Security features in Windows Vista and IE7 – Microsoft's view

Stephen Lamb

Stephen Lamb, Technical Security Advisor, Microsoft UK

With Windows Vista due to be released in early 2007, IT departments across the world are planning for the inevitable. Also currently in beta testing, Internet Explorer 7 is likely to be out by year-end. What can be expected security-wise? Microsoft presents its case.

Microsoft's message to Internet criminals is: "Hasta la Vista!" ["See you later", for non-Spanish speakers]. I have used the term here because Windows Vista, and Internet Explorer 7 (on both Windows XP and Vista), make it easier for every day users to protect themselves from Internet criminals.

Clear, Confident and Connected are the stated design goals of Windows Vista. Much has been made of the graphical user interface enhancement including the adoption of three dimensional animation and translucent effects known as Aero Glass. Considering personal computer systems with Terabyte file system capacities – and the time most people spend searching for information today – clearly it is important to revolutionise the way the operating system both presents information and provides the means to categorise it to facilitate rapid access.

Windows Vista's context-sensitive search extends beyond the file system to include the applications and operating system components including control panel applets. As someone who has productively used Windows Vista for several months I have found that going back to the old interface of Windows XP and Server 2003 somewhat frustrating.

"Confident" in the context of Windows Vista refers to the radically enhanced security architecture and features. The focus of this article is to explore the details of information security aspects of Microsoft's new client operating system. Clarity of course is vitally important when interacting with users and therefore Windows Vista's security interfaces were designed to reflect feedback from our customers. There is little point in asking highly technical questions to regular computer users hence we have made the Windows Vista messages as easy to understand as possible whilst remaining informative.

"Connected" refers to the way in which modern computer systems are increasingly networked to enable them to access information and transact with remote systems. Mobile computers by their very nature tend to be transient in their network connectivity where most users are less and less aware of exactly which network carrier they are using at any given time. As the provision of wireless hotspots, guest access to corporate networks and increasingly pervasive broadband access increases so too will the variety of networks that mobile machines will connect to on a daily basis.

It is critical to maintain sufficient network security together with ease of use.

Of course it is simplistic to suggest that the advances in security provided by Windows Vista will entirely prevent criminals from committing Internet crime – this new platform will reduce the need for users to be technically and security savvy in order to be protected. As Windows Vista is adopted, the likely threat will move ever more from the platform, to the applications and into social engineering attempts to encourage users to expose themselves to risk.

Please note: The features and functions described in this article are based on Windows Vista Beta 2 code and hence they may vary from the production code when it's released.

'Security Development Lifecycle'

Windows Vista is Microsoft's first client operating system to be developed from the ground up according to the Security Development Lifecycle (SDL) meaning that extensive process and procedures have been applied to both the design, implementation and testing of the product.

The SDL helps to ensure that software is robust to withstand attack through the implementation of rigorous security oriented architecture, design, coding and testing. SDL is an evolving process that learns from both trends in emerging threats as analysed by the Microsoft Security Response Centre (MSRC) and industry best practice. Throughout the development lifecycle each team's SDL compliance is enforced by a nominated security advisor who ensures that security reviews and testing requirements are met at every stage. Each team constructs numerous threat models to investigate the opportunity for criminals to exploit the software.

The mnemonic of STRIDE which stands for Spoofing, Tampering, Repudiation, Information Disclosure and Elevation of privilege is used when constructing Threat Models to assess the possible opportunity for attackers. Threat Trees are constructed to identify the combined effect of exploiting each aspect of the system. The mitigating steps to address weaknesses found during modelling may involve the implementation of additional controls or possibly changes to the code itself.

SDL is effective as it is founded on practical process, procedure and guidance as applied to all Microsoft development activities. Our experience of applying SDL over the last three years demonstrates a significant reduction in both the number of and the severity of software security vulnerabilities. As a result of adopting SDL from start to finish in the development of Windows Vista Microsoft believes the code is highly resilient to attack.

What do we mean by 'trust'?

People both in the security community and beyond talk about "Trust" in absolute terms. If only life was so simple. Trust is not

a binary property. We trust people in specific contexts. We may trust the manufacturer of our cars that the brakes are going to work and the service agent to maintain them. That does not mean that we would trust them to take care of our children! I trust my web browser to accurately render pages of HTML and to make me aware of sites that appear to be malicious. I have no need to trust my browser to execute code on my system outside the web context.

Adopting the Principle of Least User Access

All too often in operating systems prior to Windows Vista users are required to login in as a privileged account such as "Administrator" simply to get things done. You may question why the use of such privilege is a bad thing. Most of the time I use my computer system to access and manipulate information. Upon occasion I will choose to reconfigure my system and possibly install additional hardware and software. These are two quite different scenarios. The first is that of a "regular user" and can be achieved without additional privilege. The second requires additional privilege. If I accidentally trigger the installation of some malicious software (such as a rootkit, Worm, Spyware or a Virus) then it could automatically compromise my system if I am logged in with Administrative privilege. There is a spin-off benefit of adopting the principle of Least User Access (LUA) as I am unable accidentally to reconfigure my system.

'User Account Control'

Windows Vista introduces a privilege brokering system named User Account Control which obviates the need to login interactively with excessive privilege. Early betas of Windows Vista used alternative names for this system including "User Account Protection (UAP)", "Least User Access (LUA)" and "Federated Account Control Technology (FACT)". The reason for mentioning the alternative names is to help you follow some existing documentation. Note: LUA is a generic term hence it was deemed confusing to use it to name a feature of Windows Vista.

The requirement for excessive privilege often stems from application developers who build code using privileged accounts and hence the software they produce often assumes a similar environment. Previous versions of Microsoft Windows have required privileged accounts to be used to change the system's TimeZone setting – this setting together with several others have been changed to enable control by regular users. Figure 1 shows User Access Control prompting for the credentials of an administrative user to enable elevation of privilege.

Figure 2 shows User Access Control prompting an administrative user to give consent for a privileged operation.

The User Access Control interfaces take advantage of a virtual desktop feature of Windows Vista to isolate them from malicious software that may attempt to steal user credentials. The user experience is that the entire screen fades except the UAC dialog to signify the trusted route between UAC and the user. The following image shows the User Access Control Group Policy Objects which can be configured by either Local Policy (as shown in Figure 3) or centrally via Active Directory).

Windows Service Hardening

When attacking a system, attention is often paid to Operating System Services as they generally run with maximum system privilege and therefore compromise leads to total break down of the security system. Services are also appealing as they tend to be running whenever the system is operational.

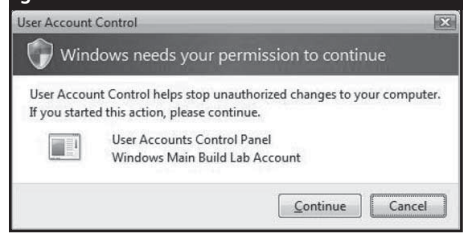
Microsoft operating system architects and developers have reviewed each service to consider exactly how much privilege is actually required in each instance and where possible limitations have been placed in the level and scope of privilege. Where necessary existing services have been broken up such that the portions requiring privilege are kept to an absolute minimum.

Security Identifiers (SIDs) have been defined for every operating system service in Windows Vista together with Access Control Lists (ACLs) to limit access to only the components that need it.

In Microsoft parlance the terms "Service Hardening" and "Service Refactoring" are frequently used to describe this approach. In addition each service has been profiled to apply Access Control Lists to restrict access purely between components on a "need to know" basis. Rules are enforced specifying the required network behaviour.

Figure 1: Prompt for administrative user

Figure 2: Prompt for administrative user to give consent



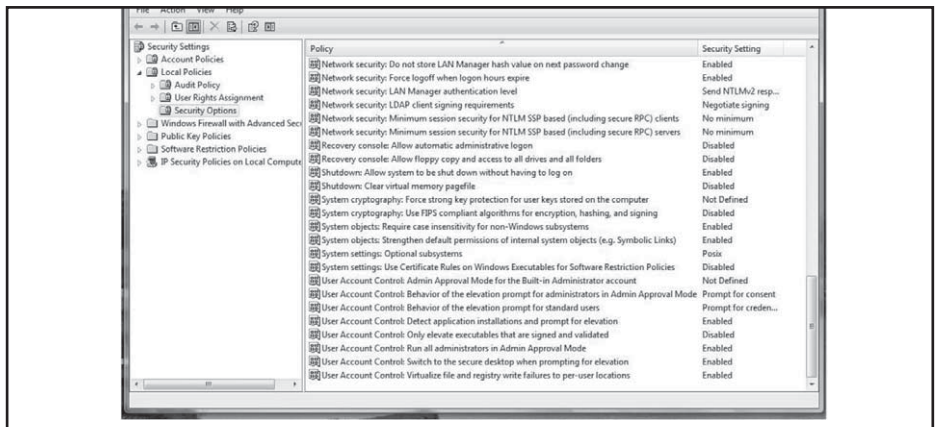


Figure 3: User Access Control Group Policy Objects

Operating System components including services now authenticate one another before allowing information to be exchanged. Figure 4 lists the use of Privilege for Services in Windows XP Service Pack 2.

Figure 5 lists the use of Privilege for Services in Windows Vista.

Internet Explorer 7+ Protected Mode

Moving on to Internet Explorer 7, the vast majority of its features work exactly the same on both Windows XP and Windows Vista. To avoid confusion the name "Internet Explorer 7+" is used to describe Internet Explorer on Windows Vista. The primary difference is that "protected mode" is exclusively available on Windows Vista as the architecture of Windows XP does not provide the means to do so. Protected Mode signifies Internet Explorer 7+'s use of absolute least privilege whereby the browser is limited to writing files only in the current user's Temporary Internet Files (TIF) directory.

Whilst extensive security code reviews have been conducted on Internet Explorer it is still possible that unforeseen exploits could take place hence Internet Explorer 7+ is treated as an untrusted application by the system. This approach is used to limit the damage of possible future security vulnerabilities in Internet Explorer. As the browser is unable to write outside the user's profile then by definition it is unable to damage the integrity of the operating system.

The use of least privilege to the extent of Internet Explorer 7+ is unique and therefore I hope that in the near future the developers of other browsers adopt this approach to protect their users from malware.

LocalSystem (Maximum privilege)	Wireless Configuration	Remote Access	Workstation	Telephony
	System Event Notification	DHCP Client	ICS	Windows Audio
	Network Connections	W32time	BITS	Cryptographic Svcs
	COM+ Event System	RASMan	Automatic Updates	Removable Storage
	NLA	6to4	WMI	Error Reporting
	RASAuto	Help and Support	App Management	Themes
	Shell Hardware Detection	Task Scheduler	Secondary Logon	TrkWks
	WMI Perf Adaptor			
Network Svc	DNS Client			
Local Svc	SSDP	WebClient	TCP/IP NetBIOS Hlp	Remote Registry

Figure 4: Use of Privilege for Services in Windows XP Service Pack 2

Windows Vista				
LocalSystem (Network Restricted)	Removable Storage	WMI	WMI Perf Adaptor	App Management
	Automatic Updates	Secondary Logon	TrkWks	
LocalSystem (Demand Started)	BITS			
Network Svc (Restricted)	DNS Client	ICS	RemoteAccess	DHCP Client
	W32time	Rasman	NLA	Browser
	6to4	Task Scheduler	IPsec Services	Server
	Cryptographic Svcs			
Local Service (Restricted) (No network access)	Wireless Config	System Event Notification	Shell Hardware Detection	Network Connections
	RASAuto	Themes	COM+ Event System	
Local Service (Restricted)	Telephony	Windows Audio	TCP/IP NetBIOS helper	WebClient
	Error Reporting	Event Log	Workstation	Remote Registry
	SSDP			

Figure 5: Use of Privilege for Services in Windows Vista

Internet Explorer's Phishing Filter

The Phishing Filter is a feature of Internet Explorer on both Windows XP and Windows Vista that exists to inform the user when the site they wish to browse to has been reported as suspicious. The Phishing Filter embraces the power of the user community each of whom are able to report sites they regard to be possible Phishing sites simply by selecting "Check this site" from the "Tools, Phishing Filter" menu. Researchers working on behalf of Microsoft analyse all reported sites to determine which are indeed malicious. Such sites are added to the database that is queried by Internet Explorer when it connects to the Internet.

It is easy for non technical people to make sense of the output from the Phishing Filter as the address bar changes colour to represent suspicious sites. Plain English text accompanies the warning to explain the danger and advise the user how to proceed.

Figure 6 shows the Phishing Filter notifying the user of a suspicious website.

Additional Internet Explorer Security Features

All URL parsing now takes place in a single function thereby reducing the attack surface of the browser. Users are prompted via the Information Bar before any existing ActiveX controls are enabled. Additional cross domain script barriers now exist to prevent malicious web sites from manipulating web content.

A new feature named "Fix My Settings" works on the basis that most users operate their browser using the default settings though some applications require the security settings to be temporarily lowered. If the user forgets to reset the security settings to the default balance of features and controlled security then the Information Bar will warn them and opt to reset Internet Explorer's security settings back to the Medium-High default.

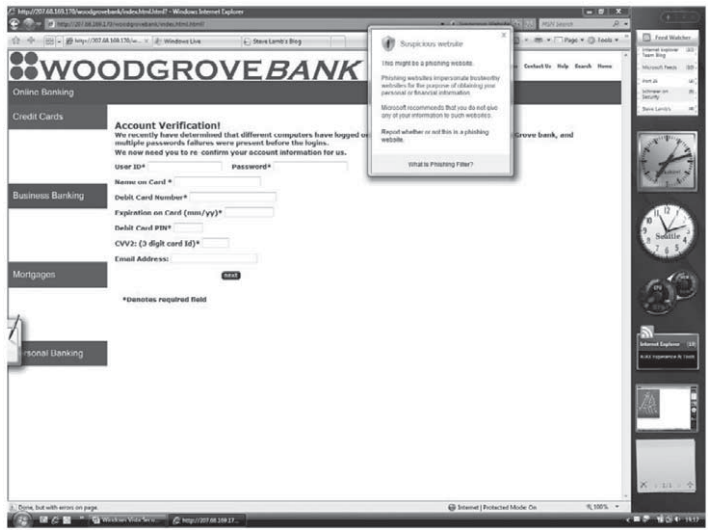


Figure 6: Phishing Filter

Windows Defender: built-in protection from Spyware

Windows Defender is the name given to the Windows Vista built-in anti-spyware feature set. As explained earlier Windows Vista includes several powerful ways of defeating spyware including the use of least privilege and the Phishing Filter. Windows Defender inspects executable code from both email and browsing to prevent embedded spyware and other types of malicious software from compromising the system.

Unified Personal Firewall and IPsec filters

Internet Protocol Security (IPsec) is an incredibly powerful set of features common to the network stacks of many modern operating systems. IPsec provides the means to define network trust boundaries thereby isolating groups of machines from one another based on their mutual proof of membership. Optionally IPsec can be used to encrypt data in transit. The beauty of IPsec is that it takes place low down in the network stack hence it is seamless to applications.Windows Vista is the first operating system to make implementing IPsec filters relatively easy. Prior operating systems have required the administrator to fathom their way through numerous obtuse interfaces when implementing even pretty simple filters. Windows Vista's personal firewall includes all of the IPsec standard functionality as defined in the associated Request For Comments (RFC) documentation. Figure 7 shows the wizard for configuring a secure authenticated connection between two systems using IPsec.

Figure 8 shows a dialog which results from connecting to a new network. This is typical of messages that ask in simple terms how to configure the firewall for network access. The security settings corresponding to both "public" and "private" networks are defined in Group Policy.

BitLocker™ Full Volume Encryption and System Integrity

One of the top security feature requests from our customers is the ability to ensure the confidentiality of data on lost and stolen machines. Bitlocker Drive Encryption is a new feature that makes it possible to encrypt the entire operating system volume.

Windows Vista Ultimate and Enterprise editions will include BitLocker though it is important to note that it will be inactive by default. Administrators can enable BitLocker through the application of Active Directory Group Policy and ensure that system recovery keys are archived centrally to provide the means for controlled recovery.

Some high-end laptops ship with built-in hard security modules known as Trusted Platform Modules (TPMs). BitLocker will take advantage of the hardware security features provided by machines with TPM 1.2 compliant systems. In such a scenario the Full Volume Encryption Key (FVEK) will be

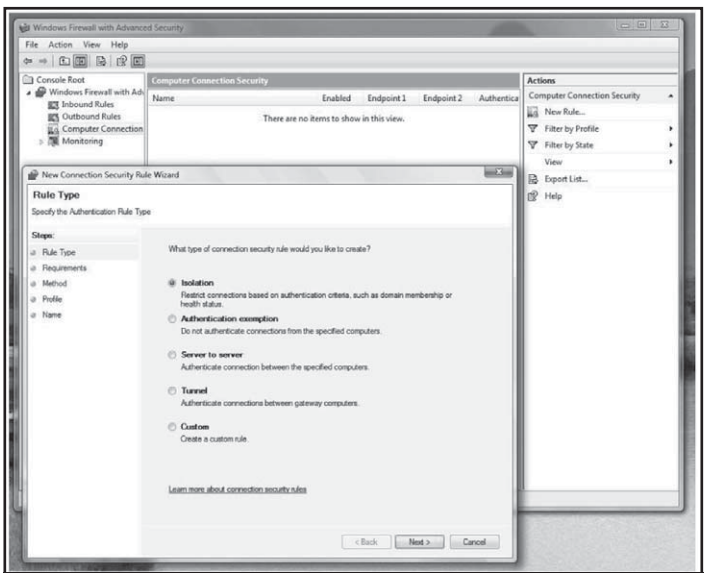


Figure 7: Wizard for configuring secure authenticated connection via IPsec

Figure 8: Dialogue resulting form connection to new network

sealed in hardware which can be configured to mandate that the user authenticates their identity before releasing the decryption keys to the operating system. Whether TPM 1.2 support exists or not BitLocker can be configured to store the FVEK on removable media such as a USB memory token.

BitLocker is designed to guard against the threat of offline attack whereby another operating system instance is used to overcome the file system access controls. Bitlocker does not protect against the threat of physical attack though it makes life significantly more complicated for the attacker.

Windows Vista assesses the integrity of the operating system at the start of the boot process and signifies to the user if it has been tampered with. Such a scenario could be the result of recovery from a hardware failure or other authorised activity in which case a recover password can be entered to restore the system to normal operation.

As a minimum consider upgrading with Internet Explorer version 7 on your Windows XP systems to take advantage of both the Phishing Filter and the improved protection from malicious websites. There are a wealth of additional security features in Windows Vista including Network Access Protection, Application Isolation through the enforcement of Mandatory Integrity Control and a radically improved cryptographic infrastructure that makes it much easier to integrate smart cards and new authentication devices.

Bibliography

(1) http://www.phrases.org.uk/meanings/hasta-la-vista.html

(2) Steve Riley, "Windows Vista System Integrity Technologies" talk from TechEd USA 2006

About the author

Stephen Lamb is Technical Security Advisor with Microsoft in the UK. He has worked for the last eleven years as a security professional during which time he has implemented technical solutions for FTSE 100 companies and their peers throughout EMEA. In addition Stephen has worked with the military and government of various countries. He has long technical experience of both Microsoft and Unix/Linux operating systems and network infrastructures.

NTFS Alternate Data Streams: focused hacking

Mike Broomfield, security consultant, NGS Software

Alternate Data Streams allow data to be stored inside hidden files, which are linked to a normal file or directory using a stream. They are one of the most effective hiding places for a hacker to store their malicious files. Read on.

When dealing with network security, administrators are often surprised by the lengths to which a skilled hacker would go to in order to cover their tracks. Black hat hackers who could be termed 'digital thugs', and who merely break into any insecure system they happen to stumble upon during mass scans of network blocks have as their only goal the defacement of as many websites as possible. On the other hand, a skilled hacker, with a more focused goal such as compromising a specific company for example, looks to network perimeters to find vulnerable servers which can then be breached, giving the attacker the opportunity to establish a base that they can then use to delve further into the targets internal network.

In order to achieve this goal, a skilled hacker needs both the time and the resources to not only install a trojan backdoor, thus allowing for later convenient reentry into the system, but also a vast array of hacking tools required to effectively attack other targets such as the internal network servers. The skilled hacker would need to hide their tools once illegitimately installed, so as to prevent themselves from being discovered by the company's network administrators. This is by no means a trivial undertaking as many of the hacking tools and trojans that the hacker might use will be detected by popular antivirus products, which will immediately alert the system administrator to the hackers' presence.

One method of hiding those files would be to use Alternate Data Streams. This article will introduce Alternate Data Streams, explain some of the more pertinent security risks associated with them and finally provide suggestions on how to minimise their impact.

What are ADS?

New Technology File System (NTFS), the file system used by Windows NT, Windows 2000/2003 and Windows XP has a feature which is practically undocumented and unknown to the majority of administrators, developers and users. This feature is labelled Alternate Data Streams (ADS). With ADS data can be stored within hidden files, and by using a stream, they can be linked to a normal file or directory. These streams are not limited in size and can be multiple streams linked to a single file. This makes ADS one of the most effective places for a hacker to conceal and store their malicious files.

History of ADS

Alternate Data Streams are found in all versions of NTFS and were developed to allow for greater compatibility with the Macintosh's Hierarchical File System (HFS). The Macintosh's file system works by using both data and resource forks to store its contents. The data fork contains the contents of the file whilst the resource fork identifies the file type and other relevant file information. This is equivalent to the file extensions Windows uses to associate files with a particular program, such as the '.doc' extension for files associated with Microsoft Office Word.

Why are ADS a risk?

In the mainstream, public awareness of ADS is extremely low, especially when compared to other techniques used to hide files and directories, such as the hidden-file attribute. Because of this there are few security programs available that are ADS-aware. Several of the most popular anti-virus products, including AVG and ClamAV, do not check