

# (IN) SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 10 - February 2007



**INTERVIEW WITH ED GIBSON, CSA AT MICROSOFT UK**  
**SPAM PROBLEM AND OPEN SOURCE FILTERING SOLUTIONS**  
**WINDOWS VISTA: SIGNIFICANT SECURITY IMPROVEMENT?**

# TABLE OF CONTENTS

Page 04 - [Corporate security news](#)

Page 07 - Microsoft Windows Vista: significant security improvement?

Page 21 - Review: GFI Endpoint Security 3

Page 26 - [Latest additions to our bookshelf](#)

Page 28 - Interview with Edward Gibson, Chief Security Advisor  
at Microsoft UK

Page 32 - Top 10 spyware of 2006

Page 34 - The spam problem and open source filtering solutions

Page 39 - [Software spotlight](#)

Page 40 - Office 2007: new format and new protection/security policy

Page 43 - Wardriving in Paris

Page 56 - [Events around the world](#)


Page 57 - Interview with Joanna Rutkowska, security researcher

Page 60 - Climbing the security career mountain: how to get more  
than just a job

Page 66 - RSA Conference 2007 report

Page 72 - ROT13 is used in Windows? You're joking!

Page 79 - Data security beyond PCI compliance - protecting  
sensitive data in a distributed environment



Welcome to (IN)SECURE 1.10  
the digital security magazine

It's been a busy year so far. We've attended the RSA Conference 2007 in San Francisco and met with some very interesting people from the security industry. A roundup of product and service releases is presented in this issue.

As you've been requesting, this issue delivers more interviews. There are articles for all levels of knowledge and with Vista being out, we cover its security improvements.

We're attending the Black Hat Briefings & Training in Amsterdam in March. If you're attending, be sure to drop me an e-mail and we'll grab a drink.

Mirko Zorz  
Chief Editor

Visit the magazine website at [www.insecuremag.com](http://www.insecuremag.com)

### **(IN)SECURE Magazine contacts**

Feedback and contributions: Mirko Zorz, Chief Editor - [editor@insecuremag.com](mailto:editor@insecuremag.com)

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

### **Distribution**

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

Copyright HNS Consulting Ltd. 2007.

# Corporate security news



## F-Secure Messaging Security Gateway goes virtual to tackle spam



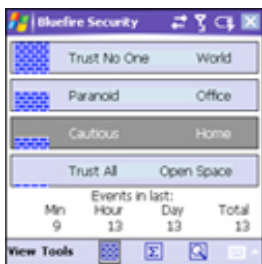
F-Secure announced the availability of its next-generation messaging security solutions, F-Secure Messaging Security Gateway appliance which blocks spam and viruses already at the gateway level. Version 4 comes with improved usability, mail queue management and support for more complex email infrastructures. While the Messaging Security Gateway is available in three different physical hardware configurations, it's now also available utilizing VMware's virtualization platform. All four versions feature the same anti-spam, anti-virus and anti-phishing features as well as an optional zero-hour protection against fast-spreading email viruses. ([www.f-secure.com](http://www.f-secure.com))

## Anti-data-leakage protection with Content Inspection Appliance 1500

Code Green Networks announced the release of its Content Inspection Appliance 1500 (CI-1500) for small and mid-sized organizations in business and government. The affordable, appliance-based solution enables IT and security managers to easily monitor content flows, discover data leaks, and implement automated policies to prevent them. Using patent-pending technology and residing at a company's Internet gateway, the Content Inspection Appliance 1500 monitors content flows on the corporate network and automatically enforces content protection policies. If it detects the unauthorized transmission of sensitive information, it invokes a management-defined policy to log, alert, block, or re-route the transmission. ([www.codegreennetworks.com](http://www.codegreennetworks.com))



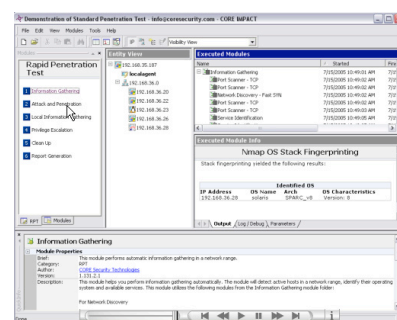
## Bluefire Mobile Security Enterprise Edition released



Bluefire announced the release of the Bluefire Mobile Security Enterprise Edition version 4.0. The product was designed with full support for Microsoft's Windows Mobile 5.0 Smartphone OS devices. Version 4.0 allows IT administrators the flexibility to customize the software to fit their specific needs. The product is now even more customized to meet the needs of large organizations with the addition of two new features – Secure key recovery for data residing on SD cards and the support for remote SQL instances assists large organizations in leveraging their existing data centers. ([www.bluefiresecurity.com](http://www.bluefiresecurity.com))

## Core Security Technologies releases CORE IMPACT 6.2

Core Security Technologies announced CORE IMPACT 6.2, which includes enhancements that enable organizations to more effectively test their security defenses against increasingly prevalent client-side attacks that rely on social engineering, such as spear phishing and e-mails with malicious content. The new version also features enhanced encryption and authentication capabilities to help testers more easily meet secure communication requirements during penetration tests, as well as expanded target platform support for testing networks with AIX systems. ([www.coresecurity.com](http://www.coresecurity.com))



## New format of 3M Confirm products with Floating Image Technology



3M announced the launch of a new format of the 3M Confirm authentication products with floating image technology that helps to protect against counterfeiting and tampering. This new format offers multi-layered overt and covert security features, and allows for the incorporation of additional security and tracking features into the same label. Confirm authentication products with floating image technology from 3M feature an optically variable device (OVD) – a unique, overt security feature. The OVD image appears to “float” above or “sink” below the surface of the label and then disappear as the viewing angle changes, which enhances the brand with a visually attractive “wow” factor. Dramatic movement of the image is easy to detect and recognize using only the human eye, enabling quick and easy authentication that helps to prove the label and product are genuine. ([www.3m.com](http://www.3m.com))

## The first managed authentication service for Mac OS X

CRYPTOCARD announced the launch of CRYPTO-MAS, the first Managed Authentication Service to fully support Apple's Mac OS X. Developed for small- and medium-sized businesses that either do not want the headache of managing their own authentication solution, or do not have the resources to install and administer two-factor authentication, CRYPTO-MAS makes it simple to eliminate unauthorized network access by protecting employees against shoulder surfing, social engineering, and other forms of password theft. ([www.cryptocard.com](http://www.cryptocard.com))



## Tenable Network Security releases passive Vulnerability Scanner 3.0



Tenable Network Security released version 3 of its Passive Vulnerability Scanner. Major enhancements include near real-time access to network vulnerability data and alerts as well as the availability of Tenable Policy Libraries which can monitor data streams and identify systems accessing pornographic or social networking sites, and inspect plain text email or IM traffic for credit card or social security information. In addition to the new capabilities available in the 3.0 release, Tenable's Passive Vulnerability Scanner continues to provide network discovery and intelligence by identifying and observing systems that are active on the network. ([www.tenablesecurity.com](http://www.tenablesecurity.com))

## Certicom launches Suite B Web security power bundle

Certicom released the Suite B Web Security Power Bundle to make it easy for IT managers to attain Suite B and FIPS compliance with security modules for web browsers, servers, and key communication protocols. As part of the U.S. government's crypto modernization



program, the National Security Agency recommended that communication devices and services use a specific set of cryptographic algorithms, known as Suite B, to protect classified and unclassified communications. The private sector is also beginning to implement the Suite B algorithms in products and services as Suite B has redefined what is considered industry best practice for cryptographic implementations. Certicom's family of Suite B products and services is the industry's most comprehensive set of cryptographic modules, including proven and optimized implementations for all of the Suite B requirements. ([www.certicom.com](http://www.certicom.com))

## Sophos releases WS1000 web control platform



Sophos launched the WS1000, the industry's first web control platform designed to provide trusted content security, application control and URL filtering in a single appliance. The WS1000 appliance ensures a secure web browsing experience as it protects against all forms of malware and productivity threats, all with no negative effect on user experience. It is designed for organizations which require a complete platform-based solution from a trusted vendor that addresses all security needs including web-specific content security, application control and URL filtering. Sophos's WS1000 protection is powered by intelligence gathered from scanning billions of web pages, identifying more than 5,000 new malware-hosting URLs daily. ([www.sophos.com](http://www.sophos.com))

## Pointsec releases Pointsec Device Protector

Pointsec Mobile Technologies released the Pointsec Device Protector solution which extends its enterprise data protection to include complete port and storage device management, effectively preventing sensitive information from falling into the wrong hands. Pointsec Device Protector effectively prevents or limits data transfers to these devices through a configurable security policy and content filtering to ensure that corporate IT infrastructure cannot be used for illegal distribution of copyrighted content or installation of malicious software. ([www.pointsec.com](http://www.pointsec.com))





## Microsoft Windows Vista: significant security improvement?

By Rob Faber

**Microsoft said the number one point of interest with the development of Windows Vista happened to be security. Windows Vista offers remarkable new and rich features in comparison with Windows XP. However, we all have to deal with the new security features Windows Vista introduced. It leaves no doubt: Windows Vista will have a tremendous impact on business. So is it really true? Are the new security features and the road ahead of us really that impressive as Microsoft claims to be? Let's take a look.**

It took a lot of time for Vista to see daylight. The first announcements almost came at the same time as Microsoft released Windows XP back in 2001. Microsoft revealed its plans for a new OS that would be far more revolutionary than ever before. The codename was "Longhorn" and it would be released somewhere in 2003. At least that was the overall plan. In the end of that year there happened to be a major vulnerability in Windows XP that made way for the "Trustworthy Computing initiative". One of the results of that step is the introduction of Windows XP Service Pack 2 (SP2) which is a step towards a more strict structure and measures taken by Microsoft to make the OS more secure by nature.

In the end of 2003 Microsoft finally came up with the first beta of Windows XP SP2. This

release concentrates most on items related to security. It is major release of Windows, one that would have impact on future releases and functionality of OS's such as Windows Vista.

Longhorn contained at first many important new developments like the Aero (Authentic, Energetic, Reflective and Open) interface changes, the WinFS storage framework, Avalon, Indigo (that concentrates on communication and collaboration), and most important: Palladium, a framework for security.

Along the way it turned out to be a hard job for Microsoft and several of too rigorous changes ended up in the trash like WinFS. After several delays finally Microsoft came up with the long expected follow up of Windows XP.

## And then there is.... Windows Vista

In the summer of 2005 the name finally changes from codename "Longhorn" to Windows Vista. Windows Vista comes in different flavours. There are currently five versions: Vista Home Basic, Home Premium, Business, Enterprise Edition and Ultimate. For a comparison of features I recommend the reader to visit the Microsoft website.

After several delays and a complete strategy change the question states: what is left of the initial plans of Microsoft with the release of Windows Vista? Well, let's have a more in depth look at the security part of this all and see what this means for your business.

### Security at the beginning: startup Windows Vista

Vista has Secure Startup which means that the entire hard drive can be encrypted prior to boot, and the encryption key will be securely stored inside a Trusted Platform Module (TPM) chip on the motherboard. Many of the methods used to circumvent permissions in the past by, for instance, using NTFS for DOS or just install a fresh copy besides the already installed OS will no longer work in simply reading data from the NTFS partition. I'll discuss this topic in the BitLocker part later on in this article.

And there is Address Space Layout Randomizer or ASLR. ASLR makes it possible that the system files load at random memory offsets, every time the system boots up. This will make it far more difficult to attack a system because attackers can't rely on files being in the same location every time. In earlier Windows versions system files always loaded to the same offset memory location

### Vista's User Account Control

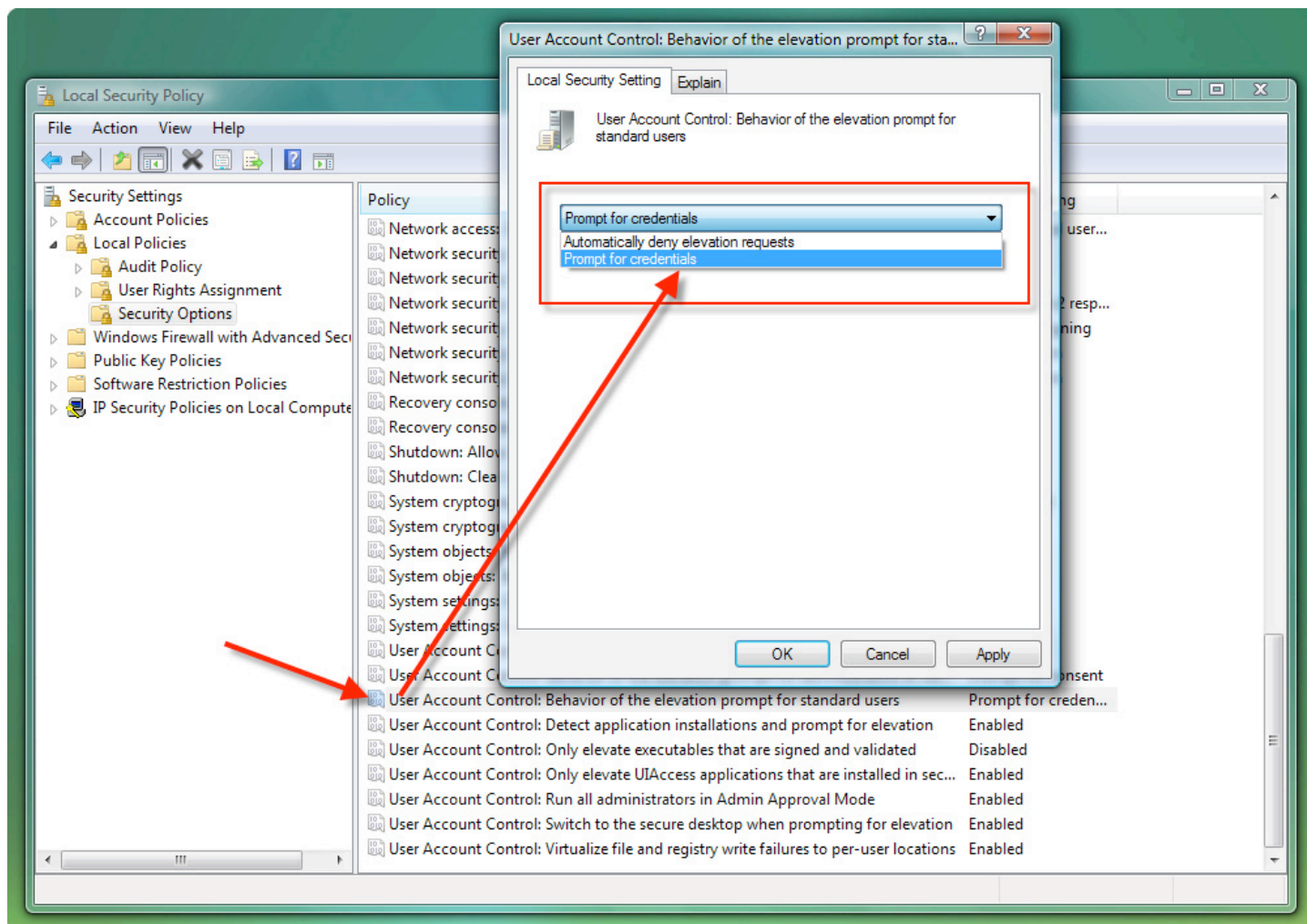
Don't we all like to have the administrator rights on our workstation? It's simple and gives us the biggest freedom. Windows users are used to work with administrative privileges in both the enterprise organization and at home. This freedom does have a big downside: more helpdesk calls being made because of accidentally or deliberately made modifications of the OS with a variety of errors

as an outcome. The result of this all is a desktop that is much harder to manage (tighten up the workstation to implement the security policy of your organization) and likely more support costs for your organization.

User Account Control (UAC) is introduced with Windows Vista and offers increased security over previous versions of Windows because it is intended to prevent unauthorized changes made by the end-user on the computer so that the system (system files) cannot be altered. UAC is based upon the concept of the so called "least-privilege". In this principle, that sounds very familiar to security professionals, an account is set up that has only the minimum amount of privileges needed for that end-user to perform the appropriate tasks. This standard user within Windows Vista is this least-privileged user. The fact is that UAC relies upon two types of accounts: an administrator account and a standard user account. To be more exact in the definition of administrator accounts: there are two different types of administrator accounts that are defined for Windows Vista.

First the powerful Administrator account, and second all the accounts that are part of the Administrators group. The powerful administrator account can perform all tasks on the system and it will not be prompted or confronted with dialog boxes. Surprisingly enough the second type of administrator accounts (those members of the Administrators group) are running almost as standard users. Almost, because these users have the possibility to elevate their privileges by simply click a button in a dialog box when prompted. The types of authentication dialogs you'll see, however, will differ depending on which type of user account is currently being used. A standard user account that is not part of an Administrators group will not simply elevate privileges, the user then must provide the appropriate credentials. Under UAC, the defined standard user can perfectly perform most daily tasks, such as using business applications, browsing internet and type a letter in a word-processor. However, when there is the need to change settings that require administrator privileges, like installing new software or change a sensitive setting, this user will be confronted with a dialog box, asking this person to give the appropriate credentials (in other words: type in





Different UAC policies

the account and password with sufficient rights). In most instances, it will be perfectly clear that a prompt will appear, because the setting will have an icon in the form of a shield next to it. This indicates higher privileges are necessary.

### Low profile administrators

As already known by many of us: a common practice is to work with normal credentials on the Windows platform. Even as an administrator. When there is a need for more privileges an administrator can use "run as..." and elevate the standard user privileges to true administrator rights.

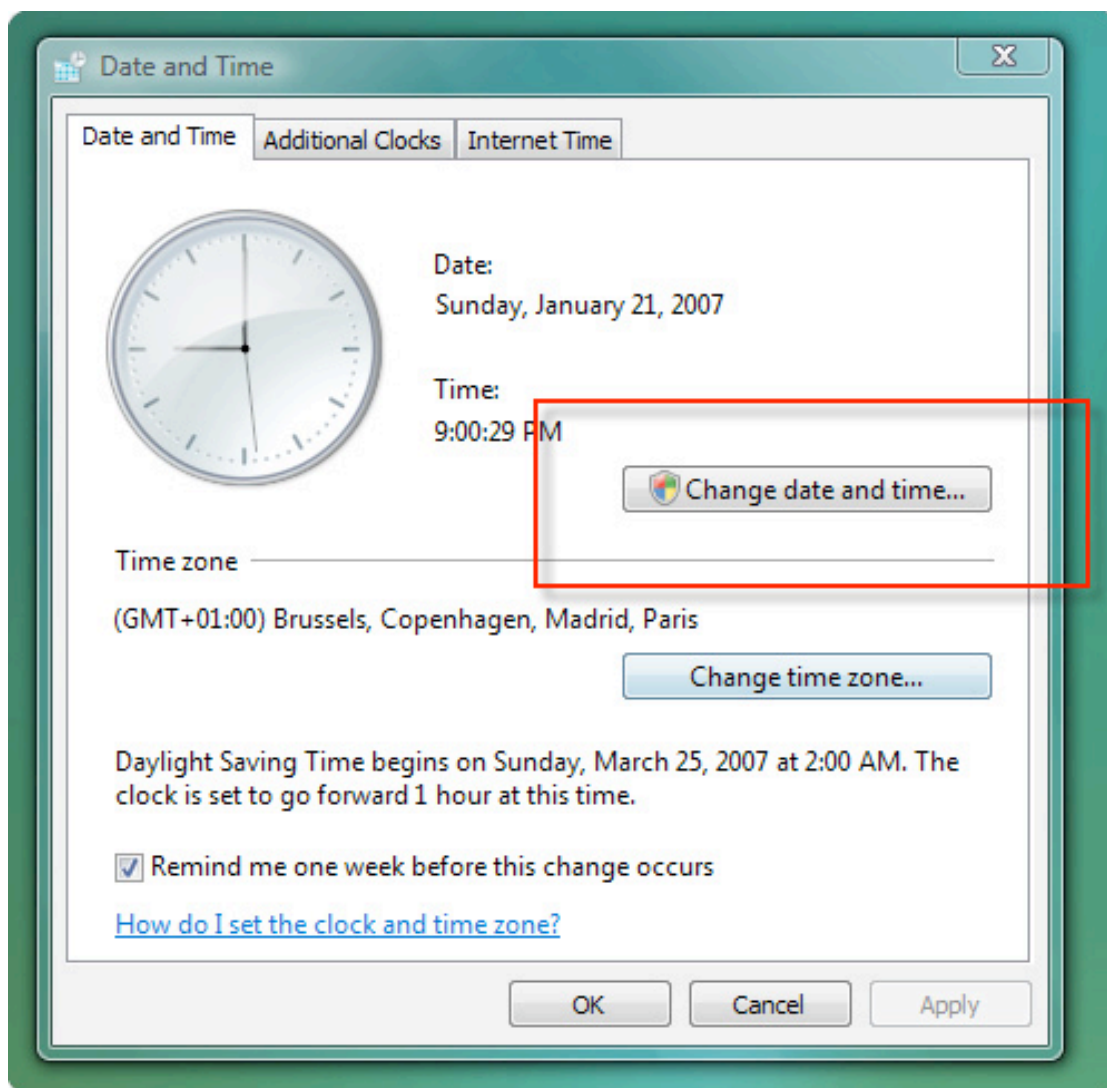
In Windows Vista you should run as a standard user rather than as an administrator, because unauthorized changes can be more easily made when you run as an administrator. The great thing is: when an administrator needs to use their administrator privileges, they don't have to use Run As because Windows Vista can automatically prompt them for

the required credentials. Behaviour can be set by a policy "UAC: behaviour of the elevation prompt".

### Running applications with UAC: virtualization

Although it will be certain that there are exceptions, most applications will run under UAC using the administrator account or a standard user account. Many applications will not run on Windows XP without administrative privileges today because they attempt to make changes to locations that the user cannot or may not access, such as C:\Program Files, C:\Windows, or HKEY\_LOCAL\_MACHINE.

Windows Vista works with registry and file virtualization to redirect attempts to write in one of the "forbidden" locations and in this way converting per-machine file and registry entries to per-user locations if the user lacks the administrative privileges.



The shield indicating to elevate privileges.

This enables standard accounts to run applications that still need to write to areas of the registry or file system that only administrators can access. The disadvantage is that this setting are not available to other users on that machine, it's stored in the users profile (not part of the roaming profile!).

Keep in mind that Microsoft gives us the life-cycle time of Vista to work on our bad application behavior and that in the next OS this downward compatibility feature would be disappeared! So it is really important to think about this fact and do something about misbehaving or not so well written applications.

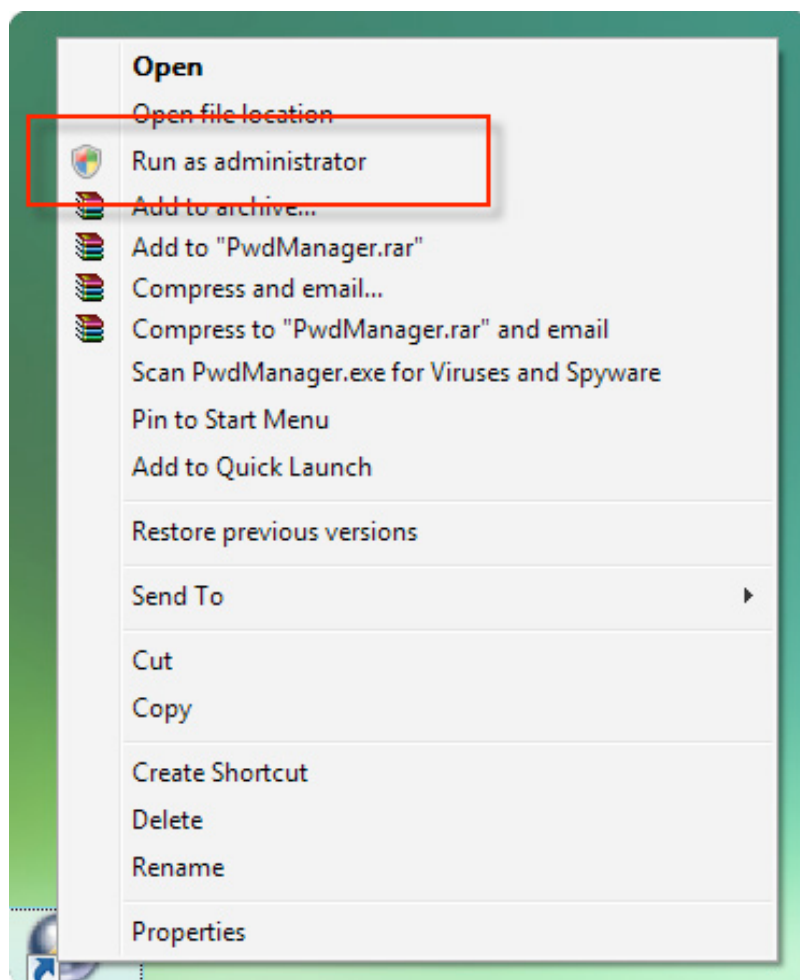
### Consequences of UAC and cost savings

As mentioned before: running without administrative privileges can be really challenging today since many applications expecting this in order to run correctly. In any way I recommend not to disable UAC. UAC is here to stay

and as professionals we have to deal with this phenomenon in the right way. For exceptions an administrator can allow a standard user to run certain applications without being confronted with a dialog box asking them to give the appropriate credentials.

This way the administrator can "elevate" the privileges of the specific application and have it always run with those privileges. An administrator can accomplish this by right-clicks the application, selects the Compatibility tab, and then select under Privilege Level: "Run this program as an administrator."

Roll out desktops with the standard user permissions can result in cost savings because a non-administrative user no longer has the ability to accidentally or deliberately install an application or otherwise affect system stability. This can decrease the helpdesk call being made.



Run as... possibility

## BitLocker

Theft or loss of corporate intellectual property is an increasing problem and concern for organizations as I wrote in my article of December 2006 of this magazine.

Protection is particularly valuable with mobile computers, which are more vulnerable to theft or loss.

Windows Vista has improved support for data protection. You can find this support on the document level by implementing Rights Management client which allows organizations to enforce policies around document usage. At the file-level by using Encrypting File System (EFS), this provides user-based file and directory encryption. EFS have the possibility to allow storage of encryption keys on smart cards, providing better protection of encryption keys.

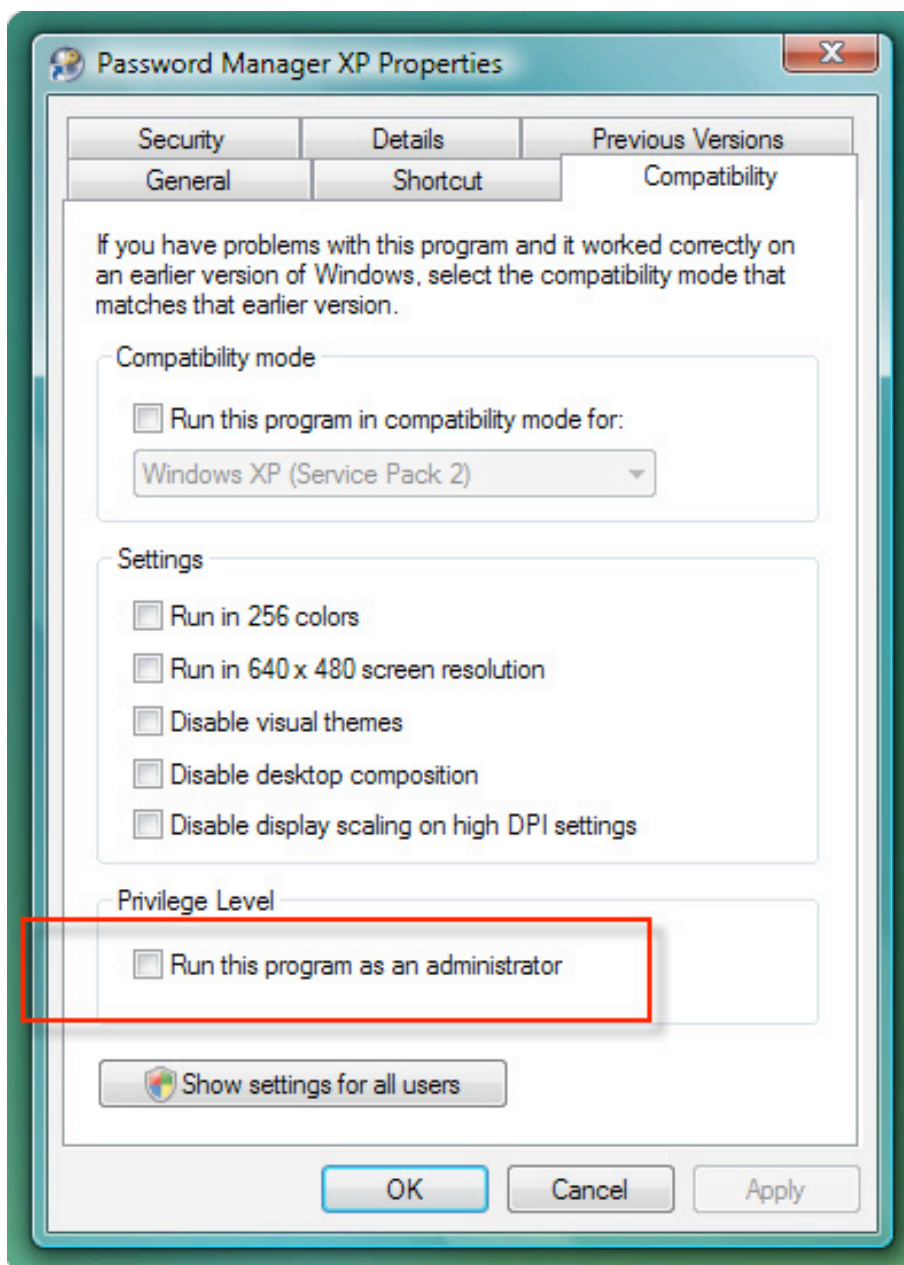
And last but not least at the machine level by using the BitLocker Drive Encryption feature. On a computer with the appropriate hardware,

BitLocker Drive Encryption provides full volume encryption of the system volume, including Windows system files and the hibernation file, which helps protect data from being compromised on a lost or stolen machine.

BitLocker provides 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 that encrypt and decrypt sectors on the hard drive. This chip is present already on new motherboards today. The key used for the disk encryption is sealed (encrypted) by the TPM chip and will only be released to the OS loader code if the boot files appear to be unmodified. TPM is in this case an implementation of a so called Root-of-Trust. The pre-OS components of BitLocker achieve this by implementing a Static Root of Trust Measurement. This is a methodology specified by the Trusted Computing Group (see also: [www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org)).



Running a program with admin credentials

- *User authentication mode*

This mode requires that the user provide some authentication to the pre-boot environment in order to be able to load the OS. Two authentication modes are supported: a pre-boot PIN entered by the user or a USB device inserted that contains the required startup key.

- *USB-Key*

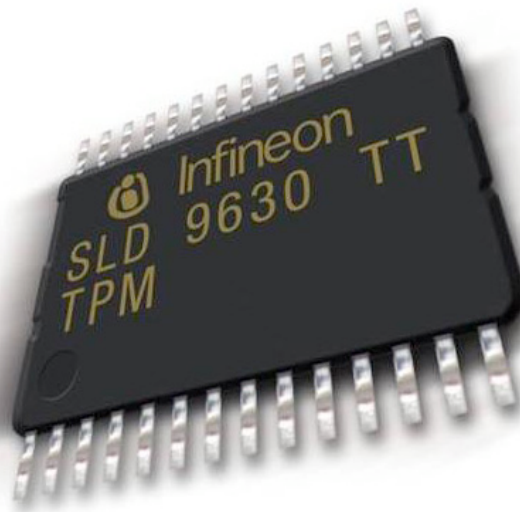
The last possible mode is where the user must insert a USB device that contains a startup key into the computer to be able to boot the protected OS.

In this mode it is required that the BIOS on the protected computer support the reading of USB devices in the pre-OS phase.

## BitLocker and encryption keys

BitLocker full volume encryption seals the symmetric encryption key in a Trusted Platform Module (TPM) 1.2 chip. This is the so called Storage Root Key or SRK. It all works with a chain of keys. The SRK encrypts the FVEK or Full Volume Encryption Key. The FVEK is then stored on the hard drive in the OS volume.

BitLocker stores blueprints of core operating system files in the TPM chip. Every time the computer is started, Windows Vista verifies that the operating system files have not been modified in an offline attack or that the hard drive is tampered with.



The TPM chip

A scenario could be where an attacker boots an alternative operating system in order to gain control of the system. In case the files have been modified, Windows Vista alerts the user and as a result TPM refuses to release the key required to proceed with the boot-process and to decrypt the volume. What happens next is that Vista goes into recovery mode thereby prompting the user to provide an appropriate recovery key to allow access to the boot volume

To get this all working you will need two NTFS volumes: a “system volume” that is at least 1.5GB in size and a “boot volume” which contains actually Vista itself. The system volume is used to install BitLocker and is not encrypted. If you meet the requirements, you let BitLocker do its work, which can take quite a while on larger hard drives. Once this process is finished the end user won’t be aware of it. Data is encrypted on-the-fly. The official Microsoft statement is that BitLocker in combination with Windows Vista can only encrypt the operating system volume. Using built-in command-line tools, BitLocker can be used to encrypt more than just the boot volume, but additional volumes cannot be encrypted using the GUI. However, I’ve seen an article about the command line interface of BitLocker where it is possible to affect other volumes. You can find this article by following this link-[bink.nu/Article9133.bink](http://bink.nu/Article9133.bink)

Microsoft announced that in Longhorn it will be possible to encrypt multiple volumes. Take notice about the fact that we are talking every time about volumes. BitLocker Drive Encryp-

tion is logical volume encryption. And as you will know: volumes can be equal to an entire drive (or less than that) but also be spread out over more physical drives.

### Manage BitLocker in the enterprise: recovery mode

There can be situations where you do have to move a hard drive from one machine to another. For example: the laptop display is damaged and the support organization wants to hand out a spare machine to that affected user.

This can be a problem because TPM and the hard drive are logically connected to each other on that specific machine. Fact is: the encryption keys to decrypt the volume are stored in the TPM of that particular machine. How can this problem be solved?

