Security and safety features new to Windows Vista

From Wikipedia, the free encyclopedia

There are a number of **security and safety features new to Windows Vista**, most of which are not available in any prior Microsoft Windows operating system release.

Beginning in early 2002 with Microsoft's announcement of their Trustworthy Computing initiative, a great deal of work has gone into making Windows Vista a more secure operating system than its predecessors. Internally, Microsoft adopted a "Security Development Lifecycle"[1] with the underlying ethos of, "Secure by design, secure by default, secure in deployment". New code for Windows Vista was developed with the SDL methodology, and all existing code was reviewed and refactored to improve security.

Some specific areas where Windows Vista introduces new security and safety mechanisms include User Account Control, parental controls, Network Access Protection, a built-in anti-malware tool, and new digital content protection mechanisms.

This article is part
of a series on

Windows Vista

New features

Overview
Technical and core system
Security and safety
Networking technologies
I/O technologies
Management and administration
Removed features

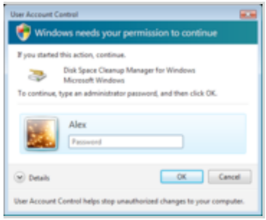
Other articles

Editions
Development history
Criticism
Mojave Experiment

Contents

User Account Control

User Account Control is a new infrastructure that requires user consent before allowing any action that requires administrative privileges. With this feature, all users, including users with administrative privileges, run in a standard user mode by default, since most applications do not require higher privileges. When some action is attempted that needs administrative privileges, such as installing new software or changing system settings, Windows will prompt the user whether to allow the action or not. If the user chooses to allow, the process initiating the action is elevated to a higher privilege context to continue. While standard users need to enter a username and password of an administrative account to get a process elevated (*Over-the-shoulder Credentials*), an administrator can choose to be prompted just for consent or ask for credentials.


User Account Control

Windows needs your permission to continue

If you started this action, continue.

Disk Space Cleanup Manager for Windows
Microsoft Windows

To continue, type an administrator password, and then click OK.

Alex

Password

User Account Control helps stop unauthorized changes to your computer.

A dialog box prevents the program from running without the permission of the user

UAC asks for credentials in a *Secure Desktop* mode, where the entire screen is faded out and temporarily disabled, to present only the elevation UI. This is to prevent spoofing of the UI or the mouse by the application requesting elevation. If the application requesting elevation does not have focus before the switch to *Secure Desktop* occurs, then its taskbar icon blinks, and when focussed, the elevation UI is presented (however, it is not possible to prevent a malicious application from silently obtaining the focus).

Since the *Secure Desktop* allows only highest privilege *System* applications to run, no user mode application can present its dialog boxes on that desktop, so any prompt for elevation consent can be safely assumed to be genuine. Additionally, this can also help protect against shatter attacks, which intercept Windows inter-process messages to run malicious code or spoof the user interface, by preventing unauthorized processes from sending messages to high privilege processes. Any process that wants to send a message to a high privilege process must get itself elevated to the higher privilege context, via UAC.

Applications written with the assumption that the user will be running with administrator privileges experienced problems in earlier versions of Windows when run from limited user accounts, often because they attempted to write to machine-wide or system directories (such as *Program Files*) or registry keys (notably HKLM)[2] UAC attempts to alleviate this using *File and Registry Virtualization*, which redirects writes (and subsequent reads) to a per-user location within the user’s profile. For example, if an application attempts to write to “C:\program files\appname\settings.ini” and the user doesn’t have permissions to write to that directory, the write will get redirected to “C:\Users\username\AppData\Local\VirtualStore\Program Files\appname\.”

Bitlocker Drive Encryption

Formerly known as "Secure Startup", this feature offers full disk encryption for the system volume. Using the command-line utility, it is possible to encrypt additional volumes. *Bitlocker* utilizes a USB key or Trusted Platform Module (compliant with the version 1.2 of the TCG specifications) to store its encryption key. It ensures that the computer running Windows Vista starts in a known-good state, and it also protects data from unauthorized access.[3] Data on the volume is encrypted with a *Full Volume Encryption Key* (FVEK), which is further encrypted with a Volume Master Key (VMK) and stored on the disk itself.

