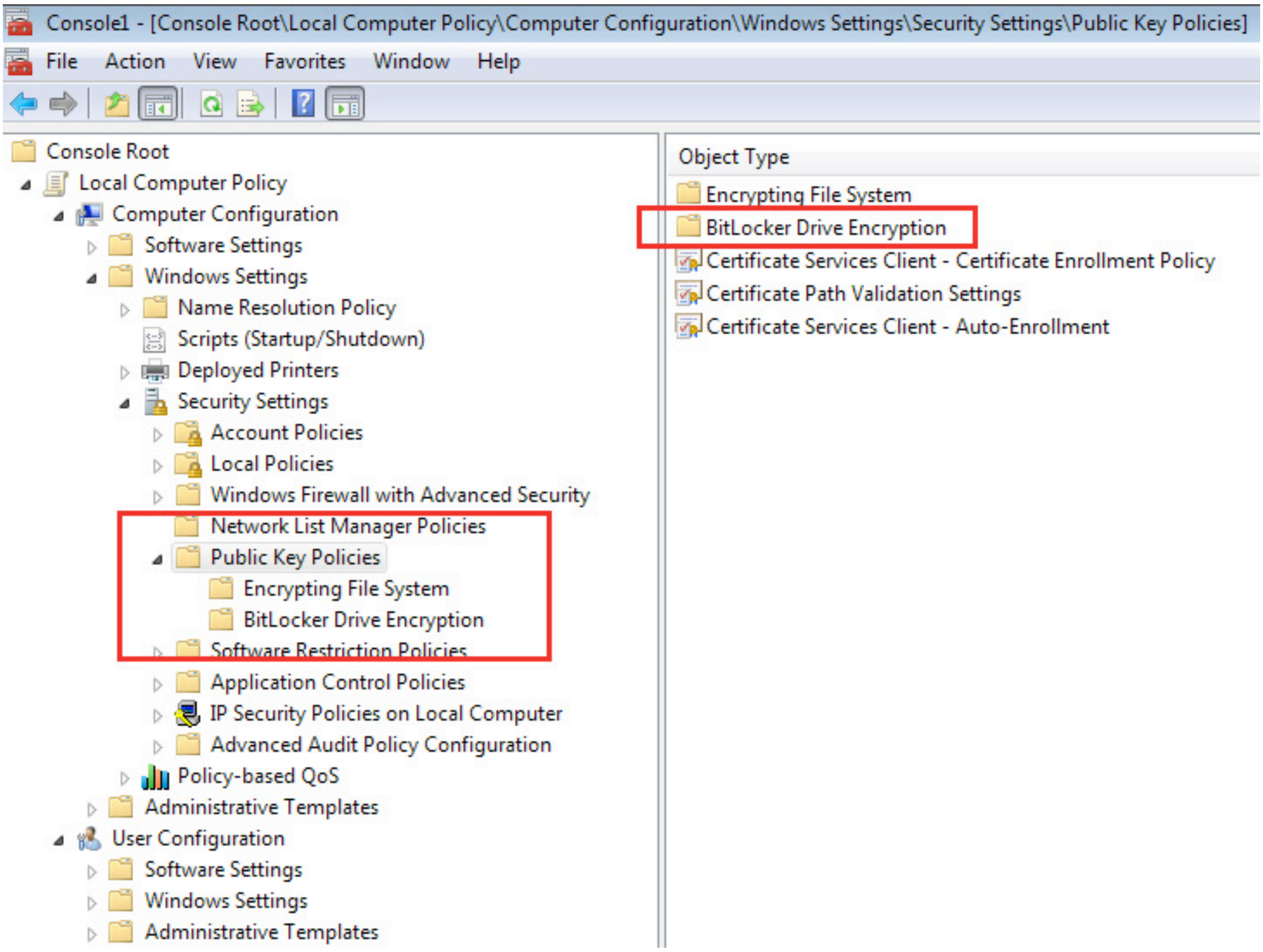
BitLocker supports and implements a diffuser algorithm to help protect the system against ciphertext manipulation attacks (to discover patterns or weaknesses). This means that plain text is XORed with a key, then put through a diffuser and finally encrypted with AES 128-bit encryption in CBC mode. CBC stands for Cipher Block Chaining, and in this mode the cipher-text from previously encrypted blocks of data will be used in the encryption of the next block. By default, Windows 7 BitLocker Drive Encryption uses AES encryption with 128-bit encryption keys and the Diffuser.

BitLocker in the enterprise environment

There can be circumstances where you have to remove a hard drive from one machine and to install it into another computer. For example, the laptop display is damaged and the support organization has a spare computer for the affected user. This can, however, be a problem since a blueprint of the original system will have already been created because the TPM and the hard drives are logically connected to each other on that specific machine. The encryption keys with which to decrypt the volume are also stored in the TPM of that particular device, so how can this problem be resolved?

When BitLocker was enabled in Windows Vista, we could use the recovery mode, which required the generation of a recovery key. That key is specific to that one machine, meaning that there will be one for every computer in a company. Enterprise organizations will need the infrastructure with which to manage and store all of the specific recovery keys in the Active Directory.

The reality is that within large businesses such maintenance can be a painful exercise in terms of manageability.


Console1 - [Console Root\Local Computer Policy\Computer Configuration\Windows Settings\Security Settings\Public Key Policies]
File
Action
View
Favorites
Window
Help
Console Root
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Encrypting File System
BitLocker Drive Encryption
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Object Type
Encrypting File System
BitLocker Drive Encryption
Certificate Services Client - Certificate Enrollment Policy
Certificate Path Validation Settings
Certificate Services Client - Auto-Enrollment

Possible recovery mechanism.

As with Windows Vista, BitLocker in Windows 7 supports the storage of recovery information in the Active Directory, meaning that you can centrally store the recovery password and key package of each user in AD DS. The key package contains the encryption key protected by one or more recovery passwords. It is possible to configure this feature via Group Policy, although this means that a lot of data must be put into the Directory. An interesting announcement has, however, referred to a Data Recovery Agent (DRA) for BitLocker in Windows 7. Unfortunately, despite searching for more details of this, there have only been brief mentions of its existence in presentations such as those from WinHEC 2008.

A DRA could work for BitLocker like the Encrypting File System (EFS) does, meaning that there is a master key that can be used to decrypt all files in an enterprise, wherever you may be. This key is associated with a specific (administrator) account, and if it is used at a workstation any EFS file can be decrypted. This is likely to be Microsoft’s approach to this issue, particularly since there is a special folder for the BitLocker certificate in the Local Security Policy, next to the EFS folder. This is used to configure the Data Recovery Agent and maybe gives us a clue about how the BitLocker recovery procedure might be implemented. Naturally, we will have to wait until the final release to see if this will actually happen.

It is also interesting that there are many new Group Policies available for the fine-tuning and management of BitLocker operations. One example is the policies connected to the BitLocker to Go feature.

Portable media encryption has been around for quite a long time now. Many portable storage devices come with their own encryption software, integrated hardware and this is sometimes combined with strong authentication features like biometrics and a pin code. There is also a variety of accessible tools, such as TrueCrypt or the commercial solution Privatecrypto from Utimaco, which supports encryption on USB storage devices. Until now, however, it has not been possible to use Bitlocker in combination with removable disks. The release of Windows 7 changes this and, in the future, support for the encryption of portable hard disks and flash memory devices will be available. This portable solution is called "BitLocker to Go."

While it is true that USB devices are useful, they also carry a serious risk (especially since the storage of sensitive data on USB keys has become popular). The theft or loss of corporate intellectual property is an increasing problem, and tops the list of concerns in most IT departments, particularly when it comes to mobile computers (laptops) and other small flash memory devices.

An organization can make use of the ability to require encryption prior to granting write access to a portable data device such as a USB flash drive. If this policy is enabled, users will be unable to store information on the portable device if they insert an unencrypted portable data drive. This will give them the option to encrypt the device first or to open it without having write access to it. This approach can be used in tandem with the option of blocking USB devices at workstations.

You can find the policies under:

```
\Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption
```

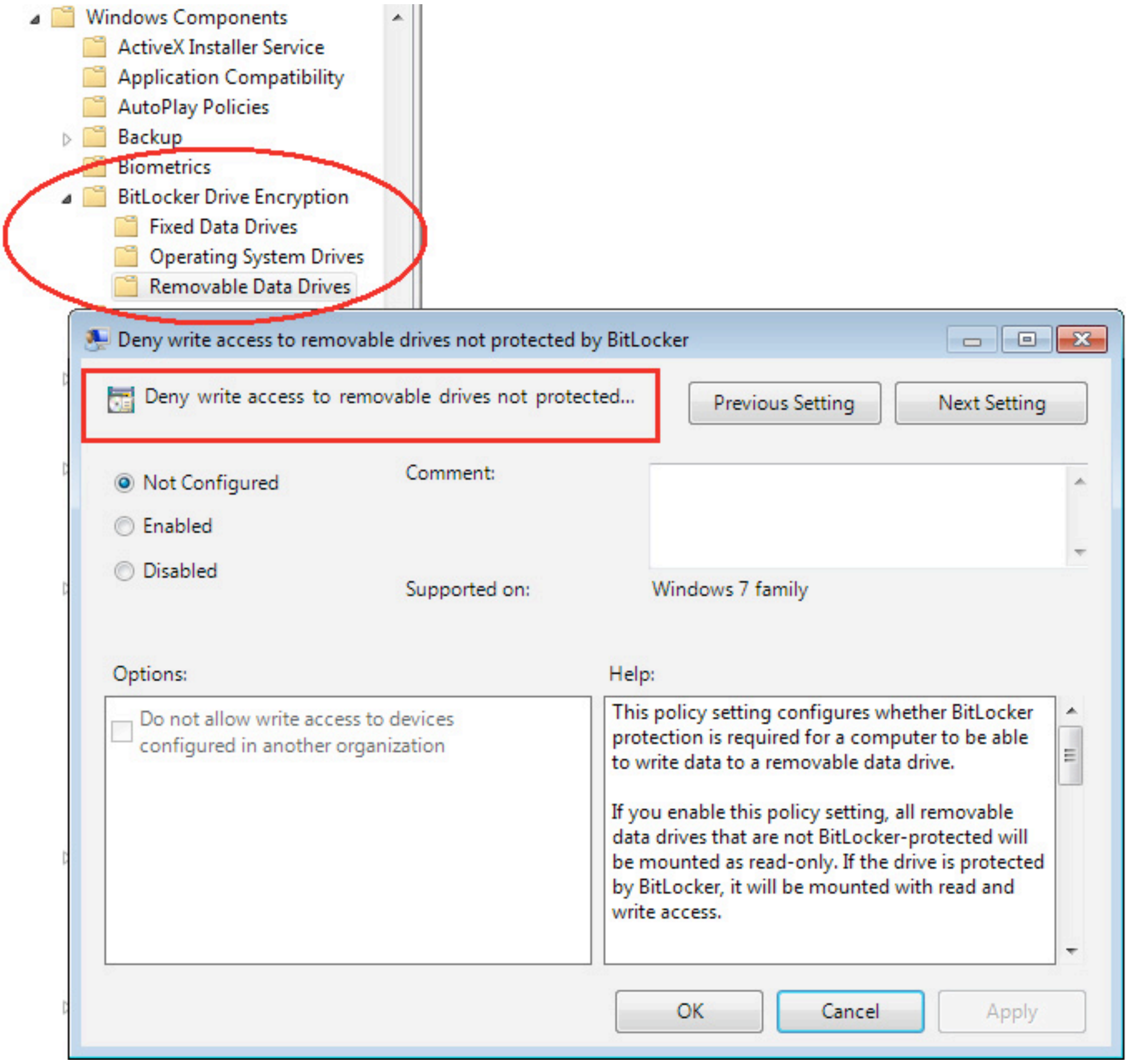
BitLocker to Go is fully integrated into Windows 7, and you can turn it on in Windows Explorer via a memory stick’s context menu, which contains a list of options. Then, before Windows can encrypt the flash drive, you have to choose a password or smart card that will later be required to unlock the device.

You can also store a recovery key in a file and print it. This key is, of course, necessary in cases where the password has been forgotten. If this happens, clicking on “forgot my password” leads to BitLocker prompting the user to enter this recovery key. This way you can unlock the flash drive. A drawback, however, is that this feature is only available in the Windows 7 Ultimate and Enterprise editions.

Finally, regarding this issue, I must refer to the news from 2008 of an attack method that allows a Bitlocker-protected machine to be compromised by booting it off a USB device into another operating system after it is shut down. The contents of the memory are then dumped. In these circumstances, the RAM retains information for up to several minutes, and this period can even be lengthened if the memory temperature is maintained at a very low level by active cooling.

The simple use of a TPM module does not offer the protection needed because the keys are held in the memory while Windows is running. The recommendation is, therefore, to power a computer down when you are not in physical control of it for a period of time (such as leaving a hotel room for a couple of hours).

Therefore, as long as you don't put the machine in some sort of hibernation or sleep mode, you're safe.



Deny write access to removable drives not protected by BitLocker

Deny write access to removable drives not protected...

● Not Configured
○ Enabled
○ Disabled

Comment:

Supported on: Windows 7 family

Options:

□ Do not allow write access to devices configured in another organization

Help:

This policy setting configures whether BitLocker protection is required for a computer to be able to write data to a removable data drive.

If you enable this policy setting, all removable data drives that are not BitLocker-protected will be mounted as read-only. If the drive is protected by BitLocker, it will be mounted with read and write access.

Deny write access to USB.

Controlling applications with AppLocker

In the past, Software Restriction Policies were used to control applications. This was a feature that I didn't think was particularly useful, because it was likely that there were only a few applications to which you might want to block access anyway. Windows 7, however, introduces the AppLocker, which allows you to restrict program execution via the Group Policy. More specifically, the AppLocker helps to control how users can access and use files such as executables and specific scripts.

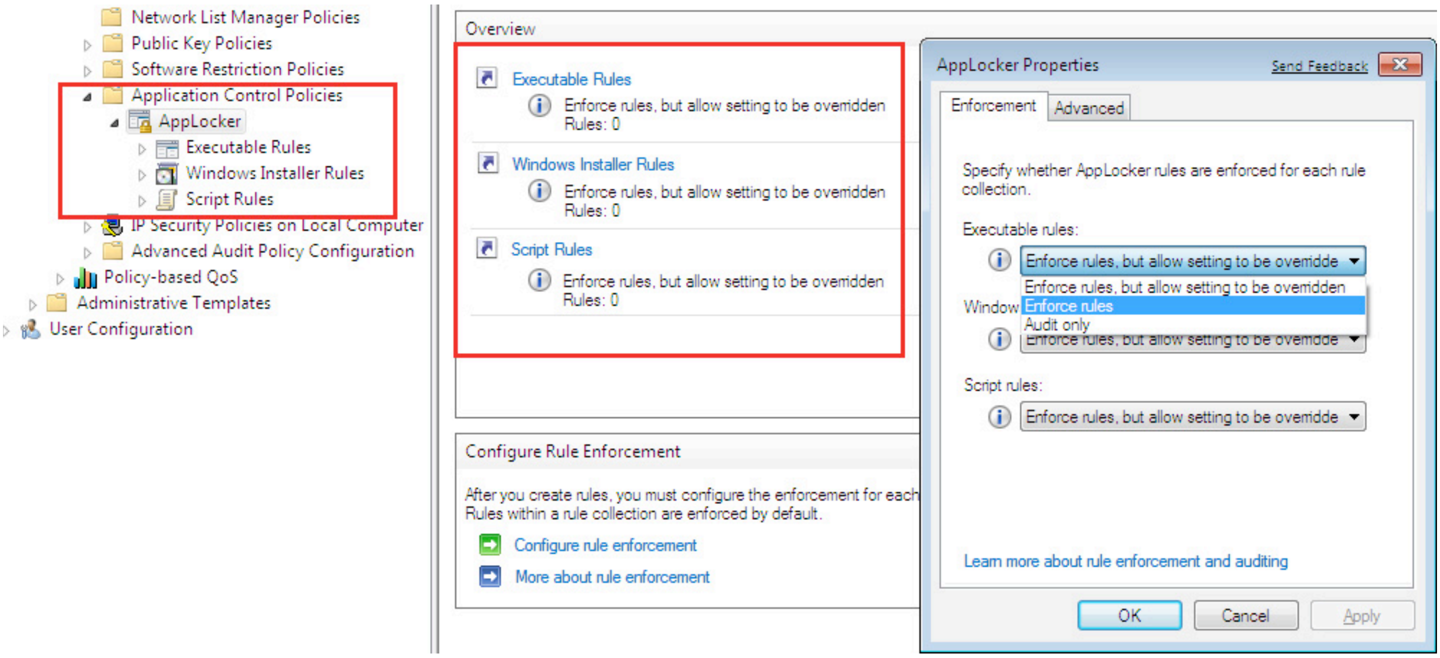
AppLocker essentially utilizes three types of rules: Path Rules, File Hash Rules, and Publisher Rules. The first two are not that new and can already be found in Vista's Software Restriction Policies. Hash Rules use a cryptographic hash of the executable to identify a legitimate program. The major downside of this type of rule is that you have to modify it whenever you update the program. If you change a program or executable it will also change the hash. Hash policies are, therefore, only effective for as long as a file remains in a consistent state. In daily operations, however, the reality is that applications are updated very frequently, meaning that hash policies can become outdated in a matter of weeks as new versions of files are released. This creates a lot of work in larger organizations, with literally hundreds of applications being out in the field.

An improvement to this situation is that in AppLocker you can define a so-called “publisher rule”, which means that there is information in the system relating to the digital signature rather than the hash value or path of a specific file. You can now use the information derived in this manner more easily, including the publisher, product name, file name and file version. You will be able to create rules that are based on the publisher and file version attributes, which remain consistent during updates to a certain level. It will also be possible to create rules that target a specific version of a file. This approach makes application management much easier, and also means that you don’t have to change all of these rules every time versions change and are updated.

Newer applications have a signature that can be used for the Publisher Rules, and Windows 7 also makes it possible to view this signature by examining the file properties of the executable.

Path Rules enable you to restrict the execution of programs to a certain directory path. For example, you can allow end-users to launch applications only from the Windows Program Files’ folders. This is safe provided that these individuals are not allowed to install programs.

The problem with this type of rule, however, is that users often also need to start applications from other locations, or that applications do not commit to the recommended paths issued by Microsoft.


Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
AppLocker
Executable Rules
Windows Installer Rules
Script Rules
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates
User Configuration
Overview
AppLocker Properties
Send Feedback
Enforcement
Advanced
Configure Rule Enforcement
Configure rule enforcement
More about rule enforcement
Learn more about rule enforcement and auditing
OK
Cancel
Apply

Executable Rules
Enforce rules, but allow setting to be overridden
Rules: 0

Windows Installer Rules
Enforce rules, but allow setting to be overridden
Rules: 0

Script Rules
Enforce rules, but allow setting to be overridden
Rules: 0

After you create rules, you must configure the enforcement for each
Rules within a rule collection are enforced by default.

Specify whether AppLocker rules are enforced for each rule collection.

Executable rules: Enforce rules, but allow setting to be overridde
Enforce rules, but allow setting to be overridden
Enforce rules
Audit only

Window Enforce rules, but allow setting to be overridde

Script rules: Enforce rules, but allow setting to be overridde

new AppLocker policies.

Windows 7 provides you with AppLocker Group Policies, which means that administrators can control the versions of applications that users can install and use scripted and via Group Policy.

You can find it here:

```
\Computer Configuration\Windows Settings\Security Settings\Application Control Policies\AppLocker
```

However, AppLocker cannot be used to manage computers running earlier versions of Windows. There might also be some minor performance degradation because of the runtime checks. Publisher Rules allow you to work in different ways. You can restrict the execution of a program to the publisher (for example, Microsoft), to the product name (MS Office), to the file name (wordpad.exe), or to the file version (3.5.0.8). Because AppLocker gets its information from the digital signature that is bound to the program executable, end users cannot circumvent this by simply renaming the executable.

All the three rule types (Path Rules, File Hash Rules, and Publisher Rules) can be applied to executables (.exe), to scripts (.cmd, .vbs, .js), to installer files (.msi, .msp) and to system libraries (.dll).

Streamlining User Account Control (UAC) in Windows 7

Windows users are accustomed to working with a high number of privileges. This freedom does, however, have a major downside in a corporate environment – namely, that more help-desk calls are made because of accidental or deliberately made modifications to the OS, with a variety of errors being the outcome. In addition, malware and other software with malicious intent can copy this type of behavior.

The result of such an approach is a desktop that is much harder to manage and an increase in the organization’s support costs. Looking for a solution, User Account Control (UAC) was therefore introduced with Windows Vista, and provides increased security because the tool is intended to prevent unauthorized changes being made by the end-user to a system (system files). UAC is based upon the concept of the so-called “least-privilege”, which effectively means an account is set up which contains only the minimum number of privileges that are required to enable a particular user to perform necessary and appropriate tasks. The standard user within Windows 7 is also this least-privileged individual.

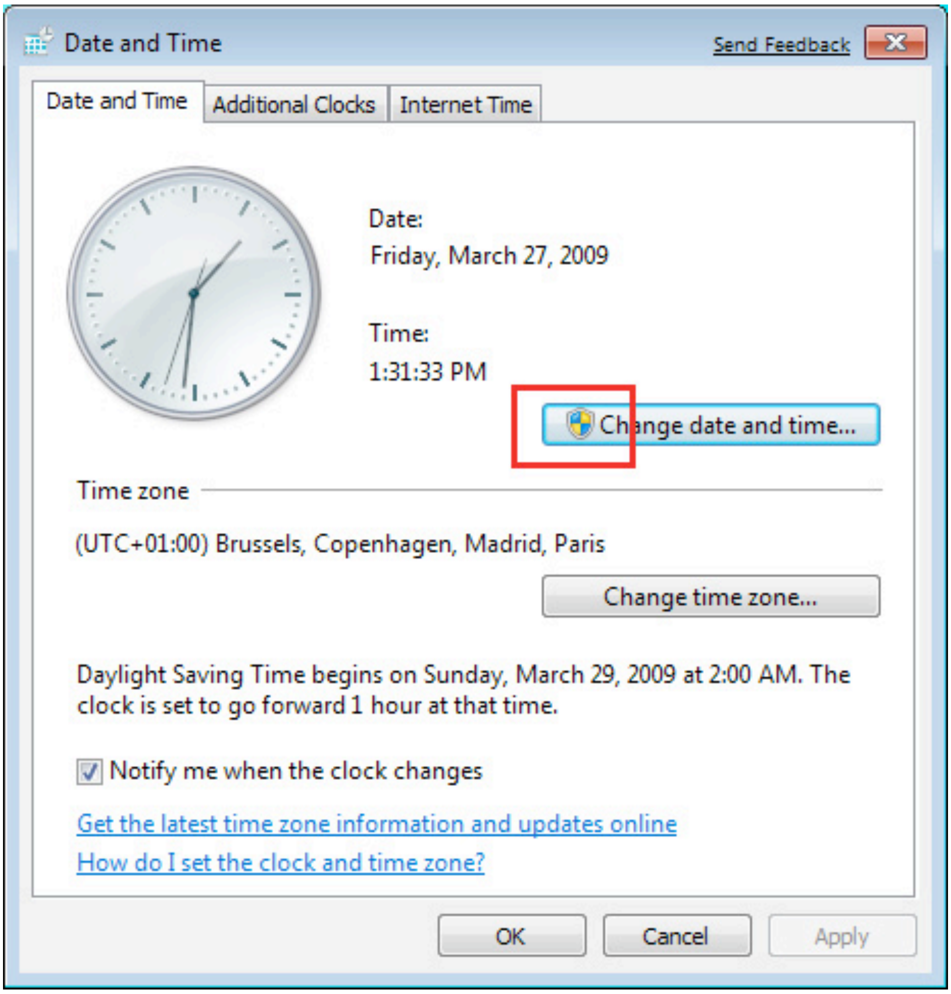
Yet this mechanism became one of the main areas of complaint by Vista users. UAC is a blunt instrument that is frequently invoked, meaning that more clicks are needed to execute a program when it involves system-level changes. Moreover, many software programs did not properly support UAC when it was first introduced, and applications created many issues that culminated in a terrible user experience. The consequence was that because there was so little control, many people just disabled the tool, with the result being decreased security and different types of problems.

What is more, if the tool is not disabled, the lack of control referred to, combined with UAC notifications in the form of pop-ups which confuse and irritate users, leads to many of them just clicking on “OK” even if they are unsure of the consequences. In these circumstances, the question must arise as to whether this approach is appropriate and if it has really resulted in security improvements.

Human behaviour in these circumstances is, of course, something that cannot be solved by a computer. Sometimes it’s fine to download software (even initiated by the user) and install a program, but on other occasions malware is trying to install itself on your machine. In such a scenario, the important and often technical decisions are up to you, the end user, to make. This means that ultimately - and yes, you will probably have guessed this - you will be presented with a dialog box asking you for confirmation and approval of something which may be damaging to your machine. Years of pop-ups and confirmation dialogs have literally trained the user to act like a monkey in an experiment; act like this or push the red button and… get a banana. Why not click “yes”, “ok”, and “next”? Off we go!

As a result of these issues, some changes were made in Windows Vista SP1. In other words, the UAC experience was relaxed a little. How much has this changed in Windows 7? Well, Microsoft has decided to give a user the chance to change the UAC notifications to something more manageable and convenient level. The user interface has also been improved by the addition of more relevant and detailed information.

In the Windows 7 UAC, the defined standard user can adequately perform most daily tasks such as using business applications, browsing the Internet and typing a letter in a word-processor. Indeed, the only time a user will be confronted with a dialog box will be in circumstances where he or she is asked to provide appropriate credentials, if they are required.



Date:
Friday, March 27, 2009

Time:
1:31:33 PM

Time zone

(UTC+01:00) Brussels, Copenhagen, Madrid, Paris

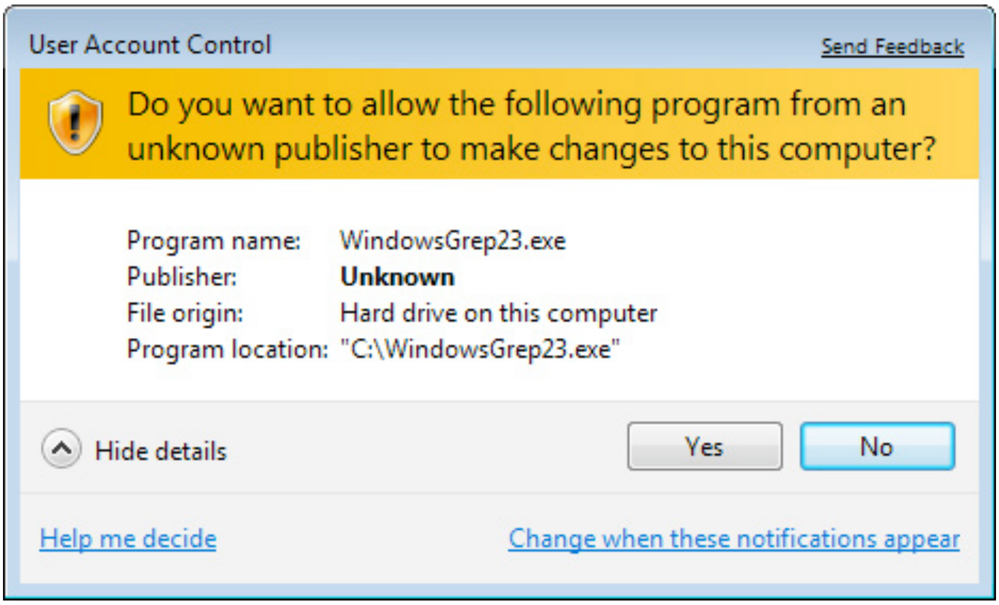
Daylight Saving Time begins on Sunday, March 29, 2009 at 2:00 AM. The clock is set to go forward 1 hour at that time.

☑ Notify me when the clock changes

Get the latest time zone information and updates online

How do I set the clock and time zone?

Relaxed UAC: the icon.



Do you want to allow the following program from an unknown publisher to make changes to this computer?

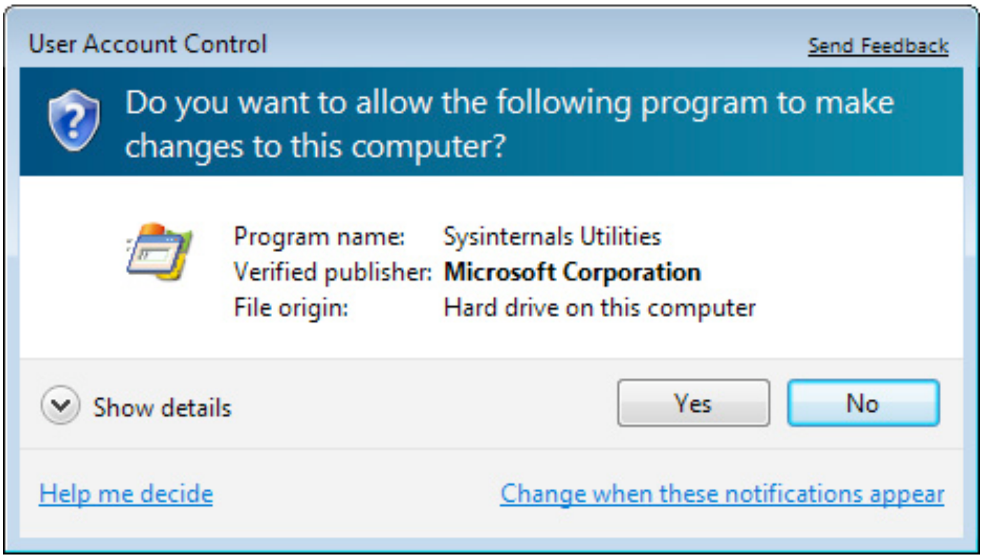
Program name: WindowsGrep23.exe
Publisher: **Unknown**
File origin: Hard drive on this computer
Program location: "C:\WindowsGrep23.exe"

Help me decide

Change when these notifications appear

UAC warning message.

In many cases, it will be perfectly clear to the user that a prompt will appear because the setting will have an icon in the form of a shield next to it. This indicates that higher privileges are required. In Windows 7, even the icons and messages presented by the UAC are more low profile. However, it should be noted that the default user account (created during the installation of Windows 7) is still a protected user, albeit with slightly different UAC settings. This default user is only faced with prompts when programs try to make changes, but not when the user does this by himself.

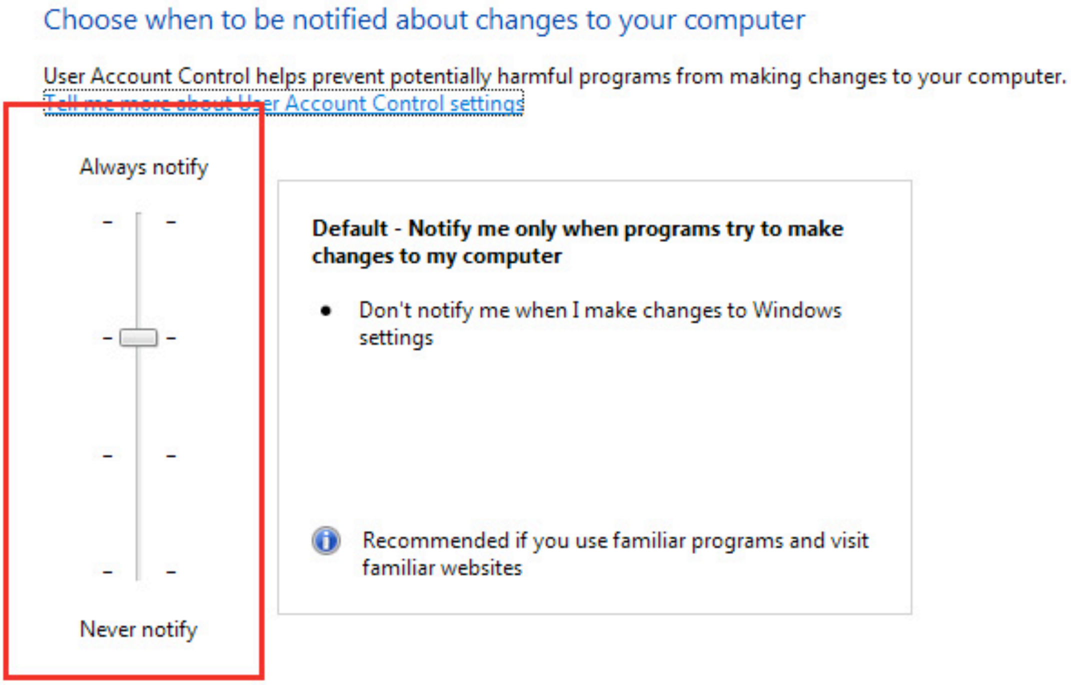


Do you want to allow the following program to make changes to this computer?

Program name: Sysinternals Utilities
Verified publisher: **Microsoft Corporation**
File origin: Hard drive on this computer

UAC notification.

The Windows 7 UAC settings have changed and give you more control. There is a slider option to change the level of notifications, and there are a couple of pre-defined options to choose from. Indeed, from the picture provided, you will see that the user can navigate to the UAC settings and change how these notifications appear. Of course, administrators can pre-define these levels.



Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.

Default - Notify me only when programs try to make changes to my computer

- Don't notify me when I make changes to Windows settings

Recommended if you use familiar programs and visit familiar websites

The UAC slider.

Microsoft is committed to the UAC because it increases overall security and also forces application developers to not only remove the annoying messages which are presented to users but also to create more secure and user-friendlier applications, with less demand for critical privileges. As an increasing amount of software is now being built to support the UAC, it is likely that this tool will work much better in Windows 7 and beyond. Indeed, the overall UAC experience is much improved in the new OS. Fewer clicks and messages are presented to the user, while having control over matters that are happening on your machine is provided in a way which limits the number of user interaction is needed.

As I have already made clear, running a machine without higher privileges can sometimes be extremely challenging since many applications still expect this wide-ranging level of control in order to run correctly. Whatever the case, I don't recommend the disabling of the UAC. It is here to stay and we have to deal with it in the most appropriate and manageable way.

Increased support for strong authentication

Compared to the alternatives, working with passwords is a weak protection method. Brute force attacks, dictionary attacks etc., are some of the weaknesses of this approach. Indeed, for many organizations, single-factor authentication (user-id and password) is no longer sufficient and a multi-factor form (like smart cards) is increasingly being introduced. Two-factor authentication is something you know (a pin code), you are (fingerprint/ biometrics) or you carry, like a token or smartcard. All of this points to multi-factor authentication being the standard in the future.

Both Windows Vista and Windows 7 have built-in authentication support for the use of smart cards, but the latter makes it possible for developers to add their own customized methods, such as biometrics and tokens, more easily. It also provides enhancements to the Kerberos authentication protocol and smart card logons. By making it easier for developers to include such solutions, the security professional will have more choice when it comes to biometrics, smart cards, and other forms of strong authentication such as fingerprint readers.

In Vista, if you want to use fingerprint logon, you have to use software provided by the fingerprint sensor vendor. In the early days of the OS, every such vendor had its own drivers, software development kits (SDKs), and applications. This had some disadvantages in terms of overall experience and compatibility. In Windows 7, the operating system provides native support for fingerprint biometric devices through the Windows Biometric Framework (WBF).

The Windows Biometric Service (WBS) is part of this, and manages fingerprint readers and acts as an I/O proxy between client applications and the biometric device, meaning that programs cannot directly gain access to the biometric data.

In a similar way, the Biometric Frameworkprint makes it easier for developers to include biometric security in their applications. Also, there is a new item in the Control Panel which is to be used for managing fingerprints.

The combination of Windows 7 (Vista as well), Server 2008 and certificate lifecycle management means that there are some great opportunities to introduce more simplified, yet stronger, authentication solutions to your organization by working with smart cards or smart tokens and rolling out and using certificates from a (Microsoft) Public Key Infrastructure.

Windows 7 firewall

The Windows Firewall was introduced with Windows Vista, and at the time represented a major improvement over XP. As a result, it became a more serious competitor in the personal firewall market. Along with the former AntiGen product range (now called Forefront client security) this is really a development that requires further attention. Overall, the firewall in Windows 7 is only slightly better than the one in Windows Vista. It still supports filtering for outgoing traffic, as well as application-aware outbound filtering, which gives it full bi-directional control.

Furthermore, the Windows 7 firewall settings are configurable by way of the Group Policy, which simplifies the management experience in enterprise organizations.

There is an option to switch between Public, Home, and Work networks, and whenever you connect to a new network, Windows will ask what kind it is. Each network has its own firewall profile, which allows you to configure different firewall rules depending upon the security requirements of a user's location. You can use the Windows firewall with the Advanced Security's snap-in filter to display only the rules for specific locations. The corresponding firewall rule sets are Public (Public), Private (Home / Work), and Domain (when a domain-connected workstation detects a domain controller).

Where Vista distinguishes between Public and Private networks, Windows 7 works with Home and Work in the default interface. In fact, Windows 7 has three types of network locations:

A Home network for your own network at home where you take part in the home group. In these circumstances, network discovery allows you to see other computers and devices on your network and other network users to see your computer. A Work network is for offices or other work related networks. It has essentially the same features, except you are unable to join a home group. Finally, a Public network is available for working in public places. Your computer is not visible to others and traffic will be blocked.

Somewhat confusing is the fact that the naming of the networks in the Firewall MMC for more advanced options and filter settings has not changed.

Under the Windows Filtering Platform (WFP) architecture, APIs are available for the firewall. The idea is that third parties can take advantage of aspects of the Microsoft Windows Firewall in their own products.

Manage the advanced Firewall settings

Like in Windows Vista there is a GUI for the configuration of the Windows Firewall item in the Control Panel. This is rather simplistic and not particularly useful to enterprise organizations because you can configure the basic settings, but not enhanced features. Accordingly, for more in depth elements, the many Group Policy settings, which can be reached by firing up the Group Policy editor snap-in, can be used. Moreover, the new Windows Firewall can also be configured with a Windows Firewall MMC snap-in.

With this Windows Firewall with Advanced Security snap-in, administrators can configure settings for the Firewall on remote computers. In enterprise organizations, however, it is more likely that you will use the Group Policies to do this centrally.

For command-line configuration of the Firewall's advanced settings, commands within the netsh advfirewall can be used. This option can also be applied if you want to script changes.

DirectAccess feature

There's a new feature that could be significant in the longer term. The whole experience of using applications is changing, and with DirectAccess the intention is to give your machine seamless access to applications while you are on the road. This means that you wouldn't have to make an explicit VPN connection to "phone back home" because this new feature does it all for you in a stealth way. It's a new solution which would enable your remote machine to stay connected to your business network as long there is an (inter)network connection. This idea is not new but it's finally making way forward to practical implementations.

From a technology standpoint it has also some advantages. In this way, your company's IT department could have updates installed, change policies, apply hotfixes, update virus scanners, block immediately connections or access - all remotely without having to bother the user. I could spend a lot of time telling you more about this, but let me instead provide you with a direct link to the relevant technical documentation (bit.ly/96VGG) so you can read about it yourself.

Conclusion

As far as security is concerned, Windows 7 is an improvement on Windows Vista, although it retains much of its kernel architecture. Interesting and more strategic developments are the DirectAccess feature, in combination with a Windows Server 2008 infrastructure, and the improvements around the Network Access Protection features. This really is something to keep an eye on.
The development process has again taken a step forward. However, Windows Vista had more impact on businesses and needed a solid plan of approach before users started to migrate to it. With Windows 7, Microsoft wanted there to be compatibility with Vista, a performance increase and an improvement of certain crucial features which Vista already offered.