In that case recovery mode can be used and requires a recovery key that is generated when BitLocker is enabled. However: that key is specific to that one machine. So for every single machine there will be a specific key. Oh no, I hear you say: how to manage that? For enterprise organizations you will need infrastructure to manage and store all the specific recovery keys - that store will be the Active Directory.

If you do not manage this properly there is a real potential for losing data if a computer fails and its drive is moved to another computer and the recovery key at that time is unavailable.

## Accidents

In case a hard drive crashes it would be possible in theory that the FVEK or Full Volume Encryption Key could be unavailable and at that time the volume can't be decrypted. For this there is also a solution. When BitLocker seals or encrypts a key it is stored on the disk as a binary large object or "blob". The "blob" is the cryptographic keyhole where the decryption key will "fit in". So it takes both the blob and the key to start decryption. There are multiple "blobs" on the disk so if one is not available or damaged another one will be tracked and used. Pretty nifty I think!

## BitLocker and backdoors

So a great mechanism but safe by any means? And by any means, we really mean "by ANY means". This is a topic that is heavily discussed. According to Microsoft, BitLocker does not have a backdoor built in. So in other words: there is no way (even for law enforcement or secret service) to get around the protection mechanism in a predefined way so the protected data is unveiled.

See also [tinyurl.com/synxs](http://tinyurl.com/synxs)

So BitLocker according to my opinion is a great mechanism, Microsoft did a great job and thought about it in an enterprise way. However, be wise and really thoroughly think about the process of implementation. Management is the key word and it is really important to consider this matter several times prior to roll out this solution.

## Smartcard support or two-factor authentication

We all know: working with passwords is a weak protection method in comparison with other alternatives. Brute force attacks, dictionary attacks and so on, all weaknesses in working with passwords. For many organizations, single-factor authentication (the good old user-id and password) is not sufficient anymore. Multi-factor authentication is the way to go. Something you know (a pin code), you are (fingerprint / biometrics) or carry something with you that you own like a token or smart-card. It all refers to multi-factor authentication.

Windows Vista does have built-in authentication support for passwords but also the use of smart cards. In fact the whole GINA of Windows is reviewed and developed from scratch by Microsoft. Windows Vista makes it possible for developers to more easily add their own custom authentication methods to Windows, such as biometrics and tokens. It also provides enhancements to the Kerberos authentication protocol and smart card logons. By making it easier for developers of such solutions, the security professional will have more choices for biometric, smart cards, and other possibilities of strong authentication to implement.

## Services hardening within Vista

Windows Service Hardening is a feature that restricts critical Windows services from doing abnormal activities in the file system, registry, network, or other resources that could be used to allow malware to install itself or attack other computers.

In the past Windows services are causing a large amount of attacks on the Windows platform. This is rather easy to explain - an attacker can rely on Windows services because it is almost always present and it is predictable code and the privilege level of that code is known by many.

Windows Vista limits the number of services that are running and operational by default. Today, many system and third-party services run in the Local System context, where any breach could wreck the machine. This includes things like disk formatting, unauthorized access to data and unintended installation of software. Windows Service Hardening reduces this damage potential of a compromised service by introducing new concepts. I will briefly discuss some highlights.

On a per-service basis security identifier (SID). This makes it possible to identify specific services and implement access control by working with ACLs. Services can be tightened up by applying explicit ACLs to resources which are private to the service, which prevents other services as well and the user from accessing that specific resource. Furthermore applying a write-restricted access token to the service process.

This access token can be used in cases where the set of objects written to by the service is bounded. Write attempts to resources that then do not explicitly grant the Service SID access will fail.

Microsoft moved services from Local System Context to a less privileged account such as Local Service or Network Service. This reduces the overall privilege level of the service, which can be compared to the already discussed User Account Control (UAC). And then the removal of un-necessary Windows privileges on a per-service basis.

Services are assigned to a network firewall policy, which will prevent unwanted or unpredicted network access outside the normal bounds of the service. The firewall policy is linked directly to per-service SID. In this case an attack platform from the local machine to the network is more difficult to accomplish or even prevented. These restrictions are under the firewall settings and they can be found in the registry:

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\System.
```

The firewall is discussed in the next section.

## BESIDES THE FIREWALL THAT HAS CHANGED, IN WINDOWS VISTA THE WHOLE TCP/IP STACK HAS BEEN RE-WRITTEN / RE-DESIGNED.

### Layered approach

Security is in most cases a layered approach and Service Hardening provides a part of this concept and is just an additional layer of protection for services based on the security principle of defense-in-depth. However it cannot guarantee services from being compromised.

The defense-in-depth strategy will certainly make it much harder to get an easy attack platform, Windows firewall, UAC, patch management practices and Integrity Levels will fill in other important layers.

### Windows Vista Firewall

At first, the Windows Vista firewall looks very similar like that of Windows XP. In fact, the user interface in Windows Vista is nearly identical to that of Windows XP. But the real secret lies underneath the surface. Most advanced setting can't be reached via the standard GUI which is more targeted towards home-end-users by all respect. You can really ultimately tune the firewall settings by using Group Policy or the firewall MMC snap-in. I'll return on that later.

Besides the firewall that has changed, in Windows Vista the whole TCP/IP stack has been re-written / re-designed. The new architecture Windows Filtering Platform (WFP) did increase the performance significantly and

there are even API's available. The new TCP/IP-stack supports IPv6 and a dual IP layer-architecture. I advise those of you who are interested in more to visit [tinyurl.com/dkklc](http://tinyurl.com/dkklc).

The firewall in Vista supports rules for incoming traffic, simply dropping all unsolicited incoming traffic that does not correspond to traffic sent in response to a request of the computer (solicited traffic) or traffic that has been specified as allowed (excepted traffic in a pre-defined firewall-rule). It seems a dull topic but is really crucial as it helps prevent the infection of computers by network-level viruses and worms that spread most of the times through incoming traffic. So far so good and nothing really new.

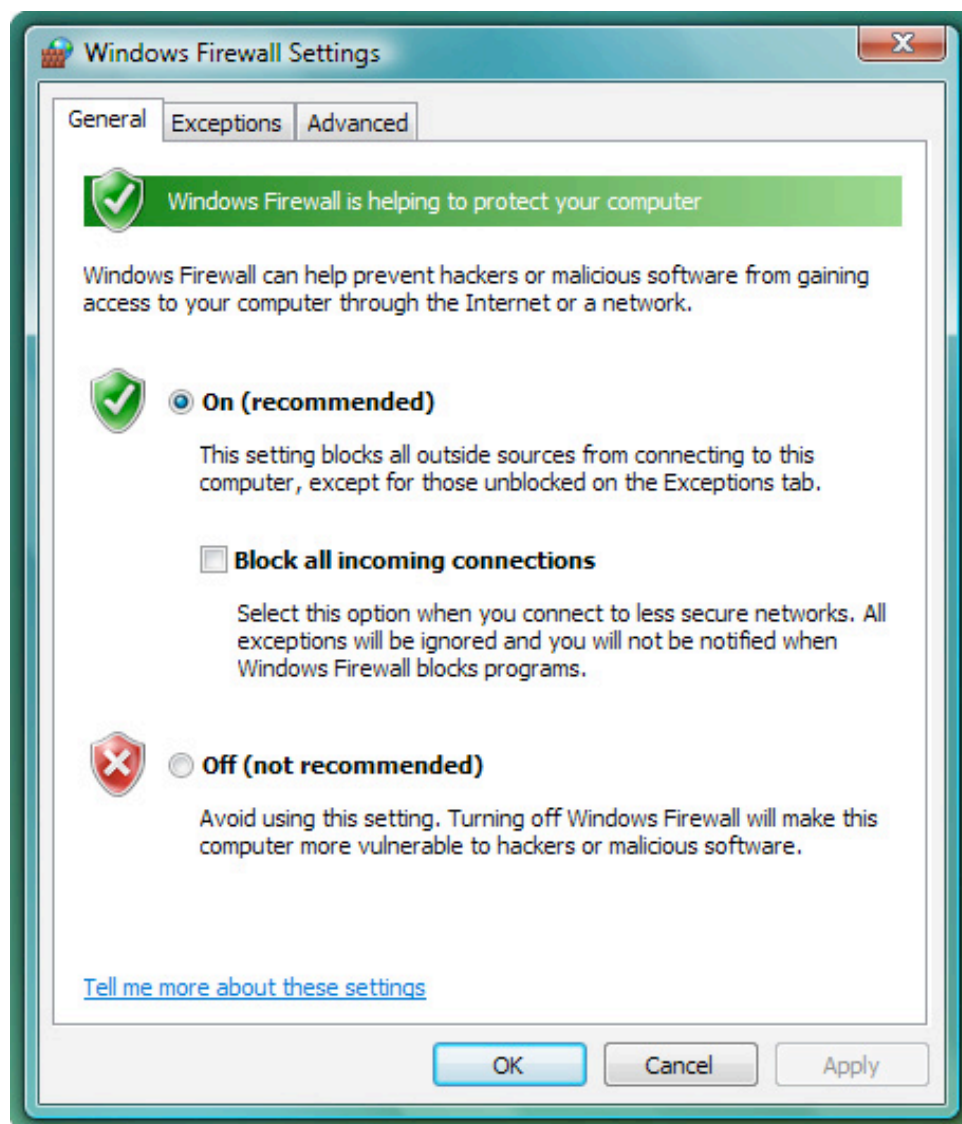
What really is new, is the fact (in comparison with windows XP) that Vista Firewall supports filtering for outgoing traffic or application-aware outbound filtering which gives full bi-directional control over traffic.

Since a whole bunch of business applications may use different ports, Microsoft decided to not enable outgoing filtering by default. The default behavior of the new Windows Firewall will then be:

- Block all incoming traffic unless it is solicited or it matches a configured rule.
- Allow all outgoing traffic unless it matches a configured rule.

Another possibility is that the Firewall in Windows Vista will allow administrators to block applications from contacting or responding to other computers in the network, like peer-networking. The Windows Vista firewall settings are configurable by Group Policy objects

to simplify management in enterprise organizations. For better configuring there is an integration between both IPsec and the firewall. It will be much easier to use, requiring less effort to configure.



Standard Firewall interface for end-users

### Manage the Firewall settings

Like in Windows XP there is a GUI for configuration of the Windows Firewall item in Control Panel. This mainly is simplistic and for enterprise organizations not very useful. You can configure basic settings for the new Windows Firewall, but you cannot configure enhanced features.

For more in-depth features and setting there are at first a whole lot of Group Policy settings which can be reached by firing up the Group Policy editor snap-in. Second the new Win-

dows Firewall can also be configured with an MMC snap-in named Windows Firewall with Advanced Security.

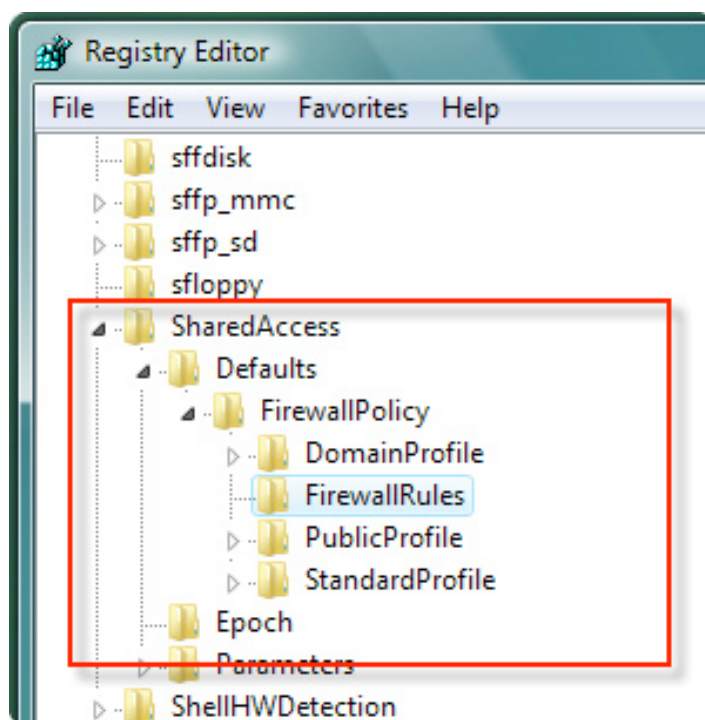
With the new Windows Firewall with Advanced Security snap-in, administrators can configure settings for the new Windows Firewall on remote computers, which is not possible for the current Windows Firewall without a remote desktop connection. In enterprise organizations it is more likely that you will be using the Group Policies to manage setting in a more central way.



For command-line configuration of advanced settings of the new Windows Firewall, you can use commands within the *netsh advfirewall*. Firewall settings are stored in the registry on the local machine and the settings can be found under the following key (I have to stress

the fact not to change these settings manually):

HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Defaults\FirewallPolicy\FirewallRules



Registry-based settings of the firewall

## Firewall profiles

The firewall of Windows Vista works with profiles: the Private Profile for working on a home network, the Public Profile for connecting to public networks and, last, the Domain Profile for computers that join a domain. The Network Location Awareness Service (NLA) detects network changes and notifies the Firewall. The firewall then can change a profile within 200 ms. If a user is not present in a domain, the user will be asked for the appropriate profile: public or private.

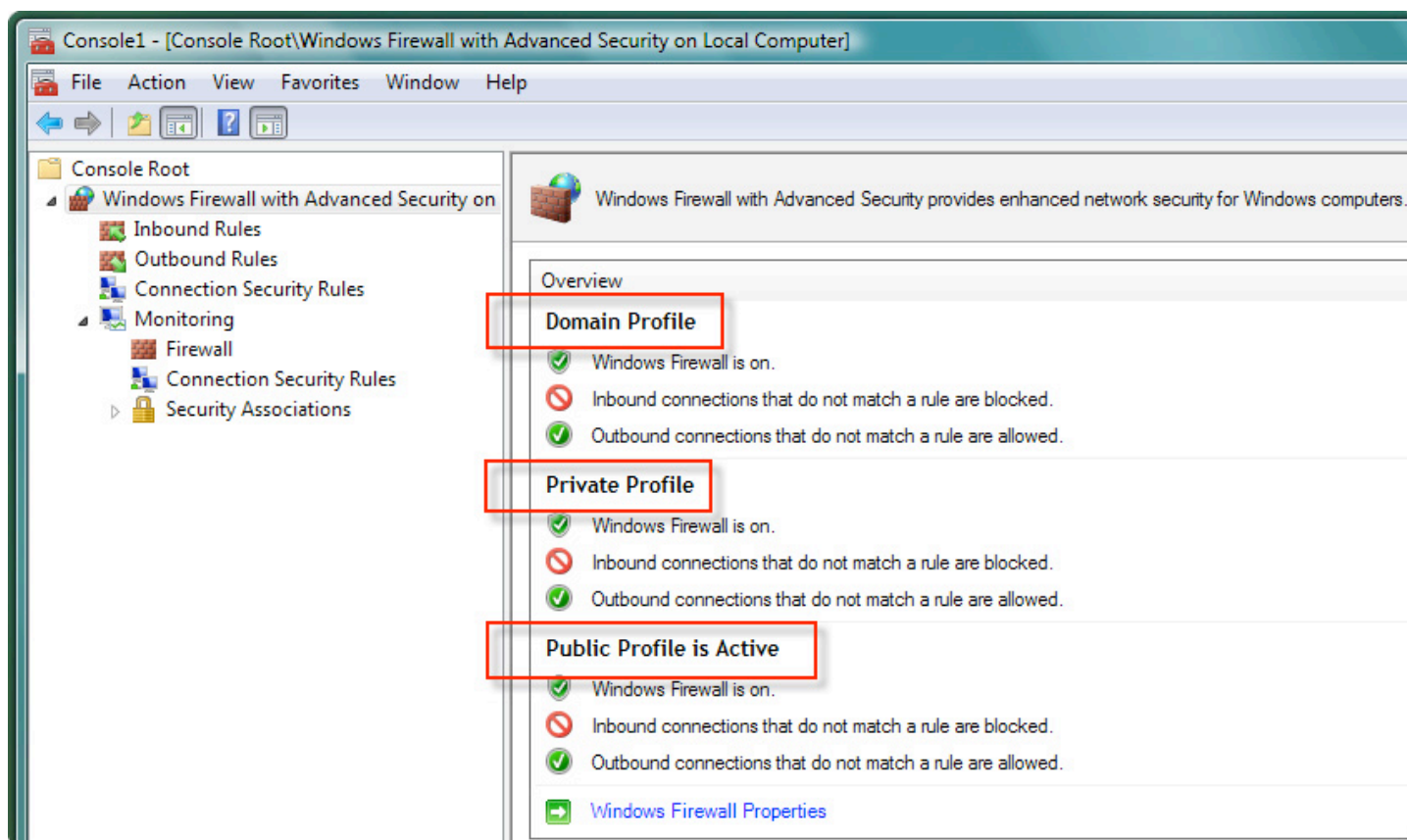
Unfortunately Vista has at this time no way of differentiating between a public and private network, so it will actually ask users whether they are attaching to a public or private network at the time that the connection is established. In future versions it will be possible to define a profile or there will be other available profiles. In the case you want to define a private network you must be a local administra-

tor in order to set this up and to connect the computer.

## Firewall and IPSec

As you will know: IPSec is a protocol standard to provide cryptographic protection for IP traffic. In Windows XP and Windows Server 2003, Windows Firewall and IPSec are configured separately. However, both the Windows firewall and IPSec in Windows can block or allow incoming traffic. In this case it would be possible to create overlapping or conflicting firewall rules and IPSec rules.

All these settings are now combined in the new Windows Firewall and can be configured using the same GUI and command line commands. Another benefit is the configuration of IPSec settings are highly simplified. Furthermore there is a less complicated way of policy configuration, improved support for load balancing and clustering and the possibility to use more cryptographic suites.



Different profiles Vista Firewall

## Network Access Protection

Users who travel with their computers or have specific roles in organizations are sometimes unable to connect to the corporate network for days or even weeks. And then after a while when they do connect, their connections might be so short that their computers do not have the ability to fully download the latest updates, get security configuration settings, and virus signatures the organization wants them to receive.

The Network Access Protection mechanism improves the security around this type of users and their computer by ensuring that when they do connect longer or are back at the office after some time, the computer is first checked against a certain baseline. When the computer doesn't meet the criteria at first the latest updates are installed and then, after the criteria are met, users can connect to the corporate network. This concept is also known as network quarantining.

Windows Vista includes an agent that can prevent a Windows Vista-based client from connecting to your private network if it is miss-

ing the latest security updates, has old virus signatures, or otherwise fails to meet your computer policy. This can be used to protect your network from remote access clients as well as LAN clients.

I personally think that there is a lot of work to do to make this a more mature service. Microsoft's current implementation of NAP is overall not that user-friendly or very useful in most larger environments. Besides that, not all network equipment can't be used, big vendors like Cisco do work in cooperation with Microsoft.

## Vista's Integrity Level mechanism

Before going more in detail on Windows Internet Explorer 7, I'll have to discuss Integrity control. Sounds this familiar? Right. Vista includes a new feature "Windows Integrity Control." This means every object that is having some kind of permission can also have an extra label that identifies its integrity level.

A user (subject) will be working with files and folders (objects) which can have integrity levels.

Integrity levels are assigned within Vista to processes (subjects) and objects and an integrity policy restricts access granted by the Discretionary Access Control (DAC) security model. We start to work with integrity levels within windows!

In reality this can have the consequence that software with a low(er) integrity level can't make changes to software of processes with a higher integrity level.

So how does this work? Integrity levels are defined by Security IDs (common known as SIDs). The RID defines the actual integrity level. The integrity levels themselves are sometimes called "Windows Integrity Levels" or "Mandatory Integrity Levels." Right now the following primary integrity levels exists:

- Low S-1-16-4096 (0x1000)
- Medium S-1-16-8192 (0x2000)
- High S-1-16-12288 (0x3000)
- System S-1-16-16384 (0x4000)

## IE7 and integrity levels

And here comes the trick: Internet Explorer 7 standard works in a low integrity level context.

The user however is working in a medium integrity level context. If you would download a piece of code or software from the internet there is a rule that is saying: no-write-up. The lower integrity level can't access or misuse the process running in a higher integrity level context (for example a process running in the context of the user).

```

C:\Windows\system32\cmd.exe
C:\Users\U_User>whoami/all
USER INFORMATION

User Name      SID
-----
vc00122\vc_user S-1-5-21-1288371706-3102028391-3400826450-1000

GROUP INFORMATION
-----
Group Name      Type      SID      Attributes
-----
Everyone        Well-known group 00000000-0000-0000-0000-000000000000 -1-1-0 Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators Alias      -1-5-32-544 Group used for deny only
BUILTIN\Users   Alias      -1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE Well-known group -1-4 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group -1-11 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization Well-known group -1-15 Mandatory group, Enabled by default, Enabled group
LOCAL BUILTIN\Administrators Well-known group -1-5-32-544 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication Well-known group -1-4-10 Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Unknown SID type -1-16-8192 Mandatory group, Enabled by default, Enabled group