Windows Firewall

Windows Vista significantly improves the firewall[4] to address a number of concerns around the flexibility of *Windows Firewall* in a corporate environment:

- IPv6 connection filtering
- Outbound packet filtering, reflecting increasing concerns about spyware and viruses that attempt to "phone home".
- With the advanced packet filter, rules can also be specified for source and destination IP addresses and port ranges.
- Rules can be configured for services by its service name chosen by a list, without needing to specify the full path file name.
- IPsec is fully integrated, allowing connections to be allowed or denied based on security certificates, Kerberos authentication, etc. Encryption can also be required for any kind of connection. A connection security rule can be created using a wizard that handles the complex configuration of IPsec policies on the machine. Windows Firewall can allow traffic based on whether the traffic is secured by IPsec.
- A new management console snap-in named *Windows Firewall with Advanced Security* which provides access to many advanced options, including IPsec configuration, and enables remote administration.
- Ability to have separate firewall profiles for when computers are domain-joined or connected to a private or public network. Support for the creation of rules for enforcing server and domain isolation policies.

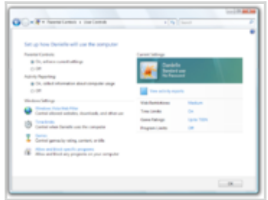
Windows Defender

Windows Vista includes Windows Defender, Microsoft's anti-spyware utility. According to Microsoft, it was renamed from 'Microsoft AntiSpyware' because it not only features scanning of the system for spyware, similar to other free products on the market, but also includes Real Time Security agents that monitor several common areas of Windows for changes which may be caused by spyware. These areas include Internet Explorer configuration and downloads, auto-start applications, system configuration settings, and add-ons to Windows such as Windows Shell extensions.

Windows Defender also includes the ability to easily remove ActiveX applications that are installed. It also incorporates the SpyNet network, which allows users to communicate with Microsoft, send what they consider is spyware, and check what applications are acceptable.

Windows Parental controls

Windows Vista includes a range of parental controls for non-domain user accounts. Windows Parental Controls rely on UAC to implement reduced rights account identities needed for offline restrictions. An administrator can apply parental control restrictions to other users on the computer. Facilities include:


Parental controls control panel

- Web content blocking, including the ability to limit web browsing to "kids websites", as well as blocking particular categories of content such as "Pornography", "Drugs", "Web e-mail", "Web chat", and so on. File downloads may also be disabled. Web content filtering is implemented as a Winsock LSP filter.
- Time limitations on when the account may be used. When active, users are blocked from logging on if not already logged on. If they are logged on and the time limit is reached, user accounts are locked using Fast User Switching without the users being logged out to prevent unsaved data in that account from getting lost.
- Restrictions on what kind of games may be played. An administrator may choose from one of five different game rating services: ESRB (United States and Canada), PEGI (Europe), USK (Germany), OFLC (Australia and New Zealand), CERO (Japan). Ratings are used to determine the highest allowed game rating. As with web content blocking, a number of categories of content may also be blocked regardless of game ratings.
- Restrictions on what programs may be executed. Implemented using Windows Software Restriction Policies.
- Activity reports to monitor and log what was done under Parental Controls through event logging interfaces
- APIs expose the policy and in-box restrictions settings, and logging functionality for parental controls functionality to be extended or replaced.

Encrypting File System

Encrypting File System (EFS) in Windows Vista can also be used to encrypt the system page file and the per-user Offline Files cache. EFS is also more tightly integrated with enterprise Public Key Infrastructure (PKI), and supports using PKI-based key recovery, data recovery through EFS recovery certificates, or a combination of the two. There are also new Group Policies to require smart cards for EFS, enforce page file encryption, stipulate minimum key lengths for EFS, enforce encryption of the user's *Documents* folder, and prohibit self-signed certificates. The EFS encryption key cache can be cleared when a user locks his workstation or after a certain time limit.