Windows 7 RC performs better than its predecessor, has an updated interface, and offers more fine-tuned functionality. Nevertheless, I haven't been able to discuss all of the detailed changes in security here. Combined features like Forefront Security, more Group Policies to give you greater control over specific settings, and Internet Explorer 8 are all important enhancements. Reading this article will, however, hopefully have given you an overview of the changes that Microsoft has planned for Windows 7.

Rob Faber, CISSP, CFI, CEH, MCTS, MCSE, is an information security consultant working for Atos Origin, a global company and international IT services provider based in the Netherlands. His specialization and main areas of interest are Windows platform security, Microsoft Directory Services, certificate infrastructures and strong authentication. He maintains his own weblog at www.icranium.com. You can reach him by e-mail at rob.faber@atosorigin.com, rob.faber@icranium.com or you can find him on the LinkedIn network.

Web 2.0 emerging threats

by Sam Masiello

There is one universal truth when it comes to Internet security: cyber criminals will leverage the vulnerabilities that exist within any technology in an effort to distribute spam, malware, and steal personal information. Less universal, however, are the definitions behind many of today's most important and widely used technology terms. As Internet technologies rapidly evolve it can lead to the coining of new, sometimes difficult to understand terms and acronyms on what seems like a daily basis.

In an effort to stay, or at least to appear as if they are staying, on the cutting edge businesses are constantly looking for ways to describe their products and services in such a way that it fits the definition of this new vernacular.

The end result of this jockeying for position leads to overly broad definitions of terms that are difficult to understand and leads to confusion amongst those on the outside looking in. The term "Web 2.0" is a recent example of one of those who definition has come to potentially mean so many different technologies that few do not consider themselves to be "Web 2.0" at this point.

Shaping the Web 2.0 platform

The Web 2.0 movement is not just about collaboration and user contributed content through wikis, personal and micro blogs, and podcasts. It is about how to send and receive information faster than ever before.

It is also about services that make the Web easier to use; breaking down the walls of what used to be considered functionality that was best performed by a desktop program and creating rich internet experiences that rivaled the functionality of their desktop counterparts.

Heading into the danger zone

As with most new technologies, the focus is initially on evolution and creating new, innovative features that will entice users and organizations to adopt them. Many companies want to be viewed as progressive so they jump on the bandwagon quickly not fully knowing or feeling educated about what bumps may lay on the road in front of them. Unfortunately, security and secure coding practices often play second fiddle while development is moving full-steam ahead so early adopters either have to look for ways to code around or fix known security issues or they are left holding the bag. This problem is often fed by a lack of best practices in the space.

Application coding flaws are not the only vulnerabilities that need to be considered when looking at the spectrum of threats introduced by a more information rich, collaborative internet. Some of the characteristics that make these technologies so powerful can also be their biggest weaknesses.

Despite the collaborative benefits that Web 2.0 sites like Twitter, Facebook, MySpace and many others provide, businesses now have the added burden of monitoring these types of sites for comments that could end up hurting their brand or reputation.

Many of these sites allow for the setup of groups where people with a common life thread (previous employees of the same organization, for instance) can gather and have a central place to collaborate. These groups can morph into community support forums where derisive comments from current or ex-employees or the leaking of confidential intellectual property can hurt not only a company's reputation but potentially also their competitive advantage.

An often understated risk with a more open Internet is the physical security danger that could result out of providing too much personal information online. Is your family going on vacation? Are your kids going to be home alone while you and your significant other enjoy a night on the town? Are there pictures of you online that some might find offensive? Any of these scenarios could result in a physical security risk with catastrophic consequences.

It is also important to consider that since social networking sites are so commonplace (Facebook currently has over 200 million active users), employers are now also using them as part of routine background checks. The key takeaway from this point is to not include information about yourself that could end up damaging your personal reputation.

The Clickjacking Threat – Fact vs FUD

Clickjacking is a Web 2.0 introduced browser and application design flaw that allows for malicious content to be overlaid on top of a legitimate application. This means that if a legitimate application is compromised by a Clickjacking exploit an unsuspecting user could be clicking on a malicious application created by a cyber criminal that is performing actions on the user's behalf in the background. These actions could range from the seemingly innocuous to disabling application security settings and data theft.

One of the ways that a Clickjacking exploit can occur on a web site is by using a technology frequently used in Web 2.0 sites called Dynamic HTML (DHTML). One of the key features of DHTML is the incorporation of the Z-axis into a web page. "Web 1.0" sites with static HTML content can generally be thought of as having been rendered in a two-dimensional plane across the X and Y axes.

Content had height and width only. With the inclusion of the Z-axis web pages can now also have depth. That means that content can be layered on top of other content. This technique has frequently been implemented using float-overs that cover what you might be trying to read on a web page. This often manifests itself on legitimate sites in the form of an invasive survey invitation or an advertisement. Although not malicious, this method to grab a user's attention is generally considered to be an annoyance. In an exploited site or application, the results could be much more sinister. Up to this point there have been several high profile Clickjacking vulnerabilities identified in widely used applications such as Mozilla's Firefox and Google's Chrome browsers and

Adobe's Flash Player. Few serious exploits have been found in the wild taking advantage of these vulnerabilities, however an absence of an exploit is not intended to minimize the seriousness of the threat. A recent vulnerability found on the popular micro-blogging web site Twitter resulted in unintended messages, or "tweets", being sent out by users who clicked on a web site button labeled "Don't Click" that was actually an exploit of the software flaw. This particular exploit did not result in theft of account credentials or other personal information, but served as a powerful proof of concept that Clickjacking exploits could easily be used for much more malicious purposes than sending out messages through a web site.

Despite their potential for damage, Clickjacking vulnerabilities can be mitigated easily by web site developers as well as end users. One of the methods that site developers can employ is known as frame busting JavaScript. Recall that one way Clickjacking manifests itself is through malicious content being rendered on top of legitimate content. If the code sitting behind a web site regularly checks to ensure that the legitimate content layer is always executing as the top layer on the page, it cannot be overlaid by a rogue application. This method is not foolproof, however as users may use plug-ins or change their browser settings to disallow JavaScript, thus defeating this countermeasure. As a user of a Mozilla based browser protection against Clickjacking can be installed via a user installed plug-in. The recently released Internet Explorer 8 browser has a form of Clickjacking protection native to the application. No previous versions of Internet Explorer offer any protection against this threat. Browser developers can get into the game as well. Similar to how browsers give users the option to globally enable, prompt for user input, or globally disable third party cookies, the same options could be given for how to handle cross-domain inline frames, a popular method for exploiting Clickjacking vulnerabilities on web sites.

Conclusion

Online threats continue to evolve every day and the social engineering tactics that cyber criminals are using to lure users into infecting their personal computers with malware or giving up their sensitive information are getting more and more difficult to identify to the untrained eye. Today's hackers are not motivated by fame or notoriety amongst their peers; rather they are motivated by money. They are also not always the most technical people you will encounter. A full service underground economy exists whereby credit card numbers and bank web site logins are traded in a bazaar-like environment, thus lowering the bar of technical expertise required to get involved in criminal activity.

Armed with the knowledge that new technologies are built before they are built securely, cyber criminals have identified Web 2.0 sites and technologies as a primary target in 2009. Clickjacking is one of the more serious of those threats because of the level of stealth that can be employed when a vulnerable application is exploited. The user being victimized will likely have no idea that they may be interfacing with a malicious application setup for the sole purpose of compromising their sensitive data.

From a user's perspective, it is also important to remember that the sky is not falling. Despite the attention that Clickjacking has been getting there are currently very few exploits in the wild taking advantage of vulnerable applications and those exploits that do exist are mostly proof of concept quality. This is not to trivialize the potential for more widespread activity, but rather to temper the amount of fear, uncertainty, and doubt that almost inevitably arises when a particular threat receives a lot of attention.

Sam Masiello is the VP of Information Security at MX Logic (www.mxlogic.com) where he oversees the MX Logic Threat Operations Center. In this role, he represents the company's primary resource for monitoring and predicting threat trends, offering insights to customers about potential threat vulnerabilities, and recommending new technologies to enhance email and Web security. Masiello has more than 18 years of e-mail systems and IT management experience, including nearly 10 years network and security systems management. He is an active member of the international MAAWG (Messaging Anti-Abuse Working Group) organization and is a current co-chairperson of the Zombie and Botnet subcommittees.

Cyber Security Malaysia || SecureAsia@KL

Conference & Exhibition

7 & 8 July 2009 • Kuala Lumpur Convention Centre

www.informationsecurityasia.com

Cyber Security Malaysia and ISC² is proud to bring you Asia's definitive information security Conference & Exhibition.

SPONSOR or EXHIBIT at this niche event where we bring you the target audience under one roof.

The Exhibition is set to show off the latest technology, products and professional services in information security. Our exhibitor profile includes; Enterprise Security Management, Business Continuity Management, Encryption Application/Devices, Information Risk Management, Software Application Developers, CIIP Solutions, Disaster Recovery and many others.

Happenings at a glance:

- VISTA Forensics Workshop for Law Enforcement Agencies
- Critical Information Infrastructure Protection (CIIP) Workshop
- Information Security Leadership Awards (ISC)²
- Internet Security Awareness Conference

Secure your participation at this premier information security event!

Exhibition Enquiries
Ms. Karen Dass
karendass@protempgroup.com
Tel. +603.6140.6666

Conference Enquiries
Ms. Michelle Lim
michelle@protempgroup.com
Tel. +603.6140.6666

Brought to you by: CyberSecurity MALAYSIA · 20 (ISC)² years of excellence · protemp ISO 9001 Certified Professional Trade Exhibition & Meeting Planners

Endorsed by: MOSTI

Gold Sponsor: IBM

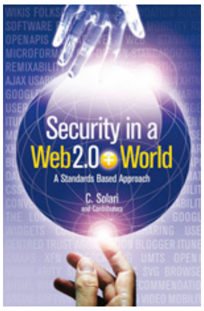
Media Partner: HELP NET SECURITY WWW.NET-SECURITY.ORG

Latest additions to our bookshelf

Security in a Web 2.0+ World: A Standards-Based Approach

By Carlos Curtis Solari

Wiley, ISBN: 0470745754



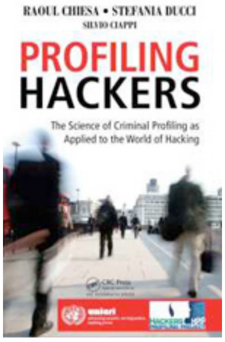
Security Standards for a Web 2.0+ World clearly demonstrates how existing security solutions are failing to provide secure environments and trust between users and among organizations. Bringing together much needed information, and a broader view on why and how to deploy the appropriate standards.

This book supports a shift in the current approach to information security, allowing companies to develop more mature models and achieve cost effective solutions to security challenges.

Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking

By Raoul Chiesa, Stefania Ducci, Silvio Ciappi

Auerbach Publications, ISBN: 1420086936



Providing in-depth exploration into this largely uncharted territory and focusing on the relationship between technology and crime, this volume offers insight into the hacking realm by telling attention-grabbing tales about the bizarre characters who practice hacking as an art.

Applying the behavioral science of criminal profiling to the world of internet predators, the text addresses key issues such as the motivation behind hacking and whether it is possible to determine a hacker's profile on the basis of his behavior or types of intrusion.

The CERT C Secure Coding Standard

By Robert C. Seacord

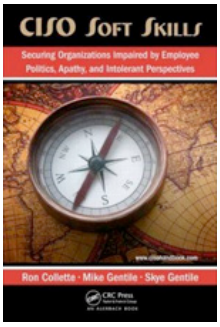
Addison-Wesley Professional, ISBN: 0321563212

This book is an essential desktop reference documenting the first official release of The CERT C Secure Coding Standard. The standard itemizes those coding errors that are the root causes of software vulnerabilities in C and prioritizes them by severity, likelihood of exploitation, and remediation costs. Each guideline provides examples of insecure code as well as secure, alternative implementations. If uniformly applied, these guidelines will eliminate the critical coding errors that lead to buffer overflows, format string vulnerabilities, integer overflow, and other common software vulnerabilities.

CISO Soft Skills: Securing Organizations Impaired by Employee Politics, Apathy, and Intolerant Perspectives

By Ron Collette, Michael Gentile, Skye Gentile

Auerbach Publications, ISBN: 1420089102

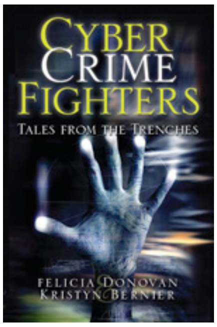


This book presents tools that empower organizations to identify those intangible negative influences on security that plague most organizations, and provides further techniques for security professionals to identify, minimize, and overcome these pitfalls within their own customized situations. The book also discusses some proactive techniques that CISOs can utilize in order to effectively secure challenging work environments. Reflecting the experience and solutions of those that are in the trenches of modern organizations, this volume provides practical ideas that can make a difference in the daily lives of security practitioners.

Cyber Crime Fighters: Tales from the Trenches

By Felicia Donovan, Kristyn Bernier

Que, ISBN: 0789739224



Written by cyber crime investigators, the book takes you behind the scenes to reveal the truth behind Internet crime, telling shocking stories that aren’t covered by the media, and showing you exactly how to protect yourself and your children. This is the Internet crime wave as it really looks to law enforcement insiders: the truth about crime on social networks and YouTube, cyber stalking and criminal cyber bullying, online child predators, identity theft, even the latest cell phone crimes. Here are actual cases and actual criminals, presented by investigators who have been recognized by the FBI and the N.H. Department of Justice.

Chained Exploits: Advanced Hacking Attacks from Start to Finish

By Andrew Whitaker, Keatron Evans, Jack B. Voth

Addison-Wesley Professional, ISBN: 032149881X

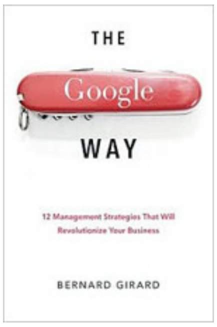
Chained Exploits demonstrates this advanced hacking attack technique through detailed examples that reflect real-world attack strategies, use today's most common attack tools, and focus on actual high-value targets, including credit card and healthcare data.

Relentlessly thorough and realistic, this book covers the full spectrum of attack avenues, from wireless networks to physical access and social engineering.

The Google Way: How One Company is Revolutionizing Management As We Know It

By Bernard Girard

No Starch Press , ISBN: 1593271840

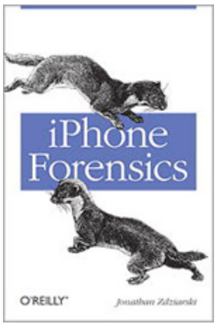

THE
Google
WAY
12 Management Strategies That Will Revolutionize Your Business
BERNARD GIRARD

Management consultant Bernard Girard has been analyzing Google since its founding and now in this book he explores Google's innovations in depth - many of which are far removed from the best practices taught at the top business schools. You'll see how much of Google's success is due to its focus on users and automation. You'll also learn how eCommerce has profoundly changed the relationship between businesses and their customers, for the first time giving customers an important role to play in a major corporation's growth.

iPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets

By Jonathan Zdziarski

O'Reilly Media, ISBN: 0596153589



With iPhone use increasing in business networks, IT and security professionals face a serious challenge: these devices store an enormous amount of information. If your staff conducts business with an iPhone, you need to know how to recover, analyze, and securely destroy sensitive data.

iPhone Forensics supplies the knowledge necessary to conduct complete and highly specialized forensic analysis of the iPhone, iPhone 3G, and iPod Touch.

Web Security Testing Cookbook

By Paco Hope, Ben Walther

O'Reilly Media, ISBN: 0596514832

Systematic Techniques to Find Problems Fast
Web Security Testing Cookbook
O'REILLY
Paco Hope & Ben Walther

The recipes in this book demonstrate how developers and testers can check for the most common web security issues, while conducting unit tests, regression tests, or exploratory tests. Unlike ad hoc security assessments, these recipes are repeatable, concise, and systematic-perfect for integrating into your regular test suite. Recipes cover the basics from observing messages between clients and servers to multi-phase tests that script the login and execution of web application features.

Cisco Secure Firewall Services Module (FWSM)

By Ray Blair, Arvind Durai

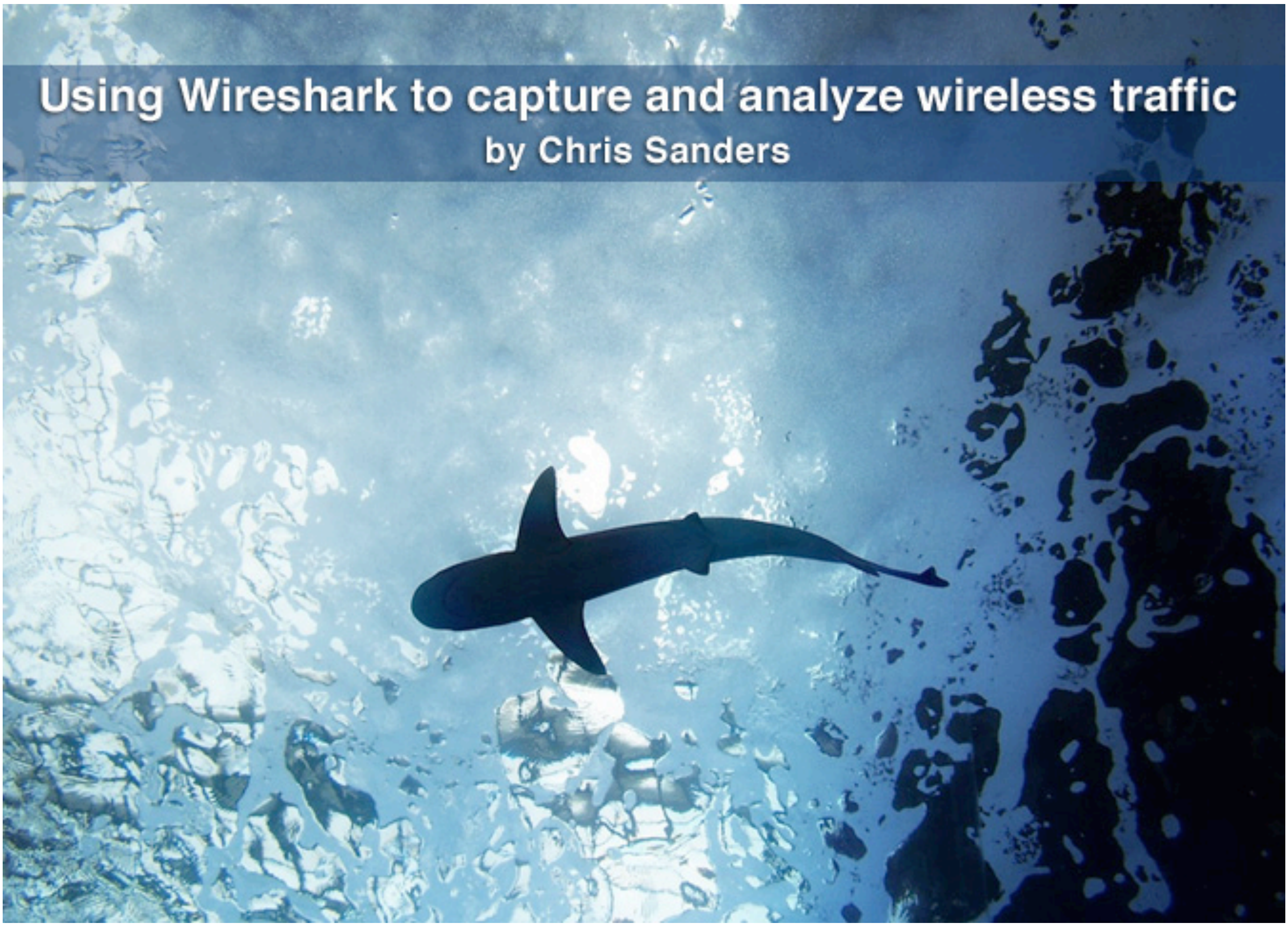
Cisco Press, ISBN: 1587053535

CISCO
SECURITY
Cisco Secure Firewall Services Module (FWSM)
Best practices for securing networks with FWSM

Cisco Secure Firewall Services Module (FWSM) covers all aspects of the FWSM. The book provides a detailed look at how the FWSM processes information, as well as installation advice, configuration details, recommendations for network integration, and reviews of operation and management. This book provides you with a single source that comprehensively answers how and why the FWSM functions as it does. This information enables you to successfully deploy the FWSM and gain the greatest functional benefit from your deployment.

Using Wireshark to capture and analyze wireless traffic

by Chris Sanders



The tricky thing about a wireless network is that you can't always see what you're dealing with. In a wireless network, establishing connectivity isn't as simple as plugging in a cable, physical security isn’t nearly as easy as just keeping unauthorized individuals out of a facility, and troubleshooting even trivial issues can sometimes result in a few expletives being thrown in the general direction of an access point. That being said, it shouldn't come as a surprise that analyzing packets from a wireless network isn't as uninvolved as just firing up a packet sniffer and hitting the capture button.

In this article I'm going to talk about the differences between capturing traffic on a wireless network as opposed to a wired network.

I'll show you how to capture some additional wireless packet data that you might not have known was there, and once you know how to capture the right data, I'm going to jump into the particulars of the 802.11 MAC layer, 802.11 frame headers, and the different 802.11 frame types.

The goal of this article is to provide you with some important building blocks necessary for properly analyzing wireless communications.

Wired vs. wireless networks

There are a lot of obvious differences between wireless and wired networks. On a wired network each node has its own individual cable allowing for predictable performance and a dedicated amount of bandwidth both upstream and downstream.

A wireless network is a shared medium meaning that all nodes on that network compete for bandwidth over a limited spectrum. It is because of this shared nature that a wireless network employs a different means of handling the transmission of data.

WIRED	WIRELESS
CSMA/CD	CSMA/CA
Dedicated bandwidth	Shared medium
Predictable	Performance decreases on load

The sharing of the wireless medium is done through an access method called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). CSMA/CA is implemented as an alternative to Carrier Sense Multiple Access with Collision Detection (CSMA/CD), which is used in wired networks. An Ethernet network has the ability to transmit data while monitoring the network for collisions. At this point it can pause, wait a certain period of time, and resend the data again. In a wireless network, a wireless network interface card cannot transmit and receive data synchronously, so it must use collision avoidance rather than collision detection. This process is handled at layer two of the OSI model.

Layer 2: Where the meat is

The second layer of the OSI model, often called the Data Link layer or the MAC layer, is where 802.11 implements all of the features that make communication through the air possible. This includes tasks such as addressing, authentication and association, fragmentation, arbitration (CSMA/CA), and encryption. All of these things are what make the data link layer important to us, and what we will be spending our time together here examining.

The tricky thing about the wireless data link layer is that these frames aren’t collected just by loading up Wireshark (our packet sniffer of choice for this article) and doing a standard capture.

I know what you're thinking: ”I’ve capture packets from my wireless NIC before and it shows layer two information just like any other packet!” Well, you are correct in saying that Wireshark displays layer two frame information for packets captured from your wireless NIC. However, it only displays the components that it would display for an Ethernet network; your source and destination MAC addresses. There is a whole heap of information you are not seeing, and in order the get that information you have to make use of a feature called monitor mode.

Monitor mode is one of many modes that a wireless NIC can be set to. In monitor mode, a wireless NIC does not transmit any data, and only captures data on the channel it is configured to listen on. When set on monitor mode Wireshark will capture and display the entire contents of an 802.11 wireless layer two frame. How you utilize monitor mode is dependent upon the drivers available for your wireless NIC and your operating system of choice.

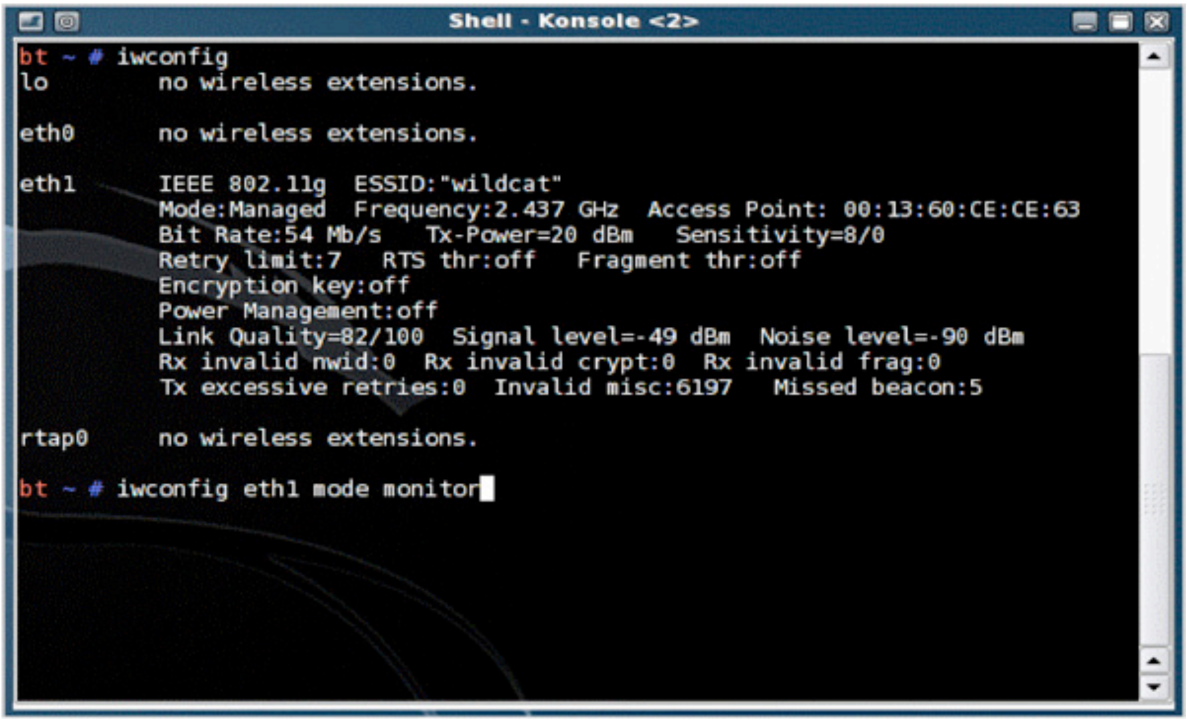
Using monitor mode in Linux

In Linux, a great majority of wireless drivers support monitor mode functionality, so changing your wireless NIC into monitor mode is a fairly simple process. Most of the wireless NIC drivers in Linux support the Linux Wireless Extensions interface so that you can configure them directly from a command shell with no additional software required. In order to determine if the wireless NIC you are using is supported by these wireless extensions, you can use the command iwconfig.

As you can see in the iwconfig output below, the eth1 interface supports Linux Wireless Extensions and displays information about the current configuration of the wireless NIC. We can easily see that the card is associated to a network with an SSID of “SANDERS” and that the card is in managed mode. In order to change the card to monitor mode, switch to a root shell and use this command:

```
# iwconfig eth1 mode monitor
```

You can verify the mode of the wireless NIC by running the iwconfig command once more. At this point you should be able to capture the appropriate data link layer wireless information.



```
bt ~ # iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      IEEE 802.11g  ESSID:"wildcat"
          Mode:Managed  Frequency:2.437 GHz  Access Point: 00:13:60:CE:CE:63
          Bit Rate:54 Mb/s   Tx-Power=20 dBm   Sensitivity=8/0
          Retry limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=82/100  Signal level=-49 dBm  Noise level=-90 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:6197   Missed beacon:5

rtap0     no wireless extensions.

bt ~ # iwconfig eth1 mode monitor
```

It is important to note that not every Linux wireless NIC driver supports Linux Wireless Extensions. However, due to the open source nature of typical Linux drivers, most other drivers have been “modified” so that they can be put into monitor mode through some alternative means. If your wireless NIC doesn’t support Linux Wireless Extensions then you should be able to do a quick Google search to find an alternative means of getting to monitor mode.

As you may remember reading earlier, one of the distinct differences between a wired and wireless connection is that the wireless connection operates on a shared spectrum.

This spectrum is broken up into several different channels in order to prevent interference from different systems in the same geographical area. This being the case, each node on a wireless network may only use one channel at a time to transmit or receive. This means that our wireless NIC in monitor mode must be explicitly configured to listen on whatever channel we want to grab packets off of. In order to set your wireless NIC to monitor on channel 6, you would use the command:

```
# iwconfig eth1 channel 6
```

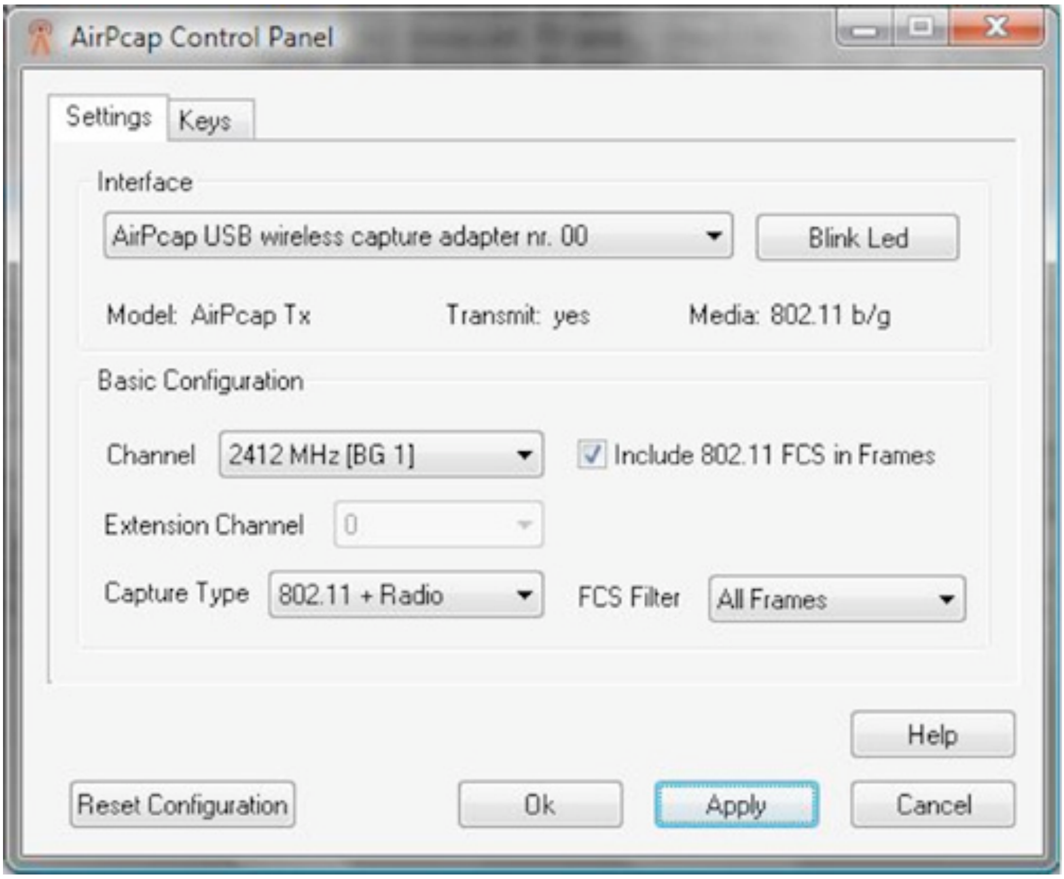
In this scenario, you would substitute whatever the assigned name for your wireless NIC interface is for eth1, and the numbers 1-11 (US) or 1-14 (International) in for the channel number.

Using an AirPcap device in Windows

Capturing wireless traffic in a Windows environment is unfortunately not as easy as a setting change. As with most Windows-based software, drivers in Windows are often not open source and do not allow for configuration change into monitor mode. With this in mind, we must use a specialized piece of hardware known as an AirPcap device.

Developed by CACE Technologies, employer of the original creator of Wireshark, an AirPcap device is essentially a USB 802.11 wireless adapter that is bundled with specialized software that will allow the device to be used in monitor mode.

Once you have obtained an AirPcap device you will be required to install the software on the accompanying CD to your analysis computer. The installation is a fairly straightforward accepting of the licensing agreement and clicking next a few times, so we won't cover that here. Once you have the software installed, you are presented with a few options you can configure in the AirPcap Control Panel.



Interface

AirPcap USB wireless capture adapter nr. 00

Model: AirPcap Tx Transmit: yes Media: 802.11 b/g

Basic Configuration

Channel: 2412 MHz [BG 1]

☑ Include 802.11 FCS in Frames

Extension Channel: 0

Capture Type: 802.11 + Radio

FCS Filter: All Frames

As you can see from the screenshot above, there isn't an incredible amount of configuration to be done on the AirPcap device. These configuration options are stored on a per adapter basis.

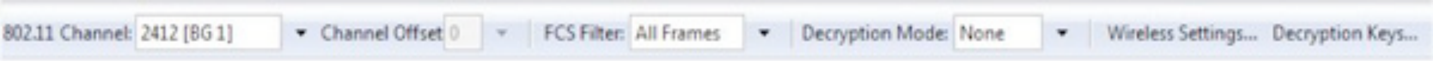
The configurable options include:

- **Interface** - Select the device you are using for your capture here. Some advanced analysis scenarios may require you to use more than one AirPcap device to sniff simultaneously on multiple channels.
- **Blink LED** - Clicking this button will make the LED lights on the AirPcap device blink. This is primarily used to identify the specific adapter you are using if you are using multiple AirPcap devices.
- **Channel** - In this field, you select the channel you want AirPcap to listen on.
- **Extension Channel** - This option is only available on 802.11n capable AirPcap devices (AirPcap nX) and allows you to select an extension channel.
- **Capture Type** - The options are 802.11 Only, 802.11+Radio, and 802.11+PPI. The 802.11 Only option includes the standard 802.11 packet header on all capture packets. The 802.11 + Radio option includes this header and also a radiotap header, which contains additional information about the packet, such as data rate, frequency, signal level, and noise level. The 802.11+PPI option includes all of the previously mentioned data, along with information for multiple antennas when supported.
- **Include 802.11 FCS in Frames** - By default, some systems strip the last four checksum bits from wireless packets. This checksum, known as a Frame Check Sequence (FCS), is used to ensure that packets have not been corrupted during transmission. Unless the application you are using for interpreting packet captures has difficulty decoding packets with FCS, check this box to include the FCS checksums.
- **FCS Filter** - This option will allow you to filter out packets based upon whether they have a valid or invalid FCS.

Aside from these configuration options you will also notice a Keys tab where you can enter and manage WEP keys for the decryption of WEP encrypted traffic. Most up-to-date wireless networks will not being using WEP for encryption, and because of this you may initially come to the conclusion that the AirPcap device is limited and/or dated, but this is not the case. It is important to realize that AirPcap supports decryption of wireless traffic in two modes. Driver mode, configurable from the AirPcap Control Panel, only supports WEP.

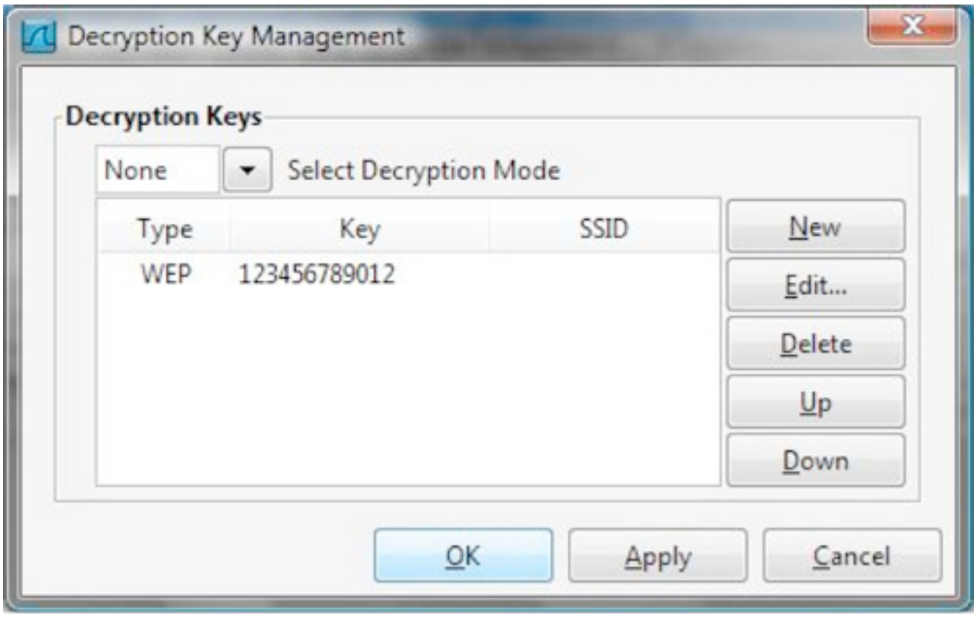
That being the case, it is recommend that decryption keys be configured using Wireshark mode, which supports WEP, WPA, and WPA2, and is managed from the wireless toolbar inside of Wireshark.

The wireless toolbar is used to configure a lot of the options we have already learned about within the Wireshark program itself. You can enable this toolbar when you have an AirPcap adapter plugged into your analysis computer by opening Wireshark, going to the View drop-down menu, and placing a checkmark next to the Wireless Toolbar option.



802.11 Channel: 2412 [BG 1]
Channel Offset 0
FCS Filter: All Frames
Decryption Mode: None

As you can immediately determine, this toolbar makes a lot of the configuration options from the AirPcap device readily available from within Wireshark. The only major difference of any concern to us is the added functionality of the decryption section. In order to take advantage of this, you will need to set the Decryption Mode drop-down box to Wireshark, and add your appropriate encryption key by clicking the Decryption Keys button, clicking New, selecting the key type, and entering the key itself.



Decryption Key Management

Decryption Keys

None — Select Decryption Mode

Type	Key	SSID
WEP	123456789012	

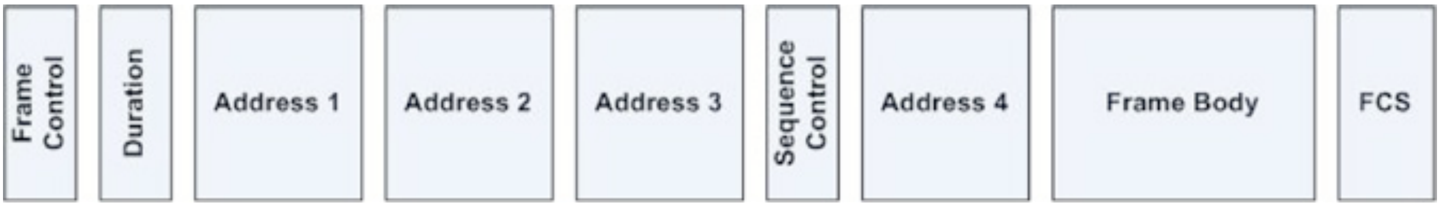
The 802.11 header

When you think about it, Ethernet really has it easy. All the MAC layer has to do is worry about a single source and destination address. An 802.11 MAC header on the other hand, has a lot more going on.

The illustration on the following page depicts the basic components of the MAC header.

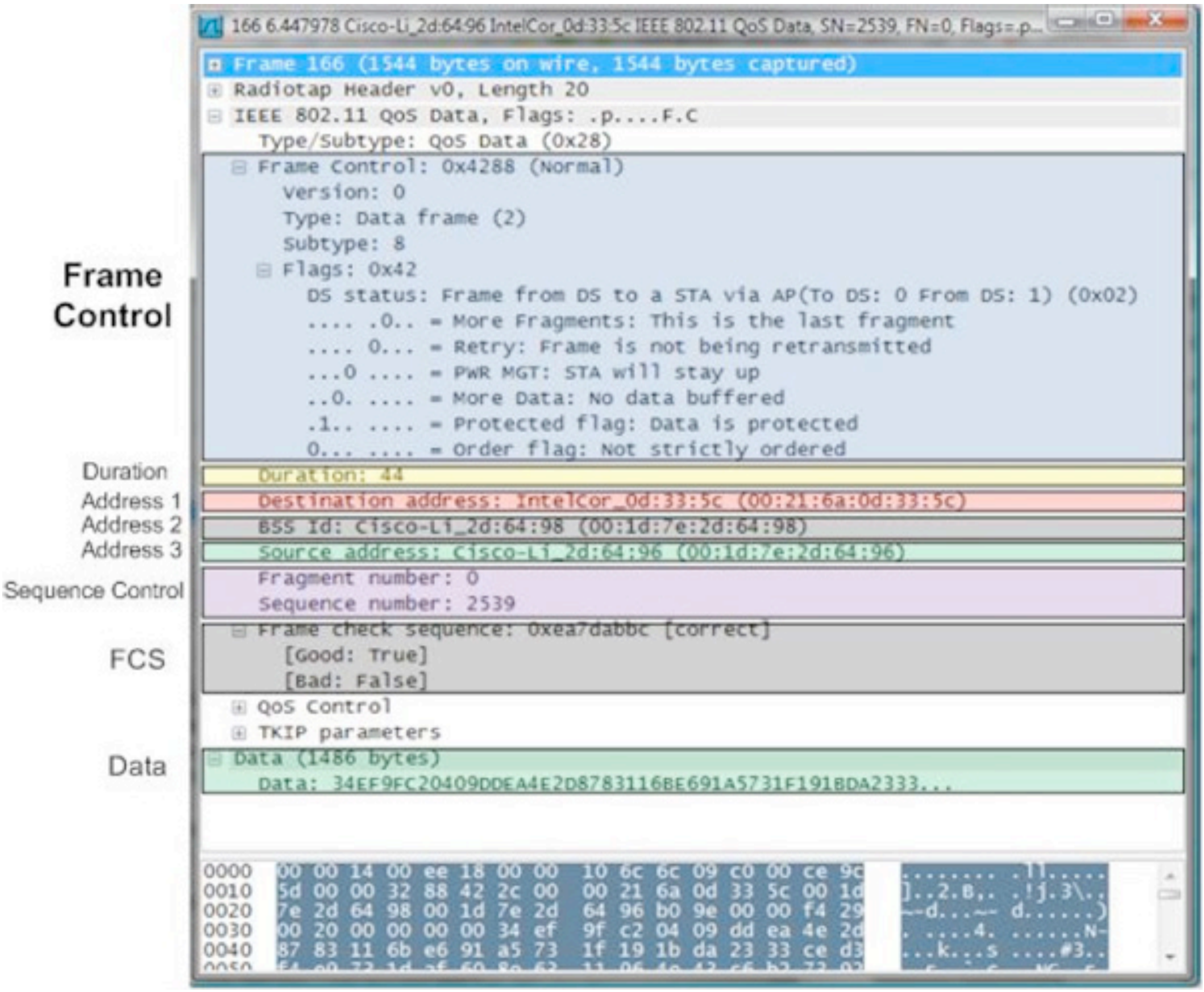
- **Frame Control** - This section specifies the type and subtype of the MAC frame, as well as other options such as whether or not the packet is a fragment, whether power management is being used, or if WEP encryption is being used. There are three main types of MAC frames. First, management frames are used for tasks such as associating to an access point. Control frames are second and they are used to control the flow of data and handle things such as acknowledgement packets. Data frames are the final type and they contain the data being transmitted across the transmission medium.

- **Duration** - When this is used with a data frame this will specify the duration of the frame.
- **Address 1** - Source address
- **Address 2** - Destination address
- **Address 3** - Receiving station address (destination wireless station)
- **Address 4** - Transmitting wireless station
- **Frame Body** - Data contained in the frame
- **FCS** - The Frame Check Sequence discussed earlier.



Analyzing Wireshark dissection of the 802.11 header

With this background knowledge we can take a look at an individual packet that has been dissected by Wireshark and find the different components of the wireless header. The frame depicted below is a standard wireless data frame. We can immediately determine this by looking at the Type listing under the Frame Control section of the packet.



166 6.447978 Cisco-Li_2d:64:96 IntelCor_0d:33:5c IEEE 802.11 QoS Data, SN=2539, FN=0, Flags=.p...

```
⊞ Frame 166 (1544 bytes on wire, 1544 bytes captured)
⊞ Radiotap Header v0, Length 20
⊟ IEEE 802.11 QoS Data, Flags: .p....F.C
    Type/Subtype: QoS Data (0x28)
  ⊟ Frame Control: 0x4288 (Normal)
      Version: 0
      Type: Data frame (2)
      Subtype: 8
    ⊟ Flags: 0x42
        DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x02)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .1.. .... = Protected flag: Data is protected
        0... .... = Order flag: Not strictly ordered
    Duration: 44
    Destination address: IntelCor_0d:33:5c (00:21:6a:0d:33:5c)
    BSS Id: Cisco-Li_2d:64:98 (00:1d:7e:2d:64:98)
    Source address: Cisco-Li_2d:64:96 (00:1d:7e:2d:64:96)
    Fragment number: 0
    Sequence number: 2539
  ⊟ Frame check sequence: 0xea7dabbc [correct]
      [Good: True]
      [Bad: False]
  ⊞ QoS Control
  ⊞ TKIP parameters
⊟ Data (1486 bytes)
    Data: 34EF9FC20409DDEA4E2D8783116BE691A5731F191BDA2333...

0000  00 00 14 00 ee 18 00 00  10 6c 6c 09 c0 00 ce 9c   ........ .ll.....
0010  5d 00 00 32 88 42 2c 00  00 21 6a 0d 33 5c 00 1d   ]..2.B,. .!j.3\..
0020  7e 2d 64 98 00 1d 7e 2d  64 96 b0 9e 00 00 f4 29   ~-d...~- d......)
0030  00 20 00 00 00 00 34 ef  9f c2 04 09 dd ea 4e 2d   . ....4. ......N-
0040  87 83 11 6b e6 91 a5 73  1f 19 1b da 23 33 ce d3   ...k...s ....#3..
```

As I mentioned previously, the Frame Control section of the packet contains a lot of information and you can see all of these options here. Looking further into this packet you should be able to clearly find all of the sections of the packet.

The great thing about analyzing wireless packets is that what you see is what you get, and the packet you just looked at is what the great majority of wireless packets will look like. The defining difference between one packet and another is the type and subtype of that packet.

Management frames such as a Beacon will still contain all of the information listed above, but rather than the data portion of the packet they will contain the data specific to that frame type. You can view a complete listing of 802.11 frame types by viewing the 802.11 standards document (bit.ly/f2l0p).

A few frame types of interest include:

- Management Type 0
    - Subtype 0000 – Association Request
    - Subtype 0001 – Association Response
    - Subtype 1000 – Beacon
    - Subtype 1010 Disassociation
    - Subtype 1011 Authentication
    - Subtype 1100 De-authentication
- Control Type 01
    - Subtype 1011 – Request to Send (RTS)
    - Subtype 1100 – Acknowledgement
- Data Type 10
    - Subtype 0000 - Data.

Wrap up

This is by no means a definitive guide on analyzing wireless traffic, but it should give you all of the information you need to get off on the right foot. We have covered why capturing layer two traffic is important to effectively analyzing wireless communications as well as the structure of these 802.11 frames.

The best thing you can do with the information presented here is to begin capturing packets on your own wireless networks. Once you start looking at common tasks such as associating to a network or completing an authentication request at the packet level, you should really get a sound grasp on what's happening in the air around you.

Chris Sanders is a network consultant based in western Kentucky. Chris writes and speaks on various topics including packet analysis, network security, Microsoft server technologies, and general network administration. His personal blog at www.chrissanders.org contains a great deal of articles and resources on all of these topics. Chris is also the founder and director of the Rural Technology Fund (www.ruraltechfund.org), a non-profit organization that provides scholarships to students from rural areas who are pursuing careers in information technology.

Q&A: Paul Cooke on Windows 7

by Mirko Zorz

Paul Cooke is the Director of Windows Product Management at Microsoft. In this interview he discusses Windows 7 security.

With such an immense user base, there must be a myriad of details you need to work on. What's the most significant security challenge Microsoft tackled while developing Windows 7?

No matter how good the technical protections are, it is important to help the user to make the best decisions that will help keep them safe from malicious users and software.

Changes in UAC are an example of this sort of work to reduce the number of prompts all users will see while helping move the ecosystem to an environment where everyone can run as a standard (non-privileged) user by default. Other great examples include the new SmartScreen Filter and Clickjacking prevention technologies that are included with Windows 7 through Internet Explorer 8.

Is the rising skill level of malicious users combined with an increasing variety of attacks becoming a significant problem when developing something as demanding as a new version of Windows?

Clearly, the sophistication and motives of malicious users has changed dramatically over the past few years. We continue to work with security researchers and others to understand not only today’s threat landscape but tomorrow’s as well. This helps us build protections into the system that help secure your PC from acquiring and running code without the user’s consent.

In addition, we continue to make sure Windows is resistant to both tampering and circumventing the protections within the system.

What has been the response of the security community to Windows 7 releases so far? Are you satisfied with the feedback? What have you learned?

The response by the security community to Windows 7 has been great so far. There has been some confusion about UAC and the changes we made there, but it provides a great example of how we can listen and work with the community to provide a product we can all be proud of.

What are the core differences between Windows 7 and Windows Vista when it comes to security?

Windows 7 builds upon the security foundations of Windows Vista and retains the development, including going through the Security Development Lifecycle, and technologies that made Windows Vista the most secure Windows operating system ever released. Core security enhancements from Vista like User Account Control (UAC), Kernel Patch Protection, Windows Service Hardening, Address Space Layout Randomization (ASLR), and Data Execution Prevention (DEP), etc. are all retained.

In addition, we have added new security features like AppLocker to help control the applications that run in their environment. We have enhanced the core BitLocker Drive Encryption to make it easier for IT to deploy and manage the technology in their environment. In addition, we have responded to customer requests to extended support for BitLocker to removable storage devices through BitLocker To Go.

Finally, Windows 7, coupled with Internet Explorer 8, provides flexible security protection against malware and intrusions for the proliferation of web based attacks that occur today.

The response by the security community to Windows 7 has been great so far.

Features that remote workers will appreciate are DirectAccess and BranchCache. How do they work and how do they secure the data?

DirectAccess is a breakthrough technology that enables workers who have Internet access to seamlessly and securely connect to their corporate network. DirectAccess works by automatically establishing bi-directional, secure connections from client computers to the corporate network. It is built on a foundation of proven, standards-based technologies like Internet Protocol security (IPsec), which is a protocol that helps secure IP-based traffic through authentication and encryption, and Internet Protocol version 6 (IPv6). IPsec is used to authenticate both the computer and user, allowing IT to manage the computer before the user logs on and IT can require a smart card for user authentication if they desire. DirectAccess also leverages IPsec to provide AES encryption for communications across the Internet.

BranchCache can help increase network responsiveness of centralized applications when accessed from remote offices, giving users in those offices the experience of working on your local area network. BranchCache also helps reduce wide area network (WAN) utilization. When BranchCache is enabled, a copy of data accessed from intranet Web and file servers is cached locally within the branch office. When another client on the same network requests the file, the client downloads it from the local cache without downloading the same content across the WAN. This is done without decreasing the security of the data—access controls are enforced on cached files in the same way they are on original files.

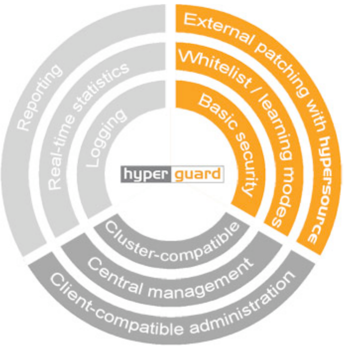
Many believe patch releases should be more frequent. Do you have any plans to intensify announcements after Windows 7 is released?

We continually evaluate the frequency in which we release security updates but we have no news to share at this time.

Save the Date!
USENIX '09

RSA Conference 2009 took place in San Francisco during April. The industry's most pressing information security issues were addressed by more than 540 speakers, in 17 class tracks containing more than 220 educational sessions. More than 325 of the industry's top companies exhibited the latest information security technologies. What follows are some of the many products presented at the show.

Cloud application security SaaS solution from Art of Defence



Art of Defence launched the Hyperguard SaaS solution which will enable cloud technology providers to offer security solutions at the web application layer. Hyperguard SaaS is built on Art of Defence's dWAF technology, suited for the diverse platform and infrastructure scenarios required to deliver applications through a cloud. Using the OWASP best practice recommendations as a starting point, Hyperguard adds high-level proactive security features such as secure session management, URL encryption and a web authentication framework. (www.artofdefence.com)

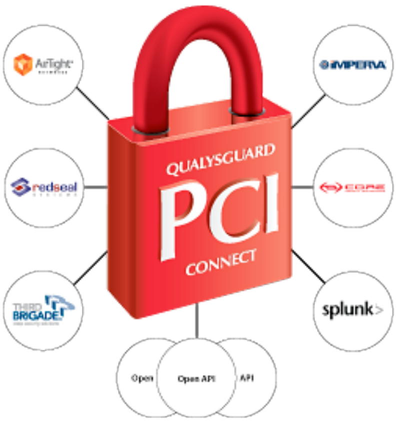
Encrypted USB drive solution with anti-malware capability

Mobile Armor added anti-malware support to its KeyArmor product group. The solution is a military level encrypted USB drive managed by the Mobile Armor enterprise policy console, PolicyServer. KeyArmor USB drives are FIPS 140-2 Level 2 validated using on processor AES hardware encryption. KeyArmor now independently provides protection against viral and malware threats. (www.mobilearmor.com)

First integrated tokenization solution for business

The nuBridges Protect Token Manager is a data security software solution to combine universal Format Preserving Tokenization, encryption and unified key management in one platform-agnostic package. The product is for enterprises that need to protect volumes of personally identifiable information and payment card numbers from theft, while simplifying compliance management. (www.nubridges.com)

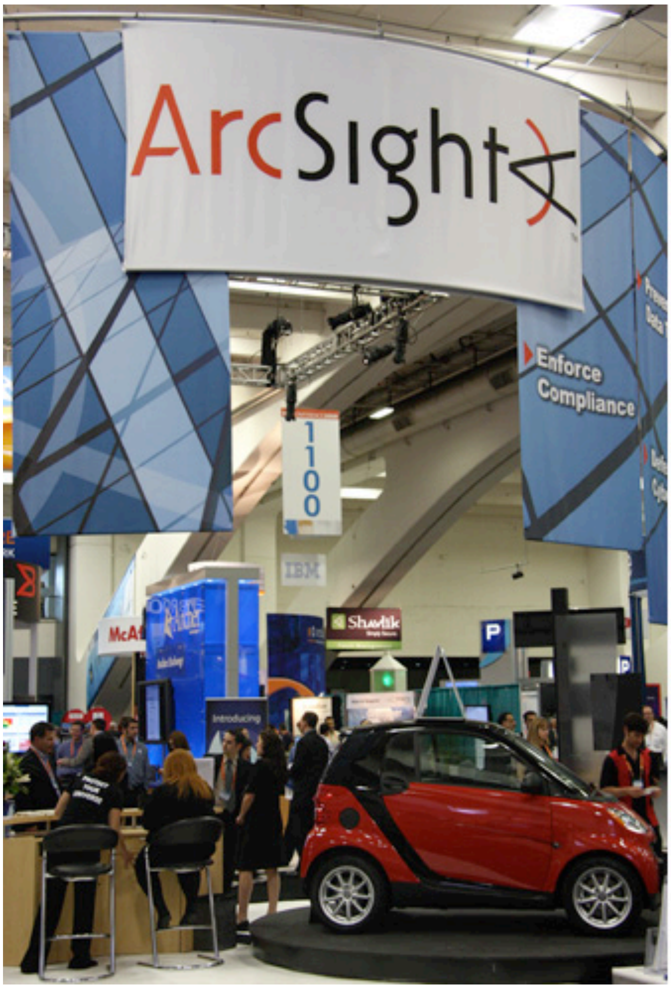
Qualys introduces QualysGuard PCI Connect



QualysGuard PCI Connect is the industry's first SaaS ecosystem for PCI compliance connecting merchants to multiple partners and security solutions in order to document and meet all 12 requirements for PCI DSS. It is an on demand ecosystem bringing together multiple security solutions into one unified end-to-end business application for PCI DSS compliance and validation. As a new addition to the QualysGuard PCI service, PCI Connect streamlines business operations related to PCI compliance and validation for merchants and acquirers all from a combined collaborative application with automated report sharing and distribution. (www.qualys.com)

First clientless smartcard authentication device for online services

Aladdin Knowledge Systems announced Aladdin eToken PRO Anywhere, the first smartcard-based strong authentication solution to combine the security of certificate-based technology with plug-and-play simplicity for end-users. The device enables remote access with strong, two-factor authentication from any computer with an Internet connection and USB port. A clientless device, eToken PRO Anywhere eliminates the need to install endpoint software for remote access, providing a seamless, simple user experience that enables secure access to sensitive data, applications and services from any location. (www.aladdin.com)



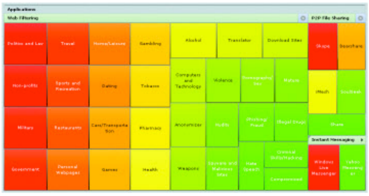
Managed Web application firewall service from SecureWorks

SecureWorks launched a Web Application Firewall (WAF) management and monitoring service that detects and blocks threats targeting Web applications found on corporate Web sites. With SecureWorks' Managed Web Application Firewall service, Web applications such as online shopping carts, login pages, forms and dynamically generated content are protected against application layer attacks that bypass traditional network and host-based security controls. SecureWorks currently supports full lifecycle management, maintenance and monitoring of Imperva SecureSphere appliances as well as monitoring for other WAF appliances that organizations may have. (www.secureworks.com)

QUALYS®
ON DEMAND SECURITY
QUALYS® THEATER
Now Playing
What Gets Measured Gets Managed:
A Quantitative Approach to VM
Brad Freeman, Global Security Services Leader
General Electric
Showing Next: QualysGuard Security and Compliance SaaS Suite

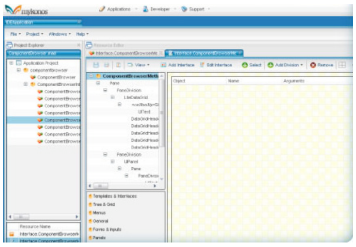
New visualization and reporting software

FaceTime Communications introduced visualization and reporting software FaceTime Insight. Using tree mapping and a modular reporting infrastructure, it provides a in-depth visibility into all facets of enterprise Web browsing. FaceTime Insight interfaces with the Unified Security Gateway to provide enterprise data visualization. (www.facetime.com)



YOUR CRITICAL BUSINESS DATA
Secured. Delivered. Compliant!
ssh tectia
Secure Data-in-Transit. Now!
Fast Track to Low Cost Compliance!
The Ideal Enterprise-class Secure File Transfer Solution
SSH Tectia Server for IBM z/OS
ACCESS

Framework for developing secure AJAX applications



Mykonos is an enterprise development framework and security service for building secure and scalable Web applications. Mykonos provides a Visual Builder for the rapid creation of applications that have security, scalability, multi-lingual support, and white-labeling built in, combined with a security service that delivers updates to keep applications protected. (www.mykonossoftware.com)

Monitor corporate e-mail and fight insider threat

Zecurion launched its email security solution, Zgate, which ensures that confidential information is not compromised through email by working as a checkpoint, filtering outgoing email messages. The software also facilitates the investigation into incidents of data breaches by placing emails in quarantine for manual processing or archiving for future review. (www.zecurion.com)

MBX systems
OEM APPLIANCES WITHOUT BOUNDARIES
CUSTOMIZED APPLIANCE SOLUTIONS WITH UNIVERSAL APPE
INFINITELY FLEXIBLE HARDWARE CONFIGURATION WITH OUT-OF-THIS-WORL
SUPERMICRO
MBX DAILY DRAWING
FREE PROTOTYPE APPLIANCE
MBX

RSA BSAFE EncryptionToolkits now free

RSA launched the RSA Share Project, a new initiative designed to bring security tools within reach of corporate and independent software developers and project leaders. The RSA BSAFE Share software is available for free download, offered as SDKs supporting C/C++ and Java. These products are fully interoperable with the applications embedded with RSA BSAFE encryption. (www.rsa.com)

New version of proactive network security management platform

Stonesoft unveiled StoneGate 5.0, its proactive network security management platform. Stonesoft provides a single centralized command center - called StoneGate Management Center - for proactive control of even the most complex networks. This center manages the entire StoneGate Platform including its firewall/VPN, IPS and SSL VPN solutions for physical and virtual environments. (www.stonesoft.com)

Strong authentication with biometrics for Windows 7

Gemalto has extended its support for strong authentication on Windows 7 using its .NET Bio solution. The solution enables multi-factor authentication using biometrics by building on the foundation provided in the new Windows Biometric Framework for Windows 7. (www.gemalto.com)

Strong authentication for mobile devices from VeriSign

VeriSign launched the VeriSign Identity Protection Mobile Developer Test Drive Program which enables mobile application developers to explore how easily and quickly they can provide users with an extra layer security that goes beyond standard secure log-ins. (vipdeveloper.verisign.com)

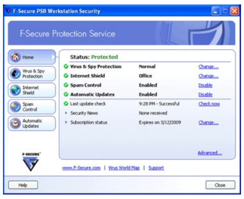
New secure software development credential from (ISC)²

(ISC)² opened registration for classes and exams for its Certified Secure Software Lifecycle Professional (CSSLPCM) which aims to stem the proliferation of security vulnerabilities resulting from insufficient development processes by establishing best practices and validating an individual's competency in addressing security issues throughout the software lifecycle (SLC). (www.isc2.org)

Lumension
IT Secured. Success Optimized.
We protect your data.
And your dollar.
Lumension
IT Secured. Success Optimized.
www.lumension.com
Vulnerability Management | Endpoint Protection | Data Protection | Reporting and Compliance

F-Secure launches new version of Protection Service for Business

PSB 4.0 provides a fast response to emerging new threats, requires less user involvement and delivers significant performance improvements. It is automatic and always up-to-date. The solution protects business desktops, laptops, file servers and e-mail servers. Its easy-to-use web-based management portal is available anywhere from the Internet. (www-f-secure.com)



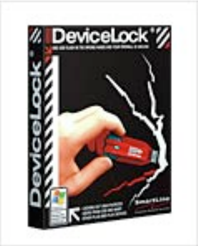
Status: Protected

Virus & Spy Protection	Normal	Change...
Internet Shield	Office	Change...
Spam Control	Enabled	Disable
Automatic Updates	Enabled	Disable
Last update check	9:28 PM - Successful	Check now
Security News	None received	
Subscription status	Expires on 3/12/2009	Change...

Advanced...

www.F-Secure.com | Virus World Map | Support

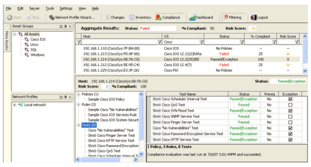
DeviceLock 6.4 retooled with new content processing engine



DeviceLock announced DeviceLock 6.4 which adds true file type detection and filtering - the first deep data analysis feature built on top of its new content processing engine. The software can intercept peripheral device read/write operations, perform analysis of the entire digital content in real time and enforce applicable file type-based security policies. True file types can now be used as a parameter for DeviceLock data shadowing policies, thus increasing the level of granularity and flexibility of controls. (www.devicelock.com)

Agentless configuration auditing for virtualized infrastructure

nCircle announced that its Configuration Compliance Manager configuration auditing solution delivers new policies that audit the configurations of the virtual infrastructure and compare the configurations to Center for Internet Security benchmarks, or hardening guides, to ensure the security of virtual machines and their hypervisor. (www.ncircle.com)



Your applications are trying to tell you something - are you listening?

by Jack Danahy

Your applications are trying to tell you something. They are saying, “I can help you find potential risks to your business, please just ask me!” Applications are the gatekeepers for all of your data – where it gets processed, transformed, and transmitted – and by their very nature, applications are best positioned to help you ensure data privacy for your customers. By listening to your applications, it is possible to know – not guess or hope – that your information is secure enough.

Understanding what your applications can tell you puts power in your hands:

- The power to know you’re compliant with regulations such as PCI DSS
- The power to know your promises are kept by protecting your customers’ private data
- The power to hold your outsourcers accountable to measurable security requirements.

Today, when you make decisions about IT security priorities, you must strike a careful balance between business risk, impact, likelihood of incidents, and the costs of prevention or cleanup. Historically, the most well understood variable in this equation was the methods that hackers used to disrupt or penetrate the system. Protective security became the natural focus, and the level of protection was measured by evaluating defensive resiliency against live or simulated attacks.

This protection has proven to be insufficient, as the escalating frequency and impact of successful exploits are proving that IT assets – and ultimately business assets and intellectual property – are not yet secure.

The ever-changing population of software components at the application layer likely leaves you inadequately informed as to where and how your data may be exposed.

Where can you turn next to help protect the security of your critical data assets? Since 75-90% of all Internet attacks target the application layer, it is clearly about time that you listen to what your applications are trying to tell you about data security.

Applications are the front line in the battle for your data. If you know what to look and listen for, your applications can provide you with a wealth of information about their strengths, weaknesses, and methods. This is the information you are, or will soon, be required to provide to regulators, your customers, your boss and your board. The knowledge you need can come from the very foundation of the application: the source code. Therein lays the facts of the real state of your data security.

That knowledge will give you the power to make truly informed risk management decisions.

The power to know you're compliant

Breaches breed regulations – it's that simple. Newer regulations that focus on data and data protection, like the PCI DSS are becoming the IT security standards of due care.

They require proof that critical data assets have been secured, most notably at the application level. Earlier attempts at regulation had often mandated required technologies or configurations, and these quickly became outpaced by changing attack methods.

This new data-centric approach mandates the protection of individual data elements (as in the case of credit card record), or potentially linked items which, when combined, can reveal personal identity or confidential information. The regulations focus on the appropriate treatment of these data elements in acquisition, transfer, storage, access, and destruction. As a result, compliance requires an in-depth understanding of the actual behavior of the application. Knowing where your data goes requires knowing all the paths and end-points with certainty. This certainty requires analysis of the source code.

The PCI is by no means alone in its increased sophistication and focus on secure treatment of data elements and services. Other regulations, like GLBA, HIPAA, and the UK's Data Protection Act focus on the confidentiality of personally identifiable information, while Sarbanes-Oxley and Basel II assert the necessity of integrity of data and financial systems. Attestations of compliance can only be credibly offered by organizations and individuals who have actually taken the time to see what is being done within the application.

Anything else is little more than a guess.

SECURITY REQUIREMENTS SHOULD BE CLEARLY ARTICULATED, AND THE METHOD FOR EVALUATING COMPLIANCE SHOULD BE PRECISE

The power to know your promises are kept

Privacy statements that accompany most Web-facing transactions are meant to give users confidence in the protections that are in place to ensure the security of their private information. In reality, application-level security is almost never mentioned.

These statements, created to address user concerns with network-focused threats and unscrupulous business behaviors, are commonly concerned only with communications protocols and disclosure policies.

As a result, applications that are at the center of the customer experience are not cited or addressed. Concurrently, assertions are being made as to the protection and safety of that data. The privacy promises you make to your customers, shareholders, and partners can only be kept if the security of your application source code is actively evaluated and maintained.

The power to hold your outsourcers accountable

Increasingly, organizations are running their business using software or services that are provided by someone else. This automation of business processes by an outside entity has typically happened without assessment and validation of the security of the software when delivered. As with any other contractual requirements, security requirements should be clearly articulated, and the method for evaluating compliance should be precise.

The source code is the only consistent, reliable place to look for this knowledge. The software speaks directly to the issues of the contracted security criteria. This clarity is not possible through simple functional or black box testing, as many times the implementation of required security is naturally invisible to such testing. Mandates for the use of only approved validation routines, communication through secure protocols, and secure data storage are examples of important security enablers that are transparent to the user or to user-styled testing.

Source code analysis is a clear and unique means to evaluate performance, measure compliance, and potentially to recover costs and impose penalties.

Secure your applications today so you can do business tomorrow

There are many elements in an application that impact data security. Source code analysis translates an application's full range of possible behaviors into a representation that provides credible facts about the security state of an application. Without going to the source code for this knowledge, organizations must go on faith, or make an uneducated guess about the security of their data. The time for such uncertainty is over.

The vulnerabilities that put your data at risk are buried in the millions of lines of source code that power your organization. Given the chance, your applications will speak out loud and clear, pointing you to their weakest points and faults. With this information, you will find that you have the power to make more effective risk-management decisions, more insightful decisions about your partnering, and more cost-effective decisions for your organization.

Jack Danahy is founder and CTO of Ounce Labs (www.ouncelabs.com) and one of the industry's most prominent advocates for data privacy and application security. Jack is a frequent speaker and writer on information security topics and has been a contributor to the U.S. Army War College, the Center on Law, Ethics and National Security, the House Subcommittee on Information Technology. His blog can be read at suitablesecurity.blogspot.com, and he can be reached at JDanahy@ouncelabs.com.

twitter security spotlight

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

@SecBarbie
Erin Jacobs - Chief Security Officer for UCB.
http://twitter.com/SecBarbie

@andrewsmhay
Security author, blogger, and advocate.
http://twitter.com/andrewsmhay

@jasonmoliver
Security Evangelist.
http://twitter.com/jasonmoliver

@ChrisJohnRiley
IT security analyst and penetration tester.
http://twitter.com/ChrisJohnRiley

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

2nd DIGITAL SECURITY FORUM

www.digitalsecurityforum.eu

26-27 JUN LISBON 2009

Hotel Ollissipo Oriente

The Digital Security Forum aims to be a reference in European security conferences and training events, allowing for infosec professionals to network and acquire knowledge, by discovering the industry`s best practices, new methodologies, technologies and tools.

Keynote Speakers

Prof. Howard Schmidt
CISSP, CISM - President & CEO of Information Security Forum, International President of ISSA

Dr. Louis Marinos
Senior Expert on Risk Management, ENISA

Adam Laurie
Director of "THE BUNKER", and developer of RFIDiot.org

Patricia Peck
Lawyer/Digital Law Expert

Workshops

Christian Bockermann
ModSecurity

This list is not final, and only includes the already confirmed participants

Registration

Open on January 2009

Pricing

Before 31st January: **€200**
From 1st February to 28th February: **€240**
From 1st March on: **€360**
All prices include VAT at 20%.

Call for Papers Deadline

The deadline for papers / proposals submission is the 10th of February 2009, and should be sent to:
cfp@digitalsecurityforum.eu

Sponsors

pontosi

Partners

diplomatatours
um sorriso de ida e volta

CATO DESIGN

Media Partners

Turismo de Lisboa

InfoSec ONline.pt

Virtually Informed - Security News

(IN)SECURE insecuremag.com

www.catodesign.com

Q&A: Hord Tipton on certification and (ISC)²

by Mirko Zorz

Hord Tipton is the executive director for (ISC)², the global leader in educating and certifying information security professionals throughout their careers.

What has been your biggest challenge as the Executive Director of (ISC)²?

(ISC)² is celebrating its 20th anniversary and there has been a tremendous culture change from a small organization to a sizable corporation. Yet while we have accomplished a lot, there is still much work to be done. With my recent trip to Asia, I discovered we have had difficulty effectively communicating with members in their native language, be it through e-mail or by phone. In June, we plan to start addressing some of these issues by implementing people who can speak the native language in countries where we have significant membership. This will help us better reach the growing information security profession in new regions as well, such as Latin America.

I also learned we need to do a better job of communicating the continuing education requirements of our certifications so members know exactly what is expected of them to maintain their credential. This may involve more information on CPEs being included in our educational programs.

There are many other initiatives that need to be taken to ensure that we are exceeding member expectations when it comes to providing the most user-friendly and quality member services on a global basis.

Security is often overlooked and with the recession biting the budget out of every section of the enterprise, how should a company approach savings in this department?

Security must be viewed as a total cost of operation that has a positive ROI in the long run. This is a difficult area to assess because it requires so many assumptions – thus the estimate of overall ROI becomes quite subjective. More tangible results can be found by looking at research figures, some of which estimate that data breaches up to around 100,000 records have risen to over $200 per record – a figure which mostly accounts for administrative costs for remedying the breach. A step that is often overlooked in the calculations is that a breach can actually be fatal to a company, particularly in today's economy with competition being very fierce. Reputation is everything. Determining adequate security is tricky business that involves saving dollars, but sometimes it involves saving your company. Ask yourself the question "How much risk can I afford?" $20 million will buy a lot of security protection.

What security threats should be most important to organizations of any level this year?

While most IT attacks today are for monetary gain, the type of threat depends in part on the type of organization. For companies such as banks, it's about protecting personal identity and proprietary information, and preventing against attacks like denial of service and extortion. Government and critical infrastructure agencies must worry about cyber terrorism. While the government is on the front end of protecting us against cyber terrorists, many of the organizations who are in charge of our nation's critical infrastructures are run by the private sector – thus they share this common threat. Finally, all organizations in the public and private sector must increasingly worry about Web 2.0, smartphones, Twitter, and other exponentially growing tech advances. As these technologies continue to accelerate, the risk posed to organizations only increases, because most employees use these tools without thinking through the security pieces.

DETERMINING ADEQUATE SECURITY IS TRICKY BUSINESS THAT INVOLVES SAVING DOLLARS, BUT SOMETIMES IT INVOLVES SAVING YOUR COMPANY

What security technologies do you find exciting and why?

Any that track advancing technologies are interesting to me. In almost every aspect of our lives today, there is very likely an IT component. Unfortunately we have not reached the point where we consistently challenge a new technology with the "what if" security questions. Do we want anyone to be able to access a program that controls the technology that powers things?

I am especially fascinated by advances in biotechnology with the integration of IT. For instance, a hacker could infiltrate someone's technology-controlled medical device, such as a pacemaker, with the intent to do harm. At universities like Stanford and Johns Hopkins, research is being conducted on such revolutionary concepts as being able to download the memory cells of a person's brain into a data file for the purpose of preserving short-term memory. If a cure for diseases for such diseases as Alzheimer's are found, that data could then be transferred to a new, regenerated brain. The security component comes into play when dealing with the transfer of data.

In short, we have tremendous tools and proven security techniques to protect our critical assets if we get to play on the front end of development of these exciting technologies. It would be a mistake to watch these advances take place and then have to address security and privacy concerns only after they are already deployed.

Some believe that certification is essential when it comes to working in the IT security industry while others think it's wasted time and money. I imagine you value certification programs, so what would you say to those not interested?

I do believe certification is vital to the furtherance of improved IT security performance and always has been. The IT security world would be in a world of hurt without understanding and acceptance of standard practices. Many professions require objective validation skills. If my barber needs certification, why shouldn't an information security professional who may be securing highly critical infrastructure.

The problem is not enough people understand what a particular certification really means. No one credential qualifies anyone for every situation.

Credentials must be mapped to job skills which should be mapped to the position. After all, without examinations, college degrees would be easy! The same principle applies to certifications.

Not all certifications are created equal either. Like ours, there are certifications that require validated work experience, professional endorsement, adherence to a Code of Ethics, and require continuing professional education.

Certified staff offers organizations additional protection in meeting regulatory compliance or in governance-related lawsuits. It also can help reduce risk involved with new projects and technologies enterprise-wide. I think it increases cooperation between security employees throughout your organization with standardized practices and terms.

What challenges does (ISC)² face in the global certification market? What are your advantages?

Challenges include languages and the translations necessary to remain an international organization. Our test questions are developed in English and undergo very detailed examination and are often difficult to convert into different languages. We also have to understand the cultural values of all countries. For example, what may be an ethical practice in the U.S. could be totally unacceptable in Singapore. Finally, we must adapt our pricing for all products to local economies.

Our major advantage comes from the common interest and passion for meeting the challenges in the IT security environment. In all the areas I have visited, the dedication to sound security practices just seems universal. Being recognized as the global “Gold Standard” is also very beneficial to our organization.

Another one of our strongest assets are our dedicated members, who are ambassadors of information security. With a strict adherence to the (ISC)² Code of Ethics as a requirement to maintaining certification, our members not only instill best practices in their organizations, but are encouraged to help develop professionals in all parts of the world, instill ethics in others, and educate private citizens about the best methods to protect themselves.

(ISC)²'S MISSION TO MAKE THE ONLINE WORLD A SAFER AND MORE SECURE PLACE INCLUDES ENCOURAGING ITS PROFESSIONALS TO BECOME INVOLVED IN HELPING SOCIETY AT LARGE

(ISC)² has a volunteer program in the U.S. designed to address the issue of online dangers facing children. Can you give our readers some details on the program?

(ISC)²’s mission to make the online world a safer and more secure place includes encouraging its professionals to become involved in helping society at large.

With today’s youth using more connected technology than ever before, they are being exposed to a variety of dangers their parents may never see.

The Safe & Secure Online program consists of an hour-long interactive presentation designed to educate school children ages 11-14 about how to protect themselves from online dangers in an increasingly electronically-connected world. The presentations are made by (ISC)²-certified professionals using materials developed by Childnet International, a charity that aims to make the Internet a safe place for children.

Safe & Secure Online was first introduced in the United Kingdom in 2006, then expanded to Hong Kong in 2007. In early 2009, it was introduced to the U.S. as a pilot program in Washington state and is currently in the process of being rolled out to other U.S. cities nationwide. To date, more than 200 (ISC)² certified members have reached more than 20,000 students.

More information can be found at www.isc2.org/awareness.

"Unclonable" RFID - a technical overview

by Srini Devadas

RFID has advanced beyond being just an identification technology – it is now an identification and authentication technology. RFID has advantages over traditional product authentication and anti-counterfeiting mechanisms, such as color shifting inks, holograms, and 2D barcodes, etc. RFID is a more efficient and reliable technology. RFID tags can be read without any manual intervention and without requiring a line of sight or physical contact with the item. RFID certainly raises the bar as an authentication or anti-counterfeiting measure, but the bar is only as high as the technical "skills" of counterfeiters, which unfortunately are reaching new heights every day.

There are various types of RFID. Basic passive RFID is prone to counterfeiting attacks. A resourceful adversary can clone a basic RFID – meaning the contents of a genuine RFID chip can be copied to another to appear the same as the genuine RFID chip. An even simpler alternative would be for an adversary to record the exchanges between a basic RFID chip and a reader, and replay them to mimic the original RFID chip. Cryptography-based RFID is secure, though expensive for wide-spread, item-level use.

Recently, a new class of simple, inexpensive and "unclonable" RFID chips was introduced to the market. These RFID chips are based on a technology called Physical Unclonable Functions (PUFs). PUF is a "silicon biometric" technology, a kind of fingerprint or DNA for silicon chips. This technology enables very strong and robust authentication of the RFID chips, and also provides a way to prevent skimming and replay attacks.

Physical unclonable functions

A Physical Random Function or Physical Unclonable Function (PUF) is a function that maps a set of challenges to a set of responses based on an intractably complex physical system (this static mapping is a "random" assignment with the randomness coming from the intrinsic variations of the physical system). The function can only be evaluated with the physical system, and is unique for each physical instance.

PUFs can be implemented with various physical systems. In the case of RFID, PUFs are implemented on silicon. Silicon-based PUFs (SPUFs) are based on the hidden timing and delay information of integrated circuits (ICs). Even with identical layout masks, the variations in the manufacturing process cause significant delay differences among different ICs.

Silicon-based PUFs derive secrets from complex physical characteristics of ICs rather than storing the secrets in digital memory. Since silicon PUFs tap into the random variation during an IC fabrication process, the secret(s) are intrinsic to the silicon itself, are extremely difficult to predict or “program” in advance of manufacture, and are essentially non-replicable from chip to chip. PUFs thus significantly increase physical security by generating volatile secrets that only exist in a digital form when a chip is powered on and running.

This means that an adversary, rather than merely examining an IC’s memory to read its stored secret, would instead need to mount an attack while the chip is running and using the secret -- a significantly harder proposition than discovering non-volatile keys.

An invasive physical attack would need to accurately measure PUF delays from transistor to transistor without changing the delays or discovering volatile keys in registers without cutting power or tamper-sensitive circuitry that clear out the registers. In addition to its inherent physical security, even the IC manufacturer cannot clone PUF-enabled ICs. That is because the random component of manufacturing variation cannot be controlled or programmed in any conventional sense by the manufacturer - it is inherent to the process itself.

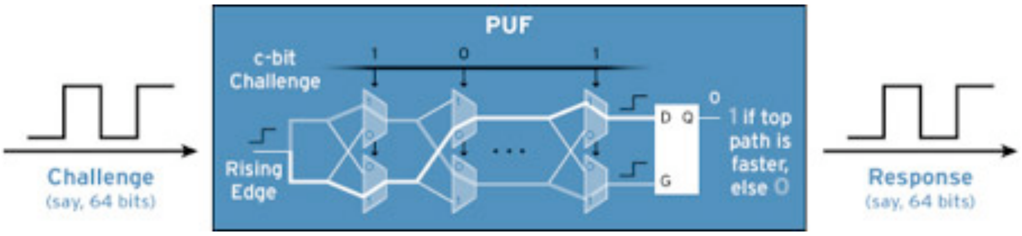


Figure 1: How PUFs work.

PUFs can be implemented in many different ways, but all PUF implementations provide a mechanism to extract the unique characteristics or secrets from the ICs. Some PUF implementations use a challenge and response protocol to extract these secrets.

Figure 1 above shows a MUX and arbiter based PUF implementation (MUX-PUF). The MUX-PUF takes a random number input as a challenge. The bit length of the challenge is implementation specific. The example above assumes a 64 bit challenge. For each challenge input, the MUX-PUF generates a response. The bit length of this response is again implementation specific; the example above assumes a 64 bit response. These challenges and responses have the following characteristics:

- The number of challenge and response pairs for each IC can be arbitrarily large (264 in this example)
- For a given challenge, the same IC nearly always has a consistent response
- For a given challenge, different ICs have different responses.

We note that the output of the MUX-PUF is typically processed through logical operations in order to enhance the variation across RFIDs and to make it hard to create a software model of the PUF.

Unclonable RFIDs: Design and implementation

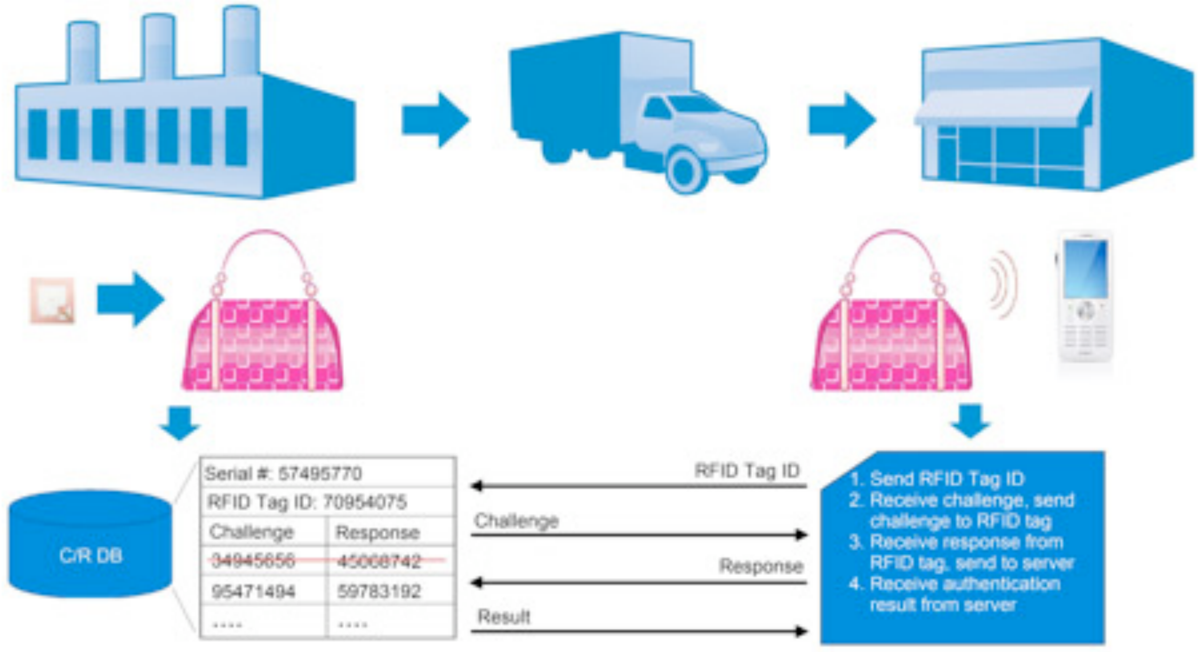
While traditional RFID technology has limitations in its use as a true anti-counterfeiting measure, it still is an almost ideal technology to talk to “things.” A critical element that has been missing is a scalable, cost-effective way to make it trusted and secure. An RFID tag that has a secret that cannot be copied would allow you to immediately distinguish a counterfeit tag from the genuine one.

A PUF-based RFID chip has its own unique secrets, derived from the silicon itself. And these secrets are:

- Essentially impossible to predict or “control” in advance of manufacture
- Essentially impossible to duplicate or clone from one chip to the next.

The figure below illustrates the PUF-based authentication process. Here, we exploit the observation that the PUF can have an exponential number of challenge response pairs where the response is unique for each IC and each challenge. A trusted party such as a product vendor, when in possession of an authentic RFID with an authentic product, applies randomly chosen challenges to obtain unpredictable responses.

The trusted party stores these challenge-response pairs in a database for future authentication operations. This database is indexed by the (unique) identifier normally associated with each RFID and/or product. For example, an EPC code that is stored in non-volatile memory on the RFID. The identification of the RFID and product is based on this conventional identifier. To check the authenticity of an RFID and the associated product later in the field, the trusted party selects a challenge that has been previously recorded but has never been used for an authentication check operation, and obtains the PUF response from the RFID. If the response matches (i.e., is close enough to) the previously recorded one, the RFID is authentic because only the authentic IC and the trusted party should know that challenge-response-pair. To protect against man-in-the-middle attacks, challenges are never reused. Therefore, the challenges and responses can be sent in the clear over the network during authentication operations. Note that the challenge-response database can be recharged with new challenge-response-pairs to increase the number of authentication events.



Serial #: 57495770	
RFID Tag ID: 70954075	
Challenge	Response
~~34945656~~	~~45068742~~
95471494	59783192
.....	.....

1. Send RFID Tag ID
2. Receive challenge, send challenge to RFID tag
3. Receive response from RFID tag, send to server
4. Receive authentication result from server

Figure 2: Overview of the PUF-based RFID authentication procedure.

The first commercially available PUF-based RFID IC operates at 13.56MHz and is based on the ISO-14443 type A specification. Although this first implementation uses a specific frequency and a command set, we note that the same PUF technology can be integrated into RFIDs that operate at other frequencies. The first implementation was designed to be the simplest passive RFID tag in order to demonstrate that the PUF-based authentication is feasible even in low-cost tags. This passive RFID IC operates just like a regular RFID IC for storing a unique identifier or EPC code; the PUF circuit is activated only for authentication.

To allow an RFID reader to access the PUF, the RFID chip supports one new command: CHALLENGE. On a CHALLENGE command, the chip accepts a 64-bit challenge from the reader, internally produces a 64-bit response for the given challenge, and returns the response bits to the reader. Also, the existing READ and WRITE commands in RFIDs can be used as the PUF commands. A WRITE into a specific address can be interpreted as the challenge command, and a READ from a specific address can be interpreted as the response command.

PUF-based "unclonable" RFID provides the following advantages:

Highly secure: The RFID chip itself cannot be cloned. The responses to challenges are generated dynamically, and are volatile. Volatile information is much harder to extract than non-volatile information. With practically unlimited numbers of challenge-response pairs available, each pair can be used only once. This essentially serves as a one-time-pad. A side channel or replay attack would fail since the adversary cannot predict the challenge and responses to be used for the next authentication event.

Simple, robust authentication: PUFs do not require any complex key storage and cryptographic computation for authentication. PUF challenge response pairs can be generated and stored at a secure location or multiple locations by independent parties that do not share information.

Thereafter, it does not matter whether a supply chain was compromised or not, a PUF RFID tagged product can be authenticated by simply comparing the response generated during an authentication event with the response recorded at the secure location.

Low cost, low power consumption: A PUF circuit is a fairly lightweight addition to the RFID chip. The initial implementation of a basic 64-stage PUF circuit and surrounding control logic added less than 0.02mm^2 in the 0.18µ technology. PUFs consume minimal extra power. Chip size, cost and power consumption are key market acceptance parameters for RFID. PUF-based RFID enhances the capabilities of basic RFID in a very cost-effective way, even for item level use.

Summary

PUF-based "unclonable" RFID provides a simple and robust anti-counterfeiting mechanism when compared to alternatives. The low cost and power consumption of PUF-based RFID makes them suitable for item-level use, a significant advantage over cryptography-based RFID. Since the PUF RFID chips cannot be cloned, a simple authentication at the point-of-sale ensures only a genuine product is sold to the customer.

This requires a significantly simpler infrastructure compared to the complex infrastructure (hardware and software) required to implement solutions based on electronic pedigree. With PUF-based RFID, authentication and identification is significantly improved based on the inability to tamper, control, clone, or duplicate the chip.

Using "unclonable" RFIDs can deliver peace of mind to many product-based industries from pharmaceutical and luxury goods to secure IDs and transportation.

Professor Srini Devadas is the founder and CTO of Verayo. Professor Devadas and his team invented PUF technology at Massachusetts Institute of Technology (MIT), Cambridge, USA. In addition to providing technical leadership and direction to Verayo, Professor Devadas serves on the faculty of MIT, as the Associate Head of the Department of Electrical Engineering and Computer Science. Professor Devadas' research interests include Computer-Aided Design (CAD) of VLSI computing systems, computer architecture, and computer security, and he has co-authored numerous papers in these areas.

Professor Devadas joined MIT in 1988, soon after completing his Ph.D at University of California, Berkeley. He received his Bachelor's degree in Electrical Engineering from IIT Madras (India).

The application security maturity (ASM) model

by Ed Adams

The Application Security Maturity (ASM) model helps organizations understand where they are in terms of their overall approach to software security. The model was developed in 2007 by Security Innovation from analyzing and plotting over ten year's worth of data about organizations and their security efforts, in particular their investment in tools, technology, people, and processes.

Based on this research, it's clear that organizations that develop and deploy the most secure software have a high maturity level; further, they only reach maturity through many trials and errors, particularly when it comes to purchasing and integrating tools into their software development and information security organizations. By understanding and using the ASM model, organizations can uncover their current maturity level and then understand the most effective course of action to increase this level quickly and pragmatically while introducing as little disruption as possible to their current development process and in-production application management.

The goal of this article is to:

1) Understand how the ASM model was created.
2) Learn how the model works and what it can tell you about your organization.
3) Help fine-tune your security-related investments in order to positively impact your software security maturity more quickly.

Creating the ASM model

The ASM model was developed after analyzing first-hand the software security activities and investments of hundreds of organizations. The initial data input for the model is based on:

Extensive software security research at Florida Institute of Technology (FIT). Led by Dr. James Whittaker, FIT project teams examined the security issues of software development processes as well as the underlying testing procedures and processes that were failing to catch so many critical software bugs. This work began in 1999 and conclusions were drawn from direct exposure to the tools, developer mindset and skill-set, and development processes used.

In-depth consulting engagements with Security Innovation clients. Security Innovation was founded by Dr. Whittaker in 2002, and since its inception, has expanded on the initial FIT research. The company's staff of security experts has helped understand, assess, and classify thousands of software bugs. Its employees have written books and created methodologies adopted by leading software developers. As with the initial FIT research, the knowledge and expertise from Security Innovation staff comes from real-world experience.

Detailed analysis of data collected via interviews and SDLC (software development lifecycle) assessments. This data was collected from over 200 organizations, many of which are Fortune or Global 500 companies. Interview data was validated and expanded upon by direct inspection and inquisition of tools, systems, and staff. In each case, baseline metrics were defined and tracked over time – in some companies for as little as 12 months, in most over a span of 3-5 years.

The combined ten-year experience of the Security Innovation team and its academic predecessor means that we have access to – and continually generate – a wealth of information about how organizations approach the software security challenge. By analyzing all of our primary data, it became evident that there are two critical categories of investments that can impact how well any company meets the challenge.

Technology & Tools (T&T)

These investments include the various software tools and applications an organization licenses or acquires to secure software during all stages of the software development life cycle (SDLC), from creating application or system requirements through final deployment. This is typically the area where most organizations, when faced with the threat of a security breach or looming regulatory pressures, first invest their dollars.

Specific investment in this area includes tools for:

- Version control
- Source code scanning
- Defect Management
- Test Automation
- Web Security vulnerability scanning
- Application-layer security mitigation (e.g., a Web application firewall).

In each area above, organizations were analyzed for both depth and breadth of application, for example in source code scanning, organizations were examined on several factors, including:

- Does the organization utilize source code scanning tools?
- If so, are there security source code scanning tools in place?
- How and where are the source code tools used, e.g., on developers' desktops, at check-in or build time, continuous integration, at a single clearinghouse/ "gatekeeper" station prior to deployment?
- Who uses the source code scanning tools, e.g., security architects, developers, testers/ QA, information security officer/analyst, etc.

People & Processes (P&P)

Investments in this area include the hiring of security staff, ongoing training programs, and improvements to the SDLC specifically for enhancing code or application security. While the typical reaction to real, perceived, or potential security threats is a tool-buying spree, over time companies learn to invest in improving security deeper in the organization by making investments in P&P, which almost always pay higher dividends than an investment in tools.

Specific examples of investment in this area include:

- Secure SDLC activities for development teams at each phase, e.g., design, code, test, et al.
- Training (both technical and awareness)
- Internal "Red Teams" (playing the role of attacker)
- Third-party security reviews (at code and as-built layers)

- Application security auditing
- Integration of Application Security with Risk Management practices.

Just as we did with T&T, each P&P area is analyzed and explored in depth and breadth. The resulting database had over 10,000 data points that were sorted, normalized, and compared to extract trend lines and conduct point-in-time analyses.

Note that having invested in all of the specifics outlined above – essentially a laundry list of security best practices – in both the T&T and P&P categories would indicate a very high security maturity level for an organization, and high maturity is the goal if and only if the investment is coupled with the culture change necessary to integrate the investments as part of operational business. Therefore, it is not a simple matter of picking and choosing a handful of investments to make in each category. Rather, it is a journey that leads organizations to eventually understand the benefit of funding and implementing the T&T and P&P investments mentioned above.

Plotting the data

Understanding these two critical elements led us to plot organizations according to these two criteria. Using a standard 4x4 grid, with the left corner (the origin) representing “low,” and the top left and bottom right corners representing “high,” we plotted an organization’s investment in Technology & Tools on the vertical Y axis and its investment in People & Processes on the horizontal, X axis.

The grid was populated from information we knew directly about organizations and their security investments. For example, to be plotted, we had to be able to determine an organization’s investment for both T&T and P&P based on our scale. From this information, we were able to:

Plot organizations over time (multiple data points). By working with an organization for an extended period of time, we were able to plot its evolution in terms of the two primary axes of the ASM model. This organization-normalized curve mirrored the generalized (all organizations) curve mentioned below.

Plot individual companies (single data points). We could plot each company we worked with according to the two major axes of the model. While a single point does not enable us to create a company-specific progression, it does help us validate an overall curve.

Determine the ASM curve (all data points). Using the information we had from companies both over time and at a point in time, a predictable ASM curve developed. This curve reliably predicts where organizations are along the curve and their likely future course of action.

While the ASM model and the typical maturity curve provide great insight for organizations to understand and alter their security investments, there are some caveats of the model that should be taken into consideration:

- The model is based upon organizations that have asked us for help, so by definition (going to a third-party source for help), they are already more aware and mature than an organization just starting its ASM journey.

- Companies may not follow the path directly, though evidence suggests that most companies will adhere to the basic curve unless they have actively decided to influence it in a severe fashion by specific investments (or panic.)

Understanding the ASM model

The ASM Model has three distinct phases based on a company’s investment in Tools & Technology and People & Processes. The phases are:

1. The Panic Scramble. Most immature organizations are in this stage. They start their security journey by responding to some event, perhaps a loss of confidential data, a Web site breach, or the discovery of a network intruder.

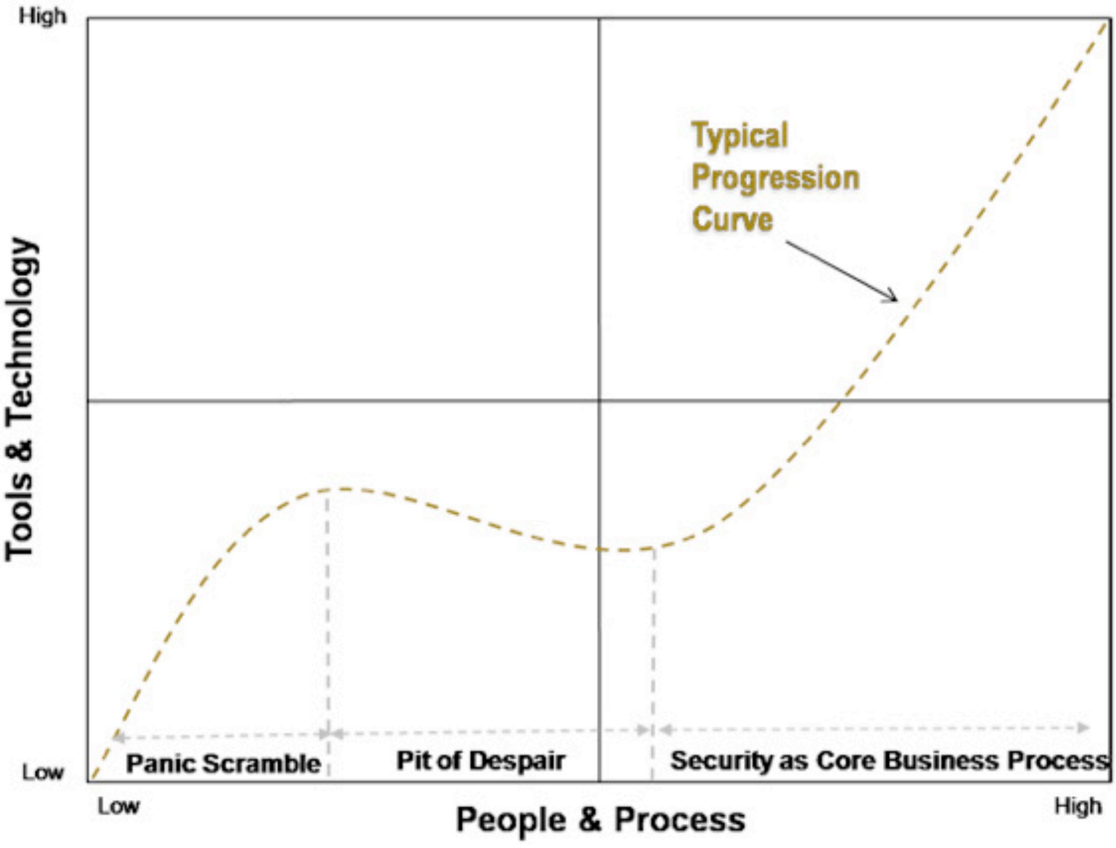
They may also enter this stage as a response to external events, such as a very public security breach at a competitor or media reports of massive data losses. Another potential catalyst is a new government or industry regulation.

Organizations that have found themselves in the Panic Scramble respond to the immediate security issues by spending money on software security tools and technologies that hold the promise of immediate impact to mitigate the perceived or real threat. However, such an investment without the requisite investment in P&P usually provides little overall return and limited security improvements; in fact, many times, tools become “shelfware” sitting unused because the developer or information security professional doesn’t know how to use them or what to do with the results the tool generates, leading to the second stage.

2. The Pit of Despair. After a relatively brief period of panic, companies revisit their security investments and find the money they have spent has had only a minor impact on their security. A few areas of the company may have benefited from the efforts, but overall, security is not pervasive in either the IT or business aspects of the organization. The organization becomes security depressed as it bemoans T&T investment and languishes while pondering what to do next.

During this stage, organizations often see a reduction in tools usage as they try to figure out how to best leverage the investment made or rethink it altogether. Typically at this stage they do begin to invest in staff training, improved processes, and utilization of security experts to help with planning and assessments. However, they also tend to lower their budget on the tools and technology side. Without major returns, and faced with continual threats, companies will remain in this stage until a major security mind shift occurs. As procedures are detailed and driven by new security awareness and requirements, senior business and IT staff finally begin to understand the critical need to invest in long-term and company-wide security hygiene. Often after enlisting the help of third-party firms, such as consultants or security auditors, or being burned by a data breach – they move to the final stage.

3. Security as a Core Business Process. Having made the important shift to understanding security as core to a successful business, organizations will begin to devote more budget (and, more importantly, time and focus) to the software tools required to ensure secure code in all phases of the software development life cycle, the training needed to educate developers and other non-IT employees, and the enhanced processes that place security into all business and IT activities.



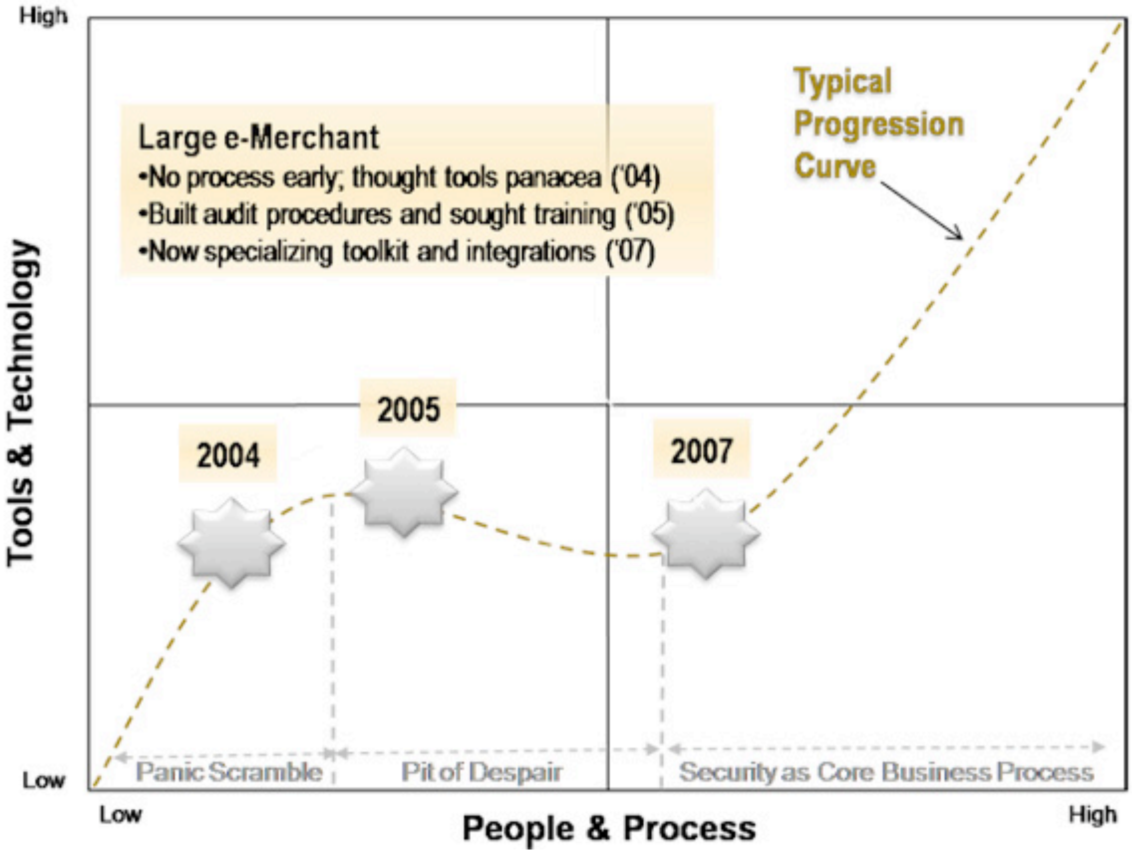
Application Security Maturity Model (ASM)

The ASM Model graphic above depicts a typical path an organization may take. Time is overlaid left-to-right and the speed at which an organization passes along this curve varies with their awareness, investments, and success of adopting new processes. Also, an organization's Pit of Despair may be deeper or elongated if they have difficulty adopting and integrating new tools and process. The duration of each stage and the slope of the curve can very depending on many factors, including:

The influence of security-minded executives. In many cases, business or IT executives can drive the move to the third stage quicker than it would happen normally. For example, an incoming executive that has already seen the value of being in Stage 3 in a previous company can often reduce the duration of the earlier stages and help the organization avoid common pitfalls.

The use of third-party consultants and service providers. The primary research for the ASM model was based on direct interaction with organizations that have made the decision to employ external security experts. These experts can demonstrate the value of more quickly embracing security as a core business process.

Seeing security as a competitive advantage. Some firms have chosen to embrace a pervasive security approach with its required increased investment in order to differentiate themselves from competitors with a more lackadaisical approach to security.



Sample ASM model plots (for Large E-commerce Organization)

Organizations can leverage the ASM Model to:

• Determine their current location along the ASM curve. Just knowing where an organization falls on the curve is a critical first step to understanding and improving overall security. With knowledge of where the company falls, the company can understand:

o How it compares to others – either competitors or best-of-breed companies

o Its likely ASM path

o The time frame expected for the stage it is in

o Their investment ratio

- Circumvent the traditional curve to accelerate activities. By understanding their current location, companies can then decide how to influence their own curve. For example, a CIO may aggressively avoid the Pit of Despair stage by embracing the proper mix of investments in tools, technology, people, and processes. That CIO may use the graph – and the organization's current plot – to help influence security investments, demonstrating the potential changes to curves as a result of too little or too late investment in all aspects of security.

- Chart the ASM path along the curve over time. A critical aspect of any security program is auditing systems, and charting the progress of the organization's dedication to security should also be undertaken. By periodically plotting the company's location on the ASM Model, a company can track its improvements as well as its efforts in relation to the average curve.

The easiest way to begin is with a self-assessment. Ask yourself where your organization is in respect to the T&T and P&P analysis areas:

1. Version control
2. Source code scanning
3. Defect Management
4. Test Automation
5. Web Security vulnerability scanning
6. Application-layer security mitigation (e.g., a Web application firewall)
7. Secure SDLC activities for development teams at each phase, e.g., design, code, test, et al.
8. Training (both technical and awareness)
9. Internal "Red Teams" (playing the role of attacker)
10. Third-party security reviews (at code and as-built layers)
11. Application security auditing
12. Integration of Application Security with Risk Management practices.

For each area, ask both the "IS" and the "HOW" questions. For example, is your organization using test automation tools and, if so, how are they being used. And then dive one layer deeper and ask how it applies directly to your organizations' security and data protection objectives. Even this simple exercise will likely uncover some stagnant investments and need for awareness improvement.

Conclusion

Understanding your Application Security Maturity level is critical to understanding your overall IT security posture and accurately assessing your data protection initiatives. Many people don't realize that applications and servers are responsible for over 90% of all security vulnerabilities; yet, more than 80% of IT security spend continues to be at the network or perimeter layer.

There is no shortage of data points and industry studies that document this dangerous phenomenon; however, there are very few resources that give you practical advice on what to do about it. The ASM Model can be your first steps down that road.

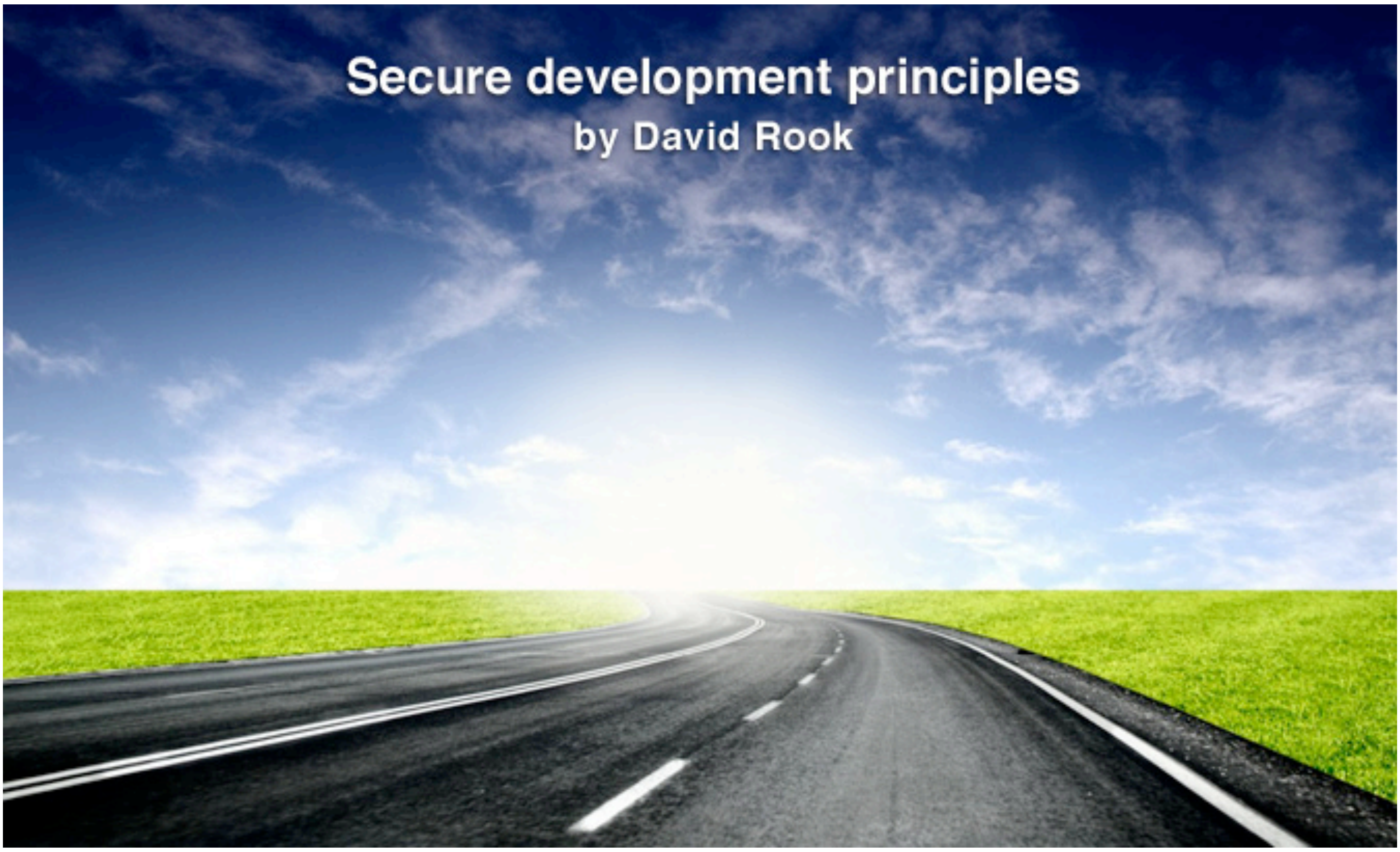
Ed Adams is the President and CEO of Security Innovation (www.securityinnovation.com). As CEO, Mr. Adams applies his information security and business skills, as well as his pervasive industry experience in the Application Quality space, to direct software security experts in helping organizations understand the risks in their software systems and developing programs to mitigate those risks. His organization has delivered high-quality risk solutions to the most recognizable companies in the world including Microsoft, IBM, Visa, Fedex, ING, Sony, Symantec, Nationwide and HP.

Mr. Adams is the founder and business owner of the Application Security Industry Consortium, Inc., an association of industry technologists and leaders establishing and defining cross-industry application security guidance and metrics. He is on the board of the National Association of Information Security Groups (NAISG).

Mr. Adams has presented to thousands at numerous seminars, software industry conferences, and private companies. He has contributed written and oral commentary for business and technology media outlets such as New England Cable News, CSO Magazine, SC Magazine, CIO Update, Investors Business Daily, Optimize and CFO Magazine. Mr. Adams is in the process of writing a book titled "Information Security Management: Survival Guide", which will be published by Wiley & Sons and is due out in November 2009.

Secure development principles

by David Rook



Give a man a fish and you feed him for a day - teach him to fish and you feed him for a lifetime. I feel this proverb can be applied to the content of most application security guidance projects and to the approaches taken by organizations that are trying to create secure applications.

Security professionals have often pointed to such projects as the bible for developers wanting to learn how to develop securely and championed various approaches to secure development, but one has to question whether current approaches actually help developers to produce secure software. We have seen the amount of recorded (given a CVE number) SQL Injection and Cross Site Scripting vulnerabilities increase from 8.6% of all vulnerabilities in 2007 to 33.46% in 2008. This growth has not slowed in 2009, with these two vulnerabilities accounting for 35.23% of all vulnerabilities this year so far.

These statistics alone must raise the question of whether the secure development projects are getting their message across to developers. More to the point - are these projects getting the right message across? I feel that these projects do a good job of telling developers what problems can occur and how to exploit these flaws but they don’t follow this up with useful guidance on how to develop applications that reduce the chance of these flaws occurring. I think this derives from the fact that the people who contribute to these projects like to be the hacker and often neglect the “boring” work of detailing the preventative measures that developers actually need to know. The work required to detail the preventative measures is tedious but essential, developers would not need to read and interpret multiple lists of “top x” vulnerabilities if they had a clear set of secure development principles. The projects that do detail how to develop securely are often bloated and cover hundreds of pages, which still leaves the majority of developers with one question: “How do I develop securely?” Providing an answer to that question is my motivation for this article and the work that will follow.

Keep things simple

Secure development education does not need to be complicated, nor does it need to explain specific vulnerabilities. That last point might seem like an alien concept to some people but I have recently been asking several experienced developers and myself whether developers need to understand specific vulnerabilities. I don’t think teaching developers about specific vulnerabilities is the most effective way to reach the goal of secure development. A developer’s education should evolve towards knowledge of the intricate details of attacks such as SQL Injection, yet almost all education efforts begin here. This is certainly an area that would benefit greatly from the KISS principle (Keep It Short and Simple) by avoiding unnecessary complexity.

The three most popular “top x” lists have 45 vulnerabilities listed between them, 42 of them have unique names despite the fact they do not represent 42 individual vulnerabilities. This only increases confusion and uncertainty instead of clearly detailing how one should build a secure application.

With the above paragraph in mind, I have attempted to take on the challenge of providing clarity around the issue of secure development by creating a set of secure development principles.

Secure development principles

I have analyzed many vulnerabilities and I have created a set of secure development principles which I feel will prevent the large majority of them. I have listed these principles below and I will elaborate on each of them in the rest of this article.

1. Input Validation
2. Output Validation
3. Error Handling
4. Authentication and Authorization
5. Session Management
6. Secure Communications
7. Secure Resource Access
8. Secure Storage.

Input validation

This principle is certainly not a silver bullet, but if you ensure that all of the data received and processed by your application is sufficiently validated you can go along way towards preventing many of the common vulnerabilities being actively exploited by malicious users. It is important for you to understand what data your application should accept, what its syntax should be and its minimum and maximum lengths. This information will allow you to define a set of "known good" values for every entry point that externally supplied data could exist.

Two main approaches exist for input validation: whitelisting and blacklisting. It would be wrong to suggest that either of these approaches is always the right answer, but it is largely accepted that validating inputs against whitelists will be the most secure option. A whitelist will allow you to define what data should be accepted by your application for a given input point, in short you define a set of "known good inputs". The blacklist approach will attempt to do the opposite by defining a set of "known bad inputs" which requires the developer to understand a wide range of potentially malicious inputs.

A simple regular expression used for whitelisting a credit card number input is shown below:

```
^\d{12,16}$
```

This will ensure that any data received in this input point is a number (\d = 0-9) with a minimum length of 12 and a maximum of 16 ({12,16}). Although this is a simple example, it clearly demonstrates the power of whitelist validation techniques because this input point will now prevent many common attacks.

The blacklisting approach will try to identify potentially malicious inputs and then replace or remove them. The example shown below will search the data received through an input point and replace any single quotes with a double quote.

```
s.replaceAll(Pattern.quote(" ' "),
Matcher.quoteReplacement(" " "));
```

The blacklisting approach is often avoided where possible, because it only protects against threats the developer could think of at the time of its creation. This means the blacklist might miss new attack vectors and have higher maintenance costs when compared to a whitelist.

Input validation best practices

- Apply whitelists (known good values) where possible.
- Reduce the data received to its simplest form. If the validation function only searches for UTF-8 input, an attacker could use another encoding method, like UTF-16, to code the malicious characters and bypass the validation function.
- Check for content (i.e. 0-9), minimum and maximum lengths and correct syntax of all inputs.

Output validation

In addition to validating all of the data your application receives, you should also follow similar processes for the data your application will output.

Some attacks such as Cross Site Scripting can take advantage of poorly validated output to attack unsuspecting end users through your application. There are three main issues associated with output validation that you should always aim to address in your application: data encoding, data format and length.

The data encoding process is slightly different depending on where your output is going to end up. For example if your data is going into a URL you need to ensure it is URL encoded. I have included an example below of a malicious value appended to a URL and how URL encoding of this data would remove the threat.

The example site has a parameter in the URL called day, this parameter will contain the current day and it will then write this into the homepage. This allows the homepage to always display the current day for the user.

```
www.examplesite.com/home.html?day=Monday
```

If we assume that the example site hasn't implemented output validation for the day parameter a malicious user could replace Monday with anything they wanted to. The parameter's lack of validation could be exploited with something like this:

```
www.examplesite.com/home.html?day=<script>alert(document.cookie)</script>
```

If a user were to access this URL, a pop-up that contained their cookie for the example site would appear. This is a simple example, but a malicious user could silently steal the cookie rather than show it to the user in a pop-up box. If the site had implemented URL encoding, the threat posed by cookie stealing JavaScript would have been nullified as I have shown below:

```
www.examplesite.com/home.html?day=%3Cscript%3Ealert%28document.cookie%29%3C/script%3E
```

A second type of encoding that should be considered is HTML Encoding. The first encoding we looked at covered encoding of data in a URL. If your data is going to be entered into a HTML page you should employ HTML Encoding.

I have included two sets of code below. The first piece of code has no output validation that could leave it vulnerable to attacks such as Cross Site Scripting.

```
#!/usr/bin/perl
use CGI;
my $cgi = CGI->new();
my $name = $cgi->param('username');
print $cgi->header();
print "You entered $name";
```

The code will accept any text into the username parameter and then use this data in the print statement:

```
print "You entered $name";
```

You can clearly see that no validation has occurred on this data. The username data should have been subjected to both input and output validation prior to it being used in the print statement.