PRIVILEGES INFORMATION
-----
Privilege Name      Description      State
-----
SeShutdownPrivilege Shut down the system Disabled
SeChangeNotifyPrivilege Bypass traverse checking Enabled
SeUndockPrivilege Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
SeTimeZonePrivilege Change the time zone Disabled
C:\Users\U_User>
  
```

Integrity level policies are associated with generic access rights and default the following rules exists:

- No-Write-Up which means that a lower Integrity Level process cannot modify a higher Integrity Level object
- No-Read-Up which means that a lower Integrity Level process having generic read possibilities
- No-Execute-Up which means that a lower Integrity Level process generic execute access

As stated before: the default policy is "no-write-up". Security tokens in every process can be assigned an integrity level and administrators can change those levels between "untrusted" and "high". Administrators can't set integrity levels higher than "high" because administrators itself run in the integrity context of "high" and no one can ever elevate (even administrators can't) an object's integrity level higher than their own level. You can see a process' integrity level by typing the command: Whoami /all. There are also tools in the market like that of Mark Russinovich (Microsoft Sysinternals). For more information visit [tinyurl.com/y8jsyn](http://tinyurl.com/y8jsyn).

## Conclusion

I believe Windows Vista is a huge improvement over the Windows XP version concerning security (and other rich features). The development really made a good step forward from a security perspective. Windows Vista certainly will have a major impact on your business and more than ever needs a solid plan and think over before starting to migrate. Many features presented and there is so much that you will at first be overwhelmed by all the changes made in this new OS.

There are some topics that will need special attention like legacy applications that probably won't work "out of the box" on Vista. Most of the times these application present "show-cases". If there anything goes wrong with this or doesn't work anymore, you like the idea of a holiday. This can really be a big issue for you and the business you're supporting.

In this article I didn't discuss all security changes. Things like code integrity and driver signing, Windows Defender (Forefront Security) and the more that 3000 Group Policy items that currently provided to you for Windows Vista. Some things need improvement like the quarantine function and USB blocking feature. Microsoft supports USB blocking on the Vista client by group policies. In my opinion not the way an enterprise organization can deal with this problem.

Reading this article will give you a glimpse of all the radically changes and strategic plans and ideas of Microsoft for the future. I hope I made clear that it is not a reasonable assumption that Microsoft didn't do anything in the past years to make Vista more reliable, secure and stable then earlier versions of Windows.

Rob P. Faber, CISSP, MCSE, is an infrastructure architect and senior engineer. He is currently working for an insurance company in The Netherlands with 22.000 clients. His main working area is (Windows Platform) Security, Active Directory and Identity Management. You can reach him at [rob.faber@icranium.com](mailto:rob.faber@icranium.com)



Subscribe to the HNS Software Alerts and  
learn about updates every Monday:  
[www.net-security.org/subscribe.php](http://www.net-security.org/subscribe.php)

Never use outdated software again.



## Review: GFI EndPointSecurity 3

By Tim Wilson

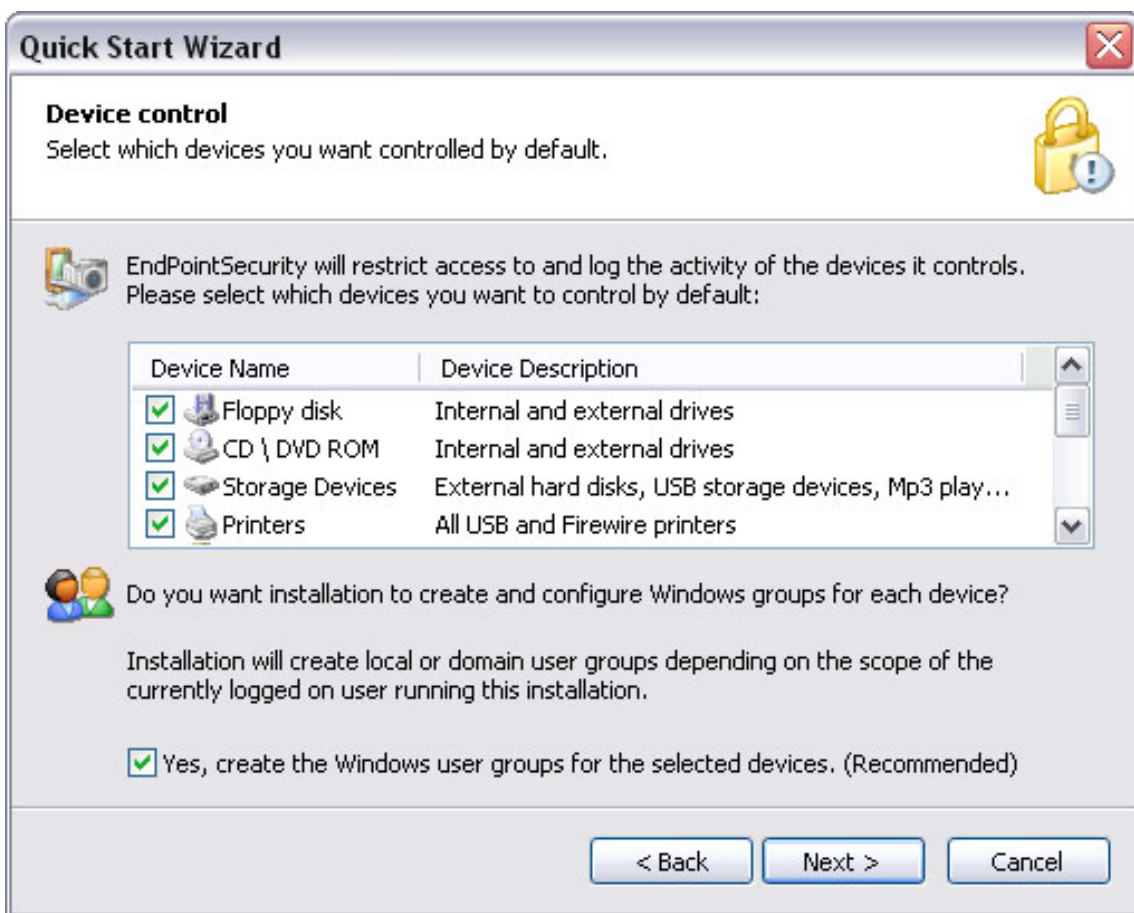
**In the past couple of years, we definitely saw an up trend of portable devices usage. From handhelds, to music players, these devices offer a number of top notch options, one of them being an effective device for storing data. With all the good characteristics this way of backing up or transferring data offers, we can also identify a security threat that can be derived from this process.**

**This is something similar to the trend of organizations banning mobile phones from some portions of their facilities. Almost every new mobile phone has a quality built-in camera, so confidential data can be easily snatched and digitalized.**

With other portable devices there is a very similar problem - technology is evolving and every new device is smaller and more powerful. It has become very easy to bypass some default system barriers and easily move potentially insecure pieces of software from the device to a specific computer, or vice versa, taking home some protected company data.

Security products such as GFI's Endpoint Security help in this line of work and add an extra layer of security to your organization network environment.

GFI EndpointSecurity is installed and managed from a central location. It is actually constructed out of two parts. The first one is GFI EndPointSecurity user console that offers the administrator means of configuring various policies and installing remote client software on to the network computers. The client software, regarded as GFI EndPointSecurity agent, is a client side service that is acting upon the protection policies from the main computer. Depending on the configuration it will either allow or deny the user access to the specific resource.



List of controlled devices.

The software in question provides a list containing a number of portable device types and places them in the appropriate groups.

Besides the general selection of media like floppies, CD and DVD ROM discs, GFI End-point has the following categories: Storage Devices (flash and memory cards, readers and set of multimedia players), PDA devices, Network adapters (Bluetooth, WLAN and infrared), Modems (mobile phones and smartphones), Digital cameras and a selection of other devices ranging from ZIP to tape drives.

GFI EndPointSecurity's line of work is pretty straightforward. I will go into more details about all the parts of the whole process later, but the process is pretty simple - you define a unique protection policy for a group of computers.

During the configuration steps you specify the resources users of some groups or domains can or cannot access. With a click of a button, that policy is updated to the client

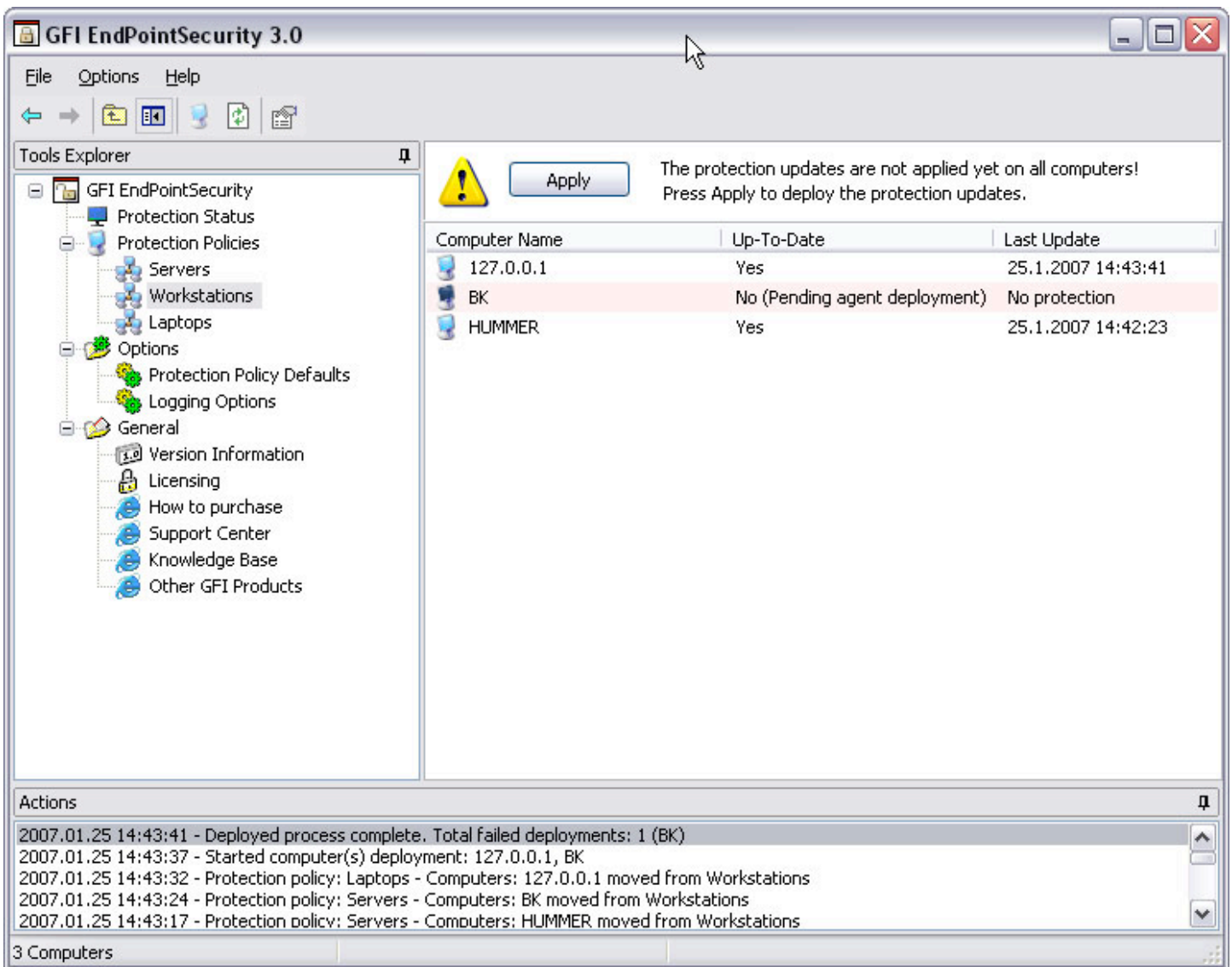
agents and they are now ready to enforce it. For instance: if you denied access to digital cameras, as soon as the user tries to connect it to her computer, the software will deny the request and properly log all the possible information about the event.

The whole process works upon a set of user groups that GFI EndPointSecurity installs by default (there is also an advanced option of setting custom groups):

- GFI\_ESEC\_Device\_ReadOnly and
- GFI\_ESEC\_Device\_FullAccess.

These groups hold information on how the users' computers will react to configured devices.

Bottom line, when the remote user plugs in a device, in our case a digital camera, the agent identifies if the device is being monitored and then checks the Active Directory or Local Users and Groups to verify if the user is a member of the privileged group. The actions are directly connected with groups.



Listing of computers added to the Workgroups protection policy.

Users can be added to the group via the product's user console or Active Directory/Local Users management console. The structure of the user console is quite spartan so it is a piece of cake to customize specific devices for controlling purposes, as well as adding users to the precise groups.

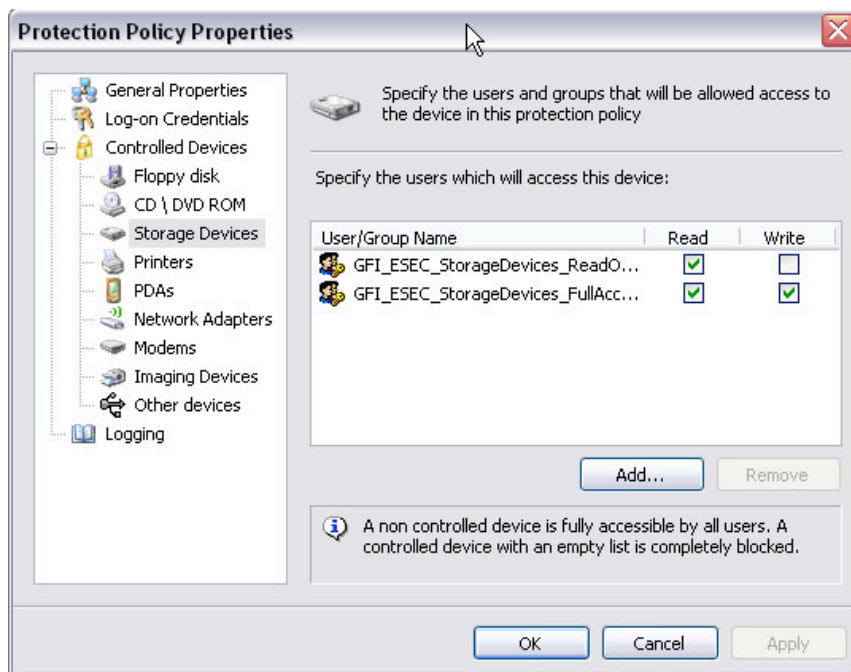
The most important part of the configuration process is setting up the protection policies. By default, GFI EndPointSecurity offers three policies: Servers, Workgroups and Laptops. These are, of course, just samples and it is simple to rename them or create your own.

I would recommend customizing this listing to the maximum, because when you start grouping your computers in these policies you will need to think about optimization. As every designated policy has its own set of rules, you need to plan on whether you will

group users by computer types (i.e. notebooks and desktops), or it will be better to control them when they are described by departments (marketing, tech support etc).

Besides being a mechanism of control, GFI's product offers some versatile logging possibilities. When an action is triggered, the agent logs to a local event log, as well as to the SQL Server if the administrator enabled this option. The SQL logs can be read and exported in a number of ways, and the event logs can be inspected with different tools, the easiest of course being the Event Viewer.

The logging is working just fine, even in the occasion when a client computer is a notebook and it periodically gets disconnected from the network. All the device access protection procedures will still be active and all the events will be saved into a buffer.

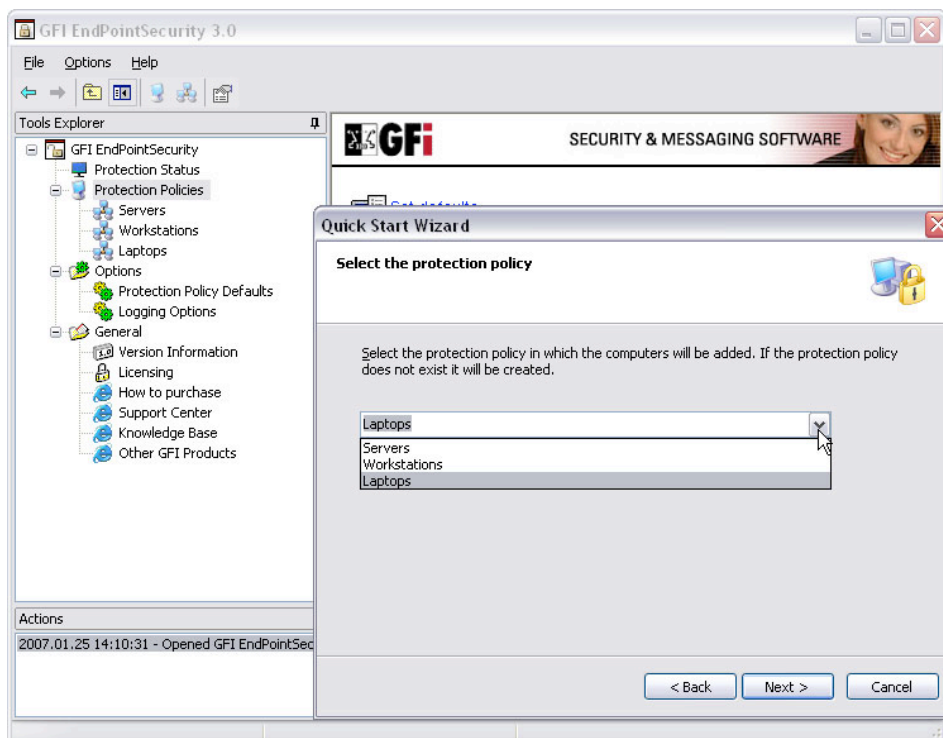


Protection policy properties with default users.

As soon as the computer connects to its "mother" network, the event data will be collected and stored. This is a nice touch, as it makes the integrity of a centralized logging place intact.

I'll mention one more thing - in mid 2006, GFI released a ReportPack add-on, a full-fledged reporting companion to GFI EndPointSecurity. It allows administrators to generate

graphical IT-level, technical and management reports based on the portable devices usage events recorded by GFI EndPointSecurity. It also enables administrators to pull together "Top 20" reports that cover the 20 users, machines, devices and applications which peaked connection activity. This addition is free for all registered users of GFI EndPointSecurity.



Default protection policies.



More than two years ago, GFI had seen a need for security solution that would take care of portable devices. Released under their LanGuard product line, Portable Storage Control started with blocking unwanted USB connections. In the mean time, the software was totally re-done and re-branded as GFI EndPointSecurity.

I tested this software in a couple of scenarios (mainly networks with Microsoft Windows XP Professional SP1 and SP2 computers) and it

worked like a charm. As you can see from this article, the software concept is pretty straight forward and every decent Windows administrator shouldn't have any problems in deploying the solution.

Bottom line is that the software proved to be fast, stable and quite efficient. If you need to manage user access to the external devices from the computers in your network, you should definitely check GFI Endpoint.

Tim Wilson is a long time system and network administrator and currently is employed by a Information Security consultancy based in California. Besides enjoying his computer hours, Tim enjoys travelling with his family and playing clarinet for a local jazz band.

**Promote your products or services for as low as \$75  
in the upcoming "product showcase" addition to  
(IN)SECURE Magazine.**

**For more information contact us at  
[marketplace@insecuremag.com](mailto:marketplace@insecuremag.com)**

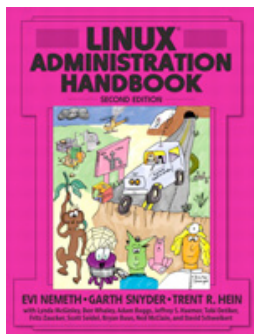


## Latest additions to our bookshelf

### **Linux Administration Handbook, 2nd Edition**

by Evi Nemeth, Garth Snyder, Trent R. Hein

Prentice Hall, ISBN: 0131480049

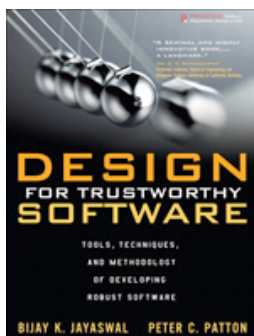


The first edition of the this title, released about five years ago was one of the definitive resources for every Linux system. Now, the authors have systematically updated this classic guide to address today's most important Linux distributions and most powerful new administrative tools. Here you can find best practices for storage management, network design and administration, web hosting, software configuration management, performance analysis and much more. System administrators should especially appreciate the up-to-date discussions of such difficult topics such as DNS, LDAP, security, and the management of IT service organizations.

### **Design for Trustworthy Software: Tools, Techniques, and Methodology of Developing Robust Software**

by Bijay K. Jayaswal, Peter C. Patton.

Prentice Hall, ISBN: 0131872508



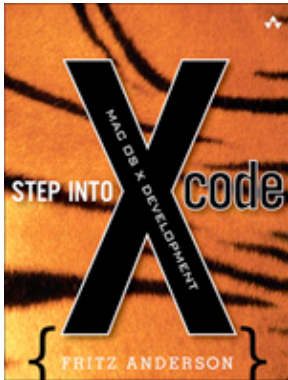
This book presents an integrated technology, Design for Trustworthy Software (DFTS), to address software quality issues upstream such that the goal of software quality becomes that of preventing bugs in implementation rather than finding and eliminating them during and after implementation.

“Design for Trustworthy Software” can be used to impart organization-wide learning including training for DFTS Black Belts and Master Black Belts. It helps you gain rapid mastery, so you can deploy DFTS Technology quickly and successfully.

## Step into Xcode: Mac OS X Development

by Fritz Anderson

Addison Wesley Professional, ISBN: 0321334221



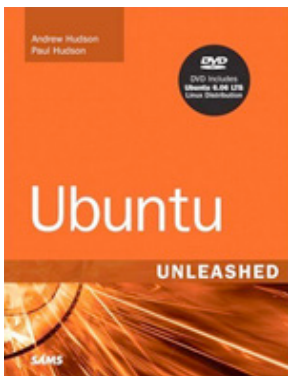
Xcode is a powerful development suite that Apple uses to build applications ranging from Safari to iTunes. But because Xcode is complex and subtle, even experienced Mac programmers rarely take full advantage of it. Mac developer Fritz Anderson has written the definitive introduction and guide to using Xcode to build applications with any Macintosh technology or language.

The book should help you master Xcode's powerful text editor, industry-standard gcc compiler, graphical interactive debugger, mature UI layout and object linkage editor, and exceptional optimization tools. One step at a time, you'll develop a command-line utility, then use Xcode tools to evolve it into a full-fledged Cocoa application.

## Ubuntu Unleashed

by Andrew Hudson, Paul Hudson

Sams, ISBN: 0672329093



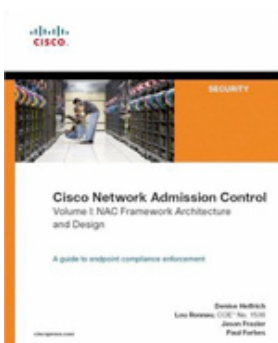
The book aims to provide the best and latest information that intermediate to advanced Linux users need to know about installation, configuration, system administration, server operations, and of course security. Written by renowned open source authors, it includes detailed information on hot topics such as wireless networks, and programming in PHP, Perl and others. It thoroughly covers all of Ubuntu's software packages, including up-to-date material on new applications, Web development, peripherals, and programming languages.

It also includes updated discussion of the architecture of the Linux kernel 2.6, USB, KDE, GNOME, Broadband access issues, routing, gateways, firewalls, disk tuning, security, and more.


## Cisco Network Admission Control, Volume I: NAC Framework Architecture and Design

by Denise Helfrich, Lou Ronnau, Jason Frazier, Paul Forbes

Cisco Press, ISBN: 158705-2415



Cisco Network Admission Control, Volume I, describes the NAC architecture and provides an in-depth technical description for each of the solution components. This book also provides design guidelines for enforcing network admission policies and describes how to handle NAC agentless hosts. As a technical primer, this book introduces you to the NAC Framework solution components and addresses the architecture behind NAC and the protocols that it follows so you can gain a complete understanding of its operation. Sample worksheets help you gather and organize requirements for designing a NAC solution.



## Interview with Edward Gibson, Chief Security Advisor at Microsoft UK

By Mirko Zorz

**Mr. Gibson is the Chief Security Advisor for Microsoft in the UK. This role comes on the heels of his retirement from a 20-year career as a Supervisory Special Agent with the Federal Bureau of Investigation. During this period, Gibson was a recognized expert in investigating complex, international money laundering schemes, asset identification and confiscation, and intellectual property theft. From early 2000 - mid 2005, Mr. Gibson was assigned to the FBI's Legal Attache office, US Embassy London, as an Assistant Legal Attaché. There, he was responsible for all FBI cyber, hi-tech, cyber-terrorism, and infrastructure investigations in the UK. His leadership resulted in the creation of a model cyber program adopted by all Legal Attache offices around the world.**

**What has been your biggest challenge in the role of Chief Security Advisor for Microsoft? Has your background expertise helped shape your role in the company?**

Most people only know of 'criminality' on the Internet through anecdotal reports. Until someone is personally affected by identify theft, social engineering, auction fraud, or other type fraudulent e-commerce activity, it is something for someone else to deal with. This should not be a surprise, as this is generally how people behave in the bricks and mortar world. However, the rules by which we

live in the bricks and mortar world are sometimes largely ineffective in the cyber world. The Internet is global, and criminals are not bound by jurisdiction, political relations, or other restrictions due to anonymity and ability to hide in plain sight.

Yes, my background has been a key driver in shaping my role in the company. I know criminals, how they behave and the tools they use, particularly in internationally complex cyber criminality. As the single point of contact for all UK law enforcement and security services at the US Embassy London in

relation to cyber investigations and laws related thereto, I had many opportunities to work with a variety of agencies in a number of countries. And each success was due to an understanding of the different cultures, laws, and priorities. This understanding was bolstered by having been a lawyer in the US prior to my appointment as a Special Agent, FBI, and qualification as a Solicitor in England / Wales, and the truly exceptional law enforcement and government representatives, without whom success would have been hard fought. With this background, I am better able and proud to represent Microsoft UK in my role as Chief Security Advisor.

**Windows Vista has just been released and Microsoft has already announced the Vista Service Pack 1. Some see this as a sign that Microsoft knowingly released the OS with security problems while others believe it to be a step forward in security awareness and applaud Microsoft for starting work on a collection of patches this early. What's your take on this situation?**

Microsoft's operating systems / platforms, applications, and processes are used by millions of people in nearly every country on this planet. It's software products are used in mission critical devices and processes (in the UK, the NHS is a prime example), defence

industry, manufacturing, finance, and government to name a few. Knowing what I do about the kinds of attacks against its applications, operating systems, and processes, by ruthless organized crime groups and people using every conceivable method to steal, compromise, extort, blackmail, or otherwise make life miserable for their own personal gain, we all can be mighty proud of the extraordinary efforts Microsoft has and continues to put into making all computer users more safe on the Internet. But remember, criminal attacks against systems is an Industry-wide problem, which is why Microsoft is working with industry partners, government, and educational institutions to help ensure understanding of the problems and develop better solutions.

It's important to remember that no software is 100% secure. We're working to keep the number of security vulnerabilities that ship in our products to a minimum. Trustworthy Computing is a long-term initiative and those changes do not happen overnight. We've made progress and our efforts are resulting in significant improvements in the security of our software. We have every confidence that - together with our industry partners - we'll continue to meet the constantly evolving challenge of security to help our customers and the industry become more secure.

## **IT'S IMPORTANT TO REMEMBER THAT NO SOFTWARE IS 100% SECURE.**

**Did Microsoft use a different approach to testing security while developing Windows Vista?**

The release of Windows Vista is the first Microsoft operating system to use the Security Development Lifecycle (SDL) from start to finish and was tested more prior to shipping than any previous version of Windows.

Building on the significant security advances in Windows XP Service Pack 2, Windows Vista includes fundamental architectural changes that will help make customers more secure from evolving threats, including worms, viruses, and malware. These improvements minimize the operating system's

attack surface area, which in turn improves system and application integrity and helps organizations more securely manage and isolate their networks.

Too often software is developed by bolting security technology onto an application and declaring it secure. The SDL was developed to provide a step-by-step process integrating secure development into the entire software lifecycle from start to finish. We have already seen the benefits of this process as it was first used for Windows Server 2003 and resulted in a 56% decrease in the number of security bulletins, compared to Windows Server 2000.

**By having the most deployed OS in the world, Microsoft is always under the microscope and has to tackle a myriad of security challenges. What are the ones that you expect to cause problems in the near future and what strategies does Microsoft use to fight them?**

As I always say, it's about people, process and technology and at Microsoft our security strategy is very much aligned to these three areas. The threat landscape is continually evolving and challenges appear in the form of malware, inappropriate security policies and the regulatory environment. Our security efforts are therefore focussed on the area of partnerships, innovation and prescriptive guidance. Microsoft is working in partnership with Government and industry groups to thwart security threats. So for example, in the UK, we are an active member of the Government backed Get Safe Online program, which aims to educate consumers and businesses on the importance of security.

We are continually developing our products to protect computer users and stay one step

ahead of the cyber criminal. So for example, as I've already mentioned, our Security Development Lifecycle is used to ensure rigorous testing of software code in products such as Windows Vista. In addition, our MSN Hotmail service blocks 3.4 billion spam messages per day.

Finally, at Microsoft, we're committed to providing guidance to help businesses and consumers act and secure their digital lives. In the UK alone, according to recent figures from APACS (the UK payments association), online banking fraud alone cost £22.5m in 2006. Therefore we are deeply engaged in customer education programs such as our partnership with GSOL. In fact, a big part of my role is to liaise between customers and our internal development teams, finding out what the problems are and seeing how they can be resolved. My number one message is that prevention is the best defense! You don't need to wait to protect yourself today. There are numerous resources available (both from Microsoft and across the industry) to help protect against the growing severity of information security threats.

## **WE ARE CONFIDENT THAT VISTA IS THE MOST SECURE AND THOROUGHLY TESTED VERSION OF WINDOWS WE HAVE EVER PRODUCED.**

**When discussing Windows Vista, Microsoft is emphasizing that it is the most secure Windows ever. Do you believe you'll be able to stand behind that in a year or two? What makes you so certain of Vista's security features? After all, we live in a world of constant evolving threats. Does 'more secure' = 'secure'?**

As mentioned previously, whilst no software is 100% secure, we are confident that Vista is the most secure and thoroughly tested version of Windows we have ever produced. Our customers expect and deserve a computing experience that is safe, private and reliable. Trustworthy Computing has fundamentally changed the way we develop and help our customers manage Microsoft software and services. Threats to security and privacy constantly evolve and the holistic nature of Trustworthy Computing highlights Microsoft's commitment to facing this changing land-

scape. Microsoft cannot do this alone, and we will continue to partner and collaborate with industry, government and academia to better protect customers and adapt to evolving security threats.

**In the past, Microsoft's security headaches were coming from full disclosure lists where researchers publicly disclosed vulnerabilities in Microsoft products without reporting them to the company. Today, the threat landscape is changing with 0-day vulnerabilities in Windows Vista being sold to the highest bidder and not reported at all. How does Microsoft deal with this problem?**

Due in part to recent reports of security vulnerabilities in a wide range of software, security is a growing concern for more and more computer users every day.

The industry is responding in part by seeking new opportunities to improve the way that security information is gathered and shared to protect customers while not aiding attackers.

Microsoft is aware of iDefense offering compensation for information regarding security vulnerabilities. Microsoft does not offer compensation for information regarding security vulnerabilities and does not encourage that practice. Our policy is to credit security researchers who report vulnerabilities to us in a responsible manner.

**Since its inception, Microsoft Patch Tuesdays have been successful. Yet, many critical vulnerabilities are announced shortly after the batch of monthly patches. Shouldn't there be more frequent patch releases?**

We investigate each security vulnerability report thoroughly to determine its impact to our customers. In combination with that investigation we also take a look at our engineering processes to help determine how we can best deliver a quality update to our customers within the consistent time frame that our customers have requested, which is currently on a monthly cycle.

There are many factors that impact the length of time between the discovery of a vulnerability and the release of a security update.

Every vulnerability presents its own unique challenges. We've been clear that bulletins can be released out-of-cycle, if necessary, to help protect customers if a level of awareness and malicious activity puts customers at risk in any way. In this case, the level of awareness and malicious activity around a vulnerability may prompt Microsoft to move to a release schedule that would deliver a fix as soon as one could be built and thoroughly tested.

Creating security updates that effectively fix vulnerabilities is an extensive process involving a series of sequential steps. When a potential vulnerability is reported, designated product specific security experts investigate the scope and impact of a threat on the affected product. Once they know the extent and the severity of the vulnerability, they work to develop an update for every supported version affected. Once the update is built, it must be tested with the different operating systems and applications it affects, then localized for many markets and languages across the globe. In some instances, multiple vendors are affected by the same or similar issue, which requires a coordinated release.

## **CREATING SECURITY UPDATES THAT EFFECTIVELY FIX VULNERABILITIES IS AN EXTENSIVE PROCESS INVOLVING A SERIES OF SEQUENTIAL STEPS.**

**Internet Explorer has been hit by a variety of vulnerabilities in the past and many patches have been released. Now that IE 7 out, does Microsoft plan a better security strategy for the most used browser?**

Security is an industry wide issue and although there is no one solution, our approach to security spans across both technological and social aspects.

In technology, we're focused on designing software that is resilient in the presence of malicious code threats (such as worms and

viruses) and that isolate the potential impact of contamination.

In the interest of helping to better protect our customers, we delivered Windows XP SP2 in 2004, which included a major security upgrade to Internet Explorer. Building on that release, Internet Explorer 7 has been redesigned and includes new security features to help protect end users against spyware and phishing attacks. A variety of new security enhancements have been added to provide end users with a host of new capabilities to make everyday tasks even easier, including dynamic security protection to help keep them safe online.



## Top 10 spyware of 2006

By Panda Software

**This is the PandaLabs list of the spyware most frequently detected by Panda ActiveScan in 2006.**

The top ranking spyware is Gator. This adware offers free use of an application if users agree to view a series of pop-up messages downloaded by Gator. Some versions of this spyware replace banners on web pages visited with those created by the malicious code itself.

Second and third place in the Top Ten are occupied by Wupd and Ncase respectively. Both offer free use of an application in exchange for displaying advertising messages. They also monitor users' Internet movements and gather data about habits and preferences. This information is then used to personalize the advertising displayed. Additionally, Ncase changes the Internet Explorer home page, as well as the default search options.

The adware CWS is in fourth place. This can be installed without users' consent or without them being fully aware of the functionality of the tool. Emediacodec, in fifth place in the Top Ten, has similar characteristics. It uses a series of techniques in order to prevent it being detected by antivirus companies. It can even terminate its own execution if it detects that it is being executed in a virtual machine environment, such as VMWare.

In sixth place in the table is Lop, a type of adware with many variants. In most cases, this malicious code installs a toolbar with search features in Internet Explorer. It also displays numerous advertising pop-ups. Winantivirus, in seventh place, is categorized as a PUP, (Potentially Unwanted Program). It is downloaded onto computers by other malicious code, such as, Downloader.LHW and exploits application vulnerabilities in order to spread. Winantivirus is also capable of damaging users' systems.

CWS.Searchpmeup is in eighth place in the list. This malicious program changes the Internet Explorer home page and the default search options. The web page that it sets as the home page uses several exploits to download malware onto computers. Next in the ranking is Winfixer2005, a PUP that searches the computer for supposed 'errors' and then demands that users buy the program in order to repair them. Finally, in tenth place comes New.net, a spy program that adds a toolbar to Internet Explorer and collects information about the user, including Internet pages visited, etc.

The information gathered by PandaLabs about spyware in 2006 highlights the prevalence -seven of the Top Ten- of adware.



Position	Spyware
1	Adware/Gator
2	Adware/WUpd
3	Adware/nCase
4	Adware/CWS
5	Adware/emediacodec
6	Adware/Lop
7	Application/Winantivirus2006
8	Adware/CWS.Searchmeup
9	Application/Winfixer2005
10	Spyware/New.net

This type of malware has grown continuously throughout the year and is expected to continue doing so in 2007. Similarly, in 2006 there has been an increase in rootkits and other malware that use similar techniques. A rootkit is a tool used to hide the processes of malicious codes, making them harder to detect.

Another significant aspect of the last year has been the appearance of a new category of malware. Rogue antispyware claims to detect spyware or to repair errors. This increasingly prevalent malware detects flaws or malicious code on computers but then demands that users pay for a registered version of the program if they want to delete these threats. WinAntivirus2006, in seventh place in the Top Ten, is a good example of this new category. Some of them, such as SpySheriff, 23rd in

the ranking, not only detect real errors or attacks but also claim to have detected malware which actually does not exist. Winfixer2005, in ninth place, is another example of malicious code that promises to repair non-existent errors.

False codecs are variants of this type of malware. EmediaCodec, in fifth place in the Top Ten, is a good example of this type of malicious code. The way this malware operates is quite simple. While the user is viewing the Internet, they are offered certain videos, normally pornographic. In order to see them, they have to install a false codec which downloads adware. Normally these are not real codecs, but passwords that register in the system and have to be installed in order to see the videos.



# The spam problem and open source filtering solutions

By Dinko Korunic



**Let us face it, modern e-mail communication relying on SMTP is fundamentally broken - there is no sender authentication. There are lot of countermeasures in form of filtering and add-on authentication, but neither of them are proved to be 100% successful (that is 100% hit ratio with 0% of false positives). Spammers always find new ways of confusing filters with random noise, bad grammar, hidden HTML code, padding, bitmap-rendered messages etc. World is becoming an overloaded and unusable mailbox of spam. I will nevertheless try to cover some of the spam problems and possible solutions, but bare in mind that all of these are just no more than a temporary fix.**

Product spam, financial spam, frauds, scams, phishing, health spam, Internet spam, adult spam, political spam, you-name-it spam. Despite Bill Gates' brave promise in 2004 ("Two years from now, spam will be solved") e-mail spam has significantly increased worldwide in the last two years in both volume and size, making over 70% of total e-mail traffic. According to the First MAAWG Global Spam Report ([tinyurl.com/y8o9y9](http://tinyurl.com/y8o9y9)) from Q1 2006, around 80% of incoming e-mail was detected as abusive. A bit later in Q3 2006 various Internet service providers in the world have reported an alarming increase of unsolicited e-mail in a very short period due to the range of new spamming techniques involved. At the end of 2006 an estimated number of the

world's total spam is around 85 billion messages per day (obviously this number is rather approximate) - and it is exponentially increasing. We all know how much it is going to cost (quick spam calculator: [tinyurl.com/y84je6](http://tinyurl.com/y84je6)).

Spammers have undoubtedly adapted and evolved: up to now they used a single IP setup for delivering their unwanted e-mail, usually hopping from one dialup to another. They have used open proxies, open mail relays and other similar easy-to-track sources. Unfortunately, it has changed - current spamming methods now include huge networks (called botnets) of zombie-computers used for distributed spam delivery and Denial of Service attacks.

Various new viruses and worms are targeting user computers, making them eventually into huge spam clusters. Not only Microsoft Windows PCs are hacked, more and more Unix and Linux servers are affected too. And it is not for the fame and the glory, but to enable crackers to install and run scripts for the remote controlled spamming. In the meantime, nobody knows how many spambots are currently harvesting the Web in search of new e-mail addresses, their new victims. There is nothing sophisticated in their attacks, only brute force and numbers. Spammers earn a living by making and delivering spam and they do it darn well.

### Reality check, 123

Due to the troublesome nature of the Internet today, the spammers and the script kiddies can easily put an anti-spam provider out of a job by simply DDoSing them to death (and doing a lot of collateral damage) - and exactly it happened to Blue Security ([tinyurl.com/rl2d7](http://tinyurl.com/rl2d7)) with their successful but quite controversial Blue Frog service. A person known as PharmaMaster took their cam-

paign as open war declaration and wiped them off from the face of the Internet within a single day. Lessons have been learned: the spammers are to be taken seriously and it seems they cannot be dealt by a single uniform blow nor with a single anti-spam provider.

What can we do about spam? There are numerous commercial solutions against unsolicited e-mail (SurfControl, Websense, Brightmail, IronPort, etc.) and some of them are rather expensive. Depending on the available budget, requirements and resources at hand, an Open Source solution could be substantially cheaper and possibly equally effective as the commercial counterpart. There is a whole range of readily available Open Source solutions for each of the popular anti-spam techniques for e-mail receivers. Some of them are in the core of the even most advanced commercial solutions. As most of the readers probably know, anti-spam solutions are most effective when different methods are combined together, forming several layers of analysis and filtering. Let us name a few of the most popular...

## VARIOUS NEW VIRUSES AND WORMS ARE TARGETING USER COMPUTERS, MAKING THEM EVENTUALLY INTO HUGE SPAM CLUSTERS.

### Blacklisting

DNS blacklisting is a simple and cheap way of filtering the remote MTA (Mail Transfer Agent) peers. For every remote peer the SMTP service will reverse its IP and check the forward ("A") record in the BL domain of DNSBL system. The advantage of the method is in its low processing overhead: checking is usually done in the initial SMTP session and unsolicited e-mail never hits the incoming queue. Due to the spam-zombie attacks coming from the hundreds of thousands of fresh IP address every day, this method is today significantly less effective today than it used to be and no more than 40% of total inbound spam can be filtered using this method. There are a lot of free DNSBL services in world, but it is probably best to use well known and reliable providers (and there are even subscription-based DNSBL services) which do not enlist half of the Internet overnight. Some of most widely

recognized are Spamhaus and SpamCop, for instance. Almost all FLOSS (Free/Libre/Open-Source Software) SMTP daemons have full RBL support and so does Postfix, Exim, Sendmail, etc. For the SMTP services which do not support DNSBL out of the box it is possible to use DNSBL tests in SpamAssassin, but that usually means no session-time checking. Another variant which Sfilter uses is to store a several DNSBL exports in the form of local blacklists for faster processing. Of course, such a database needs to be synchronized manually from time to time, preferably on a daily basis.

### Greylisting

The greylisting method ([tinyurl.com/y8y4oe](http://tinyurl.com/y8y4oe)) is a recent but fairly popular method which slightly delays an e-mail delivery from any unknown SMTP peer. A server with the greylisting enabled tracks the triplets of the

information for every e-mail received: the IP address of every MTA peer, the envelope sender address and the envelope recipient address. When a new e-mail has been received, the triplet gets extracted and compared with a local greylisting database. For every yet unseen triplet the MTA will reject the remote peer with a temporary SMTP failure error and log it into a local database. According to the SMTP RFC, every legitimate SMTP peer should try to reconnect after a while and try to redeliver the failed messages. This method usually requires minimum time to configure and has rather low resource requirements. As a side benefit it rate-limits the incoming SMTP flow from the unknown sources, lowering the cumulative load on the SMTP server.

There are still some mis-configured SMTP servers which actually do not retry the

delivery since they interpret the temporary SMTP failure as a permanent error. Secondly, the impact of the initial greylisting of all new e-mail is substantial for an any company that treats e-mail communication as the realtime-like service, since all of the initial e-mail correspondence will be delayed at least 300 seconds or more, depending on the SMTP retry configuration of the remote MTA peers. Finally, the greylisting does not do any good to the big SMTP providers which have large pools of mail exchangers (ie. more than /24).

The problems can be fixed by whitelisting manually each and every of domains or network blocks affected. Regarding the software which does the greylisting almost every Open Source MTA has several greylisting implementations available: Emserver, Postgrey, Milter-greylis, etc.

SMTP callback verification or the sender verify callout is a simple way of checking whether the sender address found in the envelope is a really deliverable address or not.

### Sender verify callout

SMTP callback verification or the sender verify callout is a simple way of checking whether the sender address found in the envelope is a really deliverable address or not. Unfortunately, verification probes are usually blocked by the remote ISP if they happen too often. Further, a remote MTA does not have to reject the unknown destinations (ie. Qmail MTA usually responds with "252 send some mail, i'll try my best"). To conclude: it is best to do verification per known spammer source domains which can be easily extracted from results of the other methods (such as the content analysis). The sender verification is supported in most FLOSS MTA: Postfix, Exim, Sendmail (via milter plugin), etc.

### Content analysis

The content-based filtering is probably the core of most anti-spam filters available. It

usually consists of several subtypes, so let us state a few. Static filtering is a type which triggers e-mail rejection on special patterns ("bad" words and phrases, regular expressions, blacklisted URI, "evil" numbers and similar) typically found in the e-mail headers or a body of an e-mail itself. False positives are quite possible with this method, so this type is best used in conjunction with policy-based systems (often named as heuristic filters) such as SpamAssassin and Policyd-weight. Such filters use the weighted results of several tests, typically hundreds of, to calculate a total score and decide if the e-mail is a spam or a ham. In this way, a failure in a single test does not necessarily decide the fate of an e-mail. At least several tests have to indicate a found spam content to accumulate the spam score enough for an e-mail to be flagged as a spam, so this results in a more reliable system. Of course, weighted/scoring type of a filter can contain all of the other filter types for its scoring methods.

The next type of the content analysis is the statistical filtering which mostly uses the naive Bayesian classifier for the frequency analysis of word occurrences in an e-mail. Such filtering, depending on an implementation, requires the initial training on an already pre-sorted content and some retraining (albeit in much smaller scale) later on to obtain a maximum efficiency. The Bayesian filtering is surprisingly efficient and robust in all real life examples. It is implemented in the very popular SpamAssassin and DSPAM solutions, as well as Bogofilter, SpamBayes, POPFile and even in user e-mail clients such as Mozilla Thunderbird. Some implementations such as SpamAssassin use an output of other spam filtering methods for a retraining which gradually improves the hit/miss ratio. Most of the implementations (DSPAM, SpamAssassin) have a Web interface which allows a per-user view of the quarantined e-mail as well as the per e-mail retraining. It improves the quality of either the global dictionary (a database of learned tokens) or the individual per user dictionaries. DSPAM, for an instance, supports a whole range of additional features such as: combining of extracted tokens together to obtain a better accuracy, tunable classifiers, the initial training sedation, the automatic whitelisting, etc.

Another popular solution is CRM114 which is a superior classification system featuring 6 different classifiers. It uses Sparse Binary Polynomial Hashing with Bayesian Chain Rule evaluation with full Bayesian matching and Markov weighting. CRM114 is both the classifier and a language. DSPAM and CRM114 are currently the two most popular and most advanced solutions in this field, and they are easily plugged into most SMTP services.

Note that plain Bayesian filters can be fooled with quite common Bayesian White Noise attacks which usually look like random nonsensical words (also known as a hashbuster) in a form of a simple poem. Such words are randomly chosen by a spammer mailer software to reflect a personal e-mail correspondence and therefore thwart the classifier. Most of the modern content analysis filters do detect such attacks - and so does SpamAssassin and DSPAM.

## Checksum-based filtering

A small but significant amount of unsolicited e-mail is the same for every recipient. A checksum-based filter strips all usual varying parts of an e-mail and calculates a checksum from the leftovers. Such a checksum is then compared to a collaborative or distributed database of the all known spam checksums. Unfortunately, spammers usually insert various poisoning content (already mentioned hashbusters) unique to an every e-mail. It causes the checksums to change and an e-mail is not recognized as known spam any more. Two of the most popular services for this type are Distributed Checksum Clearinghouse and Vipul's Razor which both have their own software and they are both supported in third-party spam-filtering software such as SpamAssassin.

## E-mail Authentication

Finally, we are left with several methods of the authentication that basically try to ensure the identity of a remote sender via some kind of an automated process. The identification makes it possible to reject all of the e-mail from the known spam sources, to negatively score or even to deny an e-mail with the identified sender forgeries and to whitelist an e-mail which is valid and comes from the known reputable domains. This method should minimize the possibility of the false positives because a valid e-mail should get higher positive scores (used for the policy filter) right from the start or even completely bypass the spam filters - which can be made more sensitive in return. There are several similar authentication mechanisms available: SPF (Sender Policy Framework), CSV (Certified Server Validation), SenderID and DomainKeys. They are mostly available as third-party plugins for most popular OSS MTA, usually in the form of Perl scripts available at CPAN. Unfortunately, neither of them is a solution recognized widely enough to be used in an every SMTP service in the world.

DomainKeys and enhanced DKIM (DomainKeys Identified Mail) protocol use a digital signature to authenticate the domain name of sender as well as content of a message. By using a sender domain name and the received headers, a receiving MTA can obtain

the public key of a such domain through simple DNS queries and validate the signature of the received message. A success proves that the e-mail has not been tampered with as well as that the sender domain has not been forged.

SPF comes in form of the DNS TXT entries in each SPF-enabled Internet domain. These records can be used to authorize any e-mail in transit from a such domain. SPF records publish the policy of how to handle the e-mail forgeries or the successful validation as well as the list of possible e-mail originating addresses. If none of those match the sender address in received e-mail, the e-mail is probably forged and the receiver can decide on the future of such e-mail depending on SPF qualifiers (SOFTFAIL, FAIL, NEUTRAL,

PASS) from a SPF policy. The problem is that SPF breaks e-mail forwarding to the other valid e-mail accounts if the domain administrator decides to use SPF FAIL policy (hard fail), although in the future SRS (Sender Rewriting Scheme) could eventually help it.

SenderID is a crossover between SPF and Caller ID with some serious standardization issues and does not work well with mailing lists (necessary Sender or Resent-Sender headers). CSV is about verifying the SMTP HELO identity of the remote MTA by using simple DNS queries to check if the domain in question is permitted to have a remote IP from the current SMTP session and if it has got a good reputation in a reputable Accreditation Service.

Dinko Korunic is currently employed as a Senior Unix/Linux Security Specialist at InfoMAR ([www.infomar.hr](http://www.infomar.hr)). He has previously worked with Croatian Academic and Research Network (CARNet) and University Computing Centre (SRCE) as Unix forensics specialist and a technical advisor. For the last decade, he has written and held numerous lectures on advanced Linux and Unix topics. He has been a Unix (AIX, Irix, SunOS/Solaris, Linux, OSF1/Tru64, Ultrix, \*BSD) system administrator and a Unix system programmer. In his spare time he writes Linux-related articles for local IT-specialist magazine Mrez@. Dinko can be reached at [dinko.korunic@infomar.hr](mailto:dinko.korunic@infomar.hr).

**LAVASOFT**  
*protect your privacy*


***The leading antispyware developer  
now delivers the best personal firewall protection***



**LAVASOFT PERSONAL FIREWALL**  
*Superior security shield against hackers, worms and Trojans*

[www.lavasoft.com](http://www.lavasoft.com)

# Software spotlight



## **WINDOWS - Cain & Abel**

<http://www.net-security.org/software.php?id=110>

Cain & Abel is a password recovery tool for Microsoft operating systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using dictionary and brute-force attacks, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols.

## **LINUX - Nagios**

<http://www.net-security.org/software.php?id=279>

Nagios is a host and service monitor designed to inform you of network problems before your clients, end-users or managers do.

## **MAC OS X - Pastor**

<http://www.net-security.org/software.php?id=617>

Pastor is a tool to store all your passwords, website logins, program serial numbers, etc. RC4-encrypted and password-protected.

## **POCKET PC - SignWise Pro**

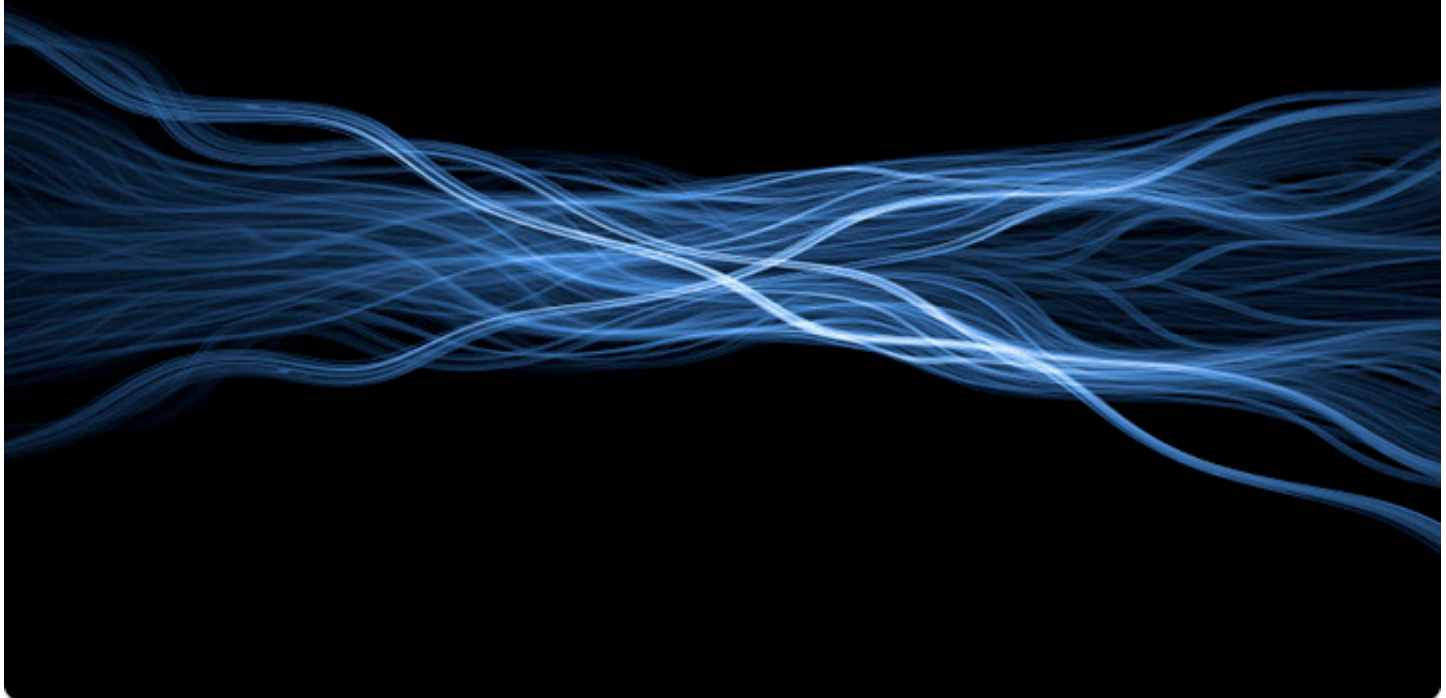
<http://www.net-security.org/software.php?id=543>

SignWise use personal hand-written signature to authenticate. Signatures are much more secure than passwords or PINs in that they cannot be lost, forgotten, or shoulder-surfed, and are difficult to forge.

If you want your software title included in the HNS Software Database e-mail us at [software@net-security.org](mailto:software@net-security.org)

# Office 2007: new format and new protection/security policy

By Andrey Malyshev



**This article analyzes the main changes in Office 2007 that concern documents and users' private data protection.**

## **New file format**

The format change does strike the eye. For instance, Word 2007 files have the extension "DOCX" instead of traditional "DOC". The most files in the previous Office versions were OLE-containers consisting of several streams with binary data.

At the end of 90s binary formats of Word and Excel were documented and available for MSDN subscribers. However, Microsoft has closed these formats after a new release of Office 2000 and up to Office 2003 they were unavailable even for Microsoft partners. It prevented all developers from writing their own software applications compatible with Office documents.

However, after Office 2007 had been released the situation changed drastically. A new file format, Office Open XML, is completely open and documented. Documentation format is available and everybody can download it from the Microsoft website. Microsoft followed the path of a well-known project OpenOffice which file format is also open and XML is

used for data storage. Apart from binary files, XML file format has a lot of auxiliary information that is why all XML files are packed by ZIP archiver.

Unfortunately, hyperlinks to XML-schemes are not available yet. Let us hope that Microsoft will fix it soon. In the example the file format is quite readable and understandable. At least we can see here the language, the text itself, and page parameters. In documentation you can find descriptions of other tags.

Office 2007 is compatible with its previous versions. If you try to open a new format file in Office 2003 you will be prompted to download a converter from Microsoft web-site and having in-stalled it on you computer you can easily work with new format files. Additionally, you have an option to save files in a new format.

## **Office 2007 files protection: Word, Excel, PowerPoint**

Whereas Office regular file format is simple and clear, the format of protected files is not that easy.



Here you can see a file “document.xml” which is “the body” of Word document:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<w:document xmlns:ve="http://schemas.openxmlformats.org/markup-compatibility/2006"
xmlns:o="urn:schemas-microsoft-com:office:office"
xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships"
xmlns:m="http://schemas.openxmlformats.org/officeDocument/2006/math"
xmlns:v="urn:schemas-microsoft-com:vml"
xmlns:wp="http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing"
xmlns:w10="urn:schemas-microsoft-com:office:word"
xmlns:w="http://schemas.openxmlformats.org/wordprocessingml/2006/main"
xmlns:wne="http://schemas.microsoft.com/office/word/2006/wordml">
<w:body>
<w:p w:rsidR="00021ED4" w:rsidRPr="00FC4BE5" w:rsidRDefault="00FC4BE5">
<w:pPr>
<w:rPr>
  <w:lang w:val="en-US" />
</w:rPr>
</w:pPr>
<w:r>
<w:rPr>
  <w:lang w:val="en-US" />
</w:rPr>
<w:t>Test Word file...</w:t>
</w:r>
</w:p>
<w:sectPr w:rsidR="00021ED4" w:rsidRPr="00FC4BE5" w:rsidSect="00021ED4">
  <w:pgSz w:w="11906" w:h="16838" />
  <w:pgMar w:top="1134" w:right="850" w:bottom="1134" w:left="1701" w:header="708"
w:footer="708" w:gutter="0" />
  <w:cols w:space="708" />
  <w:docGrid w:linePitch="360" />
</w:sectPr>
</w:body>
</w:document>
```

A file protected with a password is an OLE-container which includes encryption information, encrypted stream itself and some auxiliary information. The encryption information block is the same as in Office XP/2003. It includes the name of cryptoprovider, hash and encryption algorithms, key length, as well as data for password verification and document decryption. Though previous Office versions allowed change cryptoprovider and key length, Office 2007 has fixed encryption parameters, as follows: AES encryption with 128 bit key, SHA-1 hashing. The cryptoprovider «Microsoft Enhanced RSA and AES Cryptographic Provider» supports encryption and hashing functions.

However, in comparison with Office 2003 the new version has a new algorithm of converting passwords into keys. In previous Office versions each password was hashed with an accidental byte set that was unique for every document (salt). This operation needed only two SHA-1 iterations and was performed very

quickly. Now this operation needs 50000 SHA-1 sequential iterations. You would never notice it when opening a file because the whole process requires less than a second. However, when we start password search, the speed drops significantly. Initially estimated the speed will be approximately 500 passwords per second even on such cutting-edge processors as Intel Core 2 Duo. Thus, using one computer it is possible to find 4-5 letter passwords. There are considerable changes in the verification algorithm of “read-only” password, document protection password, book and sheet password in Excel. Previously the 16 bit hash was stored in the document. Thus, it was possible to reverse it into any suitable password. Now the hashing algorithm is determined by record in XML-file where the number of hash iterations is defined as well.

On the following page you can see that 50000 SHA-1 hash iterations and the password recovery process will take very long time.

An example of “read-only” password record in Word 2007:

```
<w:writeProtection w:cryptProviderType="rsaFull" w:cryptAlgorithmClass="hash"
w:cryptAlgorithmType="typeAny" w:cryptAlgorithmSid="4" w:cryptSpinCount="50000"
w:hash="L419ICUXKWKS4zJGA1QoY80b6ds=" w:salt="gmd47MvIcN4OwJ5dPxZL6Q==" />
```

However, we still can change or delete this password. We can either calculate the new password hash, or simply delete this tag from XML-file. Document protection passwords are stored in the same way, as well as passwords for Excel books and sheets.

### Other Microsoft Office applications

Microsoft Access security system has undergone some radical modifications. Earlier a “file opening” password was stored in the file header and could be easily extracted. Now in Access 2007 encryption goes in the same way as in Word/Excel. So it is quite problematic to retrieve a password at once. Recovering password by “brute-force” attack will take long time. The user- and group-level protection has been removed from Access from version 2007. PST-file security in Microsoft Outlook remained the same. 32-bit password hash (CRC32) is stored in the file and the password can be easily recovered.

### Office 2007 password security and password recovery strategies

First of all I would like to point out that Office documents security is considerably enhanced

in its new version. It took Microsoft 10 years (from the moment when Office 97 was released) to create a good data protection system. “File open” passwords are really strong and you will need a long time to retrieve them. Nevertheless, you still should have strong passwords. Unfortunately, the human factor has always been and will be the weakest point in any security. Even strong security system in Office 2007 will hardly help you, if your password is “John”, “love” or “sex”. A password like that will be instantly retrieved through the dictionary attack.

One computer is definitely not enough to recover strong passwords for Office 2007. However, there are applications that can unite any number computers into a cluster in order to search passwords. 1000 computers are able to maintain the speed at 500,000 passwords per second. So, we can recover relatively strong passwords provided all corporate computers are joined together into a cluster. But first and foremost one should carry out dictionary attack. A strong security policy is meant only for “file opening” passwords. All other passwords are still easy to retrieve, change, or reset.

Andrey Malyshev is the CTO of ElcomSoft ([www.elcomsoft.com](http://www.elcomsoft.com)). ElcomSoft's award-winning password file protection retrieval software uses powerful algorithms, which are constantly under development.

## The art of information security awareness



A smart way to reach total security.



InfoSecurityLab

[www.infosecuritylab.com](http://www.infosecuritylab.com)

# Wardriving in Paris

By Alexander Gostev



**We regularly conduct research into Wi-Fi networks and protocols in order to gain a picture of the current state of affairs and to highlight current security issues. We focus on Wi-Fi access points and mobile devices which support Bluetooth. This latest piece of research was conducted in Paris, partly in the city itself, and partly at InfoSecurity 2006, which was held in the French capital at the end of November 2006.**

It was very interesting to compare the data collected with similar data from InfoSecurity which was held in London in spring of this year. It was also instructive to compare data on the security of Wi-Fi networks in the business districts of these two world capitals.

As part of this research, we also planned to collect data about Bluetooth enabled mobile devices at InfoSecurity itself, in the Paris Metro, and on the streets of the city. Until now, we haven't managed to catch a single worm for mobiles devices (Cabir or Comwar) in a major city, but we were hopeful about our chances in France - after all, it was the birth-place of Cabir, the first mobile worm.

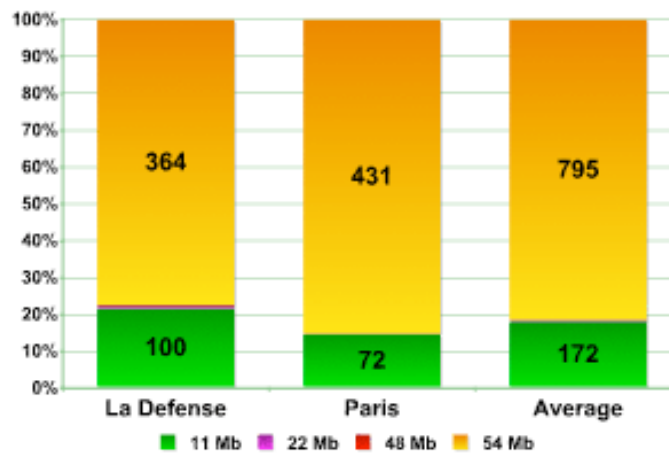
## Wi-Fi networks

We conducted our research between the 22nd and 25th of November 2006. We investigated

La Defense, the business district of Paris, where InfoSecurity was being held, and other locations in Paris. We collected data on approximately 1000 access points. We did not attempt to intercept or decrypt any data transmitted via wireless networks. We detected more than 400 Wi-Fi access points at La Defense/ InfoSecurity, and more than 500 in other regions of Paris. This was the largest number of access points which we've ever detected. London, where we conducted similar research in April, comes in second place. However, we weren't able to collect separate data for InfoSecurity, as the trade fair was being conducted within the Parisian business district itself.

## Transmission speed

As the graphs show, the data which we collected in two different locations is practically



identical. Networks which transmit data at a speed of 54MB are the most common, with the figure varying between 77% (La Defense) to more than 85% (Paris), giving an average of almost 82%. At CeBIT 2006 these networks comprised a little over half (51%) whereas the analogous figures for China and London were a mere 36% and 68% respectively.

This clearly indicates that there is far more networking equipment utilizing newer versions of 802.11 used in Paris than in London. It's difficult to believe that this difference of more than 15% is caused simply by the rapid evolution of Parisian networks in the six months since we published our figures from London.

The second most common network speed is 11MB, with between 14% and 21% of all networks transmitting at this speed, and an average figure of 17.70%. More than 58% of all networks in China transmitted at this speed, with 47% at CeBIT and 28.5% in London.

The number of networks transmitting data at speeds between 22MB and 48MB did not exceed 1% in any area of Paris. This was significantly less than the number detected in

China, Germany, and London, where they comprised up to 6% of the total).

We can therefore conclude that Wi-Fi networks are more evolved in Paris in comparison to networks in the other cities where we have conducted research. The most surprising is the significant difference between the Parisian data and the data from London, a city we had previously considered to be setting something of a benchmark.

### Network equipment manufacturers

The data we collected on network equipment manufacturers in Paris differed significantly from data we collected in other locations. We have therefore decided to analyze each data set individually.

In total, equipment from 28 different manufacturers was detected.

At La Defense, equipment from 19 different manufacturers was detected. Five manufacturers were found to be the most widespread, and equipment from these sources was deployed in more than 12% of networks detected in the business region of Paris.

Manufacturers	Percentage
Symbol	2,99%
Trapeze	2,99%
Airespace	2,14%
Cisco	2,14%
Aruba	1,92%

Equipment produced by the other 14 manufacturers was used in less than 8% of all networks. Unfortunately, it was impossible to establish the manufacturer in more than 80% of cases (Fake, unknown, user defined). This figure is far higher than that for CeBIT (66%) and London (61%).

Equipment from 21 manufacturers were detected in networks other regions of Paris. Of these, the equipment of 5 manufacturers was the most common, and used in more than 10% of the networks detected.

Manufacturers	Percentage
Senao	4,17%
Delta (Netgear)	2,18%
Gemtek	1,59%
USI (Proxim Orinoco)	1,59%
US Robotics	1,19%

Equipment from the remaining 16 manufacturers was used in less than 6% of networks. In 83% of cases, the equipment manufacturer couldn't be established (fake, unknown, user-defined), which is lower than the figures from other cities, and close to the figure for La Defense.

As the data shows, the equipment used in each location varies in terms of manufacturer. The figures for Symbol and Trapeze at La Defense, and the high amount of equipment produced by Senao in other locations are the most striking figures when the Paris data is compared to London, with Cisco having a

clear advantage in London. Equipment from Cisco was detected in Paris, as was equipment produced by Aruba, which was the third most common type of equipment in London. Overall, it should be stressed that the market share of equipment manufacturers not only differs strongly from country to country, but also from region to region within a single city.

The aggregate data for the top five equipment manufacturers in the two locations is as depicted in the table below.

In 82% of all cases, the equipment manufacturer could not be established.

Manufacturers	Percentage
Senao	4,17%
Trapeze	2,18%
Symbol	1,59%
Delta (Netgear)	1,59%
Linksys (GST)	1,19%

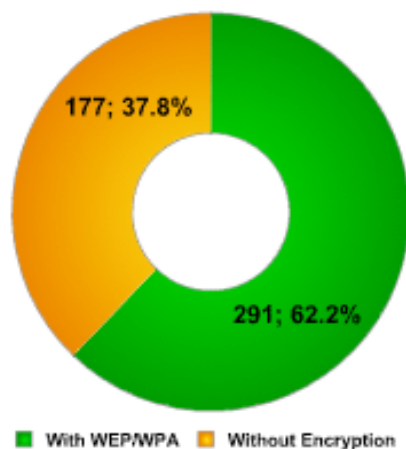
### Traffic encryption

Probably the most significant figure is the ratio of protected to unprotected access points. Older data collected by war drivers in cities

around the world show that approximately 70% of all networks do not encrypt traffic in any way. In Peking, we obtained a figure of less than 60%, at CeBIT approximately 55%, and in London 50% of networks which did not

use encryption. Our research in Paris was designed to find out whether unencrypted networks were still more common than encrypted ones, and whether London was the only 'digital fortress'.

First of all, let's look at the data collected during InfoSecurity together with the data collected around La Defense:



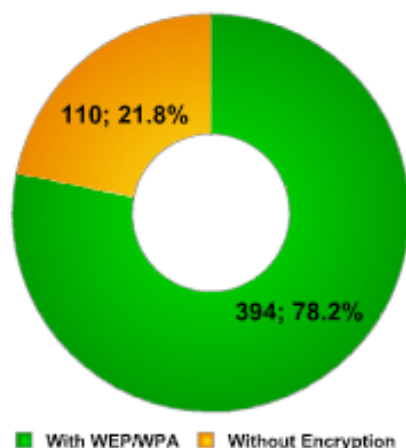
La Defense / InfoSecurity

Only 37% of networks did not use any type of encryption! This is a stunning figure, which is slightly better than the figure for London's Canary Wharf. The two regions are very similar: a great many international banks, oil and insurance companies, news agencies etc. could be targeted by hackers on the hunt for information of commercial value.

This is the lowest figure that we have come across so far. If we take into account that fact that some of the access points which make up this 37% are public access points which are located at the La Defense shopping centers, it seems to reinforce our assumption that the high number of secure networks which we

first encountered in London is general practice, and shows that system administrators are well aware of the issue.

Part of this data is naturally made up of access points at InfoSecurity. As we have previously mentioned, such access points are usually configured in a hurry, often incorrectly, and they can easily be targeted by hackers. The security of the networks detected at InfoSecurity London was worse than the security of networks in the rest of the city. It's quite possible that this was also the case in Paris, as 37% was by far from the most surprising figure which we encountered.

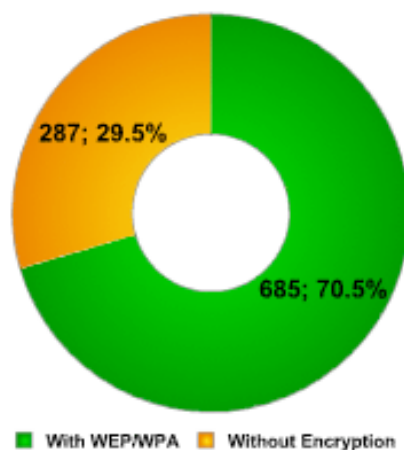


Other regions of Paris

The figures for other regions of Paris turned our preconceptions of secure wireless networks upside. A figure of 22% isn't only almost twice as good as the data we collected in the 'protected' business district, but it's the lowest percentage of unprotected networks that we've ever encountered in the course of our research. The general belief that approximately 70% of networks are unprotected was in part borne out by China (59%), Moscow (68%) and London (50%) but brought down by the data from Paris. And not just by data from the business district, where one would expect networks to be secure, but standard

access points belonging to home users also implement encryption.

Undoubtedly, one of the reasons for these figures is that wireless networks in Paris are better developed than in other cities, as is shown by their use of newer protocols and the speed of data transmission. Just as in London, we should highlight the high level of computer literacy and awareness of Wi-Fi security issues among users. The data from Paris shows that the era of unprotected wireless networks is gradually drawing to a close.



Combined data for Paris

While the data collected in other regions of London slightly detracted from the high figures collected at Canary Wharf, in Paris the opposite was true. The high figures were weakened by the public access points and the access points established by InfoSecurity participants, bringing the average number of unprotected networks down. In spite of this, however, we returned a figure of less than 30%! Paris is therefore awarded our unofficial victor's palm for the city with the best protected wireless networks, overtaking London (49%) and establishing a new qualitative benchmark. Paris is the city with the fastest and best protected Wi-Fi.

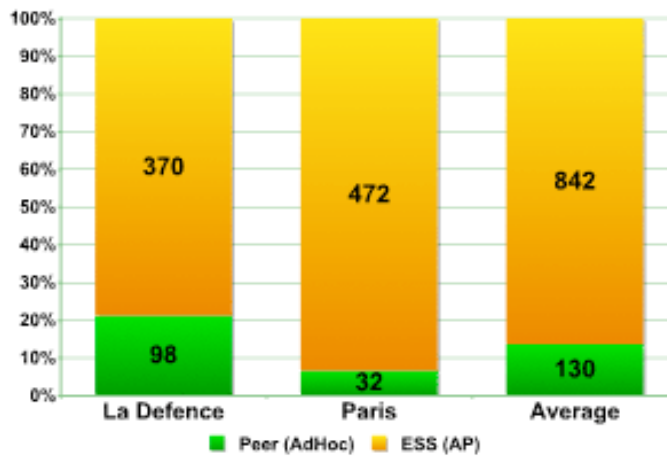
### Types of network access

Wi-Fi networks are either made up of ESS/AP access points or via Peer/AdHoc computer-to-computer connections. Data shows that approximately 90% of wireless networks are composed of ESS/AP access points. In China, the ratio of ESS/AP to Peer/AdHoc networks

was 89% to 11%, at CeBIT 2006 58% to 42% and in London 95% to 5%.

We expected to find a high number of Peer networks at InfoSecurity Paris (in London, approximately 50% of the networks were of this type.) This is because they are constructed within the framework of an exhibition (a temporary space) and use multiple connections between computers without network cables. The high number of Peer networks found at La Defense might also be due to the fact that wireless devices, such as printers, for instance, are becoming more and more popular in offices. The data collected shows that more than 20% of access points both at the trade fair and in office buildings are of the Peer type, and such networks are used exclusively to connect devices to each other.

Figures from the other regions of Paris give a ratio of approximately 9 to 1. The results are closer to those from Peking than those from London.



Types of Network Access

### Default configuration

Networks with default configuration are the juiciest morsel for hackers of wireless networks. As a rule, Default SSID means that the administrator of the access point has not changed the name of the router. This may also be an indirect indicator of the fact that the administrator account is still using the default password.

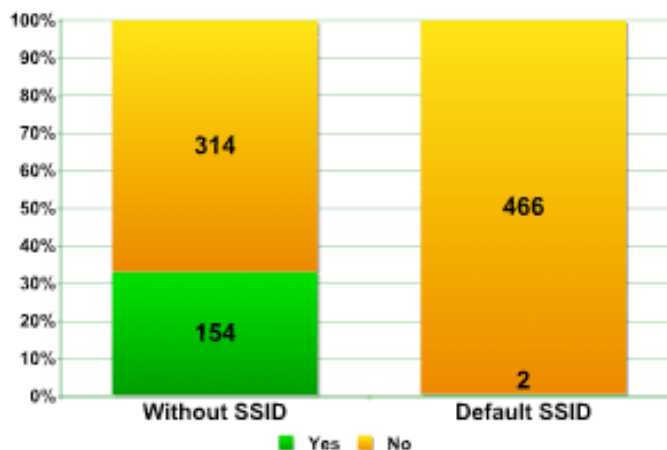
The Internet is full of information about which default passwords are used by different types of network equipment, and if a hacker knows the origin of the equipment, s/he will be able to take complete control over such a network. More than 8% of the networks in Peking retained their default configuration, which is a worryingly high figure. The situation at CeBIT was better - only two access points out of

more than 300 used default SSID. London gave us a figure of slightly higher than 3% in the city itself, and approximately 1.5% at Canary Wharf.

One of the best ways of protecting a network against war driving is to disable broadband spreading of the network identifier (SSID). Let's take a look at the networks we detected from this point of view.

The figures from La Defense are far better in terms of Default SSID than the figures from Canary Wharf. Less than 0.5% is praiseworthy.

SSID was disabled in almost 33% of networks, almost the same as the figure for London, with the French having a slight edge.



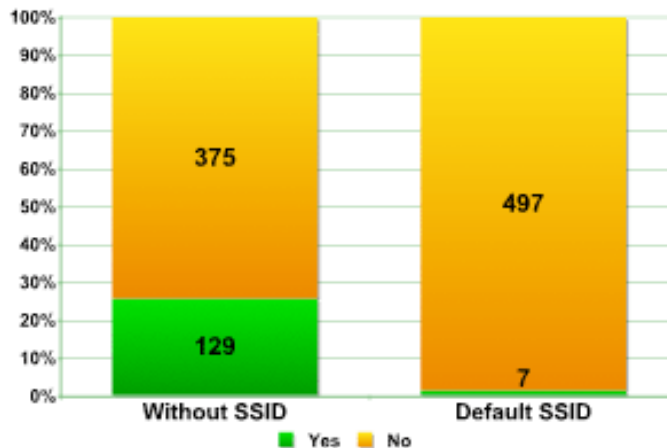
SSID Broadcast — La Defense



Taking into account the fact that we already know that wireless networks are highly evolved in Paris, the figures from other regions of the city were not surprising.

Default SSID was detected in 1.39% of networks, which was slightly lower than the fig-

ures from La Defense (to be expected) but still better than the 3.68% detected in London. The only area in which the English led the French was in terms of disabled SSID broadcast. In Paris, this was found in less than 26% of networks, in comparison to London's 32%.



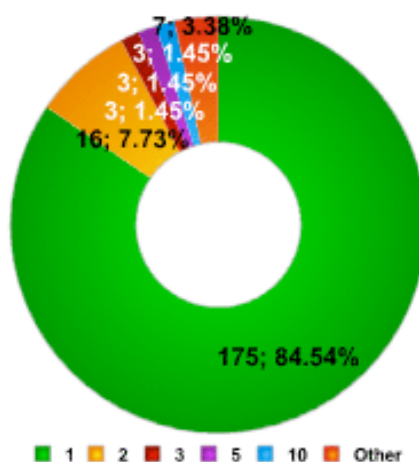
SSID Broadcast — Other regions of Paris

### Network components

This section includes statistics on the number of network access points in individual networks. Of course, a network has one or more access points but how many access points is common?

Around La Defense and at InfoSecurity 207 networks were detected. These networks contained more than 400 access points.

As the data shows, the vast majority of networks (more than 84%) only have one access point. Just as in London, networks with 4 access points were fewer in number than those made up of 2, 3, or 10 access points.



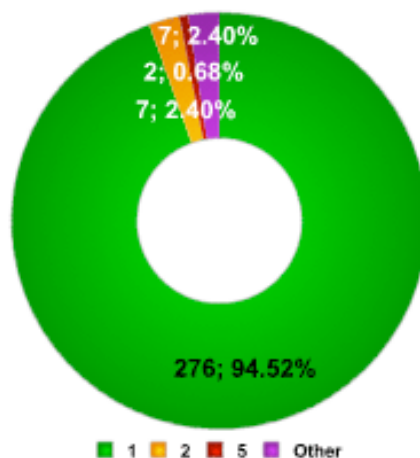
La Defense

On the other hand, there were some very large networks found, including two which had 10 and 11 access points respectively. However, there were no networks composed of 7

access points. Many access points could not be included in this data as SSID Broadcast has been disabled in the networks which they were a part of (more than 150 access points).

The 84% of networks composed of a single access point is a figure very similar to the 82% from Canary Wharf. We were interested to see if the data for London overall (51% of

networks composed of a single access point) was comparable to the data for Paris overall.



Other regions of Paris

And this is where we were surprised. Nearly 95% of the 292 networks (made up of more than 500 access points) had only a single access point. Was this due to home users, or to connections from small business? Whatever the reason, it was all the more surprising in light of the high level of encryption used in these networks, which we mentioned earlier.

As for record breaking numbers, we found three networks with 14, 16 and 18 access points respectively. These were undoubtedly public access networks. Overall, 292 networks were found, not including the more than 100 access points where SSID was disabled.

## Conclusions

The data gained from our Paris wardriving leads us to draw the following conclusions:

- The vast majority of networks transmit data at a speed of 54MB a second.
- There is an unprecedentedly high use of encryption in Parisian networks in comparison with networks in other cities around the world.
- Much of the data from the business regions of Paris coincides with data collected from similar regions of London.
- The majority of networks only have one access point, which results from the widespread use of wireless networks among home users.

Wireless devices such as printers, scanners, etc are becoming more and more widespread, making it easier to create office networks. This is clearly shown by the gradually increasing number of Peer networks.

Finally, it's not possible to identify a clear leader among the manufacturers of Wi-Fi equipment. Every country has its own preferences.

Overall, it should be stressed that our research over the past two years shows that the number of networks which use some time of encryption (WEP or WAP) is steadily increasing. In fact, one could say that the situation had changed radically over the past two years - from 70% of networks in Moscow and 60% in Peking to 30% in Paris. This is surely not due to socio-economic factors. It's a clear global trend, which shows that both users and system administrators have recognized security on open networks as being a serious issue. The life of wardrivers is going to become more difficult as it becomes more difficult to hack networks in order to steal data or simply to gain access to the Internet.

## Bluetooth

The most widespread method of transmitting data by WiFi is currently the Bluetooth protocol. Almost all modern mobile phones have a

wireless module which enables the exchange of data with similar devices, also making it possible to use the 'hands free' function. Bluetooth is an integral part of smartphones, PDAs and some laptops.

In the spring of 2006 at InfoSecurity in London we conducted our first research into Bluetooth. We detected more than 2000 Bluetooth enabled devices in "visible to all" mode. We decided to conduct similar research in Paris in order to gain comparative data which might support our conclusions. This report includes the data we gathered, and compares it to the data from London. We detected more than 1300 Bluetooth enabled devices in "visible to all" mode; although this is fewer than the 2000+ detected in London, we believe that this data is nonetheless representative.

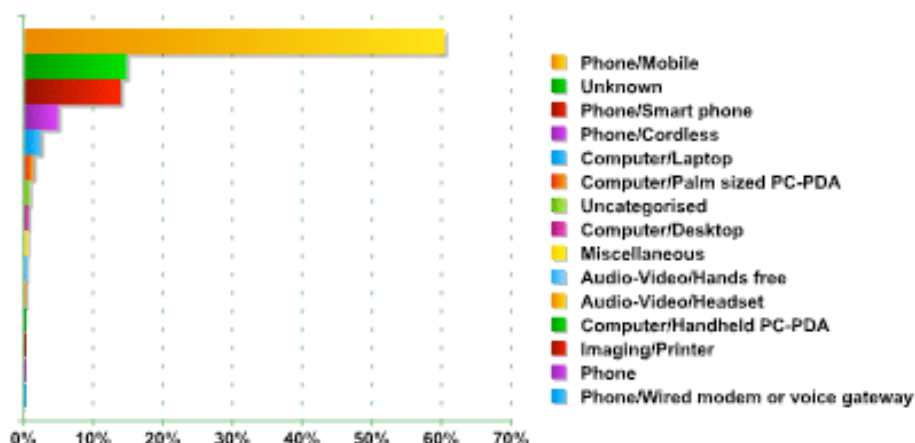
We used Blue Soleil, Blue Auditor and BT Scanner to collect data.

The research was conducted both within the InfoSecurity Paris exhibition hall, and around La Defense, the business district of Paris. Although fewer Bluetooth devices were detected than at InfoSecurity London, nevertheless, at least 30 - 40 devices could be detected at any one time within a 100 metre radius.

We also collected Bluetooth data while collecting data about WiFi networks in other regions of Paris. The areas investigated included the Paris Metro, the Gare du Nord (a major railway station), and areas with a high concentration of tourists.

### Types of device

Let's take a look at what Bluetooth devices we detected:



The graph clearly shows that the vast majority of devices are normal mobile phones. They make up approximately 60% of the total, which is 10% less than the figure for London. This is a fairly significant difference. This might be due to the fact that approximately 14% of the devices couldn't be identified correctly, which could account for the difference. Standard mobile phones do not have a fully functional operating system, and they are only theoretically vulnerable to viruses, e.g. malicious programs written in Java for Mobile.

However, all of these telephones are vulnerable due to Bluetooth protocol issues which we've written about before.

The second most popular type of device (if we exclude Unknown devices) is smartphones. They make up approximately 14% of all devices detected, which is significantly less than the 25% found in London. This is surprising, as France definitely is among the countries with the most smartphones in the world, and is one of the most developed markets for such devices. However, the statistics speak for themselves.

In third place, with almost 5% were standard cordless phones of the type often used in offices. This figure is higher than that for London, and laptops with Bluetooth were in third place in London, making up approximately 3% of all devices found.

The figures for Paris are of a similar level - more than 2%. We should stress that although this isn't a high number, the risk of hacker attacks on such devices is greater than the risk of attacks on a standard handset or smartphone. This is because the data saved on a laptop is far more extensive and attractive to hackers than data stored on a telephone.

In terms of other devices, the number of PDAs (Palm sized PC PDA and Handheld PC PDA) detected was less than 2%. This is identical to the figure from the UK, which we see as confirmation of the fact that users of such devices are very aware of Bluetooth security issues and take the appropriate precautions.

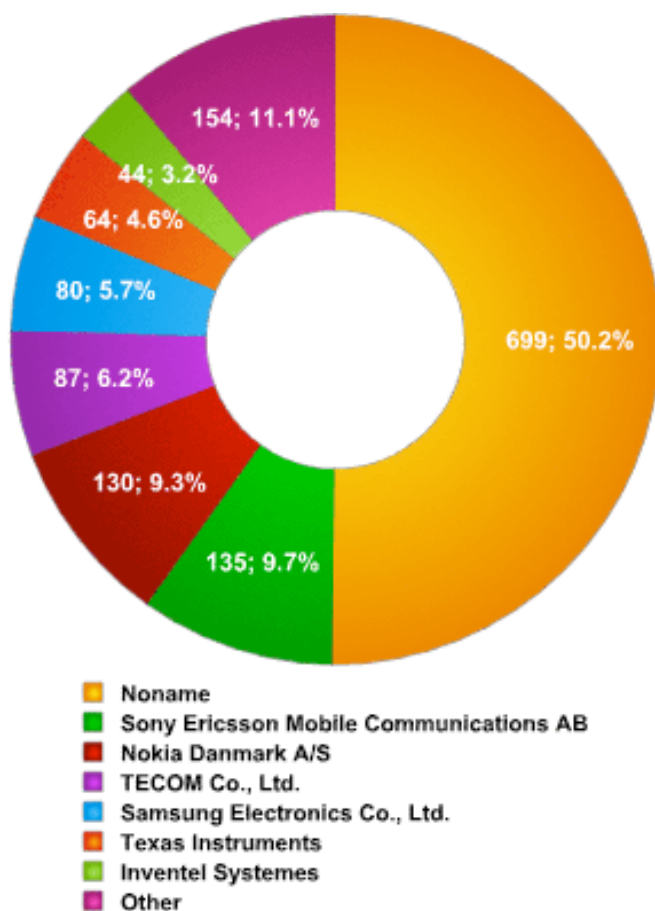
All in all, we detected more than 1300 devices of 15 different types. The number of Uncategorised and Miscellaneous devices was less than 1.5%, although we still classified this as a type of device. The single blot on our statistics was the 14% of Unknown devices.

## Equipment manufacturers

This figure is very significant: we can use data about equipment manufacturers to establish what operating system is being used (in the case of smartphones/ PDAs) or get data about an individual manufacturer's market share.

Overall, we detected equipment from 39 different manufacturers (in contrast to the 35 which we detected in London.) 6 manufacturers appeared to be the most popular, with their devices making up more than 38% of all devices detected.

Unfortunately, in approximately 50% of cases, we were unable to establish the equipment manufacturer. This is a surprising figure, as in London the percentage of such devices was only slightly over 25%. Could it somehow be connected with grey market telephones?



Equipment manufacturers - Paris

Manufacturers	Percentage
Noname	50,18%
Sony Ericsson Mobile Communications AB	9,69%
Nokia Danmark A/S	9,33%
TECOM Co., Ltd.	6,25%
Samsung Electronics Co., Ltd.	5,74%
Texas Instruments	4,59%
Inventel Systemes	3,16%
Other	11,06%

The data above shows that in Paris there is no clear market leader among equipment manufacturers; this is in contrast to London, where Nokia manufactured more than 30% of devices detected. In Paris, Sony Ericsson is in first place with 9.69% of the devices detected, but Nokia is not far behind. However, the figures from London were very different, as these two companies had almost half of the entire market share. The figure for Samsung, on the other hand, is very similar in both cities: 5.74% in Paris and 4.52% in London.

Texas Instruments is in a similar position, perhaps explained by the limited prevalence of Motorola telephones. Interestingly, well known manufacturers such as USI and Murata aren't among the list of leaders, having been squeezed out by Tecom and Inventel. However, they do come just below the top six most popular manufacturers, together with LG and Sharp. As we've mentioned in the past what type of equipment different manufacturers produce, the following data may be of comparative interest:

Brand	Phone/Smartphone	Phone/Mobile
Nokia	30%	70%
Sony Ericsson	12,5%	87,5%

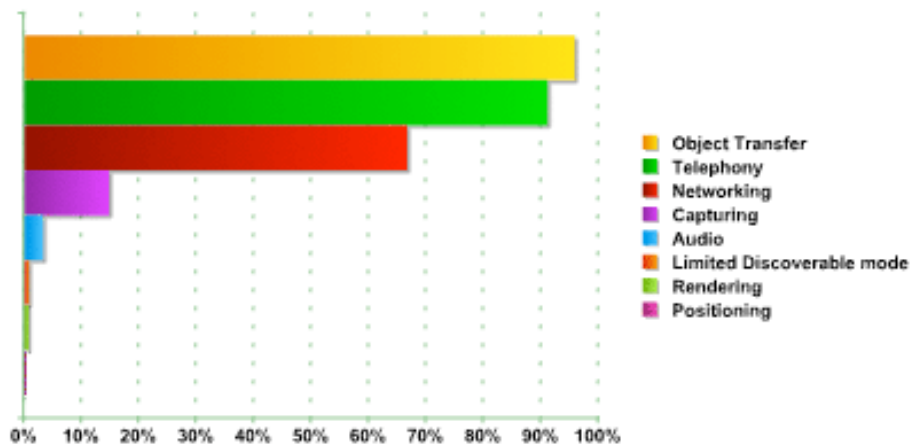
Brand	Phone/Mobile	Phone/Cordless	Other
Samsung	56,8%	40,7%	2,5%

Brand	Phone/Smartphone	Phone/Mobile	PDA
Texas Instruments	56,8%	40,7%	2,5%

### Accessible services

The data on accessible services is of great interest to us as it illustrates the opportunities both for hackers to attack handsets and for viruses to spread. When a device establishes a Bluetooth connection with another device, it makes it possible for the second device to use some of its services. For example, if you've

allowed a friend's device to connect to yours in order to exchange data, you are also making it possible for your friend's device to make calls from your phone, send SMSs, read your address book etc. And of course, it could be a hacker in place of your friend, a hacker who has used social engineering or a Bluetooth vulnerability to gain access to your device. The data we collected on accessible services

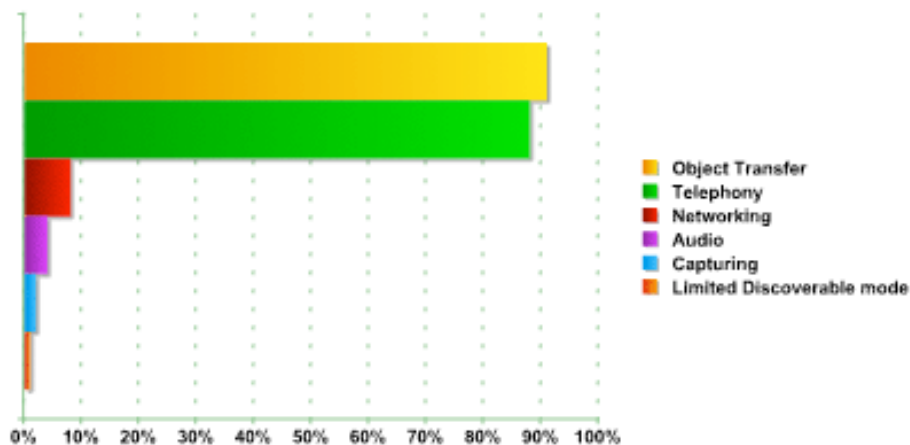


gives us a picture of what services could be accessed by remote malicious users. Let's start by taking a look at the data for all services. We detected approximately 3800 services on over 1300 devices, distributed as seen above. Given the ratio of 3800 to approximately 1300, this means that each device had, on average, around 3 accessible services. Some devices had 5 or 6 accessible services. As the graph shows, three services were the most common:

- Object Transfer (sending/ receiving files). This is used in more than 95% of devices.

- Telephony (making calls, sending messages). This is used in more than 91% of devices.
- Networking (provides Internet access and the ability to use an inbuilt modem). This is used in more than 66% of devices.

These figures are practically identical to the data we collected in London, with the difference in all three cases being less than 1.5%. As we are primarily interested in smartphones, which are among the most vulnerable Bluetooth devices, it's worth taking a look at the data relating to them separately. As the graph below shows, the ratio of devices: services is approximately 1 : 2.



There's a slight difference between the figures for smartphones and the data for other devices. With more than 93%, Object Transfer remains the most widespread accessible service, followed by Telephony with 91%, and Networking in third place, with the low figure

of slightly more than 10%. The data from our research supports our previous conclusions: although some users of Bluetooth devices are aware of the risks posed by cyber threats, user education is still needed.

Alexander Gostev is the Senior Virus Analyst at Kaspersky Lab, a leading developer of secure content management solutions that protect against viruses, Trojans, worms, spyware, hacker attacks and spam.

Confidential Notes is a practical and easy to use solution that instantly provides you with a high level of security for your mobile data.

For more information on Confidential Notes visit [www.pocketpcsecurity.com](http://www.pocketpcsecurity.com)



Confidential Notes 13:39

Enter password 1:

Enter password 2:

Forgot password?

123 1 2 3 4 5 6 7 8 9 0 - = <

Tab q w e r t y u i o p [ ]

CAP a s d f g h j k l ; ' <

Shift z x c v b n m , . / <

Ctl á ü ` \ <

Confidential Notes 13:17

Main Folder	Date	
ipaq software	13:08	4k
inet banking info	13:06	151k
shopping weekend	13:04	149b
target market	13:04	2k
city center plan	13:03	1k
dan's cellular	13:02	29b
early sketches	13:01	1024b
audio Q&A in NY	13:01	245k
wilderness sounds	13:00	225k
anna's NYSE column	12:59	892b
stock portfolio	12:58	1k
apple store london	12:57	3k
VC capital thoughts	12:57	145k

New Options

Confidential Notes 12:26

interview with the marketing manager

ARTICLE

Besides the overview on the success of the past year's event and a very positive forecast for this April's conference, journalists were presented with a rather new concept in the field of IT events - assistance for overseas visitors. I should note that he term "overseas" in this case is obviously connected to visitors outside the United Kingdom. As the Infosecurity conference is UK's top information security conference, UK Trade & Investment, the British Government agency that supports overseas enterprises

New Edit Options



## Events around the world

### **Black Hat DC Briefings & Trainings 2007**

26 February-1 March 2007 – Sheraton Crystal City  
<http://www.blackhat.com>

---

The 14th Annual Network & Distributed System Security Symposium  
28 February-2 March 2007 – Catamaran Resort Hotel, San Diego, CA, USA  
<http://www.isoc.org/isoc/conferences/ndss/07/>

InfoSec World Conference & Expo 2007  
19 March-21 March 2007 – Rosen Shingle Creek Resort, Orlando, FL, USA  
<http://www.misti.com/infosecworld2007>

WebSec Conference 2007  
26 March-30 March 2007 – London, UK  
<http://www.mistieurope.com/websec>

Black Hat Europe 2007  
27 March-30 March 2007 – Amsterdam, Netherlands  
<http://www.blackhat.com>

Business Continuity – the Risk Management Expo 2007  
28 March-29 March 2007 – Excel, The Docklands, London  
<http://www.businesscontinuityexpo.co.uk>

ARES Conference 2007  
10 April-13 April 2007 – University of Technology, Wien, Austria  
<http://www.ares-conference.eu/conf/>

If you want your event included in the HNS calendar e-mail us at [press@net-security.org](mailto:press@net-security.org)





Interview with Joanna Rutkowska,  
security researcher  
By Mirko Zorz

Joanna Rutkowska has been involved in computer security research for several years. She has been fascinated by the internals of operating systems since she was in primary school and started learning x86 assembler on MS-DOS. Soon after she switched to Linux world, got involved with some system and kernel programming, focusing on exploit development for both Linux and Windows x86 systems. A couple of years ago she has gotten very interested in stealth technology as used by malware and attackers to hide their malicious actions after a successful break-in. This includes various types of rootkits, network backdoors and covert channels.

**How did you get interested in Windows security?**

When I started to play with Windows internals, I already had a background with Linux user-mode exploitation and kernel programming. Move to Windows was a natural evolution and was mostly dictated by my curiosity.

**What's your general take on the security aspects of Windows Vista? Is it much more secure than Windows XP as Microsoft is telling us?**

Indeed, Vista introduced lots of security improvements comparing to XP. The most important one is probably the User Account

Control feature which will hopefully force people to work from restricted accounts. UAC is still far from perfect - e.g. it's pretty annoying that every single application installer (even if it is Tetris) asks for administrative credentials and the user has no real choice to continue the installation \*without\* agreeing on that. However, I see UAC as an important step towards implementing the least-privilege principle in Windows.

Also, Microsoft introduced some anti-exploitation technologies, like e.g. ASLR and invested a lot of money and time into improving the quality of the code behind the operating system and the applications.

The introduction of BitLocker technology which makes use of the Trusted Platform Module (TPM) to assure the integrity of the booting processes seems like an important improvement. Of course, this should not be thought of as a silver bullet solution against rootkits and all other malware.

In the 64-bit version of Vista, Microsoft also introduced the requirement that all kernel drivers must be digitally signed, but I don't be-

lieve this mechanism to be effective in stopping kernel malware. Also, the much discussed Kernel Patch Protection (AKA Patch Guard), should not be thought of as an effective protection against kernel compromises, as it's relatively easy to bypass by the malware authors. Still, I see those two mechanisms as useful when it comes to system compromise \*detection\* (in contrast to prevention) - at least when it comes to type I malware.

**When we look at the quality of the advisories published these days, I have the feeling that people are looking for cheap publicity.**

**In your opinion, what is the biggest mistake Microsoft has made when it comes to security in 2006?**

I don't really see any particular, spectacular mistake made by Microsoft in 2006 but there are some things which I don't fully agree with, like e.g. the design of Integrity Level mechanism which prevents only against writes not reads or issues regarding kernel protection or the fact that they concentrate only on prevention (like most other OS vendors) and haven't done anything to make systematic compromise detection feasible. I guess these are just different points of view and I would not call any of them a 'big mistake'.

**What do you think about the full disclosure of vulnerabilities?**

I'm quite neutral about this. On one hand, I think that it should be every customer's right to point out flaws in the products they buy and I really don't see why those who find bugs should be \*obliged\* to first report it to the vendor - i.e. why should they be forced to do a free Q&A with the vendor?

On the other hand, when we look at the quality of the advisories published these days, where most of the bugs reported are just some denial of services, I have the feeling that people are looking for cheap publicity. It's quite understandable that companies which are victims of those "audits" might feel a bit pissed off.

Naturally, from time to time we see a very interesting bug report, sometimes presenting a new class of bugs or a new method of exploitation. It's hard to overestimate the value of such reports for the security community, so if the author decided to release those information for free, I guess we all should only be grateful to the author.

**What is your opinion about Microsoft Patch Tuesdays? Shouldn't there be more frequent patch releases?**

I guess there should be, but I can also understand that releasing a patch is a complicated business process, because it requires lots of testing, etc. I also realize that even if we had patches released on a daily basis, that still would not be a sufficient solution, as attackers might still exploit some unknown vulnerability.

Thus, I think it's much more important that the OS itself provided various anti-exploitation technologies and also be designed to limit the damage of the potential successful exploitation (least privilege design, strict privilege separations, etc). And it's clear that Microsoft is going this way, although there's still room for improvement in this area.

**What is the most interesting fact you've become aware of while researching for your recent papers?**

It's hard to point to just one fact. Usually the most amazing thing is that something you thought of before (e.g. some attack) actually

does work after you implemented the proof-of-concept code. That's always very amazing for me.

**What's your take on the open source vs. closed source security debate?**

I don't like when people say that something is secure just because it's open source and inherently insecure, just because it's a commercial, closed source product.

Although it should be admitted that a lot of security technologies have been introduced in the open source systems for the first time, like e.g. ASLR which has been invented by PaX about 6 years ago.

**What are your future plans? Any exciting new projects?**

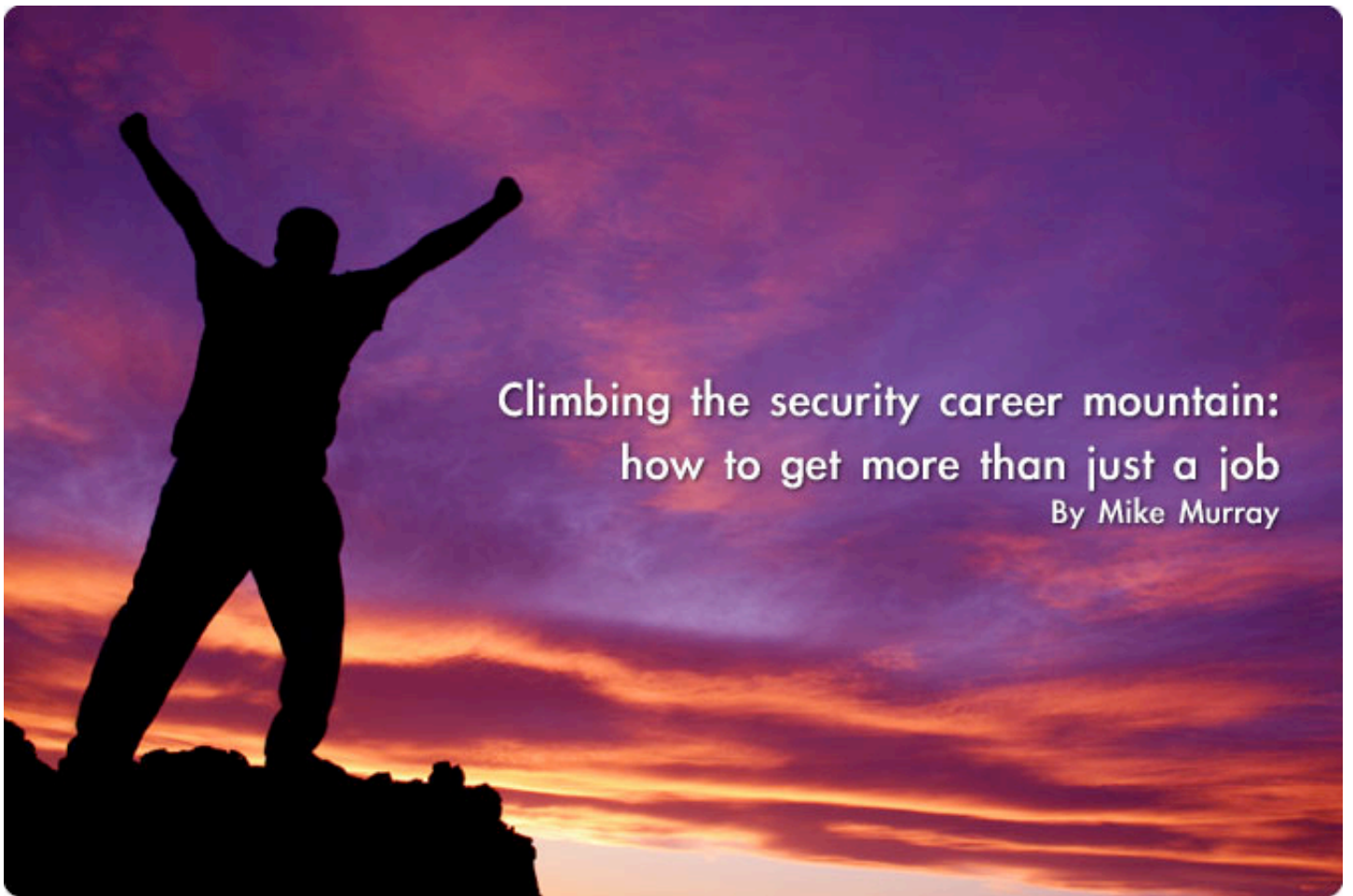
I think that I would like to focus more on the defense side now. In the past two years I have worked on several offensive techniques, starting from passive, very hard to detect covert channels ("Nushu"), then I presented "Stealth by Design", type II malware, then I showed that Vista kernel can be subverted

despite the new protection mechanism and also demonstrated that recent hardware virtualization technology can be used to create a new class of stealth malware - something I call type III malware (e.g. "Blue Pill"). And just recently I found that hardware based memory acquisition as used for forensics, believed to be absolutely reliable, because it uses so called "Direct Memory Access" to read memory, can be cheated in some cases.

Unfortunately I haven't seen any serious effort in the security world to address most of those threats. We still don't have any effective way to combat type II malware. Network intrusion detection systems and firewalls are years behind when it comes to detecting or preventing any more advanced covert channels. We still don't have any good solution to prevent or detect hardware virtualization based malware...

I would like to work more on the defense side now - I believe that we should convince OS vendors (and also CPU vendors) to make systems verifiable - so that we could come up with \*systematic\* ways to check whether the system is infected by any of type I, II or III malware.





**Climbing the security career mountain:  
how to get more than just a job**  
By Mike Murray

**“So you want to be a rock & roll star?  
Then listen now to what I say.  
Just get an electric guitar  
Then take some time  
And learn how to play.”  
The Byrds - So You Want to Be A Rock & Roll Star.**

**So, you want to be a security star, huh? Well, reading this magazine is a good start. But the reason that they have asked me to write this article is to tell you about all of the things that you need to do past that. Reading a few articles on SSH and security in Web 2.0 isn't enough to make you into a security superstar than listening to a few records will make you a rock & roll star. As the song lyric says, you have to learn how to play. That's what this article is going to be about. But first, a question: Why do you want to be in security?**

That's a tough one to answer, sometimes. Maybe you saw a movie like Hackers, War Games or Firewall (though I really hope it's not the last one). Or you went to Defcon or HOPE and think it's cool to be one of those people. Or perhaps you read the recent salary surveys that put CISSPs at the top end of the salary scale.

If it's any of those, you're in trouble. Because security isn't a career path that you should

take for the money or the coolness. I have met many people who started in security for one of those two reasons, and very few of them have actually managed to make a career out of the security field.

The most important question that you need to answer: why do I want to be a security engineer? Because, as the old self-help slogan goes, "if your 'why' is strong enough, you'll find the 'how'".

While the rest of this article is going to be about the “how” of becoming a super-star security engineer, I can’t emphasize this enough: spend some time figuring out what it is about security that calls to you over all of the other cool things you could be doing with your life.

## The Prerequisites

One of the things that makes being a security engineer so interesting is that security applies to all of the different technology areas. Thus, in developing a real career in security, there are very few areas of technology that you won’t be required to know and understand at a significant level. If you meet some of the best security professionals, you’ll quickly realize that they unix like a unix admin, Cisco routers like a CCNP, Oracle like a DBA and C++ like a software engineer. And they can keep up in a conversation with any of those people.

Because of the well-rounded skill-set required, becoming a great security professional is incredibly challenging, but also incredibly rewarding. You will spend the rest of your life learning, because any time a new technology comes out, you’ll be required to learn about it. As an example, one of the best engineers I know has spent the past couple of months learning the ins and outs of MySpace on a deep technical level.

Because of the incredibly varied skill-set required, most of the best security professionals don’t start out their career “in security”. They usually come to security from another specialization - system administration, software development, data networking or telco. Using myself as an example, I started as a system and network administrator, helping companies keep their servers, desktops and routers up and running. But I was always interested in security: it was the thing that I studied in my spare time. And I was always most interested in figuring out how to protect (and break in to) the systems that I was building and maintaining.

It’s that interest in security that is common to every long-term security professional that I have met. Talk to anyone who has had security as a large part of their career, and they’ll likely tell you about their time as a young technologist where they found either the “breaking” or “protecting” aspects of security

fascinating. I have met hundreds of information security professionals over the years, and almost all of them have a story like that, me included.

The good news is that, by the sheer fact that you’re reading this article, you probably have that interest. That’s the first step up the information security career mountain. So, let’s look at the path up the side of that big hill.

## The Security Career Mountain

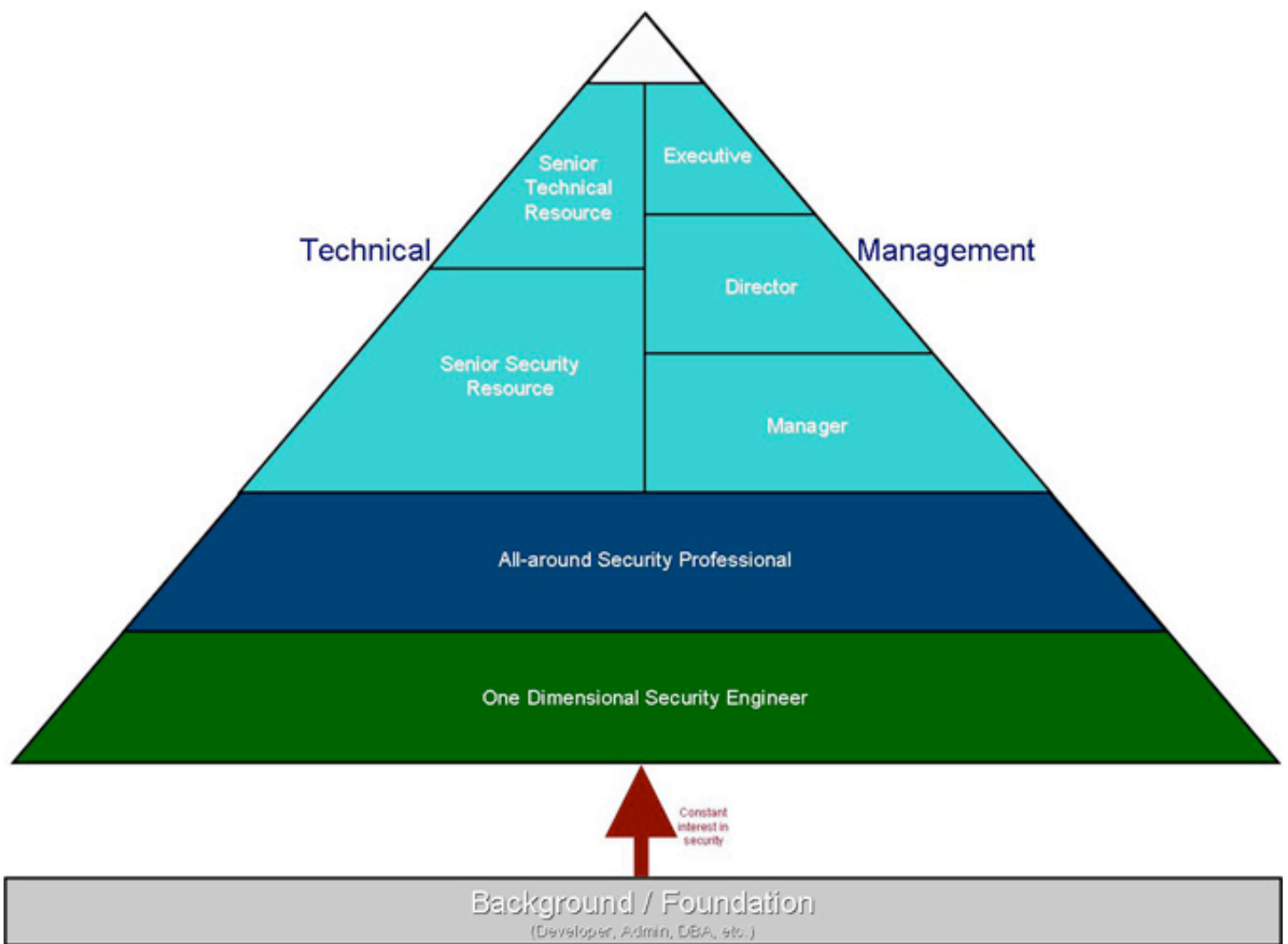
The career path of a security professional is quite varied. One of the great things about information security is that your career can be incredibly tailored to your own experience and your own desires. But there is also a general progression that most careers take - I’ll describe that general path and some of the important steps along the way.

The diagram on the following page is a general representation of the mountain that is a security career. You’ll start at the bottom, usually in another field (as I mentioned above).

Entering the security career track, you’re generally going to start out as a one-dimensional security engineer, who brings your skills from another discipline and your love of security together to be a security expert in your chosen field. This is where you’ll find job titles like “web application security engineer” or “unix security administrator”.

From there, you’ll spend a year or two gaining the all-around experience required to really be a security professional. And that’s where you have to make the hard choice: do you want to be a technical security expert or a manager? (As I’ll talk more about, this is somewhat a false choice, but it’s useful for the purpose of simplicity here). Your decision there will determine your career path for much of your career: you’ll be focused on honing either the skills of an incredibly technical security expert, or of an information security manager. And you’ll get the jobs that go along with that.

And finally, you’ll get to the snow-capped peak of the security career mountain... and you’ll have to read on to find out what’s at such a lofty summit. But, first, let’s talk in more detail about each of the camps along the mountain.



## Base Camp - The One Dimensional Security Engineer

You just decided to climb the security career mountain, and you arrived at the first camp. The air down here is still very much as it was while you were working your other career path as an admin, a coder, or engineer. In fact, your title is probably very much the same: you've probably just put the word "Security" in the title somewhere.

Success at this step involves taking the interest that we talked about before and combining it with the skills that you already have: your job at this level of your career is to learn to think like a security professional, even if you aren't one. This generally means that you're going to start learning (on an intuitive level) about the three main concepts in security: vulnerability, threat, and risk. I'm not going to go into those definitions here, but, suffice it to say that, as a security pro, you'll get to know those definitions on an experiential level. If you're already a security pro, you know what I mean: as you move up the mountain, you'll be

able to smell risks, threats and vulnerabilities in the air around you.

This is the point in your career where you need to start focusing on that. Look at all of the skills that you have, and start tying in the core concepts of security thinking into your daily tasks.

The other thing you need to do is simple: Be a sponge. This is the time in your security career where you need to learn about being a security professional absorbing what security professionals know, and what they're all about. So, what you want to do during this time in your life is to spend as much time as you can reading books and blogs, attending conferences and local meetings, listening to podcasts (like mine at episteme.ca) being active on mailing lists and online forums. In short, get to know everyone in security, learn what they know, and learn how to start doing what they do.

In other words, learn what a well-rounded security professional knows.

## Camp 2 - All-around Security Engineer

This is the point at which you've finally established your skills. You can now expound at length the difference between a cross-site scripting vulnerability and a buffer overflow, the different types of authentication factors and their strengths and weaknesses, and how to assess risk in an organization. And you can do it while you're thinking about something else. You probably have (or have thought about or decided consciously not to get) a CISSP. And you didn't have to take one of those "boot camps" to get one - you got it on the knowledge that you already had.

While your learning shouldn't stop, it probably will become more subtle. You'll stop finding the real key stuff in books and focus more on conference papers, blogs and magazines (like this one) because that's where the real "new" stuff is. This is where some people can get bored and stagnant, but that feeling is just the beginning. Because it's now time to start generating content of your own.

No, you don't have to become a writer or present at next year's BlackHat Briefings. The key here is to start to differentiate yourself as a security pro. Answer these questions, and you'll start to understand: How am I different as a security professional than the guy in the cube next to me? Or than the guy who sat behind me during my CISSP exam? What makes me unique as a security professional?

As an example, for me it has been my interest and focus on personal development. While I'm a security professional at heart, my ability to work with people to help them be better at what they do is something that not every security professional has. This is what lead Mike Rothman to dub me "Mr. Security Career" - this is what makes me different. As you reach this stage in your career, what you need to do is to figure out what it is that makes you different. Because, while you're continuing to round out your technical and security skills, it's the answer to the "what makes you different" questions that will ultimately lead you to the career that you want. Which leads you to the moment where you need to choose a path up the mountain...

**As you reach this stage in your career, what you need to do is to figure out what it is that makes you different.**

## Camp 3 - The Fork in the Road

At this point in your career, it's time to make a choice: will you head towards becoming a technical guru, or a high-powered security executive? Because it's nearly impossible to do both at once. (We'll come back to that later). Your choice at this point depends on who you really want to be in your life - what I would call your "calling". Who are you? Are you a person who comes up with neat technical solutions? Or someone who builds, leads and inspires teams of people who come up with neat technical solutions? When you dream of the perfect day at work, which do you see yourself doing?

This isn't the easiest point for most people, because it's often hard to make a choice. Especially if you're going to choose to become a great technical resource, because the pressure to go into management (especially if you're a high-performing all-around security

professional) is incredibly intense. I once asked a security super-star that I worked with why he accepted the management job that he was in when he clearly wanted to spend his time working on the technology. His answer was telling: "It's just what you do, I guess." He spent most of his days miserable dealing with staff issues, until he finally quit and went back to working as a senior-level security consultant doing high-level penetration tests and security engineering. And he has never been happier.

The key here is to know which path is most right for you. While you can change your mind later, it's probably pretty evident if you look at your temperament and skill-set. Not everybody wants to spend their life with technology, just as not everyone wants to manage. You probably have a good idea which one you want. (And if you don't, email me and I'll help you figure it out).

## Load up on Oxygen Bottles

The air from here on up gets a little rarified, and it's going to get harder and harder to breathe unless you load up on the equipment that will allow you to survive higher and higher up the career mountain. Those skills can be summed up in two words: business acumen.

And it doesn't matter which path you choose to take: both require an understanding of business at the same level. This doesn't mean that as a technical expert that you need to go off and get an MBA. But it does mean that you're going to need to understand how businesses make decisions about spending time, money and other resources to solve problems. And how things actually get done.

As an example: it's a relatively naive security professional who makes the assertion: we should work to eliminate every security hole in the organization. While that may be true from a technical perspective, and even from a risk-focused perspective, it's not at all true from a business perspective. It's your understanding of business decision-making, processes and culture that will let you operate higher and higher up the security career mountain.

## Camp 4 - Navigating The Technical Path

So, you took the technical path up the mountain. You're going to be called on more and more to do one thing: solve hard problems. There's only one thing that you can do to improve your skills at solving hard problems, and that's to practice solving hard problems. This means that you're going to have to continue to learn more and more nuanced detail around the things that you're going to become an expert in.

The biggest challenge in this path is going to be expanding your vision to see "the big picture". This relates to my previous advice on business acumen; this is where you need to learn to keep all of the details in your mind at a given time. When you're developing an authentication strategy, it's not just about which crypto algorithms you use and what the password strength is, but, as you get to be a more senior resource, the questions you need to ask are around strategy. For example: how does this authentication system play with the technology we're going to deploy next year or

the year after? What's the scalability of the system - what happens if we grow from 1000 users to 10,000 users?

## Camp 5 - The Management Path

The management path is a path that has been covered by a huge number of books and magazines out there. I'm not going to spend a lot of time on this path, except to give a quick overview. If you're trying to move forward in the management path, your skills are going to need to be about business and people. This is the point in your career where you may want to start thinking about an MBA (or at least learning the skills of an MBA), learning to play golf, and focusing on how to manage and lead security professionals.

If you're thinking about taking this path, you should check out Mike Rothman's "Pragmatic CSO" book - it will give you incredible insight into the skills and thoughts that are required to succeed on this path up the security career mountain.

## The View from the Summit

I told you that we'd talk about the "snow-capped peak" of the mountain - this is it. Summating the mountain is the point at which you transcend the path of "manager" or "technologist" - this is the point in your career at which you're generally called "visionary".

The people who get to this level are the ones who become household names: Steve Jobs and Bill Gates are popular examples. But there are examples in the security industry as well: Marcus Ranum, Mary Ann Davidson, Ron Gula, Tim Keanini and Bruce Schneier are great examples of those who have reached this pinnacle of the security career.

This is that rare person who can "cross the streams" - who can manage a business and stay involved in technology at the same time. Neither strictly managers nor strictly technologists, these are the people who are known as experts on both.

## But How do I do it?

Getting to the top of the security mountain isn't an easy task - it takes a lot of work. And, more than anything, it'll take a lot of good luck.



Talk to anyone who has been successful in security (and, in fact, any industry) and you'll hear the story of someone who has been in the right place at the right time.

In fact, that is, as I mentioned earlier, the place where you need to start: you need to start meeting people who have done what you want to do. Get to conferences and on email lists and read their blogs. Learn how they got to where they are, and take whatever advice they have that is useful to you. Then, start to apply it to your own life and career.

Most importantly, figure out what they know that you don't know. Figure out what books they've read that you haven't. What papers they read that you don't. What blogs they read. What podcasts they listen to. And do those things.

Then, do those things. But that sounds like a LOT of work!!! Yeah, I know. Here's where I share the dirtiest little secret of all great security pros: Becoming great at security IS a LOT of work.

That's the bad news. The good news is that becoming great at anything is a lot of work. Which is where that first question comes in again: you have to have a really great reason for wanting to do this one. Because, otherwise, those days when you're reading an RFC because somebody like me told you that it's worth getting to know the protocols at a really deep level (which it is), you're going to decide that you'd rather be playing Xbox360. (Heck, even if security is your calling, you're going to decide that sometimes... but the point is that you'll do it eventually if you really want to be great at this).

A 10-year veteran of the security industry, Mike Murray focuses his expertise on building successful and fulfilling careers. Dubbed "Mr. Security Career", his blog at [Episteme.ca](http://Episteme.ca) and his "Technology Career Excellence" podcast have become known as resources for those in technology who want more than just a job. His new book "Forget the Parachute, Let Me Fly the Plane" is targeted at careers in fast-moving industries like information security. Learn more at [ForgetTheParachute.com](http://ForgetTheParachute.com) and at Mike's blog at [Episteme.ca](http://Episteme.ca).



**HNS SECURITY  
SOFTWARE DATABASE**

**Get the largest selection of the best security software for Windows, Linux, Mac OS X and Windows Mobile platforms.**

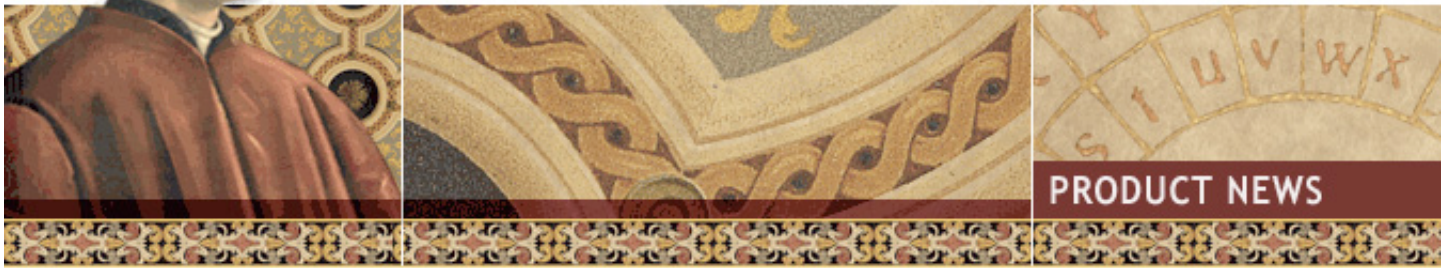
**20 CATEGORIES  
2.5 MILLION DOWNLOADS SO FAR**

**net-security.org**



# RSA CONFERENCE 2007

FEBRUARY 5-9 | MOSCONE CENTER | SAN FRANCISCO



We attended the enormous RSA Conference last week in San Francisco. With around 15,000 attendees, a myriad of in-depth lectures delivered by some of the industry's most important figures, as well as keynotes from leaders such as Bill Gates and Colin Powell, we can truly say the event was a giant success.

Companies from all over the world exhibited their products and services and a large amount of announcements were made at the show. The amount of new releases shows just how important the RSA Conference is to the security industry as a whole. What follows is a roundup of product releases announced at the show as well as a gallery of photos.

## Announcements

**Absolute Software** - Announced that Dell is bundling Computrace LoJack for Laptops with their computer accidental damage services sold to consumers.

**Aladdin Knowledge Systems** - Aladdin eSafe HellGate appliance, the company's first gateway-based anti-virus, spyware control, Web browsing security and application filtering solution specifically designed for the SMB market.

**Altiris** - SecurityExpressions 4.0 helps keep security postures consistent with security policies and regulatory mandates and enforces compliance through audits, remediation and reporting.

**Application Security** - DbProtect - an integrated suite that is built on their AppDetective and AppRadar product

**Applied Identity** - New Identisphere product suite offers unified policy access management functionality that provides organizations with a seamless solution for both managing multiple and disparate directories, and for developing and managing fine-grained user policy.

**Arcot Systems** - First-to-market integration with Microsoft Windows CardSpace identity management framework.

**Array Networks** - Beta availability of Site2Site, the first site-to-site SSL VPN solution.

**Arxceo Corporation** - Arxceo Ally ReconAlert, a free software package for Windows that enables network administrators to continuously monitor Syslog output from their Ally ip100 security appliance.

**Bradford Networks** - New NAC Director product line gives organizations running Microsoft Network Access Protection the power to manage and control guest access to the Internet while validating that guest laptops comply with established network security policies.

**Centrify Corporation** - Centrify DirectControl for Mac OS X, SmartCard Login Option, which enables Mac OS X users to join Microsoft Active Directory environments that require two-factor authentication via smart cards.

**Check Point** - UTM-1 security appliance offers medium-sized businesses and enterprise regional sites complete, multi-layered protection against Internet threats such as spyware, viruses, network attacks and more.

**ConSentry Networks** - The integration of ConSentry's network-based enforcement platform with Microsoft's admission control and endpoint posture check.

**Ecora Software** - New features in its flagship solution Ecora Auditor Professional designed to reduce the high cost of compliance mandates, lower the cost of downtime, increase security, and improve operational efficiency of IT professionals.





**FireEye** - FireEye Central Management System and the FireEye 4200 2.0 appliance that addresses the exploding threat of remotely controlled malicious software or crimeware.

**Greencastle Technology** - Innervue prevents malware and attacks by monitoring the key interfaces between hardware and the software that are needed for software execution.

**HID Global** - Crescendo series smart cards designed to provide out-of-the box, standards-compliant support for thousands of logical access control applications.

**Intellitactics** - Plans to enhance their comprehensive enterprise security management solution, Intellitactics Security Manager.

**Ixia** - New SSL security testing capabilities in its IxLoad- Triple Play test solution result in performance gains of more than 300% and add significant new features to the product.

**Kaspersky Lab** - Kaspersky Anti-Virus Mobile, a product that protects mobile phones using Symbian and Windows Mobile operating systems against mobile malware

**Lockdown Networks** - Lockdown Enforcer, is now shipping with full support for Microsoft Network Access Protection (NAP).

**Netronome Systems** - The Netronome SSL Inspector is designed for security and network appliance manufacturers, enterprise IT organizations and system integrators.

**Ping Identity Corporation** - Version 2 of its consumer authentication framework, PingLogin, is now available for download from its Web site,

**Privaris** - Participation in the RSA SecurID Ready for Authenticators Partner Program - an extension of the trusted RSA Secured Partner Program.

**Red Hat** - A complete PKI solution, Red Hat Certificate System 7.2 provides a security framework that guarantees the identity of users and ensures the privacy of communications in heterogeneous environments.

**Relational Security Corporation** - RSAM v5.0 provides many great enhancements to the existing RSAM v4.5 feature set, while also integrating with Relational Security's powerful new assessment & reporting modules.

**Route1** - MobiNET Aggregation Gateway, a sophisticated appliance-based solution that provides enterprises subscribing to Route1 MobiNET-enabled services, such as remote access, with greater manageability of data traffic that flows across the network.

**SanDisk** - TrustWatch is built around a secure network appliance and a management console, through which IT administrators can easily configure and deploy secured USB flash drives, while preventing information from being copied to unapproved devices.

**Secure Elements** - The C5 Compliance Platform is the industry's first enterprise solution built on open XML standards that enables a range of compliance solutions such as IS control auditing and benchmarking, vulnerability management, and more.

**Shavlik Technologies** - Broad vulnerability management and patch management support for Microsoft Vista clients.

**SignaCert** - Interoperability of its Enterprise Trust Service with Microsoft Network Access Protection, allowing enterprises to measure and verify the integrity of software on devices across IT systems, ensuring greater reliability, manageability, security, and regulatory compliance.

**StarNet Communications** - StarNetSSH, a fully featured suite of connection security tools for Windows-based computers, including Windows Vista.

**StillSecure** - Safe Access now delivers on the promise of 'Complete NAC' which refers to a comprehensive network access control solution that encompasses pre-connect health checks, post-connect monitoring and identity based policies.

**SurfControl** - New Global Alliance Partner Program - alliance partners will be able to deliver high-performance solutions that are complimentary or tightly integrated with SurfControl's secure Internet protection technology.

**Third Brigade** - Deep Security 5, an advanced, host intrusion prevention system that detects and prevents known and zero-day attacks targeting mission critical servers.

**Utimaco** - Support for Windows Vista BitLocker Drive Encryption.

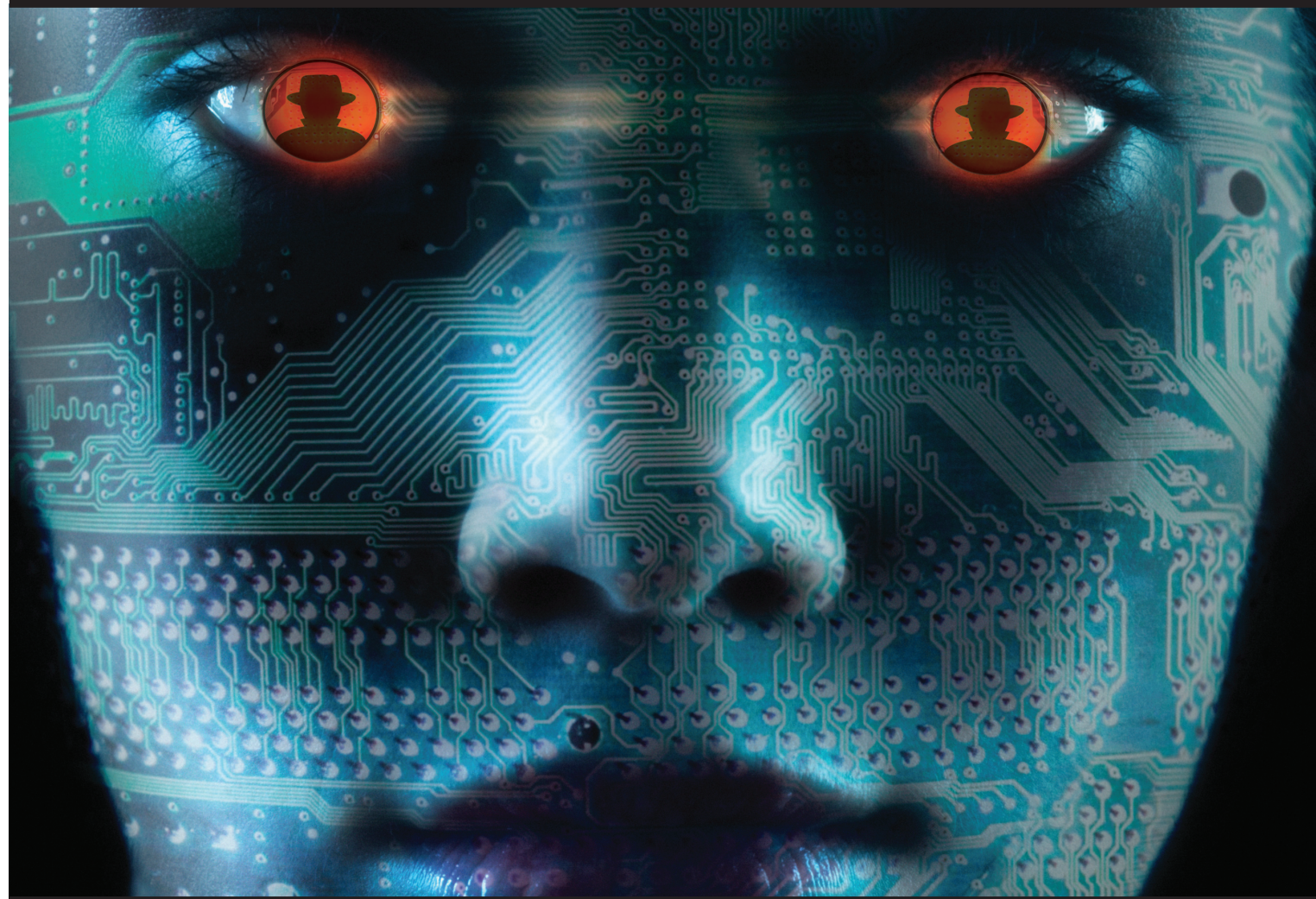
**Vernier Networks** - Support for Microsoft Network Access Protection (NAP) in Vernier's EdgeWall 7000 and 8000 series appliances.

**Voltage Security** - Voltage Security Network, a compelling new software-as-a-service solution

**Webroot Software** - Spy Sweeper Enterprise 3.0 was named "Best Anti-Malware Solution" in the Reader's Trust category of SC Magazine.



# Knowledge & Technology



Come together at Black Hat Europe.

Once again the world's ICT Security Elite gather to share their knowledge and experience with you. This is your chance to meet and network with peers and professionals at this world renown event.

Two days. Ten Classes. Thirty presentations.



## Black Hat® Briefings & Training Europe 2007

27-30 March 2007 • Mövenpick Hotel Amsterdam City Centre

[www.blackhat.com](http://www.blackhat.com)

sponsors

gold

**IOActive™**  
COMPREHENSIVE COMPUTER SECURITY SERVICES

**Lancopé®**

**SecurIST**

**CLUSTIF**

**CYBER SECURITY  
INDUSTRY ALLIANCE**

**eicar**

**Security  
TaskForce**

**WVCA**

**Microsoft®**

**WITNESS**  
SOLID EVIDENCE. INSIGHT.

**GVIB**  
CERTIFICATION  
SOFTWARE DEVELOPERS

**IR6  
FORUM**

**ISECA**

**ISSA**  
INTERNATIONAL SYSTEMS SECURITY ASSOCIATION

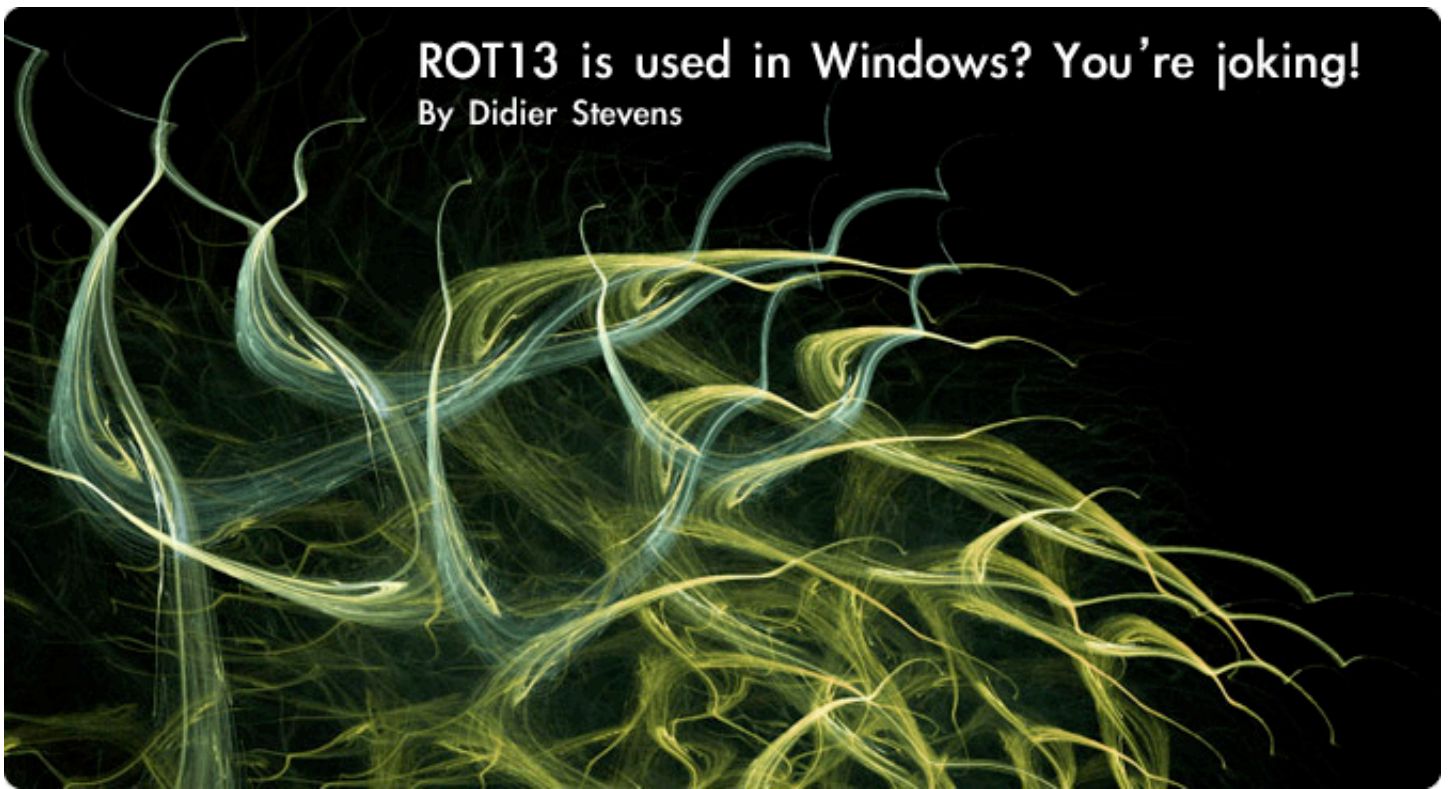
**OWASP**  
The Open Web Application Security Project

**SECURE  
SERVICE  
PLUS**

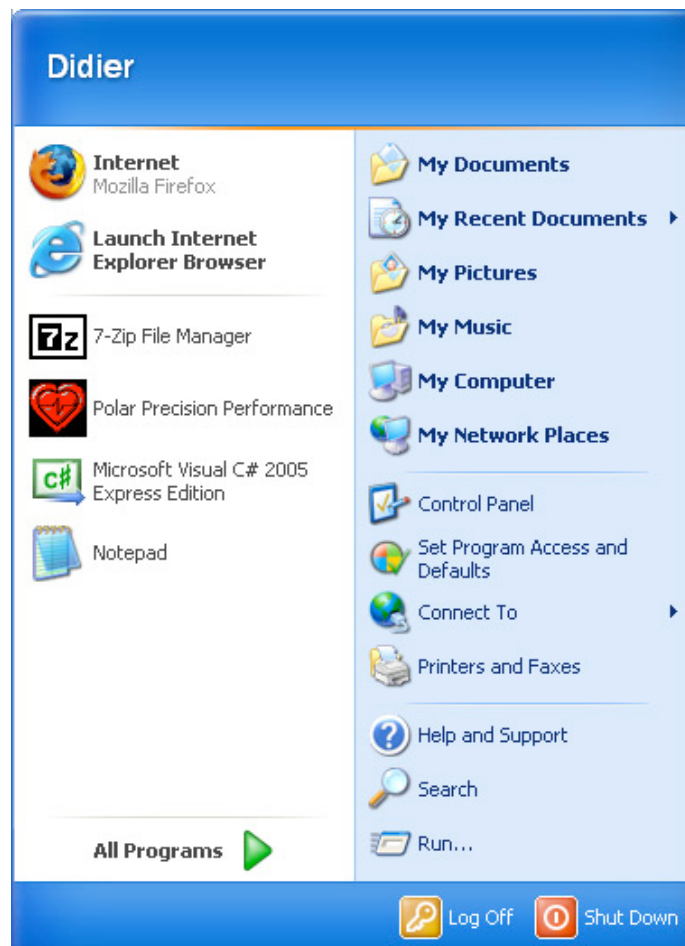
supporting associations

# ROT13 is used in Windows? You're joking!

By Didier Stevens



When Microsoft released Windows XP in late 2001, it introduced a new Start menu with quick access to frequently used programs. The left side of the menu contains two sections, the "pinned list" (at the top) and the Most Frequently Used Programs (MFUP) list (at the bottom). When you monitor the MFUP list in the Start menu, you will notice that it is not only displaying the most frequently used programs, but also new programs that were used recently. This means that there is also a kind of time-stamp involved.



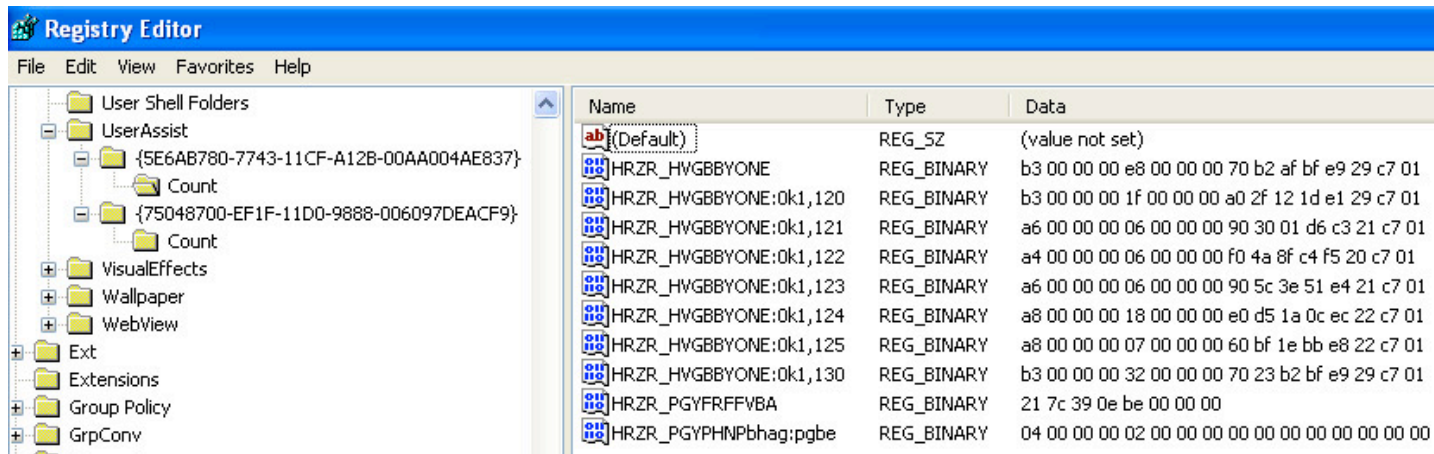


To a programmer, it is clear that the MFUP list can only be maintained by monitoring user activity. This activity has to be logged and persisted somewhere.

I developed a program to display the data of the MFUP list. This data is stored in the regis-

try. Reverse-engineering techniques were required to understand the format of the data (details about this process can be found in my blog).

Microsoft has not published documentation about these registry keys.



## Use in forensic analysis

Now imagine that you are conducting a forensic investigation: you have to compile a report about the activity of user U on workstation W.

One important element of this report is the list of programs executed by user U.

There are several techniques to compile a list of executed programs. One can look at the last access timestamps of the program files on workstation W, or examine the files in the %WINDIR%\Prefetch directory. The problem with these techniques is that they are system wide: one has to deduce from the timing window which user accessed the files. This is relatively simple if there is only one user working on the workstation, but it becomes very difficult on a Terminal Server.

The UserAssist utility helps one to compile a list of executed programs. It reads the MFUP data from the registry found under this key:

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

Notice HKEY\_CURRENT\_USER, it means that this data is user related. It ties activity such as running executables to a specific user.

When started, the UserAssist utility retrieves the data for the current user and displays it.

The display is not refreshed automatically when Windows Explorer updates the registry entries.

To refresh the display, execute the 'Load from local registry' command. But this is not the way you want to use it for a forensic investigation. When you are executing your forensic investigation by the rules of the book, you will image the storage devices of the involved machine(s) and work on a copy of the image.

To extract the HKEY\_CURRENT\_USER registry keys for a particular user from this image, you will have to locate the NTUSER.DAT file. It is located in the C:\Documents and Settings\user\_name directory. There are exceptions to this. If the workstation is a member of a Active Directory domain and roaming profiles are enabled, you can also find the NTUSER.DAT file of domain users (not of local users) on the domain controller or on a dedicated file server.

Be aware that this file will only be up-to-date with a proper logoff, pulling the plug on the workstation will not allow for synchronisation of the roaming profile.

If you find a NTUSER.MAN and no NTUSER.DAT file, you are out of luck: this is the mandatory profile setup by the system administrator. It does not persist changes made by the user. After locating the NTUSER.DAT registry hive, you will have to export the registry entries as a .REG file. The UserAssist utility cannot read registry hive files directly (I will add this feature once I find a suitable open source library), they have to be converted to .REG files.

Follow this procedure to create the .REG file:

- 1) Make a copy of the NTUSER.DAT file of the involved user
- 2) Start Regedit
- 3) Select HKEY\_USERS
- 4) Launch command File/Load Hive...
- 5) Select the copy of the NTUSER.DAT
- 6) Type a Key Name, for example Investigation
- 7) Select HKEY\_USERS\Investigation
- 8) Right-click and launch Export
- 9) Type a file name, for example Investigation
- 10) Launch command File/Unload Hive...

### Recommendations

I recommend working on a copy of NTUSER.DAT, because loading and unload-

ing a registry hive will modify the NTUSER.DAT file and create a NTUSER.DAT.LOG file.

Load Hive is only enabled for keys HKEY\_USERS and HKEY\_LOCAL\_MACHINE

If you need to limit the size of the .REG file, navigate to Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist and export this key instead of the complete registry hive.

Now that you have the exported registry hive as a .REG file, start the UserAssist utility. It will display a table with the commands you have executed, just ignore this for the moment.

Execute these steps to view the UserAssist data:

- 1) Launch Commands / Load from REG file
- 2) Select the .REG file, for example Investigation.reg

All the commands executed by the user are displayed in a table, the meaning of the data in the columns is explained below.

The screenshot shows the UserAssist 2.1.0.0 application window. The title bar reads "UserAssist 2.1.0.0". Below the title bar is a menu bar with "Commands" and "Help". The main area contains a table with the following columns: Key, Index, Name, Unkno..., Session, Counter, and Last. The table lists various system events and user actions, such as UEME\_CTLSESSION, UEME\_CTLCUACount:ctor, UEME\_RUNPIDL, and UEME\_RUNPATH, with their respective session IDs, counters, and timestamps.

Key	Index	Name	Unkno...	Session	Counter	Last
{5E6AB7...	0	UEME_CTLSESSION	238398...	5		
{5E6AB7...	1	UEME_CTLCUACount:ctor		1	2	
{750487...	0	UEME_CTLSESSION	238239...	4		
{750487...	7	UEME_CTLCUACount:ctor		1	2	
{750487...	1	UEME_RUNPIDL:C:\Documents and Settings...		1	14	1/24/2006 4:29:24 PM
{750487...	2	UEME_RUNPIDL:%csidl2%\MSN Explorer.lnk		1	13	1/24/2006 4:29:24 PM
{750487...	3	UEME_RUNPIDL:%csidl2%\Windows Media ...		1	12	1/24/2006 4:29:24 PM
{750487...	4	UEME_RUNPIDL:%csidl2%\Windows Messen...		1	11	1/24/2006 4:29:24 PM
{750487...	5	UEME_RUNPIDL:%csidl2%\Accessories\Tour...		1	10	1/24/2006 4:29:24 PM
{750487...	6	UEME_RUNPIDL:%csidl2%\Accessories\Win...		1	9	1/24/2006 4:29:24 PM
{5E6AB7...	4	UEME_UITOOBAR:0x4,7031		2	1	4/21/2006 4:23:20 PM
{750487...	9	UEME_RUNCPL		4	1	4/25/2006 10:29:01 AM
{750487...	10	UEME_RUNCPL:desk.cpl		4	1	4/25/2006 10:29:01 AM
{750487...	14	UEME_RUNPATH:C:\Program Files\Microsoft...		4	2	4/25/2006 1:05:10 PM
{750487...	11	UEME_RUNPIDL		4	10	4/26/2006 2:24:32 PM
{750487...	13	UEME_RUNPIDL:%csidl2%\Microsoft Visual C...		4	4	4/26/2006 2:24:32 PM
{750487...	15	UEME_RUNPIDL:%csidl2%		4	2	4/26/2006 2:24:32 PM
{750487...	16	UEME_RUNPATH:D:\setup.exe		4	1	4/26/2006 2:55:34 PM
{750487...	18	UEME_RUNPATH:C:\WINDOWS\regedit.exe		4	1	8/2/2006 1:16:03 PM
{750487...	12	UEME_RUNPATH:C:\WINDOWS\system32\...		4	2	8/2/2006 1:17:50 PM
{750487...	17	UEME_RUNPATH:C:\Program Files\Common ...		4	5	8/2/2006 4:54:10 PM
{5E6AB7...	2	UEME_UITOOBAR		5	6	8/2/2006 5:00:14 PM
{5E6AB7...	3	UEME_UITOOBAR:0x1,130		5	5	8/2/2006 5:00:14 PM
{750487...	8	UEME_RUNPATH		4	21	8/3/2006 2:50:54 PM
{750487...	19	UEME_RUNPATH:C:\Documents and Setting...		4	1	8/3/2006 2:50:54 PM

## Key

This value is {5E6AB780-7743-11CF-A12B-00AA004AE837} or {75048700-EF1F-11D0-9888-006097DEACF9}

These are the keys found under the UserAssist registry key, and they are included in the table to distinguish the entries.

## Index

This is a running counter, indicating the sequence of values in the registry. At first, the entries are listed in the sequence they appear in the registry. You can sort columns by clicking on the header. To revert to the original sequence, sort the column Index and then the column Key

## Name

The name of the value registry entry. This references the program that was run. This key is ROT13 encrypted, the displayed name is decrypted.

There is a registry setting to prevent encryption of the log, but the UserAssist utility does not support this setting.

ROT13, also known as the Caesar cipher, is a very simple encryption scheme where each letter is replaced with the letter thirteen places down the alphabet. A becomes N, B becomes O, and so on... For example, UEME\_RUNPATH becomes HRZR\_EHACNGU. I do not know why Microsoft decided to encrypt the UserAssist registry entries with such a simple scheme.

## Unknown

A 4 byte integer, meaning unknown. It appears to be present only for session entries (UEME\_CTLSESSION).

## Session

This is the ID of the session (a 4 byte integer). When an entry is created in the UserAssist registry keys, the session is set equal to the session of the UEME\_CTLSESSION entry. For example, assume the session ID of UEME\_CTLSESSION is 123, and you launch

notepad, then the session ID for the notepad entry will be 123.

## Counter

This is the number of times the program was executed (a 4 byte integer).

## Last

This is the last time the program was executed (an 8 byte datetime). Watch out for time zone differences when importing a REG file from a system with different regional settings. It is important to understand that there is only one entry per executed program: e.g., if notepad is executed twice, there will only be one entry in the table with Counter equal to 2 and Last equal to date and time notepad was last executed.

The result of executing these commands:

Notepad.exe

Calc.exe

Notepad.exe

is this table:

```
"UEME_RUNPATH:C:\Windows\system32\calc.exe", "", "146", "1", "3/01/2007 21:02:33"
```

```
"UEME_RUNPATH:C:\Windows\system32\notepad.exe", "", "146", "2", "3/01/2007 21:02:40"
```

You can save the table as a CSV file. This file can be imported in a spreadsheet program like Excel for further analysis or for inclusion in the forensic analysis report. To save the report, launch Commands / Save and type the name of the CSV file.

## Name entries

The key Names always start with UEME\_.

Examples are:

UEME\_CTLSESSION: session key. This appears to increase with 1 each day you use the computer. I think the 4 first bytes of the binary data (column Unknown) are also a timestamp, but of another format which I've still to understand (it appears to count in units of 53.69 seconds).

UEME\_RUNCPL: an entry created when the control panel is opened. It can be followed by a string to indicate which applet of the control panel was opened, like this entry for the Power Options applet:

UEME\_RUNCPPL:"C:\Windows\system32\powercfg.cpl",Power Options

UEME\_RUNPIDL indicates the execution of a PIDL. A PIDL is a Pointer to an ID List, every item in Explorer's namespace is uniquely identified by its PIDL. For example, executing shortcuts (.lnk) are logged with this entry.

UEME\_UIQCUT is logged for applications launched from the quick launchbar. There is no separate entry with the name or path of the launched application. I think the logic behind this is the following: the UserAssist registry keys are maintained by Windows Explorer to display the MFUP. Applications launched from the quick launchbar have already their "special" place on the Windows GUI, so there is no need to keep additional data about their usage.

More details about the different types of name entries can be found at [tinyurl.com/3y5ob4](http://tinyurl.com/3y5ob4).

### Windows Explorer

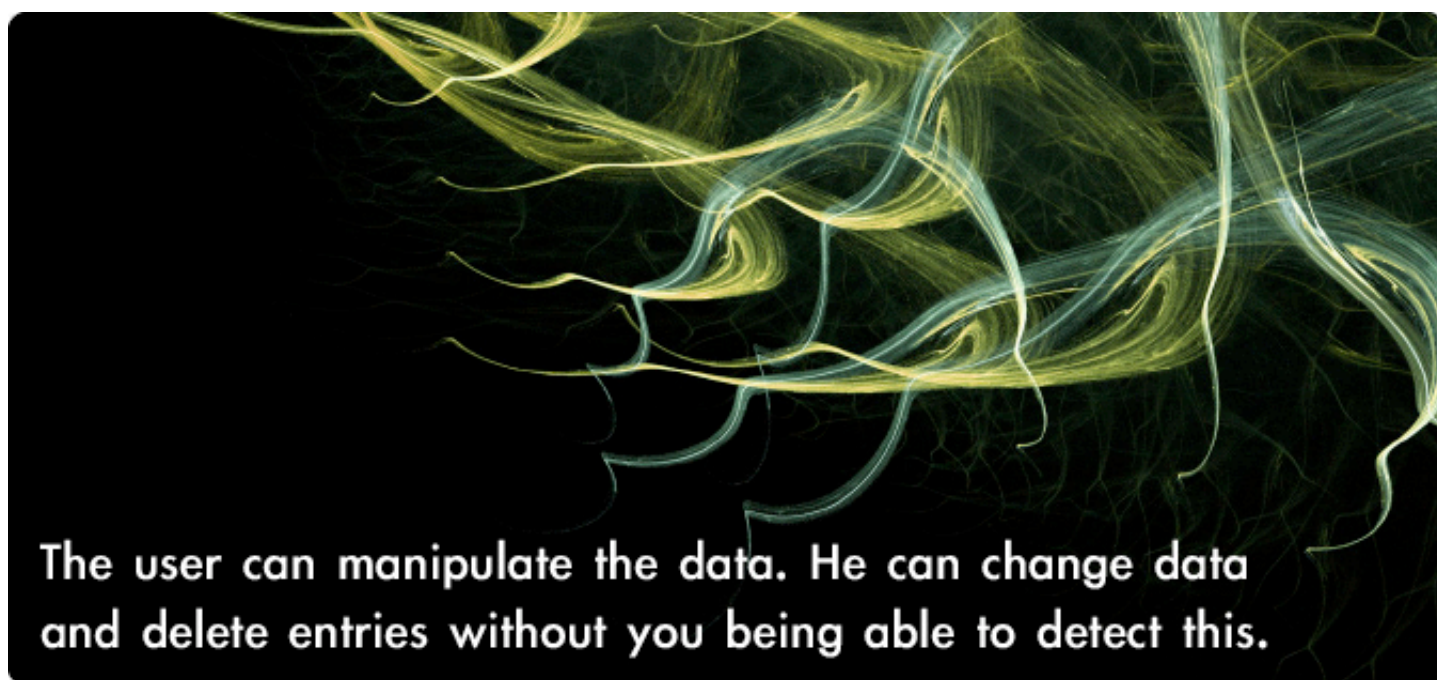
The UserAssist registry keys are maintained by Windows Explorer. You are probably famil-

iar with Windows Explorer as the utility you use to explore drives, but it does a lot more. Windows Explorer is also the standard shell in Windows: it is the program that displays the Start Menu, the Task Bar and all those other GUI elements that make up your desktop.

Here is a fun little experiment to demonstrate this (save all important work first):

- 1) Start the Windows Task Manager (CTRL+SHIFT+ESCAPE)
- 2) Select the Processes tab and search explorer.exe
- 3) Select explorer.exe and click on the End Process button
- 4) Confirm
- 5) Result: the start menu and taskbar are gone
- 6) Launch File/New Task(Run...)
- 7) Type explorer and execute, this will get your Windows Shell back.

The fact that the UserAssist registry keys are maintained by Windows Explorer has two important implications.



First implication: only programs that are launched via Windows Explorer are counted in the UserAssist keys. Programs launched by the Windows Console (CMD.EXE), a service or by any other means are not logged. If the user starts a Windows Console, you will see this in the UserAssist keys, but all programs

executed from this Windows Console will not appear in the UserAssist registry data.

Second implication: Windows Explorer runs under the user account and since Windows Explorer needs full access to the UserAssist registry keys, the user has also full access.

The user can manipulate the data. He can change data and delete entries without you being able to detect this. The way that the data is encoded in the registry does not make it easy for the user to manipulate individual entries, but the UserAssist utility also provides functions to do this.

In other words, the integrity of the UserAssist data is not guaranteed. One can only rely on the ignorance of the user about the UserAssist registry entries to maintain the integrity of the data.

There are also settings to disable the logging of commands under the UserAssist registry key: create registry key Settings\NoLog (under the UserAssist registry key) and set it equal to 1. You will have to restart Windows Explorer before this setting becomes effective. The UserAssist utility provides the Logging Disabled command to toggle this key. Re-enabling logging requires the deletion of the Settings\NoLog registry key and the restart of Windows Explorer.

### Windows Live CDs

I have also packaged the UserAssist utility in a Bart's PE plugin that I have tested with the Ultimate Boot CD For Windows (UBCD4Win). From their website: UBCD4Win is a bootable CD which contains software that allows you to repair, restore, or diagnose almost any computer problem. Their goal is to be the ultimate free hardware and software diagnostic tool. All software included in UBCD4Win are freeware utilities for Windows. UBCD4Win is based on Bart's PE. Bart's PE builds a Windows "pre-install" environment CD, basically Windows booted from CD.

Windows Live CDs are a popular troubleshooting and forensic investigation tool, they allow you to boot a (Windows) PC from a CD.

Bart Lagerweij developed BartPE, a tool to create a Windows Live CD (a Windows "pre-install" environment CD), and several people build their own tools based on his work. The

Ultimate Boot CD for Windows is based on BartPE.

Bart's PE has an open architecture, you can integrate your own tools by making a dedicated plugin. My UserAssist utility uses the Microsoft .NET Framework 2.0, which is not supported by BartPE. You need to add Colin Finck's Microsoft .NET Framework 2.0 plugin to the Ultimate Boot CD for Windows plugins to use my plugin.

Details on how to make your own UBCD4Win CD with my UserAssist Utility plugin can be found at [tinyurl.com/2fdl8l](http://tinyurl.com/2fdl8l). It has also a video showing you the UserAssist utility in action.

### Closing remarks

The UserAssist utility has also been tested with success on Windows Vista. Apparently, Microsoft did not make changes to the format of the UserAssist registry entries, they still exist and they contain the same data as in Windows XP.

My UserAssist utility is not the only program that displays and manipulates the UserAssist registry keys, but it's the only one that displays the counters, timestamps and session IDs in a Windows GUI program.

Jeremy Bryan Smith has developed a Windows GUI program that will decode and display the UserAssist registry entries, but it does not decode the binary data containing the counters, timestamps and session IDs ([tinyurl.com/3y5ob4](http://tinyurl.com/3y5ob4)).

Harlan Carvey has developed ProScripts to dump the UserAssist registry keys with the decoded name and timestamp ([tinyurl.com/3d79zu](http://tinyurl.com/3d79zu)).

The UserAssist utility was developed with Microsoft Visual C# 2005 Express, a free download from Microsoft. The source code is included when you download the UserAssist utility, you are free to adapt this code.

Didier Stevens (CISSP, MCSD .NET, MCSE/Security) is an IT Security Consultant currently working at a large Belgian financial corporation. He is employed by Contraste Europe NV, an IT Consulting Services company ([www.contraste.com](http://www.contraste.com)). You can find the UserAssist utility and other open source security tools on his IT security related blog at [DidierStevens.com](http://DidierStevens.com).



Information security – it's not a game!



## EVER FEEL LIKE YOU ARE FIGHTING A BATTLE...

- ▶ to secure and protect your remote workforce?
- ▶ to justify and get value from compliance expenditure?
- ▶ to safeguard the identity and privacy of your customers and staff?

Attend **Infosecurity Europe 2007** and discover practical strategies, solutions and technologies to defend your business.

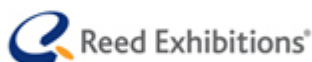
**Register FREE\* now at [www.infosec.co.uk](http://www.infosec.co.uk)**

EUROPE'S NO.1 DEDICATED INFORMATION SECURITY EVENT



24 – 26TH APRIL 2007

GRAND HALL OLYMPIA, LONDON, UK.



\*Visitors not registered by 5pm on the 20th April 2007 will be charged a £20 entrance fee



SECURE

## Data security beyond PCI compliance - protecting sensitive data in a distributed environment

By Ulf T. Mattsson

**For many years external security threats received more attention than internal ones, but the focus has changed. Worms, viruses and the external hacker were once perceived as the biggest threats to computer systems. What is often overlooked is the potential for a trusted individual with special privileges or access to steal or modify data. While viruses and worms are serious, attacks perpetrated by people with trusted insider status—employees, ex-employees, contractors and business partners—pose a far greater threat to organizations in terms of potential cost per occurrence and total potential cost than attacks mounted from outside.**

Well documented breaches have heightened the public's – and regulatory agencies' - concerns about how well companies are securing consumer-specific information captured at the point-of-acquisition. Extended partnerships lead to that more and more tasks will be performed outside the physical boundaries of company facilities which will add another level of due diligence we must take into account.

### **Insider attacks hurt disproportionately**

The reason why insider attacks hurt disproportionately is that insiders can and will take advantage of trust and physical access. In general, users and computers accessing re-

sources on the local area network of the company are deemed trusted. Practically, we do not firmly restrict their activities because an attempt to control these trusted users too closely will impede the free flow of business. And, obviously, once an attacker has physical control of an asset, that asset can no longer be protected from the attacker. While databases often are protected by perimeter security measures and built in RDBMS (Relational Database Management Systems) security functionality, they are exposed to legitimate internal users at some degree. Due to the fragmented distribution of database environments, real time patch management, granular auditing, vulnerability assessment, and

intrusion detection become hard to achieve. With the growing percentage of internal intrusion incidents in the industry and tougher regulatory and compliance requirements, companies are facing tough challenges to both protect their sensitive data against internal threats and meet regulatory and compliance requirements.

### Threats from people working inside the enterprise firewall

Threats to your databases can come from hackers, attackers external to your network, or from the numerous groups of people working inside the enterprise firewall. While firewalls

are indispensable protection for the network for keeping people out, today's focus on e-business applications is more about letting the right people into your network. Consequently, as databases become networked in more complex e-business applications, their vulnerability to attack grows. Without extra precautions taken to secure the confidential data in databases, your company's privacy is at risk. Taking the right security approach enables your e-business and protects your critical data. Threats that the system would be likely to face, for reasons that we will describe below, are 1) malicious insiders and 2) technically knowledgeable outsiders motivated by profit.

**Threats to your databases can come from hackers, attackers external to your network, or from the numerous groups of people working inside the enterprise firewall.**

### Outside threats

A second category of threat that must not be neglected is outsiders. Although their motivation is far more likely to be profit rather than to harm The Company's brand reputation, it is important to consider them in the analysis. At least two feasible scenarios exist that could provide an outsider with a vector for launching an attack on the Store Security System; both scenarios involve poorly configured store location networks. In the first scenario, a Company store location network is miss-configured such that it is directly accessible to the external Internet at large. In this scenario, an opportunistic attacker might accidentally (or otherwise) find the The Company network and begin an attack.

The second scenario would be involving a miss-configured store location network that inadvertently allows hotel guest data traffic to traverse the same network that the business systems, including the Local Security Server itself, resides on. In both cases, a successful attack on the Store Security System itself would need to include a significant additional effort to explore, analyze, and learn the operation of the Store Security System. Such an attack might well take months or more, but considering the five-year life-span of the Store

Security System, it would be wise to treat it as soon as possible, however unlikely.

### Other threats

Although we consider the above threats to be the most likely, they are in no way the only ones that exist. Similarly, other motivations for attacking the Store Security System may well also exist. The largest risk of successful attacks by these miscreants is denial of service and other forms of general havoc. Certainly, not something to be ignored, but the business impact to The Company is not likely to be as significant as in either of the previous scenarios.

### Organizations are reacting slowly

For companies to avoid the nightmare of a public breach of customer privacy, organizational accountability must be established and supported by policies and processes that enforce compliance to standards and regulations. Many states in the U.S. have adopted rigid regulations about disclosure of consumer data security breaches, and financial networks such as VISA and MasterCard will impose harsh financial consequences if a breach occurs.



## The Payment Card Industry (PCI) Data Security Standard

The PCI Data Security Standard is a set of collaborative security requirements for the protection of credit card transactions and cardholder data for all brands. The PCI standard incorporates sound and necessary security practices, such as continuous data access monitoring and control; assessments; and auditing. PCI Compliance is mandatory for any business that stores, processes, or transmits data. The PCI Security Standards Council ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)) is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. The PCI Security Standards Council's mission is to enhance payment account data security by fostering broad adoption of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International.

### PCI and beyond

Industry standards, such as PCI, have been developed to prescribe best practices for ensuring the privacy and integrity of consumer-specific information. Now is the time to address the organizational and technical issues surrounding the effective use and security of consumer-specific information. Those companies that effectively use this information to drive customer value while at the same time ensuring its privacy and integrity, will be rewarded with increased customer loyalty and improved earnings. Failure to secure consumer-specific data will result in brand erosion and crippling scrutiny from regulatory agencies and financial networks.

### Examples from the retail industry

This article will review examples and use cases from the retail industry to illustrate security principles applied in a highly distributed and exposed environment such as retail 'Store Systems' and distributed 'Store Security Systems' that are described below. Organizations today have the ability to use the information captured from points-of-sale to deliver compelling value to consumers, either as indi-

viduals or as members of communities. In many ways, this is a return to a pre-mass business concept, before consumers began to be treated as an amalgam of many different demographics, lifestyles, and buying preferences. The difference today is that organizations can achieve a level of intimacy and still perform as a large scale enterprise. Information technology makes this possible, and winners are using information and technology to better understand customer preferences and to plan their business strategies accordingly. However, such strategies do not come without risk. Today, enterprises must demonstrate compliance with industry and government regulations charging businesses with ensuring the security of this sensitive information. At the same time, databases are at increased risk from both internal and external attackers who no longer simply seek notoriety but, instead, want financial rewards.

## Primary categories of threats

### Database attacks are rising

Database attacks can have direct and severe economic consequences. Database attacks are rising and they can result in the loss or compromise of information critical to running your business day-to-day, from inventory and billing data to customer data and human-resources information. In addition databases are holding increasing amounts of sensitive information on behalf of your customers — financial records, healthcare histories, order histories, credit card and Social Security numbers. Any loss will be an operational and customer relationship disaster as well as a financial nightmare. Do you know how many employees have access to your databases? If you are using passwords for administrators, how are passwords being stored? Do you have security policies in place that include auditing your database security and monitoring for suspicious activity?

### Two primary categories of insider threats

There are two primary categories of insider threats to a typical Store System scenario: The Company employees and franchisee employees. Either or both may be enlisted by an outsider(s) or may enlist the help of an outsider in order to attack the Store Security

System. Their motivations are likely to be either profit or to cause harm to The Company by way of either a direct denial of revenue and/or by tarnishing The Company brand with the bad publicity that would almost inevitably be the result of a successful compromise. In any of the above scenarios, it should be expected that the insider will be able to learn how the Store Security System functions to a level at least significant enough to attempt an attack.

### Security breaches within organizations' technology environments

New technologies make it increasingly feasible for organizations to relate item movement to specific customer information, and to analyze that relationship to develop business strategies that are more relevant to individual

customers' needs. However, consumers, government regulatory agencies, and financial networks are growing increasingly concerned that consumer privacy is jeopardized by the potential of security breaches within organizations' technology environments.

### Dealing with new and innovative intrusions

There are no guarantees that any one approach will be able to deal with new and innovative intrusions in increasingly complex technical and business environments. However, implementation of an integrated security program which is continuously audited and monitored provides the multiple layers of protection needed to maximize protection as well as historical information to support management decision-making and future policy decisions.

**The primary problem with many compliance initiatives is a focus on existing security infrastructure that addresses only the network and server software threats.**

## More sophisticated data attacks

### Insight into data-level attacks

The primary problem with many compliance initiatives is a focus on existing security infrastructure that addresses only the network and server software threats. However the data security capabilities required to be compliant goes far beyond these technologies. Network and server software protections (network firewalls, Intrusion Prevention Systems), while important, provide no insight into data-level attacks targeted directly against a database or indirectly via a web application. Regulatory compliance requires an understanding of who is allowed to access sensitive information. Regulatory compliance requires an understanding of who is allowed to access sensitive information? From where did they access information? When was data accessed? How was data used? The bottom line is that data security requires a new approach that extends the breadth and depth of IT's ability to secure information. Most existing monitoring solutions focus on network-level issues or web traffic;

furthermore, these solutions tend to be targeted at the perimeter and thus do not inspect and audit internal traffic, partner/VPN traffic, or encrypted traffic. Finally, these solutions do not understand the complex protocols used by databases and database applications—a severe handicap when trying to detect threats to the database.

### Limitations in defending data attacks

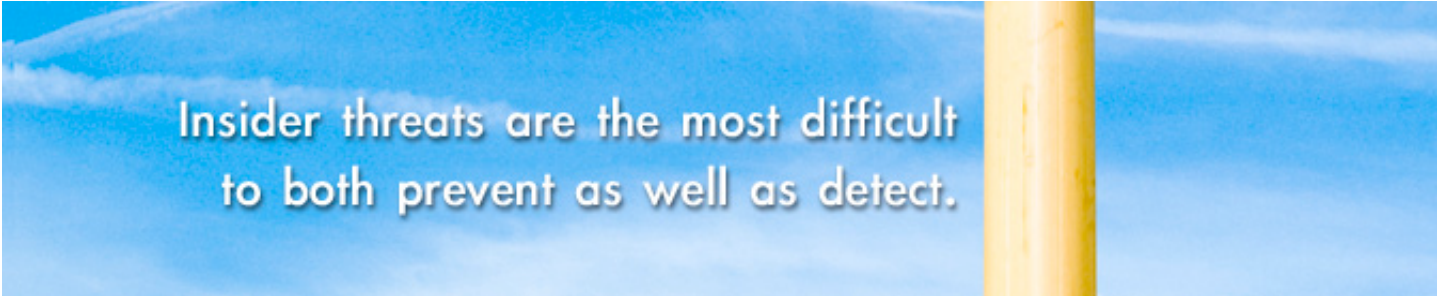
Traditional database security mechanisms are very limited in defending successful data attacks. Authorized but malicious transactions can make a database useless by impairing its integrity and availability. The proposed solution offers the ability to detect misuse and subversion through the direct monitoring of database operations inside the database host, providing an important compliment to host-based and network-based surveillance. Suites of the proposed solution may be deployed throughout a network, and their alarms managed, correlated, and acted on by remote or local subscribing security services, thus helping to address issues of decentralized management.

## Traditional approaches to data security

Traditional approaches to security have relied on the application to enforce access control for application users, the database administrator to maintain both database and application availability and network routers and firewalls to restrict access to the database and application. While problems such as the insider threat are certainly not new, the potential for abuse has never been greater due to the amount of sensitive information being collected and the willingness of criminal organizations and individuals to pay for such information. The nature of the information threat today requires more sophisticated security mechanisms within the database.

## The technology enablers

Although organizations are moving aggressively to use the Customer dimension to fine tune their business strategies, they are moving much less aggressively to utilize the technologies available to them to mitigate risks associated with the use of that data. This is not for want of technology answers, however. Technologies such as data encryption, access logging and proactive forensic analysis, penetration testing tools and services, and other techniques are available now. One of the most effective ways to can avoid a serious security breach is to protect the data in your databases. There are many aspects to information security, but the heart of securing credit card-based transactions focuses on databases.



Insider threats are the most difficult to both prevent as well as detect.

## A defense-in-depth strategy

Part of the problem lies in the fact that most companies solely implement perimeter-based security solutions, even though the greatest threats are from internal sources. Additionally, companies implement network-based security solutions that are designed to protect network resources, despite the fact that the information is more often the target of the attack.

Recent development in information-based security solutions addresses a defense-in-depth strategy and is independent of the platform or the database that it protects. As organizations continue to move towards digital commerce and electronic supply chain management, the value of their electronic information has increased correspondingly and the potential threats that could compromise it have multiplied.

With the advent of networking, enterprise-critical applications, multi-tiered architectures and web access, approaches to security have become far more sophisticated.

## "Checks and balances" to reduce successful attacks

Traditionally, insider threats are the most difficult to both prevent as well as detect. Further, it is likely that no technology solution will be adequate to safeguard against every possible attack scenario. However, other industries (notably the financial services industry) have handled insider threats for centuries. In situations where known technology weaknesses are recognized, the financial services industry typically compensates by instituting procedural "checks and balances" to greatly reduce the likelihood of successful attacks. In most cases, these checks and balances are in the form of separation of duties and multiple points of (possible) failure, the result being that no single employee can easily compromise an entire system. Instead, a conspiracy would need to exist, which is deemed to be much less likely. That same methodology of separation of duties is leveraged significantly in the recommendations made in this document in circumstances where weak points exist in the Store Security System Architecture out of necessity.

## Controlling DBA access to data

Database administrators play a critical role in maintaining the database. Performance, 24x7 availability and backup/recovery are all part of the DBA job description. These responsibilities place the job of DBA among the most trusted in the enterprise. However, the DBA shouldn't need to access application data residing within the database. The same rule should apply to highly privileged users, such as application owners. These highly privileged users shouldn't be allowed to use their privileges to access application data outside their application.

## Multiple layers of protection to maximize protection

There are no guarantees that any one approach will be able to deal with new and innovative intrusions in increasingly complex technical and business environments. However, implementation of an integrated security program which is continuously audited and monitored provides the multiple layers of protection needed to maximize protection as well as historical information to support management decision-making and future policy decisions.

## The "principle of least privilege" is ineffective

A small group of individuals perpetrate the maximum damage. Unfortunately, the problem with managing this threat effectively is that traditional and foundational security concepts—particularly that of the "principle of least privilege"—are ineffective. In computing, the principle of least privilege holds that a user is given the minimum possible privileges necessary to permit an action, thereby reducing the risk that excessive actions will negatively affect the system. In the real world this principle would mean that you are reducing the ability for IT administrators to do their jobs quickly and effectively.

## Shield your data from malicious acts and mistakes

The scenario is simple: a user has rights to query the database's customer table. He usually queries one customer at a time through the application interface, but one night, he

stays late, dumps the entire customer table into a text file, and copies it to a USB drive. This type of activity is called privilege abuse, and no database vendor has built-in protection against it. In fact, although network administrators have enjoyed firewalls for years, database administrators have been left out in the cold.

## Vulnerability assessment scanners

Vulnerability assessment scanners discover database applications within your infrastructure and assess their security strength two primary application tiers - application / middleware, and back-end databases. It locates, examines, reports, and fixes security holes and miss-configurations. As a result, enterprises can proactively harden their database applications while at the same time improving and simplifying routine audits.

## Database scanners

Database scanners are a specialized tool used specifically to identify vulnerabilities in database applications. In addition to performing some external functions like password cracking, the tools also examine the internal configuration of the database for possible exploitable vulnerabilities. Database scanning tools discover vulnerabilities through the following functions. Here are some examples:

- Passwords
- Default account vulnerabilities
- Logon hours violations
- Account permissions
- Role permissions
- Unauthorized object owners
- Remote login and servers
- System table permissions
- Extended stored procedures
- Cross database ownership chining
- Authentication
- Login attacks
- Stale login IDs
- Security of admin accounts
- Excessive admin actions
- Passwords
- Password aging
- Auditing trail
- Auditing configuration
- Buffer overflows in user name
- Buffer overflows in database link

## Protect data at rest and in transit

### Good security practice

Good security practice protects sensitive data as it is transferred over the network (including internal networks) and at rest. Once the secure communication points are terminated, typically at the network perimeter, secure transports are seldom used within the enterprise. Consequently, information that has been transmitted is in the clear and critical data is left unprotected. One option to solve this problem and deliver a secure data privacy solution is to selectively parse data after the secure communication is terminated and encrypt sensitive data elements at the SSL/Web layer. Doing so allows enterprises to choose at a very granular level (usernames, passwords, etc.) sensitive data and secure it throughout the enterprise. Application-LAYER encryption and mature Database-Layer encryption solutions allow enterprises to selectively encrypt granular data into a format that

can easily be passed between applications and databases without changing the data.

### Enable a strong security framework

Application-layer encryption allows enterprises to selectively encrypt granular data within application logic. This solution can also provide a strong security framework if designed correctly to leverage standard application cryptographic APIs such as JCE (Java-based applications), MS-CAPI (Microsoft-based applications), and other interfaces. Because this solution interfaces with the application, it provides a flexible framework that allows an enterprise to decide where in the business logic the encryption/decryption should occur. This type of solution is well suited for data elements that are processed, authorized, and manipulated at the application tier. If deployed correctly, application-layer encryption protects data against storage attacks, theft of storage media, application-layer compromises, file level attacks and database attacks.

**Good security practice protects sensitive data as it is transferred over the network (including internal networks) and at rest.**

### Allowing flexible and fine-grained control

The application usually understands which user is trying to access a given piece of data and can be programmed to understand a security policy and enforce it in the context of the application data. This can allow for flexible and fine-grained control of data access while ensuring that the critical data is encrypted before it reaches the database.

### The sooner the encryption occurs, the more secure

Due to distributed business logic in application and database environments, it is required to be able to encrypt and decrypt data at different points in the network and at different system layers, including the database layer. Encryption performed by the DBMS can protect data at rest, but you must decide if you also require protection for data while it's moving between the applications and the database

and between different applications and data stores. How about while being processed in the application itself particularly if the application may cache the data for some period. Sending sensitive information over the Internet or within your corporate network as clear text, defeats the point of encrypting the text in the database to provide data privacy. An Enterprise level Data Security Management solution can provide the needed key management for this solution. Encryption of data fields can be performed when entering data at the application layer and decrypted down stream at the DBMS layer.

### Continuous data protection

A mature solution will protect data at rest, and also while it's moving between the applications and the database and between different applications and data stores. This solution will protect data fields or files while being transported in the data flow between applications

and particularly for applications that cache the data for some period in temporary files, tables and FTP transfers. A solution should be based on industry accepted encryption standard such as AES 256 bit and allow ways to minimize the changes to the data format and/or length. Organizations typically have many third party and legacy applications in which they can not alter the DB schema so a high level of transparency can be extremely important. If the solution is not based on industry accepted encryption standard it can be strengthened by an additional layer of strong file level encryption to protect the data at rest.

Example of complementing traditional database solutions:

- Continuous encryption at the distributed end points including store systems all the way to the central systems
- Continuous encryption centrally across a few selected applications
- Transparent encryption centrally across major applications

### Decrease the encryption overhead

There is a multitude of architectures and techniques to improve performance: the alternatives fall into two broad categories – alternative topologies to decrease encryption overhead and techniques to limit the number of encryption operations.

In addition, performance and security, in real-world scenarios, are complex issues and experts should be used who understand all available options and the impact for each particular customer environment.

## Data encryption vs. compensating controls

### The effectiveness of compensating controls

Compensating controls may be considered when an organization cannot meet a technical specification of a requirement, but has sufficiently mitigated the associated risk. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configura-

tion of the control. Organizations should be aware that a particular compensating control will not be effective in all environments. Each compensating control must be thoroughly evaluated after implementation to ensure effectiveness. For organizations unable to render sensitive data unreadable (for example, by encryption) due to technical constraints or business limitations, compensating controls may be considered. The basic conclusion from this analysis is that a combination of application firewalls, plus the use of data access monitoring and logging may, if effectively applied not provide reasonable equivalency for the use of data encryption across the enterprise since such a combination of controls does have multiple weak spots, when it comes to preventing damage from careless behavior of employees or weak procedures in development and separation of duties.

### Perform a risk analysis before using compensating controls

Only organizations that have undertaken a risk analysis and have legitimate technological or documented business constraints should consider the use of compensating controls to achieve protection.

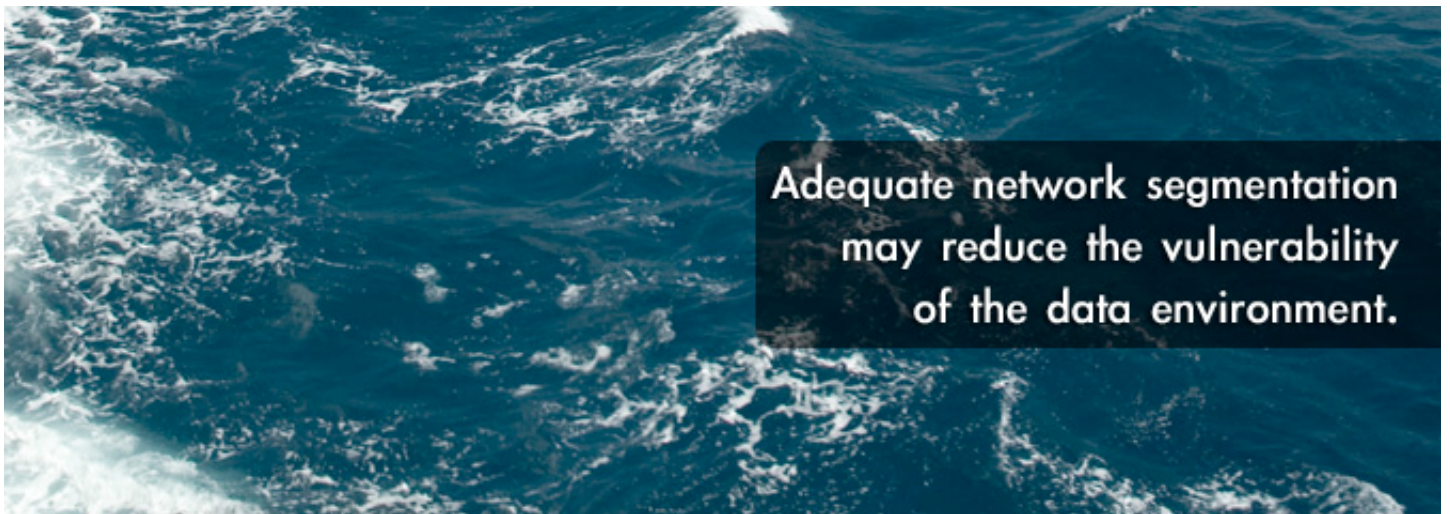
Organizations that consider compensating controls for rendering sensitive data unreadable must understand the risk to the data posed by maintaining readable data. Generally, the controls must provide additional protection to mitigate any additional risk posed by maintaining readable data. Compensating controls should consist of a comprehensive set of controls covering additional segmentation/abstraction (for example, at the network-layer), with an ability to restrict access to data or databases based on IP address/Mac address, application/service, user accounts/groups, Data type (packet filtering), restrict logical access to the database, control logical access to the database (providing separation of duties) and prevent/detect common application or database attacks (for example, SQL injection).

### Example of compensating controls

Currently there are multiple different database segments based in different geographic locations that require administration.

This environment is difficult to administer due to "over segregation", sometimes people have to break "other" rules to administer effectively. Many security/auditing tasks have to be duplicated for every environment where database resides. We need to explore the viability of this approach. The database only network segment(s) have advantages including centralized entry point to manage and monitor all activity, administrative tools can effectively manage security/auditing tasks, database environments are brought together, in a reduced number of environments, in "back office", and separate databases from application further

reducing access to environments. Adequate network segmentation, which isolates systems that store, process, or transmit sensitive data from those that do not, may reduce the vulnerability of the data environment. Network components include firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include but web, database, authentication, mail, proxy, and DNS. Applications include all purchased and custom applications, including internal and external (Internet) applications.



Adequate network segmentation may reduce the vulnerability of the data environment.

## Data intrusion prevention

### The inability to detect novel intrusive attempts

Intrusion detection systems include three basically different approaches, host based, network based, and procedural based detection. The first two have been extremely popular in the commercial market for a number of years now because they are relatively simple to use, understand and maintain. However, they fall prey to a number of shortcomings such as scaling with increased traffic requirements, use of complex and false positive prone signature databases, and their inability to detect novel intrusive attempts. The complexity of this task was dramatically increased by the introduction of multi-platform integrated software solutions, the proliferation of remote access methods and the development of applications to support an increasing number of business processes. In the "good old days", files and databases contained fewer types of information (e.g., payroll or accounting data) stored in centralized locations, which could

only be accessed, by a limited number of individuals using a handful of controlled access methods.

### Host-based intrusion detection systems (HIDS)

HIDS have their own limitations with regards to database protection. Most HIDS systems operate by either audit trail inspection or observation of system modifications; as such, they are only able to inspect those behaviors that are logged by applications or those activities that exhibit behavior on the host for which detection signatures can be created (e.g. modifications to key system files or settings, etc.).

Unfortunately, malicious queries to a database (e.g. to obtain all password/credit card data) will generate no such log entries or detectable behaviors for a HIDS to observe. As far as the database is concerned, a malicious query is just as valid as any legitimate query – it just references different data.

## Network intrusion protection systems

Traditional network-level security solutions like Network Intrusion Protection Systems (NIPS) and firewalls are designed to detect hacking attacks and exploits. Security vendors author and distribute signatures to detect common attacks such as malformed packets, buffer overflows, attempts to download UNIX password files, and zombie control communications. These signatures are produced based on analysis of known exploit tools and known operating system and application vulnerabilities, ensuring they can detect a wide variety of attacks across a diverse set of customer networks. Unfortunately, many valid database attack scenarios involve a legitimate user issuing legitimate looking commands to the database; typical database attacks do not require exploit tools or the transmission of malformed packets. All the attacker has to do is log in with a sufficiently privileged account and issue syntactically correct queries to the database. There may be nothing overtly wrong with such a malicious query other than it may attempt to access more than the usual amount of information. Consequently, such a query would not be caught by a network-based intrusion detection or prevention solution.

## Transaction level methods cannot handle OS level attacks

As more types of information were migrated to electronic formats (and ever more databases proliferated, often with little planning), there was a simultaneous increase in the number of users, access methods, data flows among components and the complexity of the underlying technology infrastructure. Add to this the demand from users for ever more sophisticated uses of information (data mining, CRM, etc.) which are still evolving and the management's enhanced awareness of the value of its information, and it is safe to say that the price of poker has gone up. Database intrusion tolerance can mainly be enforced at two possible levels: operating system (OS) level and transaction level. Although transaction level methods cannot handle OS level attacks, it is shown that in many applications where attacks are enforced mainly through malicious transactions transaction level methods can tolerate intrusions in a much more effective and efficient way.

## Database attack detection complements traditional security measures

Database attack detection augments and complements traditional security measures such as access controls, encryption, scanners, and network and host security. Database attack detection works by examining each SQL command or query that is sent to a database (typically across a network) and then verifying whether that query is malicious or not. It works in real-time or near real-time, and it detects malicious attacks from both internal and external sources. For example, consider what would happen if an attacker were to compromise a web server and then issue a perfectly valid query and it will be executed by the database without a second thought; however, this query has the ability to compromise thousands of credit card numbers from the database. Such a query would not likely be issued by a legitimate client application; as described below, with proper training a database attack detection system could easily identify this query as an attack, block the request, and alert the administrator.

## Limit authorized usage of data is necessary to avoid breaches

Putting limits on authorized usage of data is necessary to avoid breaches from the inside. Much like an ATM machine will limit the amount of money a person can take out of their own account, it is important to be able to set the limits on authorized use as part of data security policy. The data intrusion prevention system respond to threats by notifying the access control system to alter the security policy, for example by altering authorization and denying the access request before any information is transmitted to the user. Access rates may be defined as the number of records a user may access at one time, or the number of records accessed over a certain period of time. Results may address a single query exceeding the allowed limit, or a number of smaller queries, individually allowed, but when aggregated, blocked. This method allows for a real time prevention of intrusion by letting the intrusion detection process interact directly with the access control system, and change the user authority dynamically as a result of the detected intrusion.



A variation of conventional intrusion detection is detection of specific patterns of information access, deemed to signify that an intrusion is taking place, even though the user is authorized to access the information.

### The intrusion detection profile

By defining an intrusion detection profile, with an item access rate, associating each user with one of the profiles, receiving a query from a user, comparing a result of the query with the item access rates defined in the profile associated with the user, determining whether the query result exceeds the item access rates, and in that case notifying the access control system to alter the user authorization, thereby making the received request an unauthorized request, before the result is transmitted to the user. The result of a query is evaluated before it is transmitted to the user. This allows for a real time prevention of intrusion, where the attack is stopped even before it is completed. This is possible by letting the intrusion detection process interact directly with

the access control system, and change the user authority dynamically as a result of the detected intrusion. The item access rates can be defined based the number of rows a user may access from an item, e.g. a column in a database table, at one time, or over a certain period of time. In a preferred implementation, the method further comprises accumulating results from performed queries in a record, and determining whether the accumulated results exceed any one of the item access rates. The effect is that on one hand, a single query exceeding the allowed limit can be prevented, but so can a number of smaller queries, each one on its on being allowed, but when accumulated not being allowed. It should be noted that the accepted item access rates not necessarily are restricted to only one user. On the contrary, it is possible to associate an item access rate to a group of users, such as users belonging to the same access role (which defines the user's level of security), or connected to the same server. The result will be restricting the queries accepted from a group of users at one time or over a period of time.

**A mature Intelligent Escalation recognizes evolving application threats and automatically triggers application protection.**

### Inference detection and selective analysis

The user, role and server entities are not exclusive of other entities which might benefit from a security policy. Items subject to item access rate checking are marked in the policy, so that any query concerning the items automatically can trigger the intrusion detection process. This is especially advantageous if only a few items are intrusion sensitive, in which case most queries are not directed to such items. The selective activation of the intrusion detection will then save time and processor power. The intrusion detection policy further includes at least one inference pattern, and results from performed queries are accumulated in a record, which is compared to the inference pattern, in order to determine whether a combination of accesses in the record match the inference policy, and in that case the access control system is notified to alter the user authorization, thereby making the received request an unauthorized request,

before the result is transmitted to the user. This implementation provides a second type of intrusion detection, based on inference patterns, again resulting in a real time prevention of intrusion.

### Intelligent protection escalation

A mature Intelligent Escalation recognizes evolving application threats and automatically triggers heightened levels of application protection across the enterprise. A treat management system recognizes evolving application threats and automatically triggers heightened levels of application protection across the enterprise. This unprecedented intelligence provides organizations with maximum flexibility in weighing business needs and operational performance with information risk. It also ensures that an attack against a single location triggers rapid, appropriate, response throughout the distributed enterprise. In By-pass mode the treat management system

allow traffic to pass through with zero performance impact. In Passive mode it examine inbound and outbound traffic to detect security violations. In Active mode the treat management system provide full intrusion prevention to immediately detect threats, generate alerts, and block attacks.

## Intrusion prevention analysis across system layers

It is difficult to detect advanced attacks on data and data misuse by monitoring only one system layer. A method and system for overcoming the foregoing difficulties provides for the introduction of a privacy policy with enforcement points that span multiple system layers. The privacy policy is coupled with intrusion prevention analysis between multiple system layers. The scope, both in data and in time, for enforcing data privacy and encryption is then dynamically optimized between multiple system layers. that includes application database sessions, table data access, table space access, and database file level access.

## Detect advanced attacks and data leakage

In a system for overcoming the foregoing difficulties, selected rules control the amount of data that is exposed, and the time window for exposure of unencrypted data. A policy underlying the selected rules defines the extent to which data privacy is to be enforced for particular data. At the intrusion detection point, a scorecard is provided to accumulate violation attempts. On the basis of the number of violation attempts, session statistics, and data access statistics spanning multiple system layers, one can determine whether a threshold indicative of an attack has been reached. A system as described above enhances the ability to detect advanced attacks on data as well as instances of data misuse and data leakage.

## Protecting applications and servers

### The Web application security problem

All over the industry, application security experts are warning IT and security departments that the gap is growing between today's rapidly-evolving app-oriented exploits and the still-nascent defenses that most enterprises have in place. Yet, so far, most enterprises are

moving at a snail's pace. Some organizations have a large number of Web applications, and those applications are changing daily. They may have checked for vulnerabilities in a few of those apps, but any of them could lead to a breach. Security estimates that seven or eight out of every ten Websites are hosting at least one serious vulnerability that could put its data at risk. Gartner has estimated that figure at closer to 90 percent.

### The favorite vectors for Web attacks

Common vulnerabilities and exposures across the Web, include application-level attacks such as cross-site scripting, SQL injection and buffer overflow as the favorite vectors for Web attacks. SQL injection is a technique used to exploit Web-based applications by using client-supplied data in SQL queries.

SQL injection attacks are caused primarily by applications that lack input validation checks. Yet most enterprises still do not own a Web application firewall, and many don't yet do any application scanning, experts say. Web application firewalls provide essential protection against application attacks. An application firewall is an enhanced firewall that limits access by applications to the OS of a computer.

Conventional firewalls merely control the flow of data to and from the CPU, examining each packet and determining whether or not to forward it toward a particular destination. An application firewall offers additional protection by controlling the execution of files or the handling of data by specific applications. Many enterprises have never had a third party audit their apps for vulnerabilities - in fact, many large enterprises don't even know how many Websites they operate, they say. The main problem is there is no single tool that can find and fix all of the vulnerabilities.

Web application firewalls protect against some threats, but they also let others through. App scanning tools can find much vulnerability, but they are far from 100 percent effective. Ultimately, you want to build the vulnerability scanning and testing phase into your development process. Realistically, however, enterprises should be more concerned about the applications they've already deployed than about revamping their QA process.

It makes more sense to start backwards and check the apps that are exposed. Enterprises should attack the problem first by identifying all their sites and the applications running on them, experts say. An audit by a third-party expert and a scan by a vulnerability scanning tool can give the enterprise a starting point for remediation.

### PCI requirement on Web facing applications

Recently, commercial shopping cart products have been the focus of attack by hackers who seek account information. PCI DSS Require-

ment 6.5 requires that Web-facing applications be developed in accordance with secure coding guidelines to guard against such attacks. A successful SQL injection attack can have serious consequences. SQL injection attacks can result in the crippling of the payment application or an entire e-commerce site. Through this avenue of attack, an attacker can break out of the Web server and database realms, gaining complete control over the underlying system. Another serious consequence can be the compromise and theft of data that resides within the payment application infrastructure.

**Recently, commercial shopping cart products have been the focus of attack by hackers who seek account information.**

### The SQL injection problem

Most databases are set up in a way that makes breaking in relatively easy. But securing the database has become simpler. A few straightforward steps can vastly improve security, usually by locking out all users except applications and DBAs. But even that restriction doesn't completely protect your data.

One of the primary security breaches organizations experience today takes place via applications that connect to databases. Applications don't use native database security. Instead, they access the database as a "super user" and, therefore, could represent a risk to data security.

One of the most common examples of exploiting this risk is known as SQL injection. SQL injection isn't a direct attack on the database. Instead, it takes advantage of the way many Web applications that access databases are developed. SQL Injection attempts to modify the parameters passed to a Web application via a Web form to change the resulting SQL statements that are passed to the database and compromise its security. If successful, an attacker can hijack the database server and be granted the same permissions to add, drop, and change users that the application has. From that point, the database is fully exposed.

Unfortunately, the practice of SQL injection is easy to learn. Fortunately, with a little forethought, you can prevent it.

### Protection from SQL injection

There are two primary methods to protect your database from SQL injection. First, make sure that applications validate user input by blocking invalid characters and use protected queries that bind variables rather than combining SQL statements together as strings such as stored procedures. Second, install Application Level Firewalls to protect your database from SQL injection and other threats targeting web applications. If you want to know exactly what's going on with your Web servers, a Web application firewall, or WAF, is worth every penny.

Available in software or appliance form, WAFs work at the application layer, using deep-packet inspection to reveal the inner workings of Web applications while thwarting attacks made possible by insecure programming.

### Computers outside the control of its intended users

A computer may sometimes be outside the physical control of its intended users; for example, a server, USB-drive or disk may be stolen rather easily.

Therefore, it is prudent to restrict access to the computer's functions, for instance by requiring the entry of a password. It is also prudent to protect the files on the computer by encrypting them, for instance under an encryption key derived from the password. The password itself should not be kept in the clear on the computer. In this way, only parties that know the password can use the computer and read the files, even if they have direct access to the computer's storage devices. The password should be strong enough that an attacker cannot guess it and then decrypt the files. We assume that user and computer have some secure means for communicating, perhaps because the user has direct, physical access to the computer, or can establish a secure network connection with the computer. The user may type a password into the server at log-in time and in addition to we add a password supplement that may be 40 bits chosen randomly.

### Protecting credentials in applications

Passwords are the most common form of user authentication in computer systems. The password is always a weak link in any protection system. An administrative or master password should be particularly complex. According to a recent survey, 66% of enterprises have more than 100 applications, 92% of which connect to other applications using hard-coded (embedded) passwords (SOURCE: Cyber-Ark Password Survey 2006.)

When two software applications connect, a script is created which has the powerful user name and password in clear text, a serious security risk. Studies of production computer systems have for decades consistently shown that about 40% of all user-chosen passwords are readily guessed. Passwords easily guessed are known as weak or vulnerable; passwords very difficult or impossible to guess are considered strong. Only passwords are discussed in this section, but other (stronger) authentication types should be considered based on a risk assessment.

### Lock down the passwords

Below is one easy way to solve the general password protection issue by using an encryp-

tion solution that can be application transparent and resistant to 'multiple attack vectors' protecting the access to API, to databases and to SSL communication sessions. An encryption server box should be hardened and the session should be authenticated (with a password or multi-factor authentication) and encrypted (SSL or similar). Lock down the application storage of the passwords to the logins for the database, communication and the encryption server. A mature transparent file system encryption product on the application server platform can lock down the storage of the password and may also delegate a transparent authorization to the application.

### The exhaustive search attack

A slow one-way algorithm will not noticeably increase the cost of one operation (e.g. for the legitimate user when logging in), but it should substantially increase the task of mounting an exhaustive search attack. A common approach is to iterate the original one-way function many times. Some systems one-way function encrypts a known string 25 times with DES using a key derived from the user's password (another feature is that the salt value actually modifies the DES algorithm itself, making it harder for an attacker to use dedicated DES hardware to mount an attack. Given the current computer resources available, we recommend a minimum of 5000 iterations for constructing the hash algorithm.

### Password strengthening

Password strengthening is a compatible extension of traditional password mechanisms. It increases the security of passwords, without requiring users to memorize or to write down long strings.

Password strengthening does not assume any extra hardware, and does not introduce any of the vulnerabilities that come with extra hardware. These characteristics should make password strengthening easy to adopt, and appealing in practical applications. The method does not require users to memorize or to write down long passwords, and does not rely on smart-cards or other auxiliary hardware. The main cost of our method is that it lengthens the process of checking a password.

## Use salted passwords

Each password hash is associated to a small, usually random value called salt. The salt does not need to be kept secret, and it is used together with the password to generate the password hash. While the use of salted passwords does not increase the task for recovering a particular password, a salt of sufficient length should preclude pre-computed, offline dictionary attacks, as it becomes impractical to compute a large table of hashes corresponding to possible passwords and salt values in advance.

## Enforce complex passwords

One of the weakest aspects of password based authentication is the low entropy of commonly chosen passwords. The main attacks for recovering clear text passwords from hash values consist of computation of all possible passwords up to a certain number of characters (exhaustive search attack), or perhaps a list of typically chosen passwords (dictionary attack). The computation is usually performed offline and the attacker simply compares the values on the password table

with the pre-computed list. Systems should therefore enforce password complexity rules, such as minimum length, requiring letters to be chosen from different sets of characters (e.g. lower-case, upper-case, digits, special characters), etc. An appropriate password length depends on the amount of resources available to the attacker that an organization wishes to defend against. Assuming an attacker has access to optimized DES-cracking hardware, an organization may need to enforce 12-character passwords and password expiration duration of 60 days to mitigate a brute-force attack against the password hash.

## Generate random passwords

A password generator is able to a strong password policy of a random sequence of numbers, lower-case letters, and upper-case letters. These passwords are random and therefore very difficult for a hacker to guess. A password generator thwarts any key-logging attempts by automatically copying the generated password into the password field. Since your password is never typed and never copied to the clipboard, a keylogger has no chance to capture your information.

## Use non-privileged users for web applications.

### Challenge response to avoid replay attacks

Both the central and local copy will be replaced every time the user picks a new password. Both passwords will be replaced every time the computer is re-started and can no establish a secure network connection with the central key management computer. A challenge-response process may be added to avoid replay attacks if a cloned end-point server is attacked by using the manually entered password part.

### Use non-privileged users for applications

One technique for capturing password hashes is to exploit excessive permissions for database users configured to execute web-based application code that is susceptible to SQL injection attacks. When selecting a user account to provide access to a web application,

ensure the account has only the minimum privileges granted to run the application. In no cases should a user that is a member of the DBA group be allowed to run web applications that are exposed to public or less-privileged users.

### Summary of protecting passwords

Specifically, organizations can implement the following steps to protect the confidentiality of password hashes: use non-privileged users for web applications. Restrict access to password hashes, Audit SELECT statements on selected views (DBA views). Encrypt IP traffic. Enforce a minimum password length. One solution to the application-to-application password dilemma is to deploy software that moves script-based passwords into a centralized and secured point.

## Example - a retail industry scenario

Each store location is storing sensitive customer information and need to operated also in situations where the WAN connectivity to the central system is unavailable. The Local Security Server provides authorization, logging and encryption services and are managed by a support person and a system administrator at the respective store location. In this scenario a tight integration of PKI and the Store Security System is deployed. Each Local Security Server (as well as Central Security Server) retain a cached copy of the encrypted encryption key while in an operational state. The SSL private keys are stored on or in connection to the Application the servers.

### Protecting local security servers

Each Local Security Server should be locked upon start-up. While locked, all sensitive data is encrypted and presumably safely stored. During the Local Security Server start-up procedure the application gets unlocked so that it can get on with its business processing functions. Unlocking may occur through an automated or manual process – the latter is invoked in situations where the WAN connectivity is unavailable for some reason or another. The security of this process depends on the secrecy of the startup login contexts, which are unique to each store location and only used once in theory. Under the automatic unlocking process, the startup login context must be discarded after use (and wiped from memory) and then a new startup login context is automatically rotated in via the Security Administration Server, thereby greatly reducing the exposure of the startup login context.

### An attacker with a cloned local security server

The manual unlock process, on the other hand, exposes a valid startup login context to at least two people – a support person and a system administrator at the respective store location. Although the key is rotated after use, a maliciously cloned Local Security Server environment could still be unlocked using that startup login context if the cloned system remains off-line. This could enable an attacker to invoke and unlock a cloned Local Security Server in a safe environment and potentially

use the data and processes on the Local Security Server to decrypt cached/archived encrypted credit card data. The impact of a successful breach of this process could be extreme. Customer data could be compromised, resulting in customer identity theft. It is vital that a robust business process, complete with adequate checks and balances, be instituted at every store location that will run a Local Security Server. Additional technologies could be deployed to further protect this vital aspect of the Local Security Server's operation, such as smart cards. A smartcard based identification, authentication, and authorization mechanism would be a significant improvement in protecting the startup and unlock process for each Local Security Server. It is understood, however, that such measures would not be feasible to deploy at each The Company and franchisee property. As such, a robust business process as mentioned above is even more important to address carefully. In numerous other industries, mission critical applications commonly leverage technologies such as smart cards, one time passwords, and others for protecting such vital operating states as unlocking the Local Security Server.

### Local administration staff access to keys

At various times during normal Store Security System operations, store location system administration staff are likely to have access to startup login contexts and encryption keys. Despite the fact that key management has been carefully thought through to minimize these exposures, opportunities do exist for Level 1 support staff to compromise customer data. Further, detecting this sort of insider attack can be extremely difficult. The impact of a successful insider attack on the Store Security System could be quite severe. Best practices in similar data environments generally include most or all of the following measures: Background checks of all personnel involved in sensitive operations such as key management. Separation of data. Ideally, support staff who have access to encryption keys should not have access to any sensitive, encrypted data and vice versa. This, however, can be a difficult measure to implement. Separation of duties. To the extent feasible, functional duties should be separate within the data center. For example, first level support personnel who handle Local Security Server unlocking should

not also be involved with encryption key management. The above recommendations are entirely consistent with practices found in numerous other industries where similar access to sensitive customer data is required. The financial services industry, in particular, makes regular use of operational practices like these.

### Failure of PKI or authentication server

If a tight integration of PKI and the Store Security System is deployed, a failure of the PKI

would without a doubt have a devastating affect on the Store Security System. A scenario such as the CA certificate appearing on a CRL could halt the entire PKI system. Since the PKI is literally infrastructure to the Store Security System, a PKI failure could have a commensurate affect on the Store Security System, resulting in considerable business impact, and great care must be taken to ensure that the PKI is operated in compliance with all relevant PKI industry best practices and procedures.

Password protecting SSL keys is commonly done on production servers throughout various industries. On the other hand, doing so is often not feasible.

### Protection of keys in memory

It is essential that each Local Security Server (as well as Central Security Server) retain a copy of the encrypted encryption key while in an operational state. This is (obviously) a necessity of its business mission. An attacker with access to a Local Security Server could potentially peruse the system's processes and memory to acquire the key and decrypt encrypted data. The likelihood of this sort of attack succeeding is quite low, but was it to be successful; the impact could be very high. Take every reasonable precaution to protect the key while the Local Security Server is operational. Protection measures to consider should include: Memory compartmentalization - Generate a separate ID that does the actual encryption/decryption, and ensure that no other process or system ID can access its memory. Swapping - Ensure that the encryption/decryption process and its memory do not get swapped out to a virtual memory swap/page file, which could leave behind persistent residue that could include the encryption key. Memory wiping - Whenever the key is no longer needed, ensure that the memory location/variable where it was held is thoroughly wiped, so that no memory residue is left behind for an attacker to search through. Consider a centrally monitored host-based intrusion detection system on every Local Security Server to vigilantly watch for attacks on

the host itself. The above list of recommendations for encryption key handling is commonly practiced throughout various industries where sensitive data is encrypted.

### Protecting SSL keys on application servers

SSL private keys are commonly left in plain-text on Application servers. Although not directly part of the Store Security System Architecture itself, this could indirectly help an attacker get one step closer to successfully attacking the Store Security System. In particular, the plain-text SSL key could enable an attacker to masquerade as an Application server in an Application-Local Security Server conversation. The likelihood of such an attack working is quite low, but could enable an attacker to do anything that an Application server is able to do. Consider password protecting the SSL key for the Application server. Although this can be unfeasible in some operational scenarios, if it doesn't present an undue burden, it would be a good idea. Password protecting SSL keys is commonly done on production servers throughout various industries. On the other hand, doing so is often not feasible. Thus, it is not uncommon to find plain-text SSL keys in production data centers. It is less common to find plain-text keys on field-deployed servers, such as the Local Security Server servers.

## Summary of best practices in data security management

### Centralization

Best practices begin with the centralization of Data Security Management, enabling a consistent, enforceable security policy across the organization. From a centralized console, the Security Administrator defines, disseminates, enforces, reports and audits security policy, realizing gains in operational efficiencies while reducing management costs.

### Protecting data

Experts agree the best protection of sensitive information is encryption. Database level encryption provides the most comprehensive protection: Protection against storage-media thefts, storage level attacks, database layer attacks and attacks from 'super-user' access. Best practices dictate that a solution delivers:

**Focused Protection** - Choose only the sensitive data your organization needs to protect (Credit Card, Social Security #, Salary, etc). Provide individual protection for each column through individual keys to gain an extra layer of protection in case of security breach.

**Strong Key Management** - A secure system is only as good as the protection and management of its keys with integrated key management systems that control where keys are stored, who has access to them, and ensures they are encrypted and protected.

**Protecting Policy Changes** - Changes to security policy are critical events that need to be protected. It is a best practice to require more than one person to approve such changes. Protegrity delivers this through assigning the Master Key to more than one individual.

### Reporting policy

Reporting and monitoring your security policy and generating protected audit logs are fundamental best practices, and required by regulations. A comprehensive and efficient reporting should include:

**Evidence-quality Audit** - A regulatory requirement, Protegrity delivers evidence-quality

auditing that not only tracks all authorized activity, it also tracks unauthorized attempts as well as any changes to security policies – it even tracks activities of the database administrator (DBA), and provides a complete audit report of all these activities.

**Separation of Roles** - Regulations stipulate that a data security system must provide "reasonable protection from threats." Having the ability to log and review the activities of both the Security Administrator and the Database Administrator provides a checks-and-balances approach that protects from all reasonable threats.

**Selective Auditing Capabilities** - Protegrity's reporting system is highly selective, allowing your security administrators to examine the information most critical to their job.

**Protected Audit Logs** - Simply put, the audit logs themselves must be secure. Protegrity encrypts all audit logs to protect against tampering. This prevents an administrator from doing something bad and changing the logs to cover his tracks.

### Controlling access

It is estimated that 70-80% of all security breaches come from within the firewall. Controlling access to the data is a critical element to any security policy

**Control Down to the User Level** - Defining a security policy that allows centralized definition of data access, down to the data field level, on an individual-by-individual basis across the entire enterprise is best practice.

**Setting the Boundaries** - Putting limits on authorized usage of data is necessary to avoid breaches from the inside. Much like an ATM machine will limit the amount of money a person can take out of their own account, it is important to be able to set the limits on authorized use as part of data security policy. If the use of sensitive data should be limited to 9-5, Monday-Friday, then any attempt to access that data outside of those boundaries should be denied.

**Separation of Duties** - An affective security policy should protect sensitive data from all



'reasonable' threats. Administrators who have access to all data are a reasonable threat, no matter how much we trust them - trust is not a policy. Implementing a separation of duties of security definition and database operations provides a checks-and-balances approach that mitigates this threat.

### Requirements for data encryption solutions

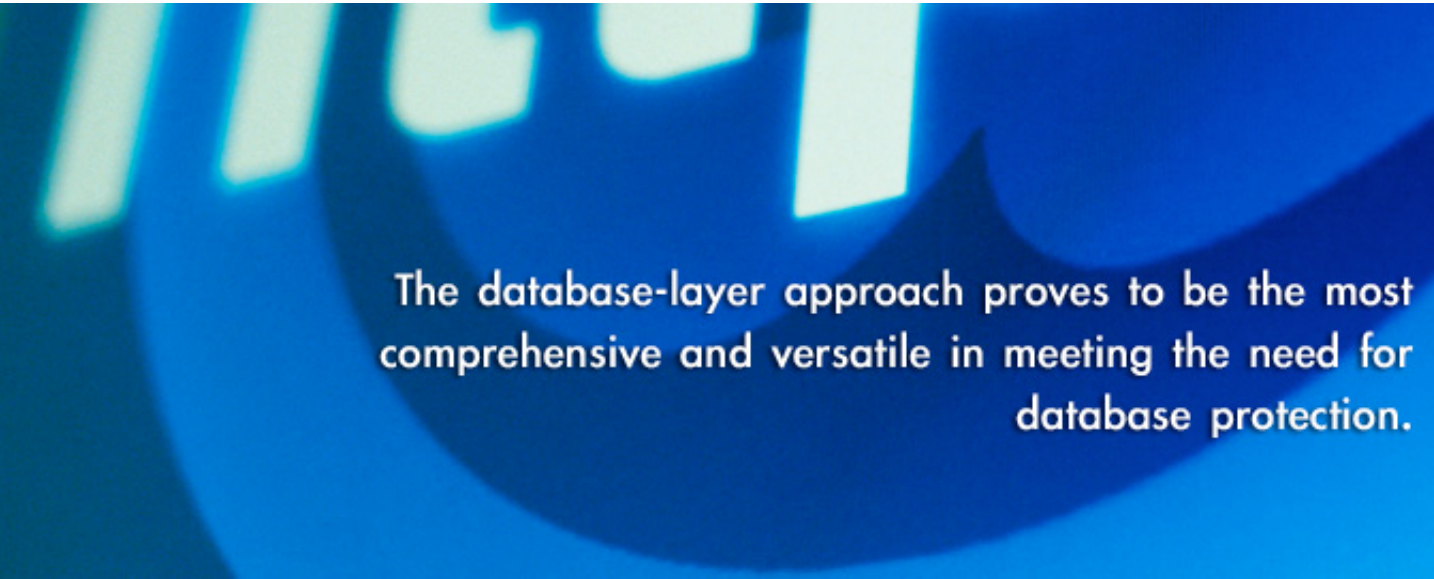
My earlier articles reviewed the requirements for data encryption solutions and summarized how implementations at three different system layers approach critical and practical requirements.

The database-layer approach proves to be the most comprehensive and versatile in meeting the need for database protection. The database-layer approach can be combined with Application-Layer encryption and Storage-Layer encryption in meeting broader protection needs in heterogeneous environments found in today's large complex organizations.

Earlier articles also reviewed alternative implementations of database-layer encryption. There are several critical goals and objectives of Database-layer security that need to be met, and enterprises are faced with choices about how to accomplish these goals. The three broad approaches to database-layer encryption are:

1. Native Database-Layer encryption
2. Programming Toolkits
3. Packaged Security Solutions:
  - Software-only packages
  - Network Attached Encryption Devices
  - Combination of the two topologies.

Each of these solutions has its advantages and disadvantages. All these alternatives provide a high level of security and physically separating the keys from the data, but Network Attached Encryption Devices lack the architecture to scale and perform in larger distributed enterprise environments with high transaction volumes.



The database-layer approach proves to be the most comprehensive and versatile in meeting the need for database protection.

Earlier articles also reviewed best practices in enterprise data protection and how to protect data at rest, and also while it's moving between the applications, databases and between data stores.

A mature solution should bring together data protection at the application, database and file levels. The encryption solution has a combined hardware and software key management architecture. A mature solution addresses the central security requirements

while providing the flexibility to allow security professionals to deploy encryption at the appropriate place in their infrastructure. It provides advanced security and usability and also smooth and efficient implementation into today's complex data storage infrastructures. The integration with Hardware Security Modules strengthens the key management facilities through the use of tamper resistant, FIPS 140-2 Level 3 cryptographic hardware.

## Conclusion

The basic conclusion is that a combination of application firewalls, plus the use of data access monitoring and logging may, if effectively applied, can not provide reasonable equivalency for the use of data encryption across the enterprise since such a combination of controls does have multiple weak spots, when it comes to preventing damage from careless behavior of employees or weak procedures in development and separation of duties.

PCI requires that Web-facing applications should be guarded against attacks that can have serious consequences. There are two primary methods to protect your database from SQL injection. First, make sure that applications validate user input. Second, install Application Level Firewalls to protect your database from threats targeting web applications.

There are no guarantees that any one approach will be able to deal with new and innovative intrusions in increasingly complex technical and business environments. However, implementation of an integrated security program which is continuously audited and monitored provides the multiple layers of protection needed to maximize protection as well as historical information to support management decision-making and future policy decisions.

Sending sensitive information over the Internet or within your corporate network as clear text, defeats the point of encrypting the text in the database to provide data privacy. The sooner the encryption of data occurs, the more secure the environment. An Enterprise level Data Security Management solution can provide the needed key management for a solution to this problem. This solution will protect data at rest, and also while it's moving between the applications and the database and between different applications and data stores.

Stronger database security policies and procedures must be in place to accommodate the new environment. Centralized database management security must be considered to reduce cost. Implementing "point" or manual solutions are hard to manage as the environment continues to grow and become more complex. Centralized data security management environment must be considered as a solution to increase efficiency, reduce implementation complexity, and in turn to reduce cost. By implementing solutions documented above, we should be in a better position to face growing database security challenges, to proactively meet regulatory and compliance requirements and to better control our sensitive data. Database security is an ongoing process, we must revisit and refine our strategy regularly to adopt new technologies and address new challenges as environment continue to evolve.

Field-level data encryption is clearly the most versatile solution that is capable of protecting against external and internal threats. A protective layer of encryption is provided around specific sensitive data items or objects, instead of building walls around servers or hard drives. This prevents outside attacks as well as infiltration from within the server itself. This also allows the security administrator to define which data are sensitive and thereby focus protection on the sensitive data, which in turn minimizes the delays or burdens on the system that may occur from bulk encryption methods.

Database attack prevention represents a valuable supplement to corporate information security by defending databases against inappropriate and malicious requests for sensitive information. By deploying database intrusion detection in the enterprise, businesses have a powerful tool for safeguarding information assets, protecting their reputation, and maintaining customer trust.

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

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

Stop gambling your safety...

**hakin9**  
Hard Core IT Security Magazine



[www.en.hakin9.org](http://www.en.hakin9.org)