The Encrypting File System rekeying wizard allows the user to choose a certificate for EFS and to select and migrate existing files that will use the newly chosen certificate. *Certificate Manager* also allows users to export their EFS recovery certificates and private keys. Users are reminded to backup their EFS keys upon first use through a balloon notification. The rekeying wizard can also be used to migrate users in existing installations from software certificates to smart cards. The wizard can also be used by an administrator or users themselves in recovery situations. This method is more efficient than decrypting and reencrypting files.

Preventing exploits

Windows Vista uses Address Space Layout Randomization (ASLR) to load system files at random addresses in memory.[5] By default, all system files are loaded randomly at any of the possible 256 locations. Other executables have to specifically set a bit in the header of the Portable Executable (PE) file, which is the file format for Windows executables, to use ASLR. For such executables, the stack and heap allocated is randomly decided. By loading system files at random addresses, it becomes harder for malicious code to know where privileged system functions are located, thereby making it unlikely for them to predictably use them. This helps prevent most remote execution attacks by preventing Return-to-libc buffer overflow attacks.

The Portable Executable format has been updated to support embedding of exception handler address in the header. Whenever an exception is thrown, the address of the handler is verified with the one stored in the executable header. If they match, the exception is handled, otherwise it indicates that the run-time stack has been compromised, and hence the process is terminated.

Function pointers are obfuscated by XOR-ing with a random number, so that the actual address pointed to is hard to retrieve. So would be to manually change a pointer, as the obfuscation key used for the pointer would be very hard to retrieve. Thus, it is made hard for any unauthorized user of the function pointer to be able to actually use it. Also metadata for heap blocks are XOR-ed with random numbers. In addition, check-sums for heap blocks are maintained, which is used to detect unauthorized changes and heap corruption. Whenever a heap corruption is detected, the application is killed to prevent successful completion of the exploit.

Windows Vista binaries include intrinsic support for detection of stack-overflow. When a stack overflow in Windows Vista binaries is detected, the process is killed so that it cannot be used to carry on the exploit. Also Windows Vista binaries place buffers higher in memory and non buffers, like pointers and supplied parameters, in lower memory area. So to actually exploit, a buffer underrun is needed to gain access to those locations. However, buffer underruns are much less common than buffer overruns.

Data Execution Prevention

Windows Vista offers full support for the NX (No-Execute) feature of modern processors. [6] DEP was introduced in Windows XP Service Pack 2 and Windows Server 2003 Service Pack 1. This feature, present as NX (EVP) in AMD's AMD64 processors and as XD (EDB) in Intel's processors, can flag certain parts of memory as containing data instead of executable code, which prevents overflow errors from resulting in arbitrary code execution.

If the processor supports the NX-bit, Windows Vista automatically enforces hardware-based Data Execution Prevention on all processes to mark some memory pages as non-executable data segments (like the heap and stack), and subsequently any data is prevented from being interpreted and executed as code. This prevents exploit code from being injected as data and then executed.

If DEP is enabled *for all applications*, users gain additional resistance against zero-day exploits. But not all applications are DEP-compliant and some will generate DEP exceptions. Therefore, DEP is not enforced *for all applications by default* in 32-bit versions of Windows and is only turned on for critical system components. However, Windows Vista introduces additional NX policy controls that allow software developers to enable NX hardware protection for their code, independent of system-wide compatibility enforcement settings. Developers can mark their applications as NX-compliant when built, which allows protection to be enforced when that application is installed and runs. This enables a higher percentage of NX-protected code in the software ecosystem on 32-bit platforms, where the default system compatibility policy for NX is configured to protect only operating system components. For x86-64 platforms, backward compatibility is not an issue and therefore DEP is enforced by default for all programs. Also, only processor-enforced DEP is used in x86-64 versions of Windows Vista for greater security.

Digital Rights Management

Microsoft is introducing a number of Digital Rights Management and content-protection features in Windows Vista, to help digital content providers and corporations protect their data from being copied.