This example uses Perl which means we can make use of the HTML::Entities Perl module to encode this data for us; the code shown below has implemented this module:

```
#!/usr/bin/perl
use CGI;
use HTML::Entities;
my $cgi = CGI->new();
my $name = $cgi->param('username');
print $cgi->header();
print "You entered ",
HTML::Entities::encode($name);
```

Any data entered into the username field will now be HTML encoded prior to it being printed. If a malicious user were to input the same JavaScript we used in the previous example (`<script>alert(document.cookie)</script>`) it would be changed to the following:

```
&lt;script&gt;alert(document.cookie)&
lt;/script&gt;
```

This would again nullify the threat posed by the malicious input. The values that have been changed (i.e. < & >) would still be written to the page but as a literal value instead of being used as a special character. This will allow you to implement strong validation techniques but also continue to display characters such as < & > on your web page.

In addition to the encoding we have explored already, we should always control the content encoding method used by the web browser. We can configure this in two places. Firstly, in the HTTP response header:

```
Content-Type: text/html; charset=utf-
-8
```

And secondly in the Meta tags:

```
<META HTTP-EQUIV="CONTENT-TYPE"
CONTENT="text/html; charset=UTF-8">
```

This will ensure that the browser correctly encodes your data. The final point to remember when you are implementing output validation is length validation. As we saw for input validation, we should define the minimum and maximum lengths for all of our data.

Error handling

Every application will eventually have to deal with an exception and it is vital that these are handled securely. If an attacker can force exceptions to occur and you fail to correctly handle these situations, you will expose sensitive information about the inner workings of the application. These detailed error messages will help attackers build a picture of your application and fine-tune their attacks.

An attack such as an SQL Injection will become significantly easy to exploit if an attacker can view the internal server error messages. I have included an example of an attempted attack and the un-sanitized error message that is returned to the attacker below:

```
http://www.examplesite.com/home.html?
day=Monday AND userscolumn= 2
```

You can see that the attacker appended **`AND userscolumn=2`** onto the URL to test for an SQL Injection vulnerability. The attacker's input was processed by the SQL Server that caused an exception to occur because the users column doesn't exist.

```
Microsoft OLE DB Provider for ODBC
Drivers (0x80040E14)

[Microsoft][ODBC SQL Server Driv-
er][SQL Server]Invalid column name
'userscolumn'.

/examplesite/login.asp, line 10
```

This type of error message is a common sight across the Internet and it will help attackers fine-tune their attacks against your application.

To prevent these kinds of errors reaching the end users of your application you need to ensure that you develop your code to handle expected and unexpected exceptions. The errors that are returned to the end users should be generic messages such as “Server error – please contact support”. There are several simple points to remember when you are trying to implement secure error handling:

- Never include information such as the line an exception has occurred on, the method that has encountered an exception or information such as stack traces.
- Never include file system paths within error messages.
- Ensure that service information such as ASP.NET version numbers are not contained within error messages.

Most languages will have their own methods for handling exceptions and I have included an example of the Try/Catch method of handling exceptions in Java on the following page.

```
import java.io.IOException;
import java.io.InputStream;
import java.net.MalformedURLException;
import java.net.URL;
public class Test {
public static void main(String[] args) {
String urlStr = “http://securityninja.co.uk/no_exist.html";
try {
URL url = new URL(urlStr);
InputStream is = url.openStream();
is.close();
} catch (Exception e) {
// Print out the exception that occurred
System.out.println("Error requesting " + e.getMessage());
}
}
}
```

In this example, we have received a request for /no_exist.html which doesn't exist on the server. The `catch` part of the code will ensure that the user is presented with the following sanitized error message:

`“Error requesting http://securityninja.co.uk/no_exist.html”`

You should always ensure that your own code provides error messages similar to the one above.

Authentication and authorization

If you fail to build strong authentication processes into your application, an attacker could access sensitive content without having to authenticate properly. Although this sounds like an issue principle number 7 (Secure Resource Access) should address, there is a clear difference between the two.

The Authentication and Authorization principle will aim to remove the following risks (this is not an exhaustive list):

- Lack of an appropriate timeout
- The use of weak passwords
- The use of weak “secret question” systems
- The use of broken CAPTCHA systems
- Failure to protect credentials in transit
- Failure to implement least privilege access.

If you are required to provide a logon within your application you should also implement timeouts and the requirement for users to set strong passwords. To determine how long your timeouts should be, you need to establish the sensitivity of the data or resource you are trying to protect. The timeout for an online bank would more than likely be shorter than the timeout for an online game site for example.

The same question should apply when you are determining how strong your users passwords should be. What are you trying to protect? In general your application should enforce the use of complex passwords with a minimum length of 7 characters. Complex passwords normally mandate the use of 3 of the following 4 elements:

- Uppercase characters
- Lowercase characters
- Numbers
- Special characters (i.e. @$^&).

Depending on the applications purpose, you should implement additional password controls such as a maximum age and prevention of password re-use. The passwords must be protected whilst being stored on application servers and whilst they are transmitted.

There are several points during the lifetime of a password that I feel require special attention.

The passwords must be stored in a secure location and encrypted, they must never be transmitted in the clear (i.e. without using protection such as SSL) and never fully visible in account management emails.

At this point, we are starting to construct a secure authentication system. But, this hard work can be undone by the incorrect use of automated systems designed to help you and your users. Almost every web application will have some form of password reminder system and a high percentage of them would have security weaknesses. These systems are designed to provide self-service capabilities to the end users, but they can also assist attackers in hijacking user's accounts. The point at which these systems traditionally fail is the secret questions used for password reminders. The answers to these questions can be easily guessed with a small amount of social engineering or brute forcing of the values. If your system used a question such as "What is your favorite capital city", the attacker knows this has a finite set of answers and can attempt to brute force the correct answer. If the secret question system fails to prevent a brute force attack, the user's password can be easily obtained. To prevent these kinds of attacks you could allow the user to define their own secret question or require the users to answer multiple questions before revealing the password.

The administrative functions should only be available to users in the admin group and the standard users must not have the capability to elevate their privileges.

In addition to weaknesses of the secret questions, many systems fail when they attempt to create information verification functions. The information verification piece of password reminder systems will often fail to demand enough information from the end user before granting them the account password. It is a common mistake made by these systems and you should attempt to avoid this where possible. Make sure that your systems require information from the user that isn't easily obtainable - such as an email address.

A second system often used during user account creation and management is CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart). As the name implies, these system are used to validate that a user (as opposed to a computer) is providing the input to your system,s but there have been many high profile failures of such systems. CAPTCHA systems implemented by Google, Microsoft and Yahoo have been broken which shows how difficult it can be to get this right. If you do decide to utilize this technology, you need to ensure that CAPTCHAS are not simple to guess (i.e. What is 2+3) or clear enough to be read by OCR software.

The final thing to remember in this principle is the enforcement of authorization through least privilege. A simple application could have two levels of access, user access and administrative access and each one will have its own access requirements. An obvious difference between the two levels of access is the authorization to use the administrative functions of the application. The administrative functions should only be available to users in the admin group and the standard users must not have the capability to elevate their privileges. The user accounts used for your application should be given the least amount of privileges required for them to function correctly. The ideal starting point would be to configure access controls to deny all access and gradually increase the access until you find the right level for each user role.

You should always avoid using client side values to make access decisions, avoid using information such as client side tokens, URL values or hidden fields because they can be manipulated to give a user elevated privileges.

Session management

When a user connects to your application, you can force them to provide logon credentials. If the user authenticates successfully, they shouldn't be expected to provide these credentials again unless the logon times out or they are executing a privileged action.

Session management allows your application to require the users to authenticate only once and also confirm that the user executing a given action is the user who provided the original credentials. To an attacker, any weaknesses in the session management layer of your application can be an easy way to bypass the hard work we have done so far in the first four principles.

Attacks against sessions are often focused on obtaining a valid session value through either exploiting your users or taking advantage of weaknesses in the session management functionality itself. Knowledge of the methods used by attackers isn't required if you secure your sessions based on the advice in this principle.

The session values used in your application should follow similar principles to the secure password requirements I outlined earlier. The session IDs used to identify individual authenticated users should be of a sufficient length to prevent brute force attacks. This length is going to be determined by the sensitivity of the data or resource you are trying to protect. I do have to stress that session ID length isn't enough to provide protection by itself; you also need to have a high amount of entropy per character in the session ID. The entropy of each character position must be considered in your creation of sessions IDs, with higher entropy per character being more secure. A session ID should be constructed from a large character set without any obvious patterns in the IDs. A pattern such as character positions 1, 4 and 5 always containing the letter C would be easily identified by automated tools and will reduce the computation time required to brute force genuine IDs.

If the above steps have been followed each user should have a strong session ID that cannot be predicted easily by attackers. We now need to ensure that these IDs are secured both on the application server and whilst they are in transit. The storage location for the session IDs should be a secure location. Refer to the principle of least privilege we have outlined earlier for guidance on how to secure access to this location. The next point we need to secure is the transmission of the session IDs and a simple answer exists for this: if the session ID is transmitted via HTTP it can be easily intercepted and re-used by an attacker - by using HTTPS instead you can protect the session ID in transit.

At this point we should have a session ID that is resistant to prediction, brute force and interception attacks but we do have a few more protection measures to implement before we can be comfortable with the security surrounding our session management. There are many examples of applications verifying whether a session ID exists, but not checking whether this is a genuine ID. If the application performs this minimal level of session ID checking, an attacker can perform session fixation attacks against your users. You should always mandate that session IDs are only accepted if they are generated by your application server and overwrite those values which are present in requests but not provided by your application.

The final two session protection mechanisms you need to provide are timeouts on sessions and changes of session IDs when users carry out sensitive actions. We have already discussed the requirement for timeouts of user logons and the same protection must be in place for sessions. You will need to identify the maximum age of any given session ID as well as a timeout for sessions. There is often the requirement to re-authenticate users during a session, for example an online bank application would re-authenticate the user prior to transferring funds. This second authentication should also prompt the creation of a second session ID and the destruction of the original ID.

Secure communications

We have mentioned in previous principles the importance of protecting specific pieces of information whilst they are in transit and we will expand on that now. The requirement to protect data in transit is not a new requirement but it is something that applications often fail to implement correctly.

This is perhaps the simplest principle to get right. Make sure your applications enforce the use of secure transport mechanisms such as SSL, TLS or SSH. You must also make sure that your application enforces specific secure versions of these mechanisms such as SSL version 3 or SSH version 2.

If this principle is so simple, how do developers get this wrong? The problems often arise from two main decisions:

1. When to use these mechanisms
2. Which version to use

The common failure surrounding decision number 1 is the failure to protect the start of a session and the session information after an authentication. You must start the protection as soon as a user lands on your site; this means making the logon pages you have HTTPS instead of HTTP. In addition to encrypting the session from the get go, you need to continue this protection throughout the whole session and not only for the submission of logon credentials. If the data is highly sensitive you should continue to provide secure transport mechanisms internally from your application server to systems such as database servers.

The final thing to address is using a mechanism that is cryptographically secure and does not have a flawed design. A good example of a protection mechanism that is not secure is SSLv2; several of its vulnerabilities come from weaknesses in its design and not through a cryptographic weakness. I mentioned two protection mechanisms earlier and they are examples of how to protect your data in transit. If you are selecting a transmission protection mechanism you should use one that is accepted as being secure, such as SSLv3, TLSv1 and SSHv2.

Secure resource access

Securing access to your application resources has been addressed in several of the previous principles but we will look at specific issues that can arise now. The issue of authenticating and authorizing users along with secure session management have been covered already but these can be undermined by poor design decisions.

If a design depends on the principle of security through obscurity it is almost certain to fail. A common approach to securing sensitive locations is to hide them from users by not publishing a link to them. This really fails to provide any level of security because automated tools will discover these locations and allow attackers to access them directly. If the location contains sensitive information (i.e. /backups) or functionality (i.e. /admin) you must provide strong access control mechanisms that ensure users accessing the location are authorized to do so. The authentication and authorization checks must not be a one-time check; each step taken by a user using sensitive functions must be evaluated. A real world example of a failure in this kind of system would be the T-Mobile website hack (2005) which lead to Paris Hilton's account being compromised. The password reset functionality of the T-Mobile website required a user to prove who they are by providing their phone number; the site would send them a unique token to enter into the site before they progressed to a password reset page. The problem with the site design was it assumed users would only ever access the password rest page if they had been authenticated. An attacker called Luckstr4w found that if you browsed directly to the password reset page you could reset the accounts password without providing any evidence of who you were. The rest, as the say, is history.

You have to assume that if your resource is accessible to any of your users, it will be possible for anyone to access it. To understand how to enforce security on these resources please refer to principle number 4 (Authentication and Authorization).

Secure storage

The final principle is secure storage. We have secured our inputs and outputs, implemented sanitized error messages, created strong access control for all of our resources and protected information in transit, but we cannot neglect the security of data at rest. The requirement to securely store data such as credit card numbers is obvious, but we must also secure data such as passwords and session details whilst they are at rest. You not only need to identify what data needs to be protected, but also which mechanisms you will use to provide the protection.

The selection of the protection mechanism should follow the same guidelines as the selection of one for secure communications - never create your own and do not use weak mechanisms such as DES, MD4 and SHA-0.

I do not want to turn this principle into a cryptography lecture but you should ensure that the following bit sizes are used for Symmetric, Asymmetric and Hash mechanisms:

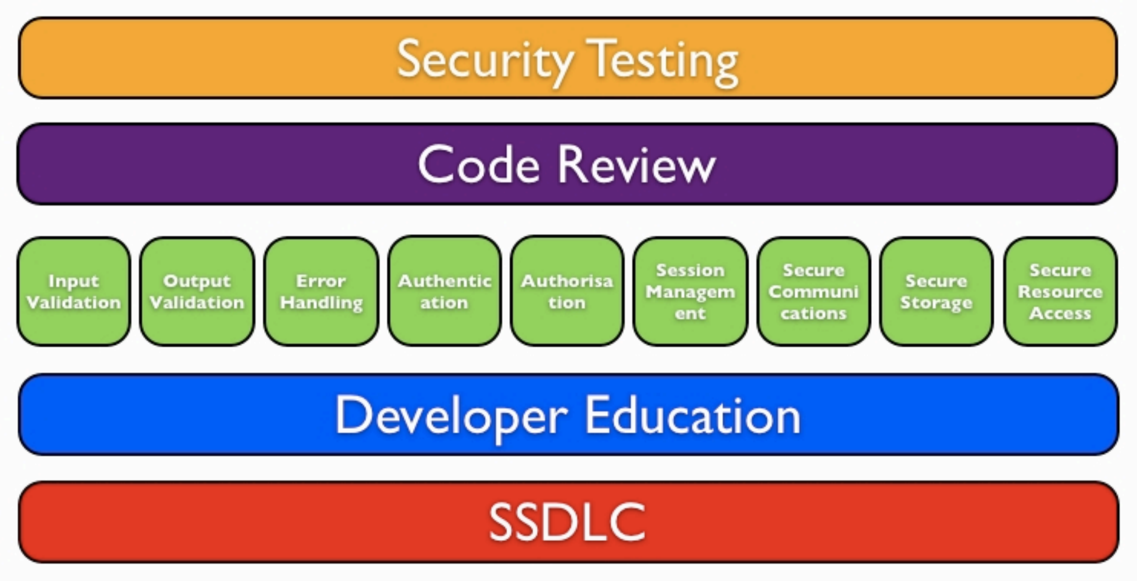
- Symmetric – 256 bits or above
- Asymmetric – 2048 bits or above
- Hashes – 168 bits or above.

You should also provide a secure location for any encryption keys you are using; storing them on the application servers generally does not provide a secure location. The final thing to avoid is the hard coding of keys into your code.

The principles place in secure development

The principles I have outlined so far will help you to develop secure software but this should be just one step in a wider secure development process. They will provide a good level of security for your application but they should not be used in isolation.

I have included an image below that shows the steps I feel need to be followed in the pursuit of a secure application and where these principles fit in:



The foundations underpinning any secure development efforts must be a clearly defined Secure Software Development Life Cycle (SSDLC) and developer education. If you do not know where, when and how security will fit into your development life cycle then it is very difficult to have security ingrained into requirements and designs.

The failure to design applications securely will lead to project delays when the code reaches the security code review and testing steps. Each phase of the SSDLC should have some level of security input and sign off, but I will not go into details on how to build an SSDLC in this article (see my article in (IN)SECURE magazine, issue 18). Developer education should be self-explanatory; this entire article is largely discussing how to educate developers on how to develop securely. A common failure within organizations is the assumption that developers know how to develop securely and they subsequently fail to invest time and money into education programs. This will never lead to secure software and organizations have to realize that developer education is a step along the path to secure software.

The principles are shown in the image but I won't dwell on this step, this article explains the principles and why I have created them. The code review step will mandate that a security focused code review be conducted for every development; this review should evaluate the code against these secure development principles. The final point to address is the testing of the development for security weaknesses. This testing should be as comprehensive as possible and test for the vulnerabilities that the secure development principles should protect against.

The important thing to remember for all of the steps is that it doesn't have to involve a large financial outlay to implement them. I have included information below detailing on how I feel you can utilize free resources to build your secure development program:

SSDLC – The Microsoft Security Development Life Cycle (SDL) is one of the leading SSDLC processes in existence. Microsoft has made a wealth of information available for free so you can base your own SSDLC on their internal processes.

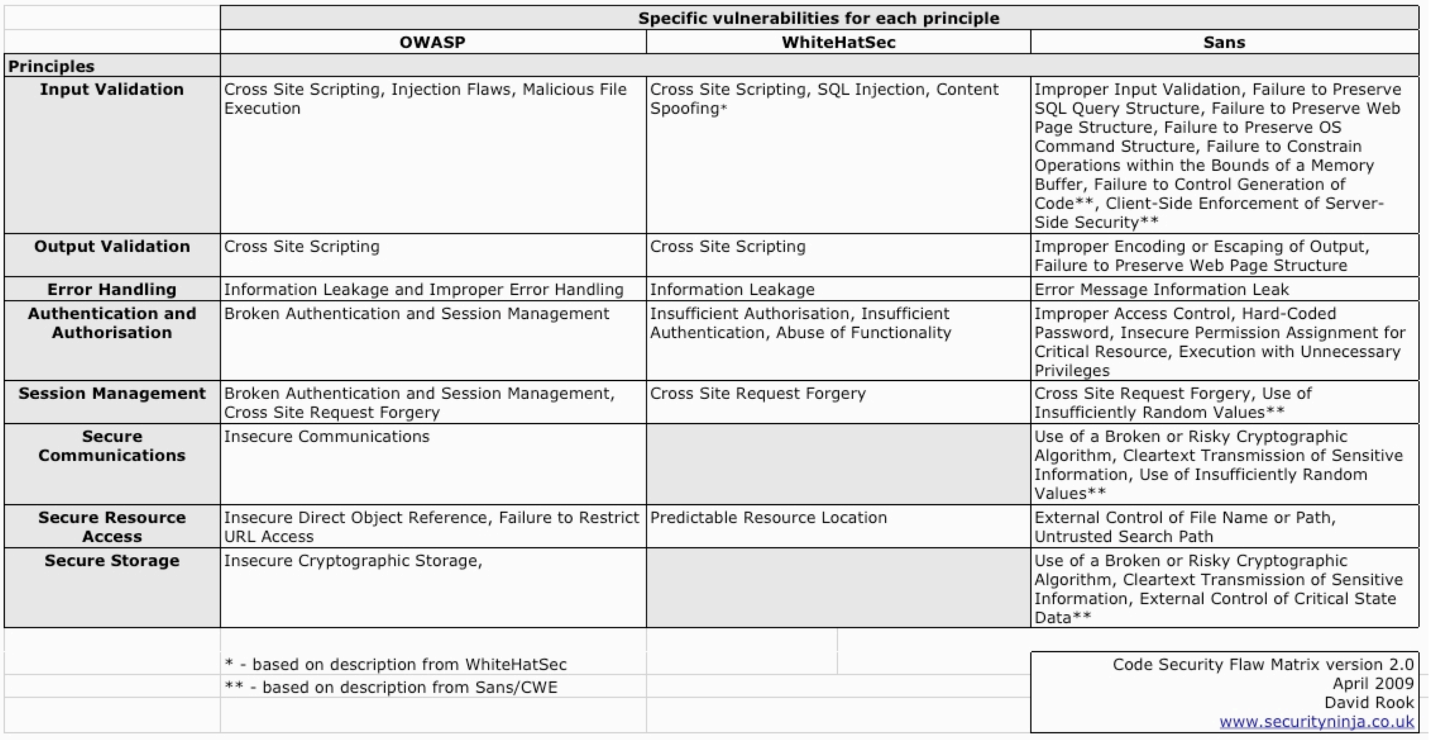
Development Education – Publications such as this one will always contain information that is useful for developers and, above all, it will be free. An avenue that is often not explored is OWASP chapter meetings. These meetings will have experts from your area presenting on application security topics that anyone can attend for free. The OWASP also have an education project that provides free materials for conducting developer awareness sessions.

Code Review – This is another area where the OWASP can help you. The OWASP Code Review Guide contains guidance on how to review code for many different vulnerabilities. There are a few free tools available and I would recommend the OWASP Code Crawler and Orizon projects to help you with your reviews.

Security Testing – The testing of an application should consist of both manual and automated tests. To help you with your automated testing I recommend using the Burp Suite and Grendel Scan.

Mapping the principles to specific vulnerabilities

The table shown below maps the secure development principles to common vulnerabilities taken from three “top x” lists. More information surrounding these mappings can be found on securityninja.co.uk/blog.



	Specific vulnerabilities for each principle		
	OWASP	WhiteHatSec	Sans
Principles			
Input Validation	Cross Site Scripting, Injection Flaws, Malicious File Execution	Cross Site Scripting, SQL Injection, Content Spoofing*	Improper Input Validation, Failure to Preserve SQL Query Structure, Failure to Preserve Web Page Structure, Failure to Preserve OS Command Structure, Failure to Constrain Operations within the Bounds of a Memory Buffer, Failure to Control Generation of Code**, Client-Side Enforcement of Server-Side Security**
Output Validation	Cross Site Scripting	Cross Site Scripting	Improper Encoding or Escaping of Output, Failure to Preserve Web Page Structure
Error Handling	Information Leakage and Improper Error Handling	Information Leakage	Error Message Information Leak
Authentication and Authorisation	Broken Authentication and Session Management	Insufficient Authorisation, Insufficient Authentication, Abuse of Functionality	Improper Access Control, Hard-Coded Password, Insecure Permission Assignment for Critical Resource, Execution with Unnecessary Privileges
Session Management	Broken Authentication and Session Management, Cross Site Request Forgery	Cross Site Request Forgery	Cross Site Request Forgery, Use of Insufficiently Random Values**
Secure Communications	Insecure Communications		Use of a Broken or Risky Cryptographic Algorithm, Cleartext Transmission of Sensitive Information, Use of Insufficiently Random Values**
Secure Resource Access	Insecure Direct Object Reference, Failure to Restrict URL Access	Predictable Resource Location	External Control of File Name or Path, Untrusted Search Path
Secure Storage	Insecure Cryptographic Storage,		Use of a Broken or Risky Cryptographic Algorithm, Cleartext Transmission of Sensitive Information, External Control of Critical State Data**

* - based on description from WhiteHatSec

** - based on description from Sans/CWE

Code Security Flaw Matrix version 2.0
April 2009
David Rook
www.securityninja.co.uk

I started this article with a proverb and I would like to end it with one of my own. The reason I have created the secure development principles is to help developers create applications that are secure and not just built to prevent the current common vulnerabilities. I feel this proverb sums it up: "Teach a developer about a vulnerability and he will prevent it, teach him how to develop securely and he will prevent many vulnerabilities." I would like to use this article as the basis for a secure development principles guide to help developers write secure code. If anyone wishes to help me contact me: davidrook@securityninja.co.uk.

David Rook works as a Security Analyst for Realex Payments in Dublin. He is a contributor to several OWASP projects including the code review guide and the browser security framework working group. David is a member of the Irish Internet Association Web Development Working Group helping to publicize web application security within Ireland. David has his own security website and blog (www.securityninja.co.uk/blog) and a Secure Development Principles website (www.securedevelopment.co.uk).

Enterprise risk and compliance reporting

by Gideon Rasmussen

Modern companies are challenged by the need to demonstrate compliance, mitigate risk and fund security initiatives. Reporting is the pursuit of simple truth. Like with many technical challenges, the underlying complexity can be daunting. This article addresses a variety of techniques to report risk and compliance statuses, raise awareness and influence remediation.

I. Preparation

Mission / vision

Document each security function's mission as a first step towards reporting. A mission can be loosely defined as the high-level goals of a team. A mission statement explains the purpose of a team from a business perspective. Vision can be defined as how the team accomplishes its mission.

A basic goal of reporting is to determine the effectiveness and current state of a given function. It becomes easier to determine at a high-level which elements should be included in reporting by keeping the mission and vision statements in mind.

Reports and data sources

Meet with each team or function and request access to their reporting. Evaluate critically each report. Determine whether the reporting accurately reflects the status based upon the mission.

At a high-level, risk and compliance reporting should meet the following goals:

• Reflect security posture and the associated risk to core business products, services and strategic goals.

- Consider assessment subjects from a variety of perspectives.
- Enable management to make informed decisions.
- Provide reporting in a timely manner, preferably through real-time automation.
- Identify a point of contact associated with each subject/finding. Accountability is critical to remediation.
- Support compliance with laws, regulations and contracts.

The process of gathering existing reports also identifies reporting points of contact and data sources. Take note of each. Begin documenting a reporting methodology at this phase as well.

Risk vs. compliance

Business management may be of the mindset that compliance is an ideal state, similar to nirvana. Identify which mandate each control corresponds to. When a control is tied back to an external requirement, management may support compliance to avoid penalties.

Risk can be subjective, which is where a well-documented reporting methodology becomes crucial. Executives want reporting in relatively simple terms. The use of high, medium and low findings with corresponding red, yellow and green colors is common. Include supporting data as well. Create a reporting methodology based upon sound principles, with management as the intended audience.

II. Identify reporting types

Baseline controls

It is necessary to have well-defined information security standards before reporting compliance status. Start by establishing a control baseline in accordance with regulations, laws and contractual obligations. A control baseline also clarifies policy into specific requirements. Refer to NIST SP 800-53 as an example. Use a control framework such as ISO 27002 or COBIT to bolster the baseline. Conduct a risk assessment to close remaining gaps. Classify each baseline control to facilitate reporting when findings are present.

Control Name	ACME0001	ACME0002	ACME0003
Requirement	Maintain a security awareness and training program.	Sensitive authentication data must not be stored after authorization.	Monitor system and network performance and capacity levels.
Environment	Enterprise	Payment Card	Enterprise
Source(s)	ISO 27002, PCI DSS, SOX Control Objectives	PCI Data Security Standard	Sarbanes Oxley IT Control Objectives
Control Category	Administrative	Technical	Technical
Control Type	Preventive	Preventive	Detective
Risk Impact	Medium	High	Medium
Domain	Personnel Security	Data Retention	Monitoring

Security metrics

Determine what types of reporting are necessary based upon mission, audience and available data. Here are a few examples and free reporting resources for inspiration.

Metric	Source
Percentage (%) of high vulnerabilities mitigated within organizationally defined time periods after discovery.	NIST: SP 800-55: Performance Measurement Guide for Information Security (bit.ly/1wvY5Z).
Percentage of business unit heads and senior manager who have implemented operational procedures to ensure compliance with approved information security policies and controls.	Corporate Information Security Working Group: Report of the Best Practices and Metrics Teams (bit.ly/Skt9h).
% of systems configured to approved standards.	Center for Internet Security: Consensus Information Security Metrics Service (bit.ly/MThR6).

The large number of metrics within the above resources may seem overwhelming. Create a spreadsheet and sort them by data sources (teams and tools), audience throughout management tiers and metric implementation phases. Dan Geer's Measuring Security Tutorial (bit.ly/bcPM9) contains a wealth of information - refer to it as well.

Risk priority

Compliance is binary, either a control is in place or not. One missing control will result in a non-compliant status, which does not represent the risk associated to business. Use risk scoring to assign potential business impact to each report finding. Start by applying a risk rating to each baseline control.

Refer to the Microsoft Security Risk Management Guide (bit.ly/flzwG) to determine impact levels and associated exposure ratings. Failure Modes and Effects Analysis (bit.ly/vctqM) has risk scoring built in. Define which ratings threshold should constitute a control that is risky and needs to be shored up.

Establish a common reporting language. The meaning and related impact of high, medium and low findings should be uniform throughout each report. Refer to NIST 800-30 (bit.ly/9EO5i) for sample risk impact definitions. This interim approach assigns a risk value to each baseline control to assist with remediation priority. Establish a comprehensive Enterprise Risk Management Methodology and incorporate it into reporting in a future phase of development.

MANAGEMENT NEEDS THE ABILITY TO DRILL DOWN FROM HIGH-LEVEL REPORTING TO SPECIFIC ISSUES

II. Implement appropriate reporting

W. Edwards Deming said "What cannot be measured cannot be managed". Business management is likely to be of the same opinion. Establish a single risk and compliance application for the entire company. The application should accept data from a variety of sources. Questionnaire functionality is needed to facilitate security self-assessments and annual security awareness training and testing. The application should accept data feeds from a variety of sources such as log and security monitoring software. Security team members will need the ability to manually enter findings from on-site assessment reports. The application should also produce security reports to support internal and external audits such as Sarbanes Oxley and PCI.

Reporting is a data-centric pursuit. Therefore, it makes sense to copy reporting data to a central repository. From a single location, it is possible to analyze data and provide reporting. It will be necessary to have a phased implementation. If a large organization is in scope, start with a line of business and scale to the enterprise over time. Duplicate existing reports in the initial phase and add new reports later. Use role-based access control to restrict reporting to those with a need-to-know. Monitor manually entered report data to ensure it is kept current.

Establish a risk and compliance dashboard

Establish enterprise reporting by management tiers. Reporting should start at a high-level, detailing risk and compliance statuses for the enterprise and individual lines of business. Take care when aggregating enterprise risk and compliance statuses to provide a high-level executive view. It can be difficult to accurately accomplish this task due to the complexity of the underlying reporting. The executive dashboard should also include security metrics and trending. Management needs the ability to drill down from high-level reporting to specific issues within underlying populations, subjects and findings. That functionality is crucial. Include a link to the reporting methodology document at the bottom of the screen for quick reference.

Consider the audience

Reporting by tiers is an effective way to present information in a manner that is meaningful to each audience. Report findings must be actionable.

- Company executives want to know the state of risk and compliance throughout the enterprise. Reporting at this level may be presented to shareholders and the audit committee.
- Line of Business management needs coordinated reporting from security teams to understand what the issues are and how they can impact business. Once an issue is confirmed, it is necessary to offer a solution, ideally with options.
- IT managers need reporting by population and low-level details used by their reports to resolve findings.
- Individual contributors need specific findings that apply to the systems and applications they administer.

Prioritize risk and compliance statuses within each reporting tier. Work closely with business and IT management to assign a remediation contact to each finding for accountability. Each finding should also include details of the issue, planned remediation activity and target remediation date.

Using the methodology detailed above, an executive should be able to click down from the line of business, to a high risk subject, associated findings and remediation plans. In practice, that functionality is a powerful way to gain visibility and funding to address critical issues.

III. Present to management

Finalize the Reporting Methodology document. This article can be used as a framework. Explain the rationale behind each report including data sources such as teams, tools, manual data entry, automation and data refresh periods. Include the importance of risk mitigation over minimum compliance. A methodology document has utility for training, continuity and audit.

Prepare a management slide presentation to introduce the reporting application, executive dashboard and remaining implementation phases. Conduct a live demo of the application during the presentation. Manage expectations up front. Be transparent about current functionality and areas for improvement. Provide a roadmap for future reporting enhancements.

An accurate reporting system is bound to identify high risk findings. Encourage management to foster a culture where high risk findings are permissible, providing remediation contacts and target remediation dates are promptly identified.

IV. Maintenance

Reporting must evolve to adapt to changes in business practices, technology and emerging threats. Keep acceptable risk and compliance ranges tied to a methodology based upon risk and reward (versus tightening ranges as metrics improve). Future phases of development can include feeds from other departments (e.g. audit), inclusion of financial risk reporting and implementation of new metrics.

If a security department does its job well, nothing happens. Business continues to function without disruption or impact. Therein lies the challenge, especially in a tight budget year. Reporting reduces subjectivity and uncertainty. Comprehensive reporting demonstrates the value of the information security program and helps drive future initiatives and funding.

Gideon T. Rasmussen is a Charlotte-based Information Security Vice President with a background in Fortune 50 and military organizations. His website is www.gideonrasmussen.com.

CyberSecurity Malaysia II SecureAsia@Kuala Lumpur
7 July-8 July 2009
www.informationsecurityasia.com

Brucon 2009
18 September-19 September 2009
www.brucon.org

6th Annual CISO Executive Summit & Roundtable 2009
10 June-12 June 2009
www.mistieurope.com/ciso

2009 USENIX Annual Technical Conference (USENIX '09)
14 June-19 June 2009
www.usenix.org/events/usenix09/

Mastering Computer Forensics
22 July-23 July 2009
www.machtvantage.com/computerforensics.html

18th USENIX Security Symposium (USENIX Security '09)
12 August-14 August 2009
www.usenix.org/events/sec09/

ICDF2C 2009: The 1st International ICST Conference on Digital Forensics & Cyber Crime
30 September-2 October 2009
www.d-forensics.org

23rd Large Installation System Administration Conference (LISA '09)
1 November-6 November 2009
www.usenix.org/events/lisa09/

Q&A: Ron Gula on Nessus and Tenable Network Security

by Mirko Zorz

Ron Gula is the CEO and CTO of Tenable Network Security. He traces his passion for his work in security to starting his career in information security at the National Security Agency conducting penetration tests of government networks and performing advanced vulnerability research. In this interview he discusses Nessus, a security tool that doesn't need an introduction.

Nessus is one of the most popular security tools in the arsenal of many. Do you have an estimate on the number of users?

Estimating the number of users is very difficult, since a single large network scanned by a single Nessus scanner could in fact audit the security of 10,000+ users. Similarly, many home users download Nessus and subscribe to our HomeFeed and only scan a few systems. We typically measure downloads of Nessus in the millions per year.

What are the features Nessus clients request the most? What can we expect in upcoming versions?

There are many different types of Nessus users. Very often, new users don't know about that Nessus can perform patch and configuration audits and they are pleasantly surprised to add this to their list of tools to perform auditing.

Experienced users often ask for features more about how Nessus is used than what Nessus does. For example, we get a lot of requests to integrate Nessus results with ticketing systems like Tivoli. However, rather than try and support all of these various use cases for ticketing, we created a standard reporting format (called a .nessus report) that makes it very easy for anyone who wants to work with Nessus data.

The performance of Nessus 4 surprised many people. We didn't get many complaints about the speed of earlier versions of Nessus, but a lot of times, people forget that Nessus performs testing that is much more comprehensive than most other scanners. Similarly, for customers that use credentials for patch audits, when we added the ability to do client side "netstat" port enumeration, this dramatically changed the way a lot of experienced Nessus users performed their audits.

As time goes by, software and threats change, and so does the process of looking for security issues. In your opinion, what should be done in order to improve vulnerability research in the future?

I think the industry is moving in the right direction with more focus on secure code development before a product is shipped, as well as more of a focus on configuration management of operational systems rather than being reactionary to newly discovered vulnerabilities.

As the CEO of a vulnerability scanner company (we do log analysis and network monitoring too!) I get some criticism for this view, but the reality is that if you are 100% patched right now, you are still 100% vulnerable to what you don't know about. Minimizing what your systems do and hardening them is the only real way to combat this sort of threat.

Where do you see the current security threats your products are guarding against in 5 years from now? What kind of evolution do you expect?

I feel that cloud computing has been overhyped, but if you are in an organization that has made a political decision to outsource some sort of business critical applications, you need the tools to understand what sort of risk this poses to your network. You may or may not be able to audit the architecture of this application. This scares me much more than any particular new threat.

Our strategy here is the same one that has helped Tenable be successful in the enterprise. We combine credentialed, network and passive vulnerability and configuration auditing into one platform. There are many cases when scanning a network to find security issues is fine. However, you may also need to be able to audit what is going on inside a host. And you may have other situations where you aren't even allowed to touch a network resource for some technical or political reason. In this case we use passive scanning technology which looks at packets to produce an inventory of systems, applications and vulnerabilities.

We feel this blended approach will suite Tenable well for the next five years against new types of security threats, as well as political threats to the audit process as well.

You are very active on the Tenable blog. Has this way of communicating with your clients in any way changed the way Tenable does business? Could a blog post with no marketing hype replace a press release in the future?

The blog is very unique medium. It allows us to address Nessus home users, Tenable customers, competitors, industry analysts, the media, the government and several other venues, all at the same time. We also recently added a professional discussions forum where Nessus users and Tenable customers can exchange information and strategies on using Nessus, gathering logs, performing security audits, and much more. A blog post will never replace a press release, because there are many business partners and media outlets whose primary source of information is reading press releases. However, most customers and Nessus users don't really read press releases.

As a company, what challenges does Tenable face in the marketplace? What do you see as your advantages, especially with the economic downturn?

Tenable is in its sixth year of business. We've had tremendous growth each year and consistently increased our Nessus and enterprise customers along the way as well. Our biggest strength is execution. Our products continually get better. We have been able to add features such as auditing anti-virus configurations, MS SQL databases settings and searching for social security numbers in documents to Nessus without a performance hit or a cost increase to our customers.

In the same way, our enterprise products have also grown. Our main management console, the Security Center, was the first traditional vulnerability scanning platform to the certified by the government to perform configuration audits. Our log analysis products now gather, compress and search logs just as fast, if not faster than our competitors.

As the economy has had a downturn, this has helped Tenable. Our existing customers have always recognized all of our different types of enterprise products, but now with limited budgets, organizations are finding they can perform scanning, patch auditing, log analysis, correlation and configuration auditing from one platform. We call this "Unified Security Monitoring".

Infosecurity Europe 2009 gathered security professionals in London in April. This huge event had over 12,500 attendees and we were among them. Here are some details from the show.

Network security for latency-sensitive SCADA environments

Apani entered into a new partnership with Telvent which will offer Apani EpiForce as a security overlay to its OASyS DNA 7.5 Supervisory Control and Data Acquisition (SCADA) platform. Deployed in many of the largest oil, gas and electric companies in the world, OASyS is a real-time, distributed solution suite incorporating interoperable applications linked through standard interfaces. (www.apani.com)

New secure VoIP offering from Alcatel-Lucent

Alcatel-Lucent's new secure voice offering - comprising its VPN Firewall Brick platform with an Alcatel-Lucent IP telephony platform - safeguards and guarantees quality-of-service for VoIP calls and protects web-facing IP telephony applications such as contact centre, mobility and unified communications tools. (www.alcatel-lucent.com)

PGP Encryption Platform extends support to IBM i for Power Systems

PGP released PGP Command Line for IBM Power Systems. PGP is continuing to extend its support for various operating systems including midrange and mainframe environments, Windows, Unix, Linux and now IBM i; making it easier for enterprises to integrate and automate business information security with end-to-end encryption. (www.pgp.com)

Data protection and vulnerability management solutions from Lumension

Lumension announced the next iterations of its Lumension Endpoint Suite and Lumension Vulnerability Management Suite. Key benefits of the Lumension Endpoint Suite include validated encryption capabilities via in-process FIPS 140-2 certification, expanded OS platform and virtualization support. (www.lumension.com)

THE AUTHENTICATION COMPANY
DIGIPASS BY VASCO
BY VASCO
DIGIPASS Pack for Remote Authentication
Replace username and password logon with a safe solut
Check Point
Our partners
DP Mobile

Web security services for PlayStation 3 and PlayStation Portable

Trend Micro's Web security services will be made available to users of both PS3 and PSP. With the increasing number of gamers now connected to the Web, Sony has taken the precautionary step to provide their handheld and video game console users with protection against online crime. (www.trendmicro.com)

Innovative authentication for Microsoft IAG

GrIDsure's authentication solution for Microsoft's Intelligent Application Gateway (IAG) allows users to authenticate themselves by remembering a minimum of a four block sequential pattern on a five-by-five grid, known as a Personal Identification Pattern (PIP). Users just enter a randomly generated number on the keypad that corresponds to their PIP on the grid. (www.gridsure.com)

Secure mobile communications platform from AEP Networks

AEP Networks launched AEP SecComm Personal, a unique communications platform that delivers enhanced grade encryption to remote work forces. The technology is eminently portable, coming as it does in a small yet robust computer bag. It's plug and play so users do not need any degree of technical skill or expertise to get the product up and running and then connect to the available networks. (www.aepnetworks.com)

The sensible solution to hard disk destruction

The small, durable and easily transportable Hard Disk Crusher can crush over 60 disks an hour. It drills through the hard disk's spindles and physically creates ripples in the platters making it impossible to recover the data. The HDC-V can destroy a disk and the data on it in just seconds without the need of a peripheral PC or workstation. (www.diskcrusher.com)

PCI compliance important to 80% of UK organizations

BREACH

Breach Security and Evolution Security Systems jointly released their 2008 UK PCI Compliance Report. Surveying UK organizations across a variety of market sectors, including healthcare, government, e-commerce, finance and banking, the report findings indicate that PCI compliance is important to eight in 10 UK organizations. Further, 57 percent, are either PCI compliant or actively working toward becoming compliant. While this represents good progress, it also indicates that the UK is trailing the US in adoption of PCI compliance. (www.breach.com)

Hardware encrypted drive for Mac users

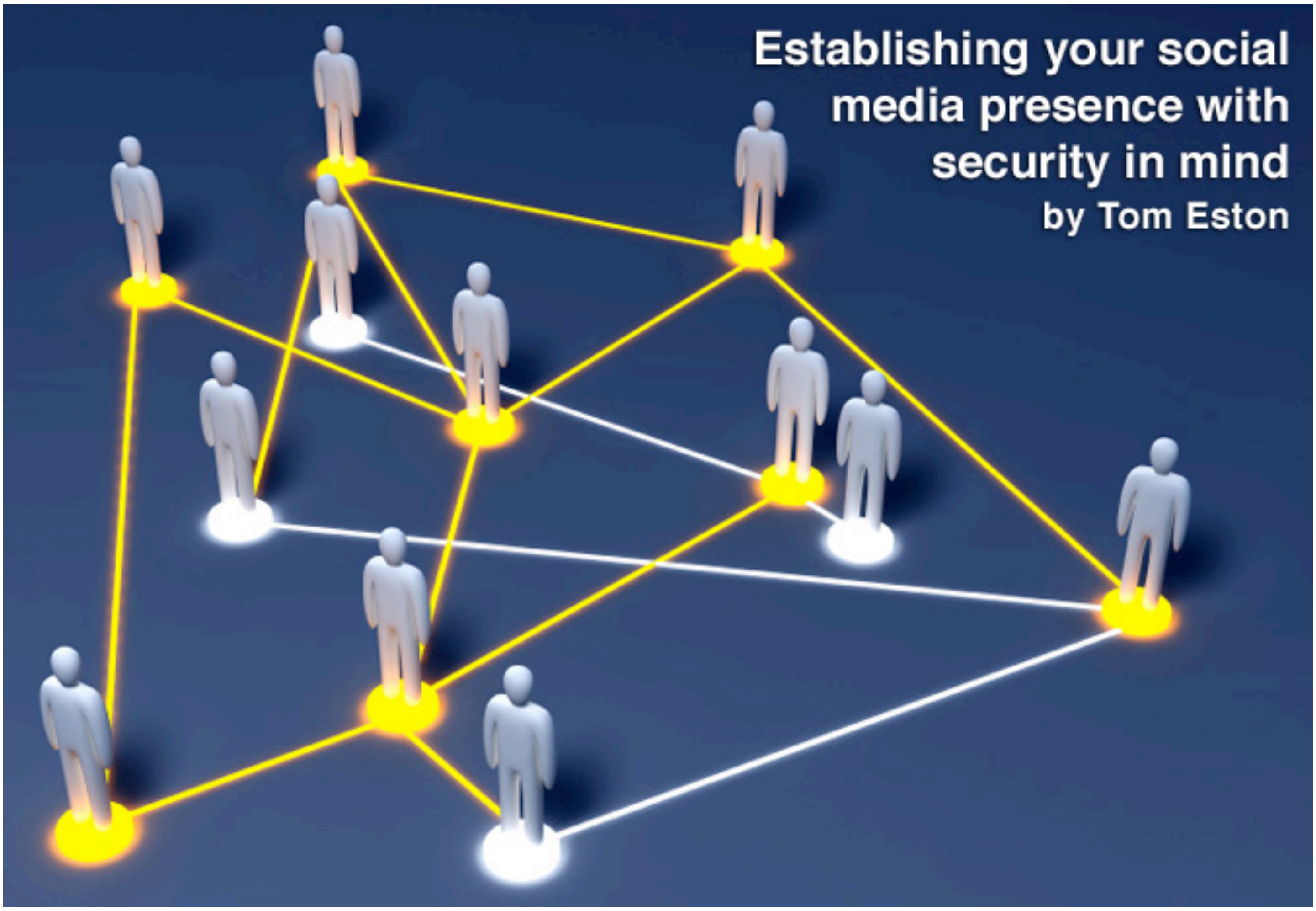
Kingston announced that its DataTraveler Vault Privacy Edition (DTVP) USB Flash drive is now compatible with Mac OS X. Data onboard the DTVP is secured by hardware-based, on-the-fly, 256-bit AES. The drive has fast data transfer rates and is protected from brute-force attacks by locking down after 10 unsuccessful login attempts. The DTVP is made of aluminum and is waterproof up to a depth of four feet. (www.kingston.com)

Organize and secure audit data with Secure Audit Vault

Kinamik Data Integrity launched the Secure Audit Vault, a tool that organizes and secures audit data for supporting auditing, control, compliance and e-discovery processes. (www.kinamik.com)

Nintendo partners with Astaro for Web security

Astaro will use its content filtering technology to deliver an Internet security service for the new Nintendo DSi Browser. The Nintendo DSi Browser can be downloaded onto the Nintendo DSi and offers users mobile internet access. Consumers can then opt into Astaro's internet security service by adjusting their browser settings. Nintendo will use Astaro's content filtering and Web security technology to provide additional parental control services to its customers and protect the Internet browsing experience for younger users. (www.astaro.com)



Establishing your social media presence with security in mind

by Tom Eston

Social media and social networking is the fastest growing technology that is being used on the Internet today. In a recent report by Nielsen, social networking is now the fourth most popular online activity - even ahead of email. It's no surprise that services like Facebook, LinkedIn and Twitter are being used by large and small businesses and millions of people every day. If you own or manage any size business, you may wonder where your business fits in and how you can use social media to promote your business.

While many companies have jumped on board the social media band wagon, there are several risks and security threats that businesses need to be aware of. Unfortunately, security is often overlooked when most businesses think about using social media.

The truth is that the threat landscape is constantly changing. The massive increase of people using social media is driving a huge increase in SPAM, malware, and other malicious attacks targeting social media and its users. But all hope is not lost! With some basic awareness about these risks and threats you can make a more informed decision on the strategy that your company may want to take to establish a social media presence with security in mind.

What is social media?

Tim Gasper, CMO and cofounder of Cork-Share (www.corkshare.com) says "Media is a means for communication. It involves a content medium - like pictures, sounds, videos, or text - and it conveys meaning and information to an audience. Sometimes that audience is you, sometimes it's your friend, or sometimes it's your crazy uncle who moved to Timbuktu."

Add social web applications like Facebook, LinkedIn, and Twitter to this media and you have "social media". Social networking is where you use these applications to network with others that have similar interests. This can involve responding to and sharing social media with others in your social network.

Here is a very simple example. Suppose I find a great news article on a web site and I decide to send the link to my Facebook page. My friends that are part of my social network on Facebook would see that I posted a link to something I was interested in, thus, they might be interested in this same article or subject matter. My friends could comment and respond to my posting adding to the conversation within my social network. In turn, they could send this link to others in their social network adding to the overall conversation.

Why use social media for business?

As a business, you are probably looking for new ways to market and promote your business and ways to provide better service to your customers and clients. Social media is a great option. Now that social media is so popular, you can get your message out about products and services to millions of people. In return, some of those people could respond by giving you business or providing instant feedback on your products or services.

Have you thought about your brand recognition lately? If you are a company that is just starting out and you want to get your “brand” out to the masses, social media is perfect for this task. Even if you are an established brand, having your brand noticed on social networks can give you an advantage over your competition with instant recognition. As a customer, I am usually looking for ways to quickly let a business know of a problem or to provide feedback on a product or service. With social media this feedback can be instant. Take Twitter for example. If your company has a Twitter account (even better when tied to your brand), you can literally receive feedback within minutes while other technologies like email, telephone, and snail mail can take much longer to interact with customers.

We talk a lot about risks and threats in the normal security world, but how do these same issues carry over to the world of social media?

Social media is just another outlet to promote your business and interact with your customers. Using a social network to interact with customers adds more of a “personal touch” to the customer service experience. Here is a great example. I had to return a defective product and I was a little upset about the item breaking so I sent a message on Twitter complaining about the problem. Although I didn’t direct this message toward the company, I received an instant reply from someone that worked in the company’s customer service department letting me know how to contact them so they could assist me. Fantastic! Just by sending me a simple message over Twitter, they made the situation better and I will encourage my friends and family to use this particular company because they made a proactive effort to improve my customer experience.

Risks and threats

We talk a lot about risks and threats in the normal security world, but how do these same issues carry over to the world of social media? Businesses specifically have certain unique risks and threats that need to be addressed: brand impersonation, information leakage, and damage to corporate reputation.

Brand impersonation

Brand impersonation is a significant concern for any type of business. This is especially important for national or worldwide brands that are well known outside of social networks. However, even a small company can be impersonated on social networks. Spammers are often to blame for impersonations on social networks by hijacking names that aren’t already taken. On Twitter, for example, it’s as easy as searching to see if a particular name is available. If it is, the spammer might register it and start using tools and scripts to generate a large follower list to use for spamming.

The good news is that Twitter and other social networks have policies against impersonation and if you find out that your brand has been hijacked, you can request that the account be removed, after you verify you do in fact “own” that particular brand.

Twitter is adding a new twist in the near future with “pro” level accounts that you would have to pay for (bit.ly/1ZZTc). While there is not a lot of information about how these accounts work, it is rumored that pro level accounts will have some means for verifying that your company owns a brand prior to activating the account.

Registering your name or brand on social networks today is just as vital as registering a domain name - if you don’t take it now, someone else will!

Information leakage

Do you know what your employees are posting on social networks? How do you know if employees are intentionally or unintentionally posting confidential or proprietary information to social media or networking sites? If you don’t look yourself you will never know! For example, employees might start sending messages on Twitter or posting Facebook updates about unannounced layoffs or an acquisition of another company before it is announced to the public. These are just two simple examples but it could be much, much worse. Just use your imagination!

Damage to corporate reputation

Information posted on social networks can spread like wildfire and can quickly damage a company’s reputation. On Twitter, these short 140 character messages can be forwarded or “retweeted” to others and become easily searchable.

Take for example what recently happened to Amazon.com when people started to tag “#AmazonFail” not only on Twitter but lots of other social media as well. Amazon created an online uproar when a technical glitch caused gay and lesbian books to have their sales ranking removed and the books be classified as “adult”, thus making the books harder to locate in a search (bit.ly/14miGx).

In just 24 hours, the reaction was swift! The hash tag #AmazonFAIL was the number one search term on Twitter, a Facebook group was created that had 1,200 members, and there were 5,000 blog posts about the issue. Talk about putting your company in damage control overdrive! While this was eventually corrected by Amazon - and apologies were given - it goes to show what could happen when people want to spread viral complaints or misinformation about your company. Just think if these were positive things being said about your company. Unfortunately, as we all know, bad news gets around more than the good news!

What’s out there about your company?

A recent Sophos poll (bit.ly/tL8f2) revealed that 63 per cent of system administrators worry that employees share too much personal information that could put your company information at risk. As an example, lets take a look at the three most popular social media and networking web sites that may have your specific company’s confidential or proprietary information.

LinkedIn groups and company profiles

LinkedIn is a social network specifically for building business relationships and to provide professional networking. There are two interesting aspects of LinkedIn that may hold very specific information about your company: LinkedIn groups and company profiles.

LinkedIn groups can be created by anyone and can be about virtually any topic. Most of the groups out there are focused on current and former employees, college networks, recruiting and marketing. You can do a search for your company by clicking on “Search Groups” at the top of the main LinkedIn page.

When searching for group information, try different ways your company name may be displayed or known. Based on your results look at each group carefully, you might be surprised at some of the information you find.

The next area of LinkedIn that may have juicy information about your company are the company profile pages. To search for your company profile, simply click on “Search Company” at the top of the main LinkedIn page. Just like when searching for company specific groups, you might be surprised at the wealth of information about your company in these profiles.

Just like groups, company profiles can be created by anyone and can contain information and details about your company. One thing you may not know is that these company profiles act as Wiki type pages where anyone on LinkedIn with a verified company email address can make changes to your company profile page.

One problem I found is that many former employees still have a company email address in their LinkedIn profile and can still edit the profile pages for a former company. The only mitigating control I have found is that LinkedIn will put a “Last edited by” note on the profile so people will know who made the last edit. I can only imagine the interesting things a former employee or a hijacked profile could do to a company profile!

Facebook Groups and Pages

Now that Facebook has grown to over 200 million users, it would be no surprise if you found lots of information about your company on Facebook. Facebook is not just a social network application for friends and family to stay in touch anymore! Facebook has recently evolved to embrace businesses and company information. Yes, it’s true! Facebook would love to have your company and personal data to aggregate and collect!

Facebook groups are similar to groups in LinkedIn, however, they are only visible to Facebook members and they are not searchable outside of Facebook. Facebook groups can be made private and can also be set to have a moderator approve group membership. These groups provide a discussion forum as well as the ability to post photos and other multimedia.

Facebook pages, on the other hand, are slightly different. These pages can be searched on through a regular search engine like Google and provide the page owner with detailed tracking and statistics with page views and visitor information. Facebook pages are a new feature to the site and provide a way for Facebook to drive more traffic to popular topics and information.

Searching for information about your company couldn't be easier in Facebook. Simply type in your company name in the search box in the upper right side of the main Facebook page and you will get information separated by several different tabs (People, Pages, Groups, Events, Web). Clicking on each of these will drill down to specific information about what you are searching for.

Again, just like LinkedIn, you may find everything from customer complaint groups to employees giving away the jewels! Keep in mind that for all of these searches you will need to use or create a Facebook account. Pages are the one exception as you can search for these with any search engine (Google, Yahoo, etc.).

Twitter

Twitter is currently the hottest social media and networking application today. If you are not familiar with Twitter, think of it as a short messaging service or what some call “microblogging” service. You have 140 characters to tell the world what you are up to. Continuing the theme from LinkedIn and Facebook, there could be a lot of valuable information about your company on Twitter.

It’s easy to find information on Twitter. Go to search.twitter.com and type in your company name. You can also use the “Advanced Search” or put in typical search operators such as OR, AND, “ “ etc. Just like when searching LinkedIn and Facebook, remember to try different spellings of your company name and different ways people may know your company. One thing you might find interesting is all the customer complaints if you are in a service type of business. This alone can be an eye opener for some!

Another service that is more of a “private” version of Twitter is called Yammer. This service only allows networks to be created by others with the same email address. For example, if your email address is tom@company.com only other “@company.com” email addresses can view posts from others in your social network. These posts can’t be viewed by others outside of the private network. To find company information on Yammer you need to sign up with a company email address to view what’s being posted about your company.

Internet posting policies

Now that you have searched the three most popular social media and networking sites for your company information, did you find anything of value? Did you see employees posting things that they probably shouldn't? Are you sounding the alarm about the potential of information getting out that might damage corporate reputation? The good news is that there is a policy more companies are starting to adopt. These are called "Internet Posting Policies".

What is an Internet posting? It is any type of post or comment on any type of social network. This should include all of the social networking sites (LinkedIn, Facebook, Twitter, etc.) blogs, forums, and other multimedia such as YouTube, Vimeo and more. Contained in an Internet Posting Policy are guidelines for employees on how they should post things about or relating to your company. Because social media is so prevalent and more people are using it (inside and outside your company), boundaries must be defined as far as what is acceptable and what is not in regards to Internet postings. Keep in mind, you are not censoring free speech or telling employees they can't talk about the company! These are just rules and guidelines employees need to follow.

While every company has different requirements and levels of risk, a good starting point is the template that Cisco has provided. Cisco has shared their Internet Posting Policy for other companies to use (bit.ly/w0wVC). I highly recommend using the Cisco template to model a policy for your specific business and requirements.

Monitor your brand and company information on social networks

Lastly, what good is finding all this information about your company on social media and networks without a proactive monitoring program? There are two things your company should define. First, how often should you look for information on social networks? Is this weekly, monthly, quarterly? Second, what tools or services should you use to monitor your brand?

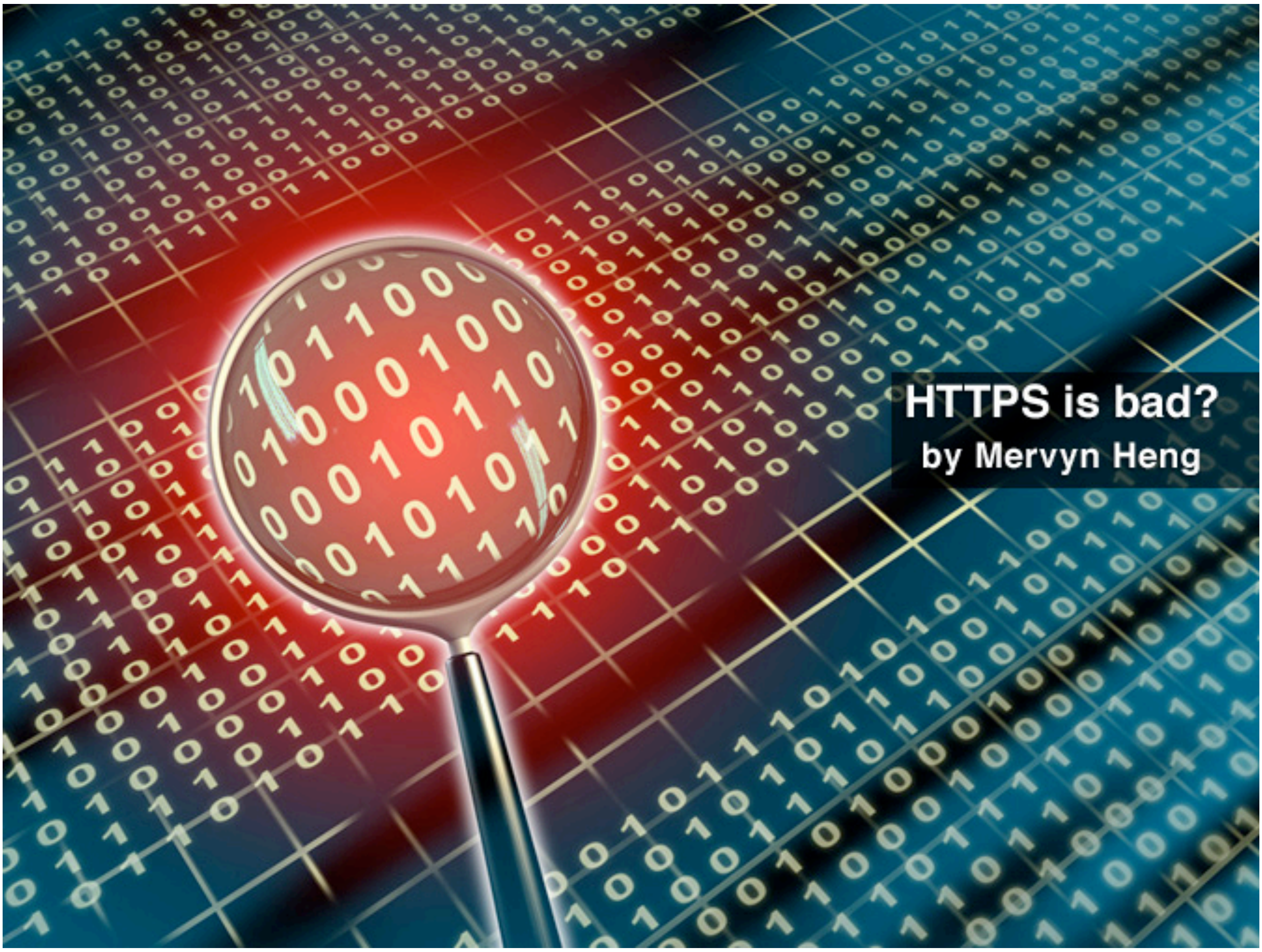
The cost effective model

I highly suggest starting with monitoring your brand with a simple, cost effective solution that you can do on your own. Start with the Twitter search function and create a search on your company and related keywords. Next, subscribe to these searches using Google Reader or some other RSS reader. Do the same for Google Blog and News searches by creating these RSS feeds through the Google Alerts functionality. Then, create an account on both Facebook and LinkedIn. Embed yourself in existing company groups and pages so you can periodically monitor these sites for company information.

Finally, another tool I recommend you try is Maltego (www.paterva.com/maltego/). Maltego allows you to visually see how your company information may be linked to other information found from many different sources including social networks in a nice GUI visual format. The free version of Maltego is somewhat limited in functionality, but the commercial version is only $430!

In this article I have outlined what social media is, how it works, the benefits, risks, what information is out there about your company and more. Now it's up to you to decide how to best use this information to define a social media strategy for your company. Get together with the business and marketing or public relations people in your company and partner with them from a security perspective. Social media and networks don't have to be a risk or threat to your company as long as you take proactive steps to ensure security is involved along the way.

Tom Eston is a penetration tester for a Fortune 500 financial services organization. Tom currently serves as the security assessment team lead. He is actively involved in the security community and focuses his research on the security of social media. Tom is a contributing author to a social media eBook and has written a Facebook Privacy & Security Guide that is used in several major universities as part of student security awareness programs. Tom is also a frequent speaker at security user groups and conferences. You can find Tom blogging on Spylogic.net and as one of the co-hosts of the Security Justice Podcast. Locate him on Twitter as agent0x0.



HTTPS is bad?

by Mervyn Heng

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) is a protocol that promises integrity of data transmitted over this channel and prevents prying parties from spying on the communication between two entities. Information security professionals constantly advocate the implementation of HTTPS within the enterprise to secure sensitive data and critical transactions. Consumers are also sold on the benefits of HTTPS. This buy-in has cascaded to the market and providers have been pressured into incorporating HTTPS into their products and services.

The employment of HTTPS is now universal and has created an illusion that HTTPS is trustworthy thus resulting in a blind eye turned to what traffic traverses over this “secure" protocol. Hackers have started exploiting this misconception by incorporating HTTPS into their insidious activities to take advantage of this complacency. This is evidenced by non-existent monitoring of outbound HTTPS connections in most cases due to the misplaced trust in this protocol.

Perimeter access controls focus on restricting inbound connections originating from the Internet. Access control mechanisms such as firewalls, VPNs, DMZs and 2-factor authentication are relied on to limit access into the internal network.

These factors highlight the threat posed by the HTTPS protocol. It is shocking to interact with administrators who are still oblivious to the abuse of this protocol and the threat it poses to their environments. Users are often victims due to ignorance and the lack of protection.

Threats

Administrators favor traditional client-server remote administration tools (eg. SSH, pcAnywhere, VNC) as they provide convenient access to machines. Remote administration clients are thus obvious targets for attackers looking to gain system control. This attack vector is often thwarted by perimeter defenses that typically require an established VPN session before permitting access to authorized remote clients located in the internal network.

LogMeIn is a radical tool that perforates existing edge defenses and permits remote access from anywhere over the Internet. How does LogMeIn work?

The remote client (ie. LogMeIn host) establishes a persistent outbound HTTPS connection to LogMeIn's server and this link facilitates reverse tunneling from an external browser.

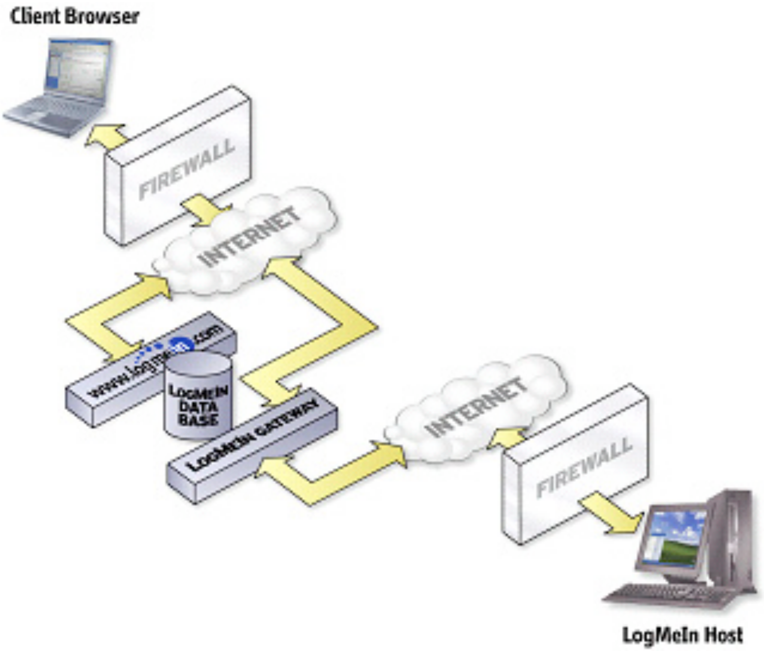
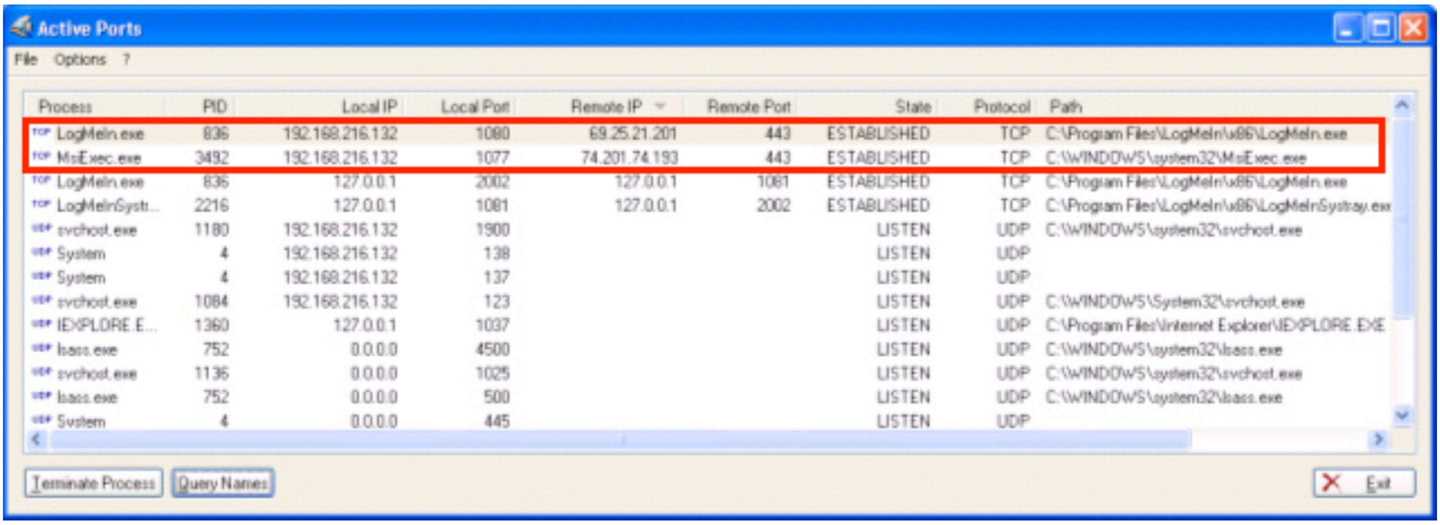


Figure 1: LogMeIn architecture.
Source: LogMeIn user manual.

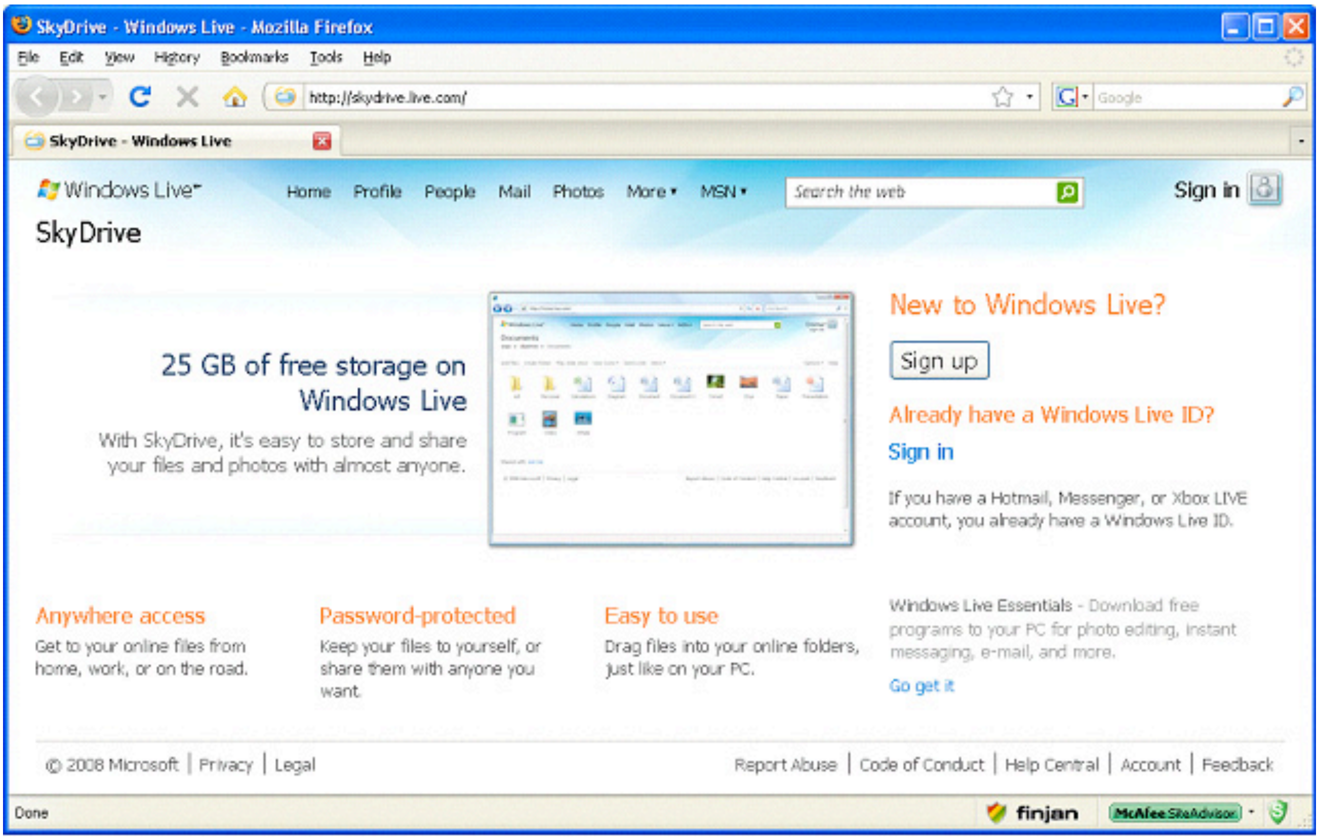


Process	PID	Local IP	Local Port	Remote IP	Remote Port	State	Protocol	Path
TCP LogMeIn.exe	836	192.168.216.132	1080	69.25.21.201	443	ESTABLISHED	TCP	C:\Program Files\LogMeIn\x86\LogMeIn.exe
TCP MsiExec.exe	3492	192.168.216.132	1077	74.201.74.193	443	ESTABLISHED	TCP	C:\WINDOWS\system32\MsiExec.exe
TCP LogMeIn.exe	836	127.0.0.1	2002	127.0.0.1	1081	ESTABLISHED	TCP	C:\Program Files\LogMeIn\x86\LogMeIn.exe
TCP LogMeInSyst...	2216	127.0.0.1	1081	127.0.0.1	2002	ESTABLISHED	TCP	C:\Program Files\LogMeIn\x86\LogMeInSystray.exe
UDP svchost.exe	1180	192.168.216.132	1900			LISTEN	UDP	C:\WINDOWS\system32\svchost.exe
UDP System	4	192.168.216.132	138			LISTEN	UDP	
UDP System	4	192.168.216.132	137			LISTEN	UDP	
UDP svchost.exe	1084	192.168.216.132	123			LISTEN	UDP	C:\WINDOWS\System32\svchost.exe
UDP IEXPLORE.E...	1360	127.0.0.1	1037			LISTEN	UDP	C:\Program Files\Internet Explorer\IEXPLORE.EXE
UDP lsass.exe	752	0.0.0.0	4500			LISTEN	UDP	C:\WINDOWS\system32\lsass.exe
UDP svchost.exe	1136	0.0.0.0	1025			LISTEN	UDP	C:\WINDOWS\system32\svchost.exe
UDP lsass.exe	752	0.0.0.0	500			LISTEN	UDP	C:\WINDOWS\system32\lsass.exe
UDP System	4	0.0.0.0	445			LISTEN	UDP	

Figure 2: Persistent outbound HTTPS connection to LogMeIn.

Users may install this remote administration tool at the request of a third party vendor to avoid having to raise a Business Partner (BP) connection request to save time and effort. It could be as innocent as users wanting to have remote access to their workstation so that they can work from the comfort of their homes. This tool puts the corporate security at risk as the access credentials are either in the hands of a third party or could potentially be compromised through password stealing Trojans installed on the user's home computer. LogMeIn becomes a potential backdoor into your network when compromised.

Data theft is an increasing concern to companies protecting their valuable intellectual property. Companies ban the use of portable storage devices, webmail, Instant Messaging and Peer-to-peer (P2P) file sharing to tackle this menace. In instances where a ban cannot be enforced, corporations attempt to monitor their traffic for hints of data leakage. Microsoft offers free 25GB password-protected online storage, SkyDrive, to its Windows Live users. Users can store files in personal, shared or public folders. Shared folders are only accessible to parties that the owner furnishes admittance to. SkyDrive is very simple to use and secure as the whole session (except for public folders) is protected using HTTPS.


SkyDrive - Windows Live - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://skydrive.live.com/
Google
SkyDrive - Windows Live
Windows Live
Home Profile People Mail Photos More ▾ MSN ▾
Search the web
Sign in
SkyDrive
Sign up
Sign in
Go get it
Done
finjan
McAfee SiteAdvisor

25 GB of free storage on Windows Live

With SkyDrive, it's easy to store and share your files and photos with almost anyone.

New to Windows Live?

Already have a Windows Live ID?

If you have a Hotmail, Messenger, or Xbox LIVE account, you already have a Windows Live ID.

Anywhere access

Get to your online files from home, work, or on the road.

Password-protected

Keep your files to yourself, or share them with anyone you want.

Easy to use

Drag files into your online folders, just like on your PC.

Windows Live Essentials - Download free programs to your PC for photo editing, instant messaging, e-mail, and more.

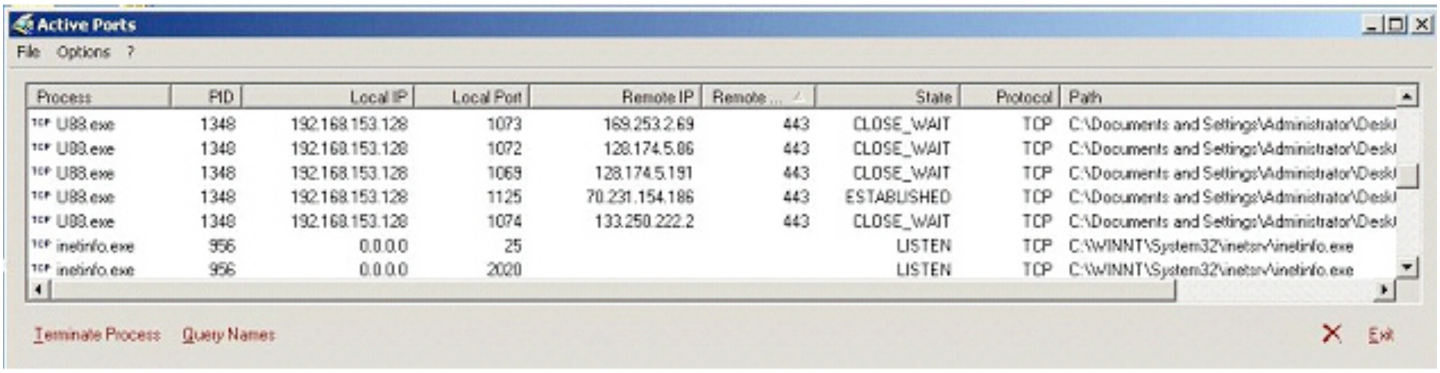
© 2008 Microsoft | Privacy | Legal

Report Abuse | Code of Conduct | Help Central | Account | Feedback

Figure 3: SkyDrive.

Human error is commonly a contributing factor to security breaches. An employee may mistakenly upload an important document onto their shared or public folder with devastating consequences. This facility can easily be used to siphon out corporate intellectual property right under the noses of employers and sold for a handsome profit to competitors. The beauty of this medium is that the industrial spy can create an account using fake particulars, host the stolen information offsite and the buyers collect their "goods" without the need to physically meet.

Anonymous web proxies hosted externally by third parties furnish unauthorized Internet access to users. These Anonymizers are prohibited from functioning effectively using web-filtering technologies that block access to these domains. These bypass tools have evolved to circumvent these filtering instruments and UltraSurf is the most powerful one that is readily available on the Internet. It is a standalone executable application that can be launched without needing to be installed. The feature that differentiates it from other Anonymous Proxy tools is the use of possibly compromised DSL machines to relay outbound HTTPS requests. The use of "Zombies" to act as web proxies is very sophisticated, as most enterprises do not block DSL IP address blocks.



Process	PID	Local IP	Local Port	Remote IP	Remote ...	State	Protocol	Path
TCP U88.exe	1348	192.168.153.128	1073	169.253.2.69	443	CLOSE_WAIT	TCP	C:\Documents and Settings\Administrator\Deskt
TCP U88.exe	1348	192.168.153.128	1072	128.174.5.86	443	CLOSE_WAIT	TCP	C:\Documents and Settings\Administrator\Deskt
TCP U88.exe	1348	192.168.153.128	1069	128.174.5.191	443	CLOSE_WAIT	TCP	C:\Documents and Settings\Administrator\Deskt
TCP U88.exe	1348	192.168.153.128	1125	70.231.154.186	443	ESTABLISHED	TCP	C:\Documents and Settings\Administrator\Deskt
TCP U88.exe	1348	192.168.153.128	1074	133.250.222.2	443	CLOSE_WAIT	TCP	C:\Documents and Settings\Administrator\Deskt
TCP inetinfo.exe	956	0.0.0.0	25			LISTEN	TCP	C:\WINNT\System32\inetsrv\inetinfo.exe
TCP inetinfo.exe	956	0.0.0.0	2020			LISTEN	TCP	C:\WINNT\System32\inetsrv\inetinfo.exe

Figure 4: Proxy IP addresses.

A user may naively just want to spend some time on a non-work related website using UltraSurf but unwittingly introduce malware as a result of this action. Hackers would employ UltraSurf to mask their origin.

These techniques are even more potent when used in combination. Imagine a hacker acquiring LogMeIn credentials from a victim then accessing the remote corporate machine using UltraSurf. Once in control of the corporate machine, they possess both the physical machine and all information deposited on it. The attacker is at liberty to load the tools and scripts they need to target other systems within the same network. Launching UltraSurf on the compromised remote client, they will then proxy out of the corporate network to deposit all stolen information onto their SkyDrive repository. Once the hacker is done, they can either erase their tracks (i.e. tools, logs and browser cache) or securely wipe the entire hard drive to destroy evidence.

Remediation

The first step in tackling the threat posed by HTTPS is the documentation of clear policies on the usage of HTTPS and communicating them to users. User awareness and understanding is essential to winning their cooperation in order to reduce the margin of human error and inherent security risks. Incorporating a Data Classification program is complimentary as this evidently stipulates that information be labeled based on their level of sensitivity for proper identification and handling. This prevents employees feigning innocence when they are in breach of clearly communicated policies and strengthens the company's position in the eyes of the law.

Forget about attempting to block tools. There will always be intelligent people who will create or source for a new tool to suit their needs. Existing tools can also be manipulated to easily evade detection. In the case of UltraSurf for example, the use of packers to compress the original payload results in a different hash of essentially the same tool to obfuscate its "appearance". The tool author offering upgrades to a newer version is equally as effective at defeating discovery.

Blacklist or whitelist? IT practitioners have been conditioned to tackle security issues using a blacklist approach. Blacklisting can be employed but is not advisable as it requires administrators having to constantly monitor new trends and reacting. Blacklisting is the road to futility. Whitelisting authorized outbound HTTPS traffic is the most practical and proactive option to managing this protocol. Identify business essential HTTPS connections and explicitly permit them in your access controls. Exercise some prudence and flexibility by permitting specific non-business HTTPS sites (e.g. government services, Internet banking) that employees may need to access. A comprehensive study of permissible HTTPS sites must be conducted before implementing a complete whitelist. A change control process should be in place to facilitate the addition of new HTTPS requirements as and when they arise.

Monitor HTTPS communications traversing your perimeter. This proposition does not imply scrutinizing every single HTTPS connection and the data being exchanged, as this may constitute a breach of privacy in certain countries. Collect HTTPS statistics (e.g. source, destination, timestamp) on a monthly basis to assist in identifying anomalies or suspicious outbound connections.

It is as simple as performing lookups on destination addresses that are not familiar for verification. Suspicious connections would warrant further examination. HTTPS inspection may be justified if you suspect activities resembling misuse or malice. This can be performed using SSL inspection tools available in the market for valid investigation purposes.

Conclusion

You don't believe that these activities are occurring in your organization? Review your logs and you may be in for a surprise.

Companies need to shake off their false sense of security and get down to the basics. Technologies assist with protecting the organization's prized resources but it is the effective policies and willing employees that form a strong foundation to reducing the risk of compromise. HTTPS was designed to provide point-to-point integrity but like any other protocol, it unfortunately has its hazards thus companies cannot block it entirely but have to supervise it.

Mervyn Heng, CISSP, is a Security lead for the Asia Pacific region in a large American computing hardware manufacturer. His main responsibilities include performing security risk assessments, infrastructure reviews as well as carrying out incident handling and forensic investigations. When he is not hunting for loopholes, Mervyn is busy with his many hobbies such as photography and sports.

Software spotlight

EULAlyzer 2.0 (www.net-security.org/software.php?id=754)

EULAlyzer can analyze license agreements in seconds, and provide a detailed listing of potentially interesting words and phrases. Discover if the software you're about to install displays pop-up ads, transmits personally identifiable information, uses unique identifiers to track you, or much much more.

ZOC (www.net-security.org/software.php?id=369)

This terminal emulator and telnet/Secure Shell client is well known for it's outstanding user interface. It lets you access character based hosts via telnet, modem, Secure Shell (SSH/SSH2), ISDN and other means of communication. It can be used to connect to Unix/Linux hosts and shell accounts, BBSes, 3270 mainframes (via TN3270 emulation) or internet muds.

Foremost (www.net-security.org/software.php?id=318)

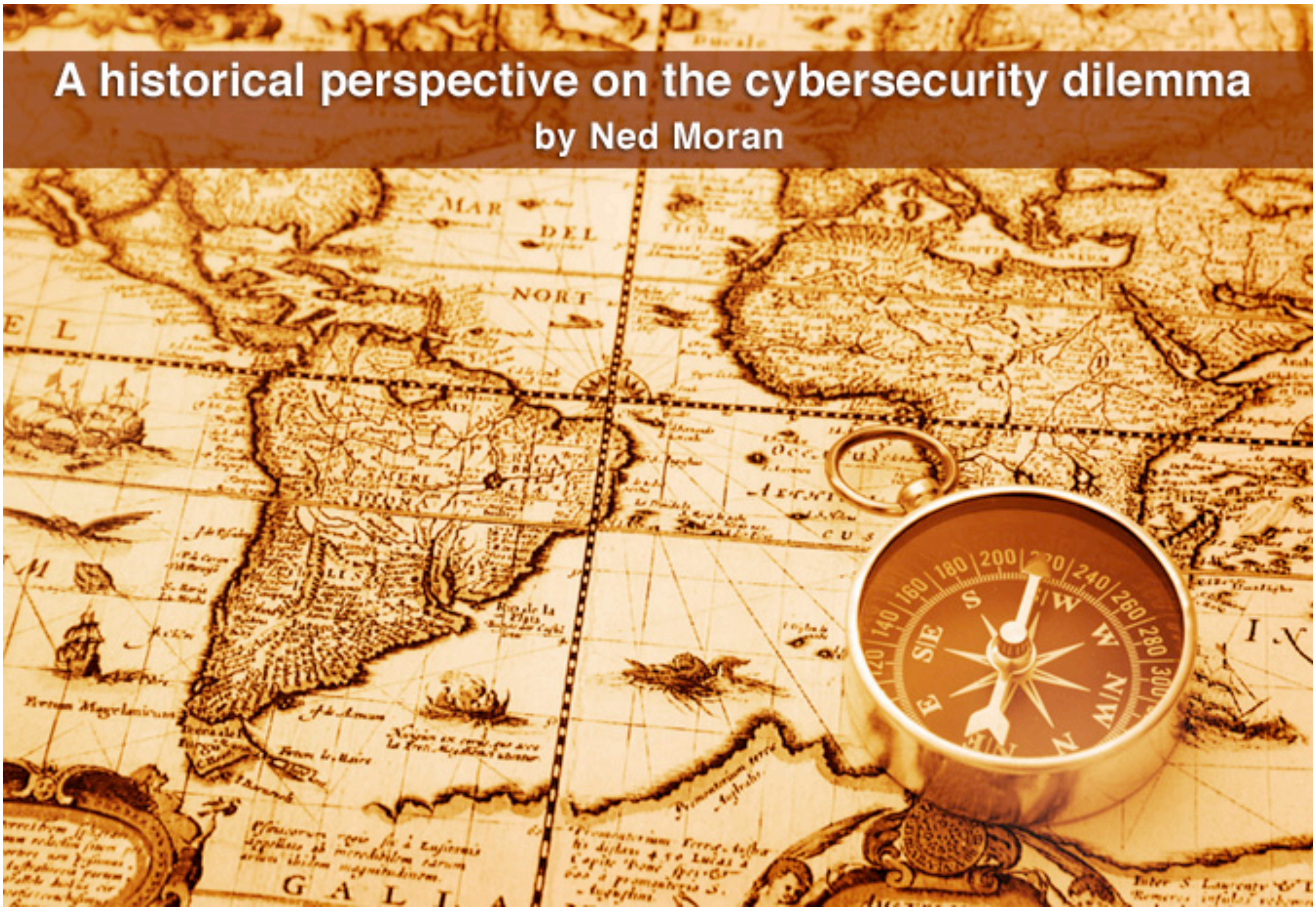
Foremost is a console program to recover files based on their headers and footers. Foremost can work on image files, such as those generated by dd, Safeback, Encase, etc, or directly on a drive. The headers and footers are specified by a configuration file, so you can pick and choose which headers you want to look for.

ArpAlert (www.net-security.org/software.php?id=335)

This software listens on a network interface (without using 'promiscuous' mode) and catches all conversations of MAC address to IP request. It then compares the mac addresses it detected with a pre-configured list of authorized MAC addresses. If the MAC is not in list, arpalert launches a pre-defined user script with the MAC address and IP address as parameters.

A historical perspective on the cybersecurity dilemma

by Ned Moran



In his seminal article Cooperation Under the Security Dilemma, Robert Jervis notes that "many of the means by which a state tries to increase its security decrease the security of others." This is particularly true when a nation-state adopts strategies, tactics, and weapons that are perceived to favor the offense. Jervis also notes that "whether defensive weapons and policies can be distinguished from offensive ones, and whether the defense or the offense has the advantage" determine the likelihood of instability and conflict in the international system.

As the US and other nation-states debate how to integrate cyber warfare strategies, tactics, and weapons into its arsenals, the framework of analysis provided by the security dilemma may help determine whether or not instability and war are more or less likely.

A careful assessment of cyber warfare, in the context of the security dilemma and the balance between offense and defense forces, is needed because it is widely assumed without critical analysis that cyber warfare is inherently offensive.

US Federal Government officials have widely acknowledged that both government and private sectors are under sustained attack and currently there is little to no ability to defend against these attacks. If this perception that cyber warfare favors the offense at the expense of the defense takes root among national security policy makers, then the prospects for global instability will likely increase.

This article seeks to test the perception that cyber warfare is inherently offensive by testing its key characteristics. Attributes of cyber warfare will be examined with an eye towards determining whether they favor the offense or the defense. This analysis will in turn be used to determine whether the creation and deployment of cyber warfare strategies, tactics, and weapons creates instability in the international system and makes war more likely.

Characteristics of cyber warfare

In an effort to determine its offensive or defensive nature, the following seven characteristics of cyber warfare will be analyzed: terrain, mobility, ease of conscription, surprise, duality of knowledge, use of force and firepower.

Terrain

As Jervis notes, "anything that increases the amount of ground an attacker has to cross, or impedes his progress across it, or makes him more vulnerable while crossing, increases the advantage accruing to the defense." In the context of cyberspace, natural fortifications like oceans and mountains do not exist. Nation-states are connected by fiber optic cables delivering 1s and 0s at the speed of light. As a result, attackers can deliver malicious code to a targeted system in near real-time. Although defenders can develop fortifications in cyberspace via the implementation of firewalls and intrusion detection or prevention systems, these tools are by no means foolproof. With appropriate research, a knowledgeable attacker can design an assault that either circumvents or defeats these defenses. For example, during the cyber attacks in Estonia, defenses were constantly overwhelmed by the aggressors. According to Wired Magazine's account of the Estonia cyber conflict, "the attackers were constantly tweaking their malicious server requests to evade the filters". This example demonstrates that, in cyber warfare, terrain clearly favors the offense as attackers can quickly close on their targets and overcome defenses with relative ease.

WHILE ZERO-DAYS CAN BE USED TO CONSTRUCT BOTNETS, THEY CAN ALSO BE USED TO LAUNCH DEVASTATING ATTACKS AGAINST SCADA SYSTEMS THAT CONTROL CRITICAL INFRASTRUCTURE TARGETS

Surprise

According to Robert Jervis, "weapons and strategies that depend for their effectiveness on surprise are almost always offensive." In cyber warfare, zero-day exploits are effective precisely because the defense is not prepared for cyber weapons. A zero-day exploit is malicious code that exploits a previously unknown or un-patched vulnerability in computing software. The initial variant of the Conficker worm, that has as of now infected approximately 10 million computers, exploited a previously unknown vulnerability in the Windows family of operating systems.

While zero-days can be used to construct botnets, they can also be used to launch devastating attacks against Supervisory Control and Data Acquisition (SCADA) systems that control critical infrastructure targets. Engineers at the Department of Energy's Idaho National Labs used a zero-day exploit that remotely disabled a power generator during a simulated cyber attack code named "Aurora". These zero-day attacks are successful solely because defenses are not designed to stop them. As a result, cyber weapons reliance on surprise for effectiveness inherently favors the offense.

Mobility

Mobility is closely linked to terrain in the context of the speed of attack. Military analysts generally agree that mobility favors the offense as it enables aggressors to initiate surprise attacks and quickly overwhelm the defense. In Grasping the Technological Peace Keir A. Lieber notes that "in military terms, mobility is the ability of troops and equipment to from one place to another.”

Germany's use of highly mobile tanks during the opening stages of World War II demonstrates the offensive advantages of mobility. Cyber armaments are also highly mobile weapons systems. They can be launched from multiple computers, irrespective of geographic location, and can close on their designated targeted in near real-time. For example, the botnet used to attack Estonia was comprised of as many as one million infected computers located in various countries - including the US.

This type of distributed botnet allows an aggressor to rapidly converge on a target from multiple locations in near real-time. It, therefore, appears that cyber warfare is highly mobile and, when it is combined with the reliance on surprise, favors the offense.

Ease of conscription

In Offense, Defense, and War Stephen Van Evera states that "technologies that favored mass infantry warfare (e.g., cheap iron, allowing mass production of infantry weapons) strengthened the offense because large mass armies could bypass fortifications more easily." In cyber warfare the ease of constructing large botnets parallels the ease of raising and arming large armies. Returning to the example of Estonia, the attackers were able to quickly raise an army of as many as one million bots in a matter of days. In another example, in March 2006 attackers were able to generate as much as 1.3 gigabits per second during an attack against German domain register Joker.com. Even targets with firewalls and other sophisticated defenses in place would have a difficult time defending against this gigabit-level Distributed Denial of Service (DDOS) attack. As Joker.com noted, the DDOS attack "was enough to overload our lines, causing communication problems between our border routers and the upstream providers, and thereby interrupting all services." This ease of conscription of cyber infantry and ability to launch high volume attacks confer a considerable advantage to the offense.

Duality of knowledge

Cyber warfare, unlike other forms of conventional and unconventional warfare, is solely a knowledge-based activity. Weapons and fortifications are virtual and access to expensive physical resources is not needed. During the Cold War, a nation-state's military power was measured by its conventional or nuclear arsenal. To build a conventional and nuclear arsenal, large investment in raw materials, human capital, and money were required. In contrast, with cyber warfare the only resources required are access to computer hardware, an Internet connection, and knowledge in computer science. Further, the knowledge used to build fortifications, such as firewalls or intrusion detection systems, can be easily used to create weapons designed to bypass and defeat these fortifications. This type of dual use knowledge appears to favor the offense in that the adversary will be incapable of distinguishing between offensive and defensive postures. Further, this type of dual use knowledge aptly describes the security dilemma that occurs when one state's enhanced security measures result in a loss of security for its rivals. In cyber warfare, as defenders build online fortifications, rivals are threatened because defenders have also developed a capability to bypass or defeat these fortifications.

Use of force

Any nation-state with a cyber weapons arsenal has more response options than countries without cyber warfare capabilities. It is widely believed that Russia, as evidenced by the attacks against Estonia and Georgia, is able to field an impressive DDoS capability. A DDoS capability allows a country to initiate more easily an economic or information embargo with digital weapons. This DDoS, or other cyber warfare capability, may allow an aggressor to easily use force with more precision and limit the use of conventional military weapons. For example, while the Georgia cyber attacks were conducted in association with a conventional military assault, the Estonia cyber attacks were conducted without a conventional military parallel. Despite these differences, in both cases Russia attempted to compel its adversary to change its behavior.

Many experts argue that there is no evidence that the Russian government was directly responsible for organizing cyber attacks in Estonia. However, recent admissions by Russian State Duma official Sergei Markov that his staff participated in the Estonia attacks indicate these attacks occurred with at least tacit approval of the Russian government. This ability for an aggressor to more easily use force against an adversary appears to favor the offense as it lowers the barrier to entry into conflict, gives the offense more options and therefore encourages the use of force. As a result, it is possible conflict will be more frequent. While digital conflicts are typically not bloody, frequent cyber attacks between adversaries may well lead to escalations of force that result in conventional military conflicts.

Firepower

While the above attributes favor of the offense, firepower appears to favor the defense. According to Stephen Van Evera, "technology that gave defenders more lethal firepower (e.g., the machine gun) strengthened the defense." Cyber warfare strategies, tactics, weapons that target SCADA systems, which operate critical infrastructure like power grids and oil and gas pipelines, could generate technologies that favored mass infantry warfare (e.g., cheap iron massive firepower through their capacity to effect massive economic and physical damage). Their generation of firepower could result in mutually assured destruction as nation-states begin to understand the threat to critical infrastructure posed by a rival’s cyber warfare arsenal. This sense of mutually assured destruction appears to favor the defense as nation-states will be deterred from launching a first strike cyber attack for fear of an in kind response.

Prospects for instability

Although the above list of cyber warfare characteristics is not exhaustive, on balance they demonstrate that cyber warfare is decidedly offensive. The key characteristics of cyber warfare examined, including terrain, mobility, ease of conscription, surprise, duality of knowledge, and the use of force, appear to favor the offense. In contrast, firepower favors the defense. Not only do these characteristics favor the offense, they also lower the costs of becoming a military power - albeit an asymmetric military power.

As stated earlier, during the Cold War nation-states invested tremendous amounts of raw materials, human capital, and money in order to develop robust conventional or nuclear forces. This high barrier to entry prevented all but a handful of states from becoming a global military power. However, the advent of cyber warfare drastically lowers the inherent costs of becoming a military power. As demonstrated by the attacks in Estonia and Georgia, all that is required to wage a digital war is a cadre of technically sophisticated individuals willing to organize a larger population of motivated patriots with access to low-end computing resources and an Internet connection.

Therefore, as a nation-state deploys cyber warfare strategies, tactics, and weapons, its rivals will feel more insecure. This pattern accurately describes the security dilemma that states that any actions taken by a nation-state to increase its own security will result in a decreased sense of security in its rivals.

History demonstrates that when the security dilemma has been exacerbated and the offense is stronger than the defense instability reigns and war is increasingly likely. Historians typically point to World War I as an example of conflict that was a direct result of the security dilemma. Prior to World War I France entered into a series of entangling alliances that were designed to bolster its security. These alliances caused Germany to feel less secure and it responded by creating rival alliances. These successive moves and countermoves exacerbated the security dilemma and laid the groundwork for war.

Promoting stability

It is therefore essential that national security policy present a concerted effort to develop policies designed to ameliorate this burgeoning security dilemma. Policies that could reduce tensions as cyber warfare forces are deployed include improving the redundancy and resiliency of critical infrastructure targets. For example, if the redundancy and resiliency of SCADA systems governing the power grid were improved so that an attack on the power grid would cause minimal damage, then defenders would be less threatened by a rival’s build-up of cyber weapons and attackers would have less motivation to build up cyber forces. In this instance, although an attack against a power grid may successfully destroy it, the target's backups would stand ready to replace the fallen primary systems.

These backup systems could be designed differently and protected by a separate line of defense, thereby increasing the complexity of executing a successful attack on both the primary and back-up systems.

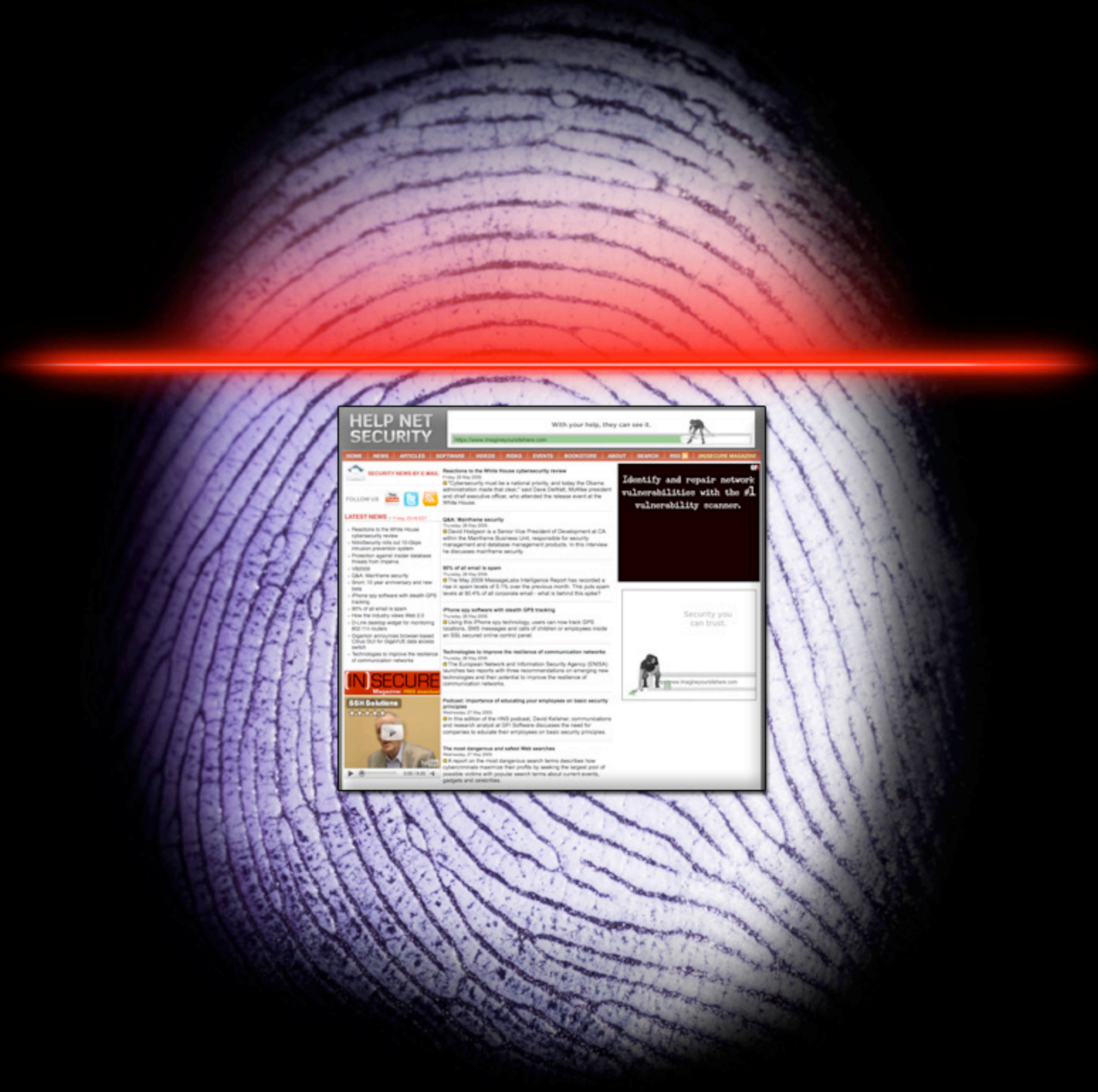
Other policies that could decrease the possibility of cyber war include defining explicit redlines. A nation-state should clearly state what critical infrastructure assets are of national importance and explain to its adversaries that it will retaliate in kind to attacks on these assets.

As demonstrated above, a country with powerful cyber weapons can rely on a deterrent effect to discourage its rivals from carrying out cyber attacks on its critical infrastructure targets. A clear annunciation of values and response options, including attacks on SCADA systems and critical infrastructure, may work in tandem to deter an adversary from launching an attack and therefore ameliorate the security dilemma.

Conclusions

While it appears that the development and deployment of cyber warfare strategies, tactics, and weapons favors the offense and exacerbates the security dilemma, stability can still be achieved. Although cyber warfare is inherently offensive, nation-states can still develop strategies and tactics that will ameliorate the security dilemma.

Ned Moran is an Adjunct Professor of Information Privacy and Security at Georgetown University. Mr. Moran also works with the Project Grey Goose team and investigates how nation-states use cyberwarfare strategies, tactics, and weapons to compel and deter adversaries. Ned can be found on twitter at www.twitter.com/moranned



Q&A: Brent Huston on security in general, CEO challenges and MicroSolved

by Mirko Zorz

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

Unlike what I'd call a "regular CEO" you enjoy quite a bit of technical tinkering and dwell into security research. What drives you?

I was a technician to start with. I have always been a technical security guy and spent my early years at MicroSolved doing hands on penetration testing, exploit development and security research. I guess you could say I grew into being the CEO after we hired a person to be the CEO and he left the company 28 days later. It was a necessity that someone do it, so I took it on. That led me to a focus on growing my marketing and leadership skills as well as my technical skills.

My wife would say it made me a "more rounded person", but the truth is, I enjoyed learning the business skills as much as reading packet dumps. I really like helping management and board folks understand the real world threats in their own language and I am very happy that that has proven to be a talent of mine.

How does the technical aspect fit into your responsibilities as the CEO?

These days I split my time between marketing, leadership and technical research, primarily focused on our HoneyPoint line of products for security visibility. The good news is that those technical threat vector insights has helped us grow MicroSolved, since we bring some unique knowledge and capabilities to our clients that stem from our in depth exposures to bleeding edge attack techniques.

How would you assess the current state of Internet security threats?

I think the state of the OS and networks, in general is much improved. Some of the very basics we talked about for years (firewalls, patching, etc.) are starting to become mainstream and common practice. I think security at the application layer and designing for failure are currently the biggest challenges. I think our industry has a lot of bad habits.

We rely on user awareness to solve problems that awareness won't solve, like malware. We also tend to engineer IT environments and applications as if best practices were in place, when in reality, they rarely are. We need to embrace the idea that designing for failure is much more real world than designing by best practice. We know, from experience, that failure happens - thus we have to design our systems, networks and applications to minimize the damages that failure can cause. Again, malware as an example, if we know that some user will click on the dancing gnome and get a nasty infection, then we have to design user IT environments and server/data connectivity in such a way that we maintain confidentiality, integrity and availability even when some machines in the user base are compromised. Ideally, we would continue to strive for prevention, but increase our capabilities in detection by moving away from heuristics and identifying abnormal behaviors and then create automated responsive processes that allowed components in the IT environment to defend themselves while humans enable greater controls and take deeper protective actions. Until we can embrace this type of security at the system, network and application level, attackers will continue to have the upper hand.

We rely on user awareness to solve problems that awareness won't solve, like malware.

What type of developments do you see ahead?

What keeps me up at night is embedded devices and their applications. We have just seen malware that turns small modems and routers into bots, but what happens when the blender, coffee maker, refrigerator and your house are all "smart" components? We have already seen small scale infections of automobile computers and cell phones, so what kinds of embedded targets are we creating every day? From the "smart energy grid" to our dependence on our cell phones and from embedded network devices to "smart appliances", we are going to see a world where all things are connected and all things are a target. Malware at the embedded level may well be the scourge of information security when the young professionals we are mentoring today reach the season of their careers. Such attacks and infection capabilities could make bots seem "nostalgic" like some of us look upon defacements of days gone by today.

Of course, that said, there is good news here, too. The future is not all about fear. We are getting better at designing for security. We will likely create much more secure applications and computing platforms in the future. Even while attackers continue to evolve their craft, so too do the developers, programmers and engineers. There will be new bugs, for sure, but there will also be innovations in protective technologies that help reduce our overall exposures to these technical risks.

What do you see as the areas of true innovation when it comes to computer security?

I really hope that people move away from signature-based technologies. Today, when I do forward looking talks, it is usually around the two core ideas of finding new ways to design/engineer for failure tolerance and the idea that behavioral detective tools are much smarter. We know what attackers do and we know how they behave. There are really very few "game changing" attack techniques. This was the reason I built HoneyPoint in the first place. We have created a toolset around the ideas of capturing and detecting behaviors that normal users don't or shouldn't do, but that we know fit common behaviors of malware or human attackers.

I am a strong believer in the idea that we have to turn the tables on attackers and take away their ability to act with confidence. If they can't scan the network for targets, that reduces their target set. If they can't access data on the servers and workstations because they don't know which ones are real and which ones are HoneyPoint Trojans, then their capabilities are reduced again. If they are sniffing the network and our HoneyBees are putting fake credentials on the wire, then they don't know what accounts are real and what ones will trigger alerts. Basically, we keep chipping away at their capability to know what is real and what is a trap until they become significantly less of a risk because we have reduced their options drastically.

You are very active both on Twitter and on your blog. How have these means of communication shaped the way MicroSolved does business?

Twitter and other social networks have been great for us. We are big fans of Seth Godin and the idea of building a tribe. We have been able to grow the business even in down economies because we have focused on the idea that every single thing we do needs to bring value to customers and the tribe in general.

Our partners often say that we are too focused on the clients and that we give away too much software, knowledge and tools for free. We feel just the opposite, that the customer has to be the focus and that value is real way that we earn their trust. Twitter and other social networks, the stateofsecurity.com blog and all of the public education, pro-bono work and stuff we do are the keys that unlock the true value of our relationship with our clients and the tribe at large.

I think every CEO should talk to customers as much as possible. I think too many CEOs are locked away from the public and their client base.

Should more CEOs take a moment to talk to their peers and customers this way?

I think every CEO should talk to customers as much as possible. I think too many CEOs are locked away from the public and their client base.

You have to be engaged with them, you have to work in the trenches with your tribe and at the same time have enough vision to make strategic decisions. I don't think enough companies operate this way. I treasure hearing from clients and having them pull me aside for conversations. I love hearing from them on twitter or through the blog. Heck, unlike some other CEOs, you can even call me on the phone. Clients are the center of MicroSolved and I wouldn't have it any other way!

You recently released HoneyPoint Personal Edition v2. How long did the development process take?

Going from 1.0 to 2.0 took about 30 days of development time. Testing/QA took about 2 weeks of time.

We work hard on the development of the new products and on bringing the easiest to use, most capable products to market that we can.

Right now, we are about to release HoneyPoint Security Server Console 3.00 and then a whole new architecture for the HoneyPoints/HornetPoints themselves. That's a lot for us and keeps our engineers and technical team hopping (or buzzing) as the case may be.

What are the major news in this release?

In the new Personal Edition we changed the interface to make it easier to use, added in the "defensive fuzzing" techniques of HornetPoints (Patent-Pending) and brought the flexibility of plugins to the product. That means that in addition to detecting scans, probes and attacks, you can also allow HornetPoints to try and defend themselves by attempting to crash the offending malware or tool that is doing the probing and you can use the plugins to automate a variety of responses from custom alerting/SEIM integration to updating other security controls or modifying the security posture of your system that is under attack.

Pretty cool stuff that our Security Server product had that we wanted to bring to the independent host product. There's a lot more to come as well. We are working on plans for more updates and capabilities for Personal Edition, even as I write this.

MicroSolved has sponsored and contributed to various open source initiatives and working groups. What projects do you support and why?

For a variety of reasons, I am not going to mention them by name. We do a lot of vulnerability research and much of that is working with a variety of open source projects. We enjoy fantastic relationships with the OSS developers and we contribute to helping many of them make their products more secure on an ongoing basis.

We consider it as a part of training new engineers and doing research on new tools, QA on tool updates and other integrated work on the business. Instead of doing those things with no outcome, we often use OSS projects as the basis for the work and then share our findings, new security vulnerabilities and other results with the project leaders. That way everyone wins! We also have a large set of tools that we contribute to community. Our web site is currently being revamped to feature them more prominently, but we have a number of free software tools that we give away when you attend our events or speaking engagements.

We also maintain the stateofsecurity.com blog, the @honeypoint Twitter feed of ongoing attack sources in real time and publish our "State of the Threat" presentations that we have been giving ongoing for more than five years.

The why is easy. The community has given so much to us over the last nearly 20 years we have been in business that we just continually strive to give back!

What are your future plans?

You will see more HoneyPoint stuff from us and more work on identifying emerging threats. You can count on us to keep looking for new ways to fight the insider threat and to help clients and members of the tribe make more rational choices about security, risk and compliance.

You can read Brent’s Twitter stream at www.twitter.com/lbhuston.

Black Hat Europe 2009
by Vlatko Kosturjak

There is no need to explain Black Hat to the security community. For those who don't know, Black Hat is a common place where security researchers present 0-day vulnerabilities or new methods of discovering vulnerabilities. In other words - a deeply technical conference.

Black Hat is actually a commercial version of hacker gatherings like the Chaos Communication Congress (CCC), Defcon or Hackers on Planet Earth (HOPE). The attendance fee is the biggest argument for the "commercial" attribute. The attendance fee for most of the hacker underground conferences doesn't go over 100 EUR, while for Black Hat briefings it can be around 2000 EUR if you apply for it on the day before the event starts.

The price for trainings ranges from 1000 EUR to 3000 EUR, depending on workshop complexity, lecturer and day of registration. Although may prices seem steep at first glance, if you come for the training or to the conference once, it is very likely that you'll come next year as well. Believe me, you won't ask for the price.

Black Hat events are held in USA, Europe and Japan on an annual basis. From the very beginning the European Black Hat is held in Amsterdam. More precisely, in the Movenpick hotel close to the main station in Amsterdam.

Same as last year, Black Hat was divided into two parts. The first part was reserved for training which took place during the first two days of the event. The second part included the briefings. Trainings are like workshops that focus on a specific topic, where authors of tools or methods teach you in a very detailed way how to take advantage of it. This time around, trainings covered a wide range of topics: from testing RFID security to SAP penetration testing.

Zac Franken and Adam Laurie held a very interesting training session about RFID security. Both men are legends in the security field. During two days they taught RFID security, and demonstrated man-in-the-middle (MiTM) attacks using RFID.

Adam Laurie

Another compelling training session was about hardware hacking, lead by Joe Grand (also known as Kingp1n). Attendants learned how to open hardware devices and perform security analysis on them.

Four new vulnerabilities were disclosed during the conference. There was a potential fifth vulnerability, but it was not disclosed or presented because the vendor did not release the patch on time. Black Hat organizers are fans of responsible disclosure of vulnerabilities where it is advised to wait for the vendor to release the patch before talking about the vulnerability details in public.

On the first day of the Black Hat briefings, Jeff Moss, director of Black Hat, made a short introduction for the event. After Jeff finished his welcome peech, the invited keynote speaker was ready to present. The speaker for this year was Lord Erroll, and his keynote had an interesting title (and posed an interesting question): Privacy protecting People or People protecting Privacy. Lord Errol is a crossbench member of the UK's House of Lords and takes pride in "voting against stupid government ideas whoever is in power". As he is a technical person, he is often in such situations.

After the keynote speech, Mariano Nunez Di Croce demonstrated security vulnerabilities in SAP systems. Mariano also presented his tool that helps with security testing of SAP infrastructure. Even though many of the presented problems can be mitigated with the implementation of correct configuration parameters or by upgrading the SAP systems – it is a very common occurrence that SAP systems are not configured properly or are not updated.

Moxie Marlinspike reprised his presentation from Black Hat DC. He demonstrated attacks related to HTTP and HTTPS connections on web pages. It was very interesting hearing about the details related to the attacks, as well as about the reactions he got from various people. You can download his tool, sslstrip, from his web page. Sslstrip is a proof of concept implementation of the attack he covered.

Emmanuel Bouillon talked about common errors in the implementation of Kerberos and how those errors can be exploited during attacks. Kerberos is used in both Windows and Unix/Linux worlds, so this lecture got a lot of attention.

Roelof Temmingh and Chris Bohme, authors of the popular Maltego tool, presented the latest features of Maltego. It was an interesting lecture during which Roelof and Chris demonstrated how dangerous 2.0 services could be (like Facebook and/or Gmail) to the privacy of the employee.

Jeff Moss

Roberto Gassira' and Roberto Piccirillo from Mobile Security Lab demonstrated a practical attack consisting of hijacking mobile data connections. The attack exploits a few design and configuration vulnerabilities through SMS configuration messages. The attack depends on user to accept sent configuration messages. That means you should think twice about automatically accepting such messages when they come.

Eric Filiol demonstrated security mistakes in the OpenOffice suite. As OpenOffice gained popularity in office suites market, the analysis of this software was long overdue. Eric presented a thorough security analysis - ranging from design weaknesses to bugs. The conclusion? You don't need to migrate to other office suites. From a security perspective, there isn't a better one.

Rob Havelt demonstrated the 802.11 FHSS wireless standard and made a thorough security analysis.

Benjamin Caillat made a nice lecture about shellcode art, during which he demonstrated his own shellcode tool called WiShMaster.

Bernardo Damele Assumpcao Guimaraes talked about advanced techniques in SQL injections. He talked mainly about how to better exploit SQL injections in different databases. Bernardo is the author of sqlmap tool for exploiting SQL injection attacks.

As Black Hat is a commercial type of gathering, there is no side content as on underground counterparts (Defcon or CCC for example). It consists mainly of parties organized by different vendors. Traditionally, the most interesting party is the Core party.

It’s worth noting that Google was not present at Black Hat this year. It may suggest that Google is suffering from the financial crisis just like many other companies.

This is probably the last time that the European Black Hat conference was held in Amsterdam. The conference grows every year, and the organizers want to expand it to three parallel tracks, so they must find a new place to host it. As Amsterdam is not able to host three parallel tracks, it is very likely that European Black Hat will move to Barcelona next year. As this is one of the rare quality technical conferences, this represents very good news for participants because they can expect a lot more content than before.

If you still aren’t sure about going to the conference next year, I'll make it easy for you. Go. Especially if you are into information security on a technical level.

Jeff Moss (Dark Tangent), director of Black Hat

On the last day of the conference, we talked with Jeff Moss (also known as Dark Tangent), director of Black Hat, about the Black Hat conference and its future.

Today is the last day of Black Hat, are you satisfied with this year’s conference?

In short – yes, I'm satisfied. It is a good year. The current economic situation does not help, but I'm very satisfied with the content. There were quite a few surprises this year. Even though every year I feel there is place for improvement, I also feel we are getting better as well. This is the best year for Amsterdam so far.

What lecture did you like this year? Is there any specific talk you want to mention?

We have only two tracks in Amsterdam so we have to choose lectures carefully. I would have to say RFID training because RFID technology is used in passports nowadays. Also, I would like to mention the Kerberos lecture as most organizations today use Kerberos for authentication but few are aware of risks when it’s misconfigured.

Any future plans for Black Hat?

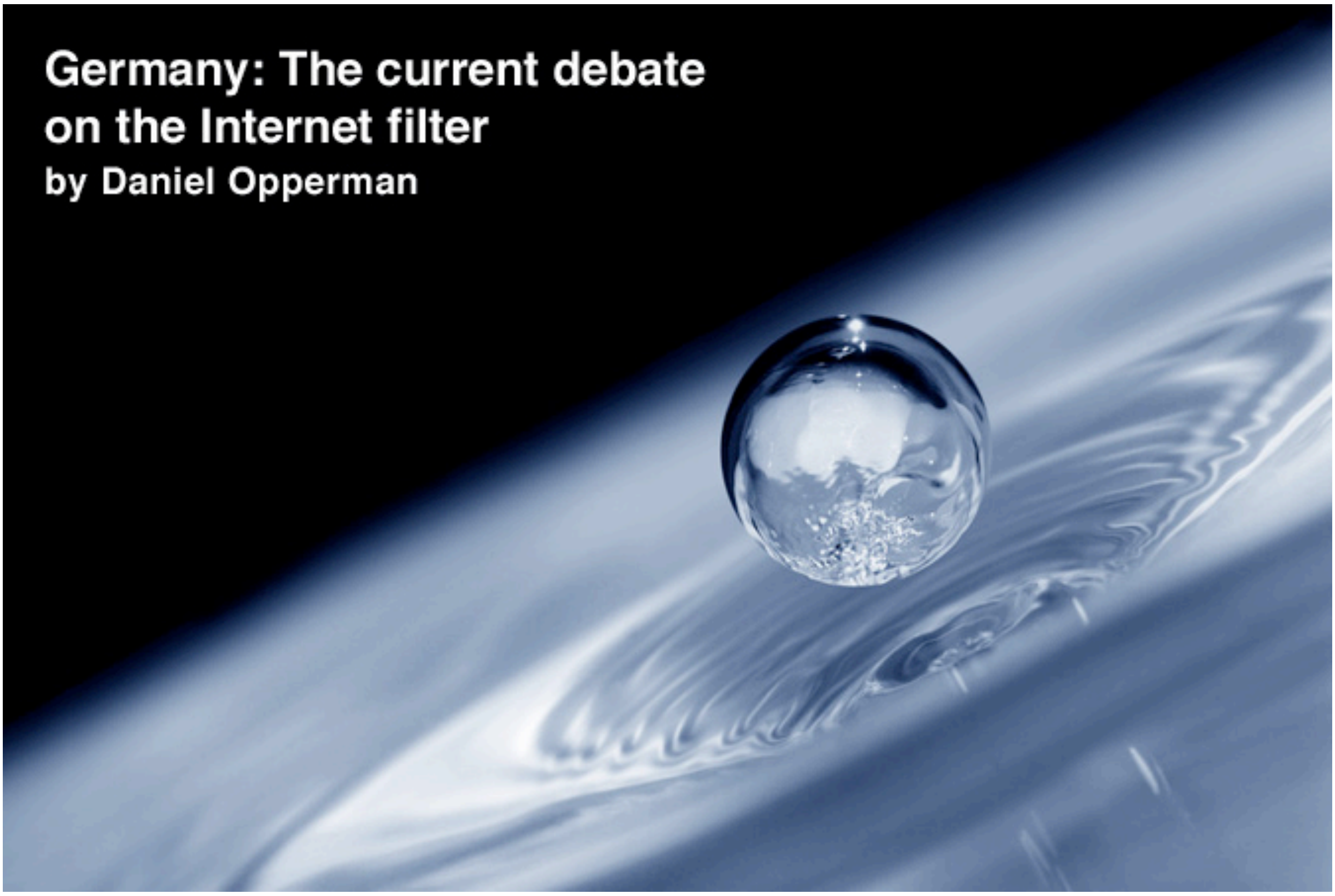
As we want to expand the European Black Hat on three tracks, and Amsterdam is not capable of handling it – we are moving to Barcelona. Also, we will not do Black Hat Japan this year. We are looking for a new location where Black Hat will be held for Asian participants.

We are working on Black Hat social web pages where you could get the summary of the projects on which security researchers are working and where you can share with friends or colleagues on which lectures you want to go. It will not be a Facebook or a LinkedIn replacement, but it will be communication oriented towards people interested in topics that Black Hat is covering. Also, it will give some interaction to people who cannot come to Black Hat events.

Vlatko Kosturjak is a security specialist from Croatia, Europe. He specialized in penetration testing and ethical hacking, IT auditing, OS/Network security hardening and ISMS development according to international security standards. He also has extensive experience in Linux on almost every platform (from PDAs to mainframes). Vlatko holds stack of Linux and Security certificates. You can reach him through his website at kost.com.hr.

Germany: The current debate on the Internet filter

by Daniel Opperman



When talking about cybercrime, there is one topic that is discussed frequently and often results in public outrage by many Internet users and non-users as well. It is child pornography that I am talking about - a problem that harms thousands of children physically and mentally and is a business where millions of dollars are spent each year worldwide.

Child pornography is nothing new and is not connected exclusively to the Internet. In fact, this form of abuse exists for centuries (probably as long as humankind itself). But with the Internet, producers and consumers found an easy, fast, cheap and anonymous way to get and distribute it. And "getting" is really the appropriate word (not "buying").

Estimations say that about 80% of child porn consumers are not involved in it for financial interest but trade pictures and movies as a "hobby". Besides websites (which usually exist only for a limited amount of time), e-groups, newsgroups, bulletin board systems, chat rooms or peer-2-peer networks (P2P) are also used to access the material. In recent years different approaches have been tried out to combat this form of crime on the Internet. One has been the identification of consumers by their credit cards which they use to buy child porn material. Another one - the one that is the focus of this article - is the filtering of websites that contain explicit material.

The new agreement in Germany

The most recent example of a country trying to combat child pornography on the Internet with filters is Germany. On May 17th, 2009, the German Minister of Family, Ursula von der Leyen signed an agreement with five of the seven biggest Internet Service Providers (ISPs) in Germany to block websites that contain child pornography. This agreement was the result of long negotiations between the parties and not all ISPs supported the arrangements with the Ministry.

The ISPs Freenet and 1&1 declared that the lack of a legal basis for such an agreement made it difficult for them to accept the contract. Also, civil society organizations like the Chaos Computer Club (a hacker organization advocating privacy rights and data protection) or MOGIS (representing victims of child abuse) stated that they were not in favor of the governmental approach. Their central arguments are that just cloaking websites does not solve the original problem and that there is a risk of introducing censorship on the Internet. Indeed, the Ministry plans do not include democratic control of what is going to be filtered. Taking in consideration similar attempts in other countries, the success of filtering child pornography remains disputable.

In recent years Scandinavian countries put in place filter regimes with the goal of combating child pornography on the Internet. Norway started the first initiative in 2004 by using DNS-blocking and closing down servers like it was suggested by the British Internet Watch Foundation (IWF) at that time. Today, the Norwegian block list contains around 8000 URLs and 18.000 hits are being blocked every day. It is interesting to mention that not all ISPs in Norway are participating in the filter regime.

Some time later Sweden, Denmark, and Finland also started using filters to block access to child pornography. After the Scandinavian countries, the Netherlands, Switzerland and Italy also introduced a similar system. Also, other non-European countries like New Zealand, South Korea, Canada, Taiwan and the USA use filter systems to block child pornography.

Unlike most of the other countries (except for Finland and Italy), Germany is going to force the remaining ISPs by law to participate in the filter regime. So far the agreement is based on a (more or less) mutual understanding. And with the majority of the big ISPs participating in it, the big majority of the users will have to live with it. The companies Deutsche Telekom, Vodafone/Arcor, Alice/HanseNet, Kabel Deutschland and Telefonica O2 Germany (representing 75% of the German market) already signed the agreement.

The new draft of the law is already on its way to be discussed in Parliament (Bundestag) in the coming weeks. The main aspects are the block lists that will be compiled by the Federal Criminal Investigation Agency (BKA) and which will have to be kept secret and utilized by all ISPs. Opening one of the websites mentioned on the list will lead to a stop website which contains a short explanation why the user cannot access the content. As at least two communication laws may have to be changed and the Constitution (Grundgesetz, GG) is expected be affected. An evaluation of the new law will take place two years after the law is passed (IF it is passed).

Supporter and opponents

The most important argument that Minister von der Leyen and her supporters use is the fact that as members of a democratic government they are obliged to act against child pornography on the Internet. Notwithstanding all the criticism, they cannot lean back and refuse any activities just because they might turn out to be of little effect. A government that will not try even the least thing possible to end child abuse would probably be confronted later with much harsher criticism than the one they're getting now. In the issue at hand, the argument of the re-victimization is a strong one. By this I mean the double effect of abuse (once during the production of the photo or film material and later again during the unlimited access of the material on the Internet). The protection of a child that became victim of such an abuse justifies going against the distribution of the material. Since the hosting of the files outside of national legislation makes it difficult to act against the server that offers the content, filtering is a method to limit access to it as much as possible.

Members of the BKA justify the law by stating that the greater part of child pornography users are not part of organized child abuse circles (whose members would and will invest time and energy into finding ways of circumventing the filters). Following the reasoning of BKA President Jörg Zierke, 80% of the users of child pornography websites will be scared off by the stop website and give up looking for such content. He classifies the rest of them as hardcore users who will try to find a way to go around the filters. This group, he says, will have to be confronted with other means of investigation. Another argument is the self-regulation of the market. Therefore, the reduction of clicks on certain content will equal reduction of demand and, at last, the ebbing of supply.

“What supply?” the critics are asking, underlining that the largest quantity of child pornographic material is not being traded over websites but within other spheres of the Internet, or even in very traditional ways (by mail). This is especially true for producers of such material who work on a commercial level. The communication between producers and buyers happens on the Internet, but the transport of the material on a DVD is executed by snail mail. It is only much later, after the buyers start trading the material with others for free, that it appears on the Internet. For example, on Usenet or on P2P servers - both not affected by DNS-blocking of child pornographic websites.

The second aspect critics of Internet filter bring up is that blocking certain websites that contain child pornographic material will neither significantly influence the commercial market nor really reduce the distribution of the material, as the majority of it is found in other places of the Web (mentioned in the introduction of this article). The 2008 report of the British Internet Watch Foundation (IWF), announcing a decrease of child pornographic websites, must also be analyzed from this perspective.

It stays unclear if the suppliers of such material really left the Internet or if they just switched from websites to other parts of the Net. Besides that, it is very easy to circumvent DNS-blocking. Instructions on how to do this can be found on several websites on the Internet. Most of them are not even connected to child pornography - they just deal with the question of filtering in general.

IT security specialists, members of civil societies and police investigators in different countries complain about the ineffectiveness of Internet filters, the lack of consistency of public institutions in going against the producers of child pornography, and the disregard of democratic rights and principles.

IT security specialists, members of civil societies and police investigators in different countries complain about the ineffectiveness of Internet filters, the lack of consistency of public institutions in going against the producers of child pornography, and the disregard of democratic rights and principles.

Hannes Federrath, Professor of Information Security at the University of Regensburg (Germany) considers filtering "absolutely ineffective". In his opinion, there are better methods than using filters – for example, working with hash values. Investigators of the Swedish police are also disappointed by the success of the methods used in the country.

In an interview with the German magazine Focus, the Swedish chief investigator against child pornography and child abuse Björn Sellström stated that the methods introduced to limit access to child pornography on the Internet did not reach their goal. Instead, the number of child porn websites on the Swedish filter list has been growing since the system was initiated.

Representatives of the ISPs also admit that filtering does not solve the problem of child pornography. It just covers the crimes for the public. They would prefer clarification and education combined with cooperation with police investigators to prosecute the producers and professional distributors. In 2008, German ISPs informed the police about child pornography on the Internet in several hundreds of cases.

The question is if these cases are really worked on by the investigators. Christian Bahls from the German organization MOGIS (which represents victims of child abuse) states that his organization is aware of several servers in Germany which offer child pornographic material. Although he was able to track down the location of the servers, the police did not close them down.

Furthermore, Bahls underlines that the introduction of filters cannot be combined with the German constitutional law. Similar criticism regarding the lack of police activity comes from the Netherlands, where the journalist Karin Spaink found a considerable number of child pornographic websites that were hosted in the Netherlands. Some of them even appeared on the block list of one the Dutch ISPs, but there were no attempts by the police to shut them down. Spaink also pointed out (in an article published on her own website) that cooperation between European countries was insufficient. To prove the point, she mentioned the example of the Finnish block list that showed 138 Dutch websites offering child pornography.

Even though both countries are fighting against child pornography, their activities were obviously limited to covering websites and they were not cooperating to investigate the servers or the producers.

Conclusion

For the German government (and probably for other governments as well) it is a dilemma - to defend methods that are obviously useless against child pornography on the Internet, or not? One of their main difficulties is that they are willing to solve the problem but they do not know how. Nevertheless, they cannot admit to having major problems with the understanding of the dynamics of cybercrime without losing their credibility. But maybe Minister von der Leyen is trying to solve another problem with the introduction of filters? This year is the year of the parliamentary elections. Affirming to act against child pornography will definitely get some votes for the Christian conservative party (CDU) she belongs to, especially as the discussion about Internet filters popped up on the headlines of major newspapers.

As a member of a democratic Government, von der Leyen should also be aware that the concern of introducing a highly undemocratic procedure does get the attention of those interested in maintaining democratic standards. Because, in the end, the Federal Criminal Investigation Agency (BKA) would be the only institution who could add websites to or remove them from the secretly kept block list - without any democratic control of their decisions. Critics see this as a first step towards introducing censorship or opening the door for lobby groups that would love to see more websites being filtered. This could be sites with political content, as well as religious, gambling or music websites.

Representatives of the music industry have already shown high interest in the new German law and claimed that file sharing websites should be banned from the net as well. This already happened partly with the Pirate Bay website in Sweden and Denmark. In Finland, Internet activist Matti Nikki's website, on which he informs the public about censorship on the Internet, became the target of the national filter regime after he got hold of and hosted the block list of the responsible police agency.

In Germany, the current debate is not the first regarding Internet filtering. In 2002, public authorities managed to block two websites that were hosted in the USA and contained neo-nazi material. The result? Thanks to the available information about the methods of bypassing filters, these two websites had even more visitors than before.

Daniel Oppermann is a political scientist from Germany, currently writing his PhD thesis on Internet Governance, Cybercrime, and Internet filtering. He is a research fellow at the Observatorio Politico Sul-Americano in Rio de Janeiro and can be reached at dan.oppermann[at]gmail.com.

A risk-based, cost-effective approach to holistic security

by Ulf Mattsson

Data security plans often center around the "more is better" concept. These call for locking everything down with the strongest available protection and results in unnecessary expenses and frequent availability problems and system performance lags. Alternatively, IT will sometimes shape their data security efforts around the demands of compliance and best practices guidance, and then find themselves struggling with fractured security projects and the never-ending task of staying abreast of regulatory changes.

There is a better way - a risk-based classification process that enables organizations to determine their most significant security exposures, target their budgets towards addressing the most critical issues and achieve the right balance between cost and security. In this article, I discuss the risk-analysis processes that can help companies achieve cost-savings while measurably enhancing their overall data security profile by implementing a holistic plan that protects data from acquisition to deletion.

Step 1: Determine data risk classification levels

The first step in developing a risk-based data security management plan is to determine the risk profile of all relevant data collected and stored by the enterprise, and then classify data according to its designated risk level. Sounds complicated, but it's really just a matter of using common sense. Data that is resalable for a profit - typically financial, personally identifiable and confidential information - is high risk data and requires the most rigorous protection; other data protection levels should be determined according to its value to your organization and the anticipated cost of its exposure - would business processes be impacted? Would it be difficult to manage media coverage and public response to the breach? Then assign a numeric value for each class of data; high risk = 5, low risk = 1. Classifying data precisely according to risk levels enables you to develop a sensible plan to invest budget and efforts where they matter most.

Step 2: Map the data flow

Data flows through a company, into and out of numerous applications and systems. A complete understanding of this data flow enables an enterprise to implement a cohesive data security strategy that will provide comprehensive protections and easier management resulting in reduced costs.

Begin by locating all the places relevant data resides including applications, databases, files, data transfers across internal and external networks, etc. and determine where the highest-risk data resides and who has or can gain access to it (see 'attack vectors' section below). Organizations with robust data classification typically use an automated tool to assist in the discovery of the subject data. Available tools will examine file metadata and content, index the selected files, and reexamine on a periodic basis for changes made. The indexing process provides a complete listing and rapid access to data that meets the defined criteria used in the scanning and classification process. Most often, the indices created for files or data reflect the classification schema of data sensitivity, data type, and geographic region. High risk data residing in places where many people can/could access it is obviously data that needs the strongest possible protection.

When the classification schema is linked to the retention policy, as described above, retention action can be taken based on file indices. Additionally, the reports based on the indices can be used to track the effectiveness of the data retention program.

While we're discussing data retention policies, it's important to remember that data disposal also needs to be a secure process; usually you'll opt to delete, truncate or hash the data the enterprise no longer needs to retain.

Truncation will discard part of the input field. These approaches can be used to reduce the cost of securing data fields in situations where you do not need the data to do business and you never need the original data back again. It is a major business decision to destroy, truncate or hash the data. Your business can never get that data back again and it may be more cost effective to transparently encrypt the data and not impact current or future business processes. In addition, the sensitive data may still be exposed in your data flow and logs prior to any deletion or truncation step.

Hash algorithms are one-way functions that turn a message into a fingerprint, at least twenty bytes long binary string to limit the risk for collisions. The Payment Card Industry Data Security Standard (PCI DSS) provides standards for strong encryption keys and key management but is vague in different points regarding hashing. Hashing can be used to secure data fields in situations where you do not need the data to do business and you never need the original data back again. Unfortunately a hash will be non-transparent to applications and database schemas since it will require long binary data type string. An attacker can easily build a (rainbow) table to expose the relation between hash values and real credit card numbers if the solution is not based on HMAC and a rigorous key management system. Salting of the hash can also be used if data is not needed for analytics.

Done properly, data classification begins with categorization of the sensitivity of data (i.e., "public," "sensitive," "confidential," etc). Classification goes on to include the type of data being classified, for example, "sensitive, marketing program," and where applicable, the countries to which the data classification applies. The classification allows the organization to automate the routines for flagging, removing, or archiving applicable data. Pay particular attention when automating the removal of data; consider instead alerting the user privileges of data requiring attention.

Additionally, an understanding of where all the sensitive data resides usually results in a project to reduce the number of places where the sensitive is stored. Once the number of protection points has been reduced, a project to encrypt the remaining sensitive data with a comprehensive data protection solution provides the best protection while also giving the business the flexibility it needs, and requires a reduced investment in data protection costs.

Step 3: Understand attack vectors (know your enemy)

Use your data risk classification plan and the data flow map, along with a good understanding of criminals favored attack vectors, to identify the highest risk areas in the enterprise ecosystem. Currently web services, databases and data-in-transit are at high risk. The type of asset compromised most frequently is online data, not offline data on laptops, backup tapes, and other media. Hacking and malware proved to be the attack method of choice among cybercriminals, targeting the application layer and data more than the operating system. But these vectors change so keep an eye on security news sites to stay abreast of how criminals are attempting to steal data.

There are two countervailing trends in malware, both likely to continue. One trend is toward the use of highly automated malware that uses basic building blocks and can be easily adapted to identify and exploit new vulnerabilities. This is the malware that exploits un-patched servers, poorly defined firewall rules, the OWASP top ten, etc. This malware is really aimed at the mass market – SMEs and consumers. The other trend is the use of high-end malware which employs the “personal touch” – customization to specific companies, often combined with social engineering to ensure it’s installed in the right systems. This is the type of malware that got TJX, Hanaford, and now Heartland according to a recent report published on KnowPCI (www.knowpci.com.) The point is: the more we create concentrations of valuable data, the more worthwhile it is for malware manufacturers to put the effort into customizing a “campaign” to go after specific targets. So, if you are charged with securing an enterprise system that is a prime target (or partner with/ outsource to a business that is a major target) you need to ensure that the level of due diligence that you apply to data security equals or exceeds that expended by malicious hackers, who are more than willing to work really, really hard to access that data.

Reports about recent data breaches paint an ugly picture.

Reports about recent data breaches paint an ugly picture. In mid-March Heartland Security Systems has yet, they claim, to be able to determine exactly how many records were compromised in the breach that gave attackers access to Heartland’s systems, used to process 100 million payment card transactions per month for 175,000 merchants. Given the size and sophistication of Heartland's business--it is one of the top payment-processing companies in the United States--computer-security experts say that a standard, in-the-wild computer worm or Trojan is unlikely to be responsible for the data breach. Heartland spokespeople have said publicly that the company believes that the break-in could be part of a "widespread global cyber fraud operation."

According to a report in Digital Transactions and other news sources, in January 2009 Heartland apparently managed to find malware neatly tucked away on one of its payment-processing platforms after learning late in the Fall of 2008 that company might have a data breach in which unencrypted card numbers were captured during the authorization process. The key question here for many security professionals is why and how it took so long to find the malware. A post on a Wired News security blog, claiming to come from a Heartland employee stated that Heartland "might have caught it, or even prevented it, if we'd known what the government and the involved companies knew about some of the other recent breaches, but that data hadn't been shared with us." Unfortunately that problem is being repeated again, with virtually no “lessons learned” information released about the Heartland breach.

What we have ‘learned” is something that many of us already know - compliance does not equal security. Credit-card payment processers such as Heartland are already bound to follow a set of security standards known as the Payment Card Industry Data Security Standard (PCI DSS), covering issues such as maintaining secure networks, protecting stored cardholder data, and keeping antivirus software up to date.

Heartland was certified as PCI compliant last year, and other recent victims of break-ins, including RBS Worldpay, can make similar claims. The latest news reports that the malware was set to grab and transmit data - possibly looking for transmissions that represented authorization requests that were unencrypted while in transit over private networks. So Heartland could have been 100% compliant with PCI DSS, while its systems harbored a known weakness in the standard that hackers have now targeted.

Bill Homa, who stepped down as the CIO for the Hannaford retail chain after the company suffered a data breach in February 2008 that exposed 4.2 million payment card records , told Storefront Backtalk (www.storefrontbacktalk.com) that he considers Microsoft's OS to be "full of holes... If you limit your exposure to Microsoft, you're going to be in a more secure environment, adding that Microsoft's philosophy is decentralized, forcing IT to manage more points. That means more license fees for Microsoft and more potential security gotchas for the CIO." He also said that he thinks it is astonishing that current PCI regulations do not require end-to-end encryption. Homa also added that he believes "there's no such thing as a secure network... If you think your network is secure, you're delusional."

That brings us back to our risk-based plan to protect data itself rather than focusing all our attention on securing the systems that the data resides on.

Most data breaches are caused by external sources but breaches attributed to insiders, though fewer in number, typically have more impact than those caused by outsiders. Nearly three-quarters of the breaches examined in the Verizon Business 2008 Data Breach Investigations Report (bit.ly/KDwCy) were instigated by external sources. Just 18% of the breaches were caused by insiders but the insider incidences were much larger in terms of the amount of data compromised.

The average number of records per breach was approximately 1.2 million.

The cases included in this study encompass an astounding 230 million compromised records, a large portion of publicly disclosed records were breached during the four-year time frame of the study. The average number of records per breach was approximately 1.2 million. The median, however, is much lower at 45,000, indicating a skew in the dataset toward a few very large breaches. Even so, over 15 percent of cases involved more than 1 million records. Some type of cardholder data was compromised in 84 percent of cases.

Obviously these statistics correlate to the financial motivation of the criminals. Related findings support this statement, as fraudulent use of stolen information was detected following 79 percent of breaches. Additionally, 32 percent of cases involved one of the many types of personally identifiable information (PII). This is likely attributable to the usefulness of this type of data for committing fraud and other criminal activities.

Step 4: Cost-effective protections

Cost-cutting is typically accomplished in one of two ways: reducing quality or by getting the most out of a business' investment. Assuming you've wisely opted for the latter, look for multi-tasking solutions that protect data according to its risk classification levels, supports business processes, and is able to be change with the environment so that you can easily add new defenses for future threats and integrate it with other systems as necessary.

Concerns about performance degradation, invasiveness, application support, and how to manage broad and heterogeneous database encryption implementations too often produce hard barriers to adopting this important security measure.

Some aspects to consider when evaluating data security solutions for effectiveness and cost-control include:

Access controls and monitoring

The threat from internal sources including administrators will require solutions that go beyond traditional access controls. Effective encryption solutions must provide separation of duties to prevent a DBA to get hold of the keys. A centralized solution can also provide the most cost effective strategy for an organization with a heterogeneous environment.

Although some of the legal data privacy and security requirements can be met by native DBMS security features, many DBMSes do not offer a comprehensive set of advanced security options; notably, many DBMSes do not have separation of duties, enterprise key management, security assessment, intrusion detection and prevention, data-in-motion encryption, and intelligent auditing capabilities. This approach is suitable for protection of low risk data.

Tokenization

The basic idea behind tokens is that each credit card number that previously resided on an application or database is replaced with a token that references the credit card number. A token can be thought of as a claim check that an authorized user or system can use to obtain the associated credit card number. Rule 3.1 of the PCI standard advises that organizations “Keep cardholder data storage to a minimum.” To do so, organizations must first identify precisely where all payment data is stored. While this may seem simple, for many large enterprises it is a complicated task because the data discovery process can take months of staff time to complete. Then security administrators must determine where to keep payment data and where it shouldn’t be kept. It’s pretty obvious that the fewer repositories housing credit card information, the fewer points of exposure and the lower the cost of encryption and PCI initiatives.

In the event of a breach of one of the business applications or databases only the tokens could be accessed, which would be of no value to a would-be attacker. All credit card numbers stored in disparate business applications and databases are removed from those systems and placed in a highly secure, centralized tokenization server that can be protected and monitored utilizing robust encryption technology.

Tokenization is a very hot “buzzword” but it still means many things to different people, and some implementations of it can pose an additional risk relative to mature encryption solutions. Companies are still being required to implement encryption and key management systems to lock down various data across the enterprise, including PII data, transaction logs and temporary storage. A tokenization solution would require a solid encryption and key management system to protect the tokenizer. Organizations use card numbers and PII data in many different places in their business processes and applications that would need to be rewritten to work with the token numbers instead.

The cost for changing the application code can be hard to justify by the level of risk reduction. The risk of changing already working application code can also be hard to justify. This approach is suitable for protection of high risk data. Please see the discussion of tokenization at bit.ly/4bcZz.

File level database encryption

File level database encryption has been proven to be fairly straight forward to deploy and with minimal impact on performance overhead, while providing convenient key management.

This approach is cost effective since it installs quickly in a matter of days, utilizes existing server hardware platforms and can easily extend the protection to log files, configuration files and other database output. This approach is the fastest place to decrypt as it is installed just above the file system and encrypts and decrypts data as the database process reads or writes to its database files. This enables cryptographic operations in file system by block chunks instead of individually, row-by-row since the data is decrypted before it is read into the database cache. Subsequent hits of this data in the cache incur no additional overhead. Neither does the solution architecture diminish database index effectiveness, but remember that the index is in clear text and unprotected within the database.

This approach can also selectively encrypt individual files and does not require that "the entire database" be encrypted. Database administrators can assign one or more tables to a table space file, and then policies can specify which table spaces to encrypt. Therefore, one needs only to encrypt the database tables that have sensitive data, and leave the other tables unencrypted. However, some organizations choose to encrypt all of their database files because there is little performance penalty and no additional implementation effort in doing so.

Production database requirements often use batch operations to import or export bulk data files. If these files contain sensitive data, they should be encrypted when at rest, no matter how short the time they are at rest. (Note: some message queues such as MQ Series write payload data to a file if the message queue is backed up, sometime for a few seconds or up to hours if the downstream network is unavailable.) It may be difficult to protect these files with column level encryption solutions. This approach can encrypt while still allowing transparent access to authorized applications and users.

This approach is suitable for protection of low risk data. Be aware of the limitations with this approach in the areas of no separation of DBA duties and potential issues that operating system patches can cause.

File encryption doesn’t protect against database-level attacks. How are you going to effectively and easily keep administrators from seeing what they don’t need to see with file-level encryption? Protection of high risk data is discussed below.

Experience from some organizations has shown that the added performance overhead for this type of database encryption is often less than 5%. However, before deciding on any database file encryption solution, you should test its performance in the only environment that matters: your own.

End-to-end encryption is an elegant solution to a number of messy problems.

Field level encryption and end-to-end encryption

Field level full or partial encryption/ tokenization can provide cost effective protection of data fields in databases and files. Most applications are not operating on and should not be exposed to all bytes in fields like credit card numbers and social security numbers, and for those that do require full exposure an appropriate security policy with key management and full encryption is fully acceptable. This approach is suitable for protection of high risk data.

Continuous protection via end-to-end encryption at the field level is an approach that safeguards information by cryptographic protection or other field level protection from point-of-creation to point-of deletion to keep sensitive data or data fields locked down across applications, databases, and files - including ETL data loading tools, FTP processes and EDI data transfers. ETL (Extract, Transform, and Load) tools are typically used to load data into a data warehousing environments. This end-to-end encryption may utilize partial encryption of data fields and can be highly cost effective for selected applications like an e-business data flow.

End-to-end encryption is an elegant solution to a number of messy problems. It’s not perfect; field-level end-to-end encryption can, for example, break some applications, but its benefits in protecting sensitive data far outweigh these correctable issues. The capability to protect at the point of entry helps ensure that the information will be both properly secured and appropriately accessible when needed at any point in its enterprise information life cycle.

End-to-end data encryption can protect sensitive fields in a multi-tiered data flow from storage all the way to the client requesting the data. The protected data fields may be flowing from legacy back-end databases and applications via a layer of Web services before reaching the client. If required, the sensitive data can be decrypted close to the client after validating the credentials and data-level authorization.

Today PCI requires that if you're going outside the network, you need to be encrypted, but it doesn't need to be encrypted internally. If you add end-to-end encryption, it might negate some requirements PCI have today, such as protecting data with monitoring and logging. Maybe you wouldn't have to do that. The PCI Security Standards Council is looking at that in 2009.

Data encryption and auditing/monitoring are both necessary for a properly secured system - not one vs. the other. There are many protections that a mature database encryption solution can offer today that cannot be had with some of the monitoring solutions that are available. Installing malicious software on internal networks to sniff cardholder data and export it is becoming a more common vector for attack, and by our estimates is the most common vector of massive breaches, including TJX, Hannaford, Heartland and Cardsystems.

Storage-layer encryption or file layer encryption doesn't provide the comprehensive protection that we need to protect against these attacks. There is a slew of research indicating that advanced attacks against internal data flow (transit, applications, databases and files) is increasing, and many successful attacks were conducted against data that the enterprise did not know was on a particular system. Using lower-level encryption at the SAN/NAS or storage system level can result in questionable PCI compliance, and separation of duties between data management and security management is impossible to achieve.

Compensating controls

PCI compensating controls are temporary measures you can use while you put an action plan in place. Compensating controls have a “shelf life” and the goal is to facilitate compliance, not obviate it. The effort of implementing, documenting and operating a set of compensating controls may not be cost effective in the long run. This approach is only suitable for temporary protection of low risk data.

Software based encryption

Many businesses also find themselves grappling with the decision between hardware-based and software-based encryption. Vendors selling database encryption appliances have been vociferously hawking their wares as a faster and more-powerful alternative to software database encryption. Many organizations have bought into this hype based on their experiences with hardware-based network encryption technology. The right question would be about the topology or data flow. The topology is crucial. It will dictate performance, scalability, availability, and other very important factors. The topic is important but the question is usually not well understood. Usually, hardware-based encryption is remote and software-based encryption is local but it doesn't have anything to do with the form factor itself. Instead, it is about where the encryption is happening relative to your servers processing the database information.

Software to encrypt data at the table or column levels within relational database management systems is far more scalable and performs better on most of the platforms in an enterprise, when executing locally on the database server box. Software based encryption combined with an optional low cost HSM for key management operations will provide a cost effective solution that proves to be scalable in an enterprise environment.

The most cost effective solutions can be deployed as software, a soft appliance, a hardware appliance or any combination of the three, depending on security and operational requirements for each system. The ability to deploy a completely "green" solution, coupled with deployment flexibility, make these solution alternatives very cost effective also for shared hosting and virtual server environments. The green solution is not going away. There's too much at stake.

In a data warehouse users may search among 100 million encrypted records or maybe five billion records. It's crucial how much time is consumed for each decryption since a person may wait for hundreds or millions of records to be decrypted before the answer come back.

If you do it locally, close to the data, you may have a response time of around five micro-seconds for each record and then you multiply by 100 million if you have 100 million records and so on. Compare those five micro-seconds for local encryption to the case of remote encryption. You may have a thousand times greater latency and total processing time, so if you add up that time the user may wait for an hour instead of one second.

In online transaction processing, one user may not see a difference between local and remote encryption. If one user is looking for one record in the database, the difference between five microseconds and five thousand microseconds is not noticeable. But if you have a high volume of processing on your website or data warehouse, it will matter. If you add up all of your transactions and each of them takes a thousand times longer than necessary, you will hit multiple resource constraints and you will overload your computer. It can really cripple the user's experience and business operations. It is interesting also to notice that a fast network doesn't really help you. If you summarize all the steps that need to be processed for the data to go all the way from the database, over to another appliance and back, that path length is so much higher that the network speed doesn't really help you.

Another thing to think about when you dissect a remote appliance solution is this; if you want to be secure, you actually need to encrypt the data traveling over the wire between the appliance and your database server. Guess what? It costs you more overhead to encrypt that traffic than to do the encryption in the first place. Another myth is that the speed and the power of the appliance is going to affect the total speed of the encryption and decryption processing. The marketers will say, "Well, we can stack appliances so that you can harness this enormous power of these boxes. Put it on a fast network and you can really offload the processing." Seems to make sense at first, until all of the factors above are taken into consideration.

Is the additional risk of developing a custom system acceptable?

Build vs. buy

Many projects that have made the build vs. buy decision purely based on the misconceived notions from management about one option or the other. This is a decision that requires analysis and insight. Why re-invent the wheel if several vendors already sell what you want to build? Use Build or Buy Analysis to determine whether it is more appropriate to custom build or purchase a product. When comparing costs in the buy or build analysis, include indirect as well as direct costs in both sides of the analysis. For example, the buy side of the analysis should include both the actual out-of-pocket cost to purchase the packaged solution as well as the indirect costs of managing the procurement process. Be sure to look at the entire life-cycle costs for the solutions.

- Is the additional risk of developing a custom system acceptable?
- Is there enough money to analyze, design, and develop a custom system?
- Does the source code have to be owned or controlled?
- Does the system have to be installed as quickly as possible?
- Is there a qualified internal team available to analyze, design, and develop a custom system?
- Is there a qualified internal team available to provide support and maintenance for a custom developed system?
- Is there a qualified internal team available to provide training on a custom developed system?
- Is there a qualified internal team available to produce documentation for a custom developed system?
- Would it be acceptable to change current procedures and processes to fit with the packaged software?

Outsourcing

Outsourcing can be a less cost effective approach in the long run and it will not solve the liability aspect.

Outsourcing may also raise worries regarding security, hidden costs, loss of IT control, network bandwidth issues, lack of interoperability, vendor lock-in and service level agreements.

In many cases it may be more effective from a cost and data security standpoint to protect the data in the current system without changing the applications or the infrastructure. Recent incidents suggest that cybercrooks are increasingly beginning to target payment processors. Attacking a processor is much more serious than attacking a retailer. A processor sits at the nerve centre of the payment process and processes and also potentially store far more payment card data than any retailer. On the formal accounting side, outsourcing can be charged as expense, whereas the cost of developing an in-house system is capitalized, and may affect the capital budget.

Also look for efficiency gains when evaluating the cost-effectiveness of solutions. Centralized management of encryption keys reduces costs and complexity as well as potentially reducing system down time. Centralized policy enforcement, reporting and alerting supports compliance efforts and simplifies management chores as well as reducing risk and the costs of producing reporting for auditors.

A cost effective approach can be to use a single solution and process to provide a high quality of data across development, testing and staging environments and to protect sensitive data across development, testing, staging and production environments.

Step 5: Deployment

Focus initial efforts on hardening the areas that handle critical data and are a high-risk target for attacks. Continue to work your way down the list, securing less critical data and systems with appropriate levels of protection.

Be aware though that the conventional “Linked Chain” risk model used in IT security - the system is a chain of events, where the weakest link is found and made stronger - isn’t the complete answer to the problem. There will always be a weakest link. Layers of security including integrated key management, identity management and policy-based enforcement as well as encryption of data throughout its entire lifecycle are essential for a truly secure environment for sensitive data.

It is critical to have a good understanding of the data flow in order to select the optimal protection approach at different points in the enterprise. By properly understanding the dataflow we can avoid less cost effective point solutions and instead implement an enterprise protection strategy. A holistic layered approach to security is far more powerful than the fragmented practices present at too many companies. Think of your network as a municipal transit system - the system is not just about the station platforms; the tracks, trains, switches and passengers are equally critical components.

Many companies approach security as if they are trying to protect the station platforms, and by focusing on this single detail they lose sight of the importance of securing the flow of information. It is critical to take time from managing the crisis of the moment to look at the bigger picture. One size doesn't fit all in security so assess the data flow and risk environment within your company and devise a comprehensive plan to manage information security that dovetails with business needs. Careful analysis of use cases and the associated threats and attack vectors can provide a good starting point in this area.

It is important to note that implementing a series of point solutions at each protection point will introduce complexity that will ultimately cause significant rework. Protecting each system or data set as part of an overall strategy and system allows the security team to monitor and effectively administer the encryption environment including managing keys and key domains without creating a multi-headed monster that is difficult to control.

Centralized management of encryption keys can provide the most cost effective solution for an organization with multiple locations, heterogeneous operating systems and databases. All standards now require rotation of the Data Encryption Keys (DEK’s) annually and some organizations choose to rotate some DEKs more frequently (such as a disconnected terminal outside the corporation firewall such as a Point of Sale system).

Manual key rotation in a point solution would require an individual to deliver and install new keys every year on all the servers. Automated key rotation through a central key management system reduces most of this cost and can potentially reduce the down time.

Distributed point solutions for key management would include an initial investment for each platform, integration effort, maintenance and operation of several disparate solutions. It is our experience that manual key rotation in a point solution environment inevitably leads to increased down time, increase resource requirements, and rework. Key management and key rotation is an important enabler for several of the protection methods discussed above.

Centralized management of reporting and alerting can also provide a cost effective solution for an organization with multiple heterogeneous operating systems and databases.

This solution should track all activity, including attempts to change security policy, and encrypted logs to ensure evidence-quality auditing. Just as the keys should not be managed by the system and business owners, they should not have access to or control over the reporting and alerting logs. A system with manual or nonexistent alerting and auditing functionality can increase the risk of undetected breaches and increase audit and reporting costs.

Find the right balance between cost and security by doing a risk analysis.

Although it's always admirable to get the most for less, it's important to keep the return on data security investments in perspective. A recent report by the Ponemon Institute, a privacy and information management research firm, found that data breach incidents cost $202 per compromised record in 2008, with an average total per-incident costs of $6.65 million. Find the right balance between cost and security by doing a risk analysis. For example field level encryption with good key management may lower the probability of card exposure (for example from 2% to 1% for a given year).

A breach cost may be viewed to be $200 per card ($30 - $305 according to Gartner and Forrester, April, 2008). If 1 million cards would be exposed, an appropriate investment in a file protection solution with an integrated and sophisticated key management and protection system would be about $2 million.

All security spend figures produced by government and private research firms indicate that enterprises can put strong security into place for significantly less expenditure - about 10% the average cost of a breach. That's a good figure to remember when the accounting hatchet seems poised to descend on data security budgeting.

Conclusion

Risk-based prioritization replaces the all too common and costly triage security model - which is ineffective whether you're triaging based on compliance needs or the security threat of the moment - with a thought-out logical plan that takes into account long range costs and benefits as well as enabling enterprises to target their budgets towards addressing the most critical issues first. It's a balanced approach that delivers the enhanced security, reduced costs and labor with the least impact on business processes and the user community.

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.

ICDF2C 2009

International Conference on Digital Forensics & Cyber Crime

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

www.d-forensics.org

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

TRACKS

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

CALL FOR PAPERS

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

CALL FOR PRESENTERS

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

ICST

New York State Division of Criminal Justice Services DCJS

CREATE-NET

HELP NET SECURITY
WWW.NET-SECURITY.ORG

UNIVERSITY AT ALBANY
State University of New York