- PUMA: Protected User Mode Audio (PUMA) is the new User Mode Audio (UMA) audio stack. Its aim is to provide an environment for audio playback that restricts the copying of copyrighted audio, and restricts the enabled audio outputs to those allowed by the publisher of the protected content.[7]
- Protected Video Path - Output Protection Management (PVP-OPM) is a technology that prevents copying of protected digital video streams, or their display on video devices that lack equivalent copy protection (typically HDCP). Microsoft claims that without these restrictions the content industry may prevent PCs from playing copyrighted content by refusing to issue license keys for the encryption used by HD DVD, Blu-Ray Disc, or other copy-protected systems.[7]
- Protected Video Path - User-Accessible Bus (PVP-UAB) is similar to PVP-OPM, except that it applies encryption of protected content over the PCI Express bus.
- Rights Management Services (RMS) support, a technology that will allow corporations to apply DRM-like restrictions to corporate documents, email, and intranets to protect them from being copied, printed, or even opened by people not authorized to do so.
- Windows Vista introduces a *Protected Process* [8], which differs from usual processes in the sense that other processes cannot manipulate the state of such a process, nor can threads from other processes be introduced in it. A *Protected Process* has enhanced access to DRM-functions of Windows Vista. However, currently, only the applications using *Protected Video Path* can create Protected Processes.

These Digital Rights Management features have been criticised by some as more restrictive than useful for the user.

Application isolation

Windows Vista introduces *Mandatory Integrity Control* to set integrity levels for processes. A low integrity process can not access the resources of a higher integrity process. This feature is being used to enforce application isolation, where applications in a medium integrity level, such as all applications running in the standard user context can not hook into system level processes which run in high integrity level, such as administrator mode applications but can hook onto lower integrity processes like Windows Internet Explorer 7 or 8 (the latter of which is in beta, as of August 31, 2008). A lower privilege process cannot perform a window handle validation of higher process privilege, cannot SendMessage or PostMessage to higher privilege application windows, cannot use thread hooks to attach to a higher privilege process, cannot use Journal hooks to monitor a higher privilege process and cannot perform DLL–injection to a higher privilege process.

Windows Service Hardening

A new security feature called *Windows Service Hardening* prevents Windows services from doing operations on file systems, registry or networks[9] which they are not supposed to, thereby reducing the overall attack surface on the system and preventing entry of malware by exploiting system services. Services are now assigned a per-service Security identifier (SID), which allows controlling access to the service as per the access specified by the security identifier. A per-service SID may be assigned during the service installation via the *ChangeServiceConfig2* API or by using the `SC.EXE` command with the *sidtype* verb. Services can also use access control lists (ACL) to prevent external access to resources private to itself.

Services in Windows Vista also run in a less privileged account such as *Local Service* or *Network Service*, instead of the *System* account. Previous versions of Windows ran system services in the same login session as the locally logged-in user (Session 0). In Windows Vista, Session 0 is now reserved for these services, and all interactive logins are done in other sessions.[10] This is intended to help mitigate a class of exploits of the Windows message-passing system, known as Shatter attacks. The process hosting a service has only the privileges specified in the *RequiredPrivileges* registry value under *HKLM\System\CurrentControlSet\Services*.

Services also need explicit write permissions to write to resources, on a per-service basis. By using a write-restricted access token, only those resources which have to be modified by a service are given write access, so trying to modify any other resource fails. Services will also have pre-configured firewall policy, which gives it only as much privilege as is needed for it to function properly. Independent software vendors can also use Windows Service Hardening to harden their own services.

Authentication and logon

Graphical identification and authentication (GINA), used for secure authentication and interactive logon has been replaced by Credential Providers. Combined with supporting hardware, Credential Providers can extend the operating system to enable users to log on through biometric devices (fingerprint, retinal, or voice recognition), passwords, PINs and smart card certificates, or any custom authentication package and schema third party developers wish to create. Smart card authentication is flexible as certificate requirements are relaxed. Enterprises may develop, deploy, and optionally enforce custom authentication mechanisms for all domain users. Credential Providers may be designed to support Single sign-on (SSO), authenticating users to a secure network access point (leveraging RADIUS and other technologies) as well as machine logon. Credential Providers are also designed to support application-specific credential gathering, and may be used for authentication to network resources, joining machines to a domain, or to provide administrator consent for User Account Control. Authentication is also supported using IPv6 or Web services. A new Security Service Provider, CredSSP is available through SSPI that enables an application to delegate the user's credentials from the client (by using the client-side SSP) to the target server (through the server-side SSP). The CredSSP is also used by Terminal Services to provide single sign-on.

Windows Vista can authenticate user accounts using Smart Cards or a combination of passwords and Smart Cards (Two-factor authentication). Windows Vista can also use smart cards to store EFS keys. This makes sure that encrypted files are accessible only as long as the smart card is physically available. If smart cards are used for logon, EFS operates in a single sign-on mode, where it uses the logon smart card for file encryption without further prompting for the PIN.

Fast User Switching which was limited to workgroup computers on Windows XP, can now also be enabled for computers joined to a domain, starting with Windows Vista. Windows Vista also includes authentication support for the *Read-Only Domain Controllers* introduced in Windows Server 2008.

Cryptography

Windows Vista features an update to the Crypto API known as Cryptography API: Next Generation (CNG). The CNG API is a user mode and kernel mode API that includes support for Elliptic Curve Cryptography (ECC) and a number of newer algorithms that are part of the National Security Agency (NSA) Suite B (http://www.nsa.gov/ia/industry/crypto_suite_b.cfm) . It is extensible, featuring support for plugging in custom cryptographic APIs into the CNG runtime. It also integrates with the smart card subsystem by including a Base CSP module which implements all the standard backend cryptographic functions that developers and smart card manufacturers need, so that they do not have to write complex CSPs. The Microsoft Certificate Authority can issue ECC certificates and the certificate client can enroll and validate ECC and SHA-2 based certificates.

Revocation improvements include native support for the Online Certificate Status Protocol (OCSP) providing real-time certificate validity checking, CRL prefetching and CAPI2 Diagnostics. Certificate enrollment is wizard-based, allows users to input data during enrollment and provides clear information on failed enrollments and expired certificates. CertEnroll, a new COM-based enrollment API replaces the *XEnroll* library for flexible programmability. Credential roaming capabilities replicate Active Directory key pairs, certificates and credentials stored in *Stored user names and passwords* within the network.

Network Access Protection

Windows Vista introduces Network Access Protection (NAP), which makes sure that computers connecting to a network or communicating over a network conform to a required level of *system health* as has been set by the administrator of the network. Depending on the policy set by the administrator, the computers which do not meet the requirements will either be warned and granted access or allowed a limited access to network resources or completely denied access. NAP can also optionally provide software updates to a non-compliant computer to upgrade itself to the level as required to access the network, using a *Remediation Server*. A conforming client is given a *Health Certificate*, which it then uses to access protected resources on the network.

A *Network Policy Server*, running Windows Server 2008 acts as health policy server and clients need to use Windows Vista or newer. A VPN server, RADIUS server or DHCP server can also act as the health policy server.

Other TCP/IP stack security features

- The interfaces for TCP/IP security (filtering for local host traffic), the firewall hook, the filter hook, and the storage of packet filter information has been replaced with a new framework known as the Windows Filtering Platform (WFP). WFP provides filtering capability at all layers of the TCP/IP protocol stack. WFP is integrated in the stack, and is easier for developers to build drivers, services, and applications that must filter, analyze, or modify TCP/IP traffic.

- In order to provide better security when transferring data over a network, Windows Vista provides enhancements to the cryptographic algorithms used to obfuscate data. Support for 256-bit and 384-bit Diffie-Hellman (DH) algorithms, as well as for 128-bit, 192-bit and 256-bit Advanced Encryption Standard (AES) is included in the network stack itself and in the Kerberos protocol and GSS messages. Direct support for SSL and TLS connections in new Winsock API allows socket applications to directly control security of their traffic over a network (such as providing security policy and requirements for traffic, querying security settings) rather than having to add extra code to support a secure connection. Computers running Windows Vista can be a part of logically isolated networks within an Active Directory domain. Only the computers which are in the same logical network partition will be able to access the resources in the domain. Even though other systems may be physically on the same network, unless they are in the same logical partition, they wont be able to access partitioned resources. A system may be part of multiple network partitions. The Schannel SSP includes new cipher suites that support Elliptic curve cryptography, so ECC cipher suites can be negotiated as part of the standard TLS handshake. The Schannel interface is pluggable so advanced combinations of cipher suites can substitute a higher level of functionality.

- IPsec is now fully integrated with Windows Firewall and offers simplified configuration and improved authentication. IPsec supports IPv6, including support for Internet key exchange (IKE), AuthIP and data encryption, client-to-DC protection, integration with Network Access Protection and Network Diagnostics Framework support. To increase security and deployability of IPsec VPNs, Windows Vista includes AuthIP which extends the IKE cryptographic protocol to add features like authentication with multiple credentials, alternate method negotiation and asymmetric authentication. [11]

- Security for wireless networks is being improved with improved support for newer wireless standards like 802.11i (WPA2). EAP Transport Layer Security (EAP-TLS) is the default authentication mode. Connections are made at the most secure connection level supported by the wireless access point. WPA2 can be used even in ad-hoc mode. Windows Vista enhances security when joining a domain over a wireless network. It can use *Single Sign On* to use the same credentials to join a wireless network as well as the domain housed within the network. [12] In this case, the same RADIUS server is used for both PEAP authentication for joining the network and MS-CHAP v2 authentication to log in to the domain. A bootstrap wireless profile can also be created on the wireless client, which first authenticates the computer to the wireless network and joins the network. At this stage, the machine still does not have any access to the domain resources. The machine will run a script, stored either on the system or on USB thumb drive, which authenticates it to the domain. Authentication can be done wither by using username and password combination or security certificates from a Public key infrastructure (PKI) vendor such as VeriSign.

- Windows Vista also includes an Extensible Authentication Protocol Host (EAPHost) framework that provides extensibility for authentication methods for commonly used protected network access technologies such as 802.1X and PPP.[13] It allows networking vendors to develop and easily install new authentication methods known as EAP methods.

- Windows Vista Service Pack 1 includes Secure Socket Tunneling Protocol, a new Microsoft proprietary VPN protocol which provides a mechanism to transport Point-to-Point Protocol (PPP) traffic (including IPv6 traffic) through an SSL channel.

x86-64 -specific features

- 64-bit versions of Windows Vista enforce hardware-based Data Execution Prevention (DEP), with no fallback software emulation. This ensures that the less effective software-enforced DEP (which is only safe exception handling and unrelated to the NX bit) is not used. Also, DEP, by default is enforced for all 64-bit applications and services on x86-64 versions and those 32-bit applications that opt-in. In contrast, in 32-bit versions, software-enforced DEP is an available option and by default, is enabled only for essential system components.
- An upgraded Kernel Patch Protection, also referred to as *PatchGuard*, prevents third-party software, including kernel-mode drivers from modifying the kernel, or any data structure used by the kernel, in any way; if any modification is detected, the system is shutdown. This mitigates a common tactic used by rootkits to hide themselves from user-mode applications.[14] PatchGuard was first introduced in the x64 edition of Windows Server 2003 Service Pack 1, and was included in Windows XP Professional x64 edition.
- Kernel-mode drivers on 64-bit versions of Windows Vista must be digitally signed; even administrators will not be able to install unsigned kernel-mode drivers[15]. A boot-time option is available to disable this check for a single session of Windows. 64-bit user-mode drivers are not required to be digitally signed.
- *Code Integrity* check-sums signed code. Before loading system binaries, it is verified against the check-sum to ensure it has not modified. The binaries are verified by looking up their signatures in the system catalogs. The Windows Vista boot loader checks the integrity of the kernel, the Hardware Abstraction Layer (HAL), and the boot-start drivers. Aside from the kernel memory space, *Code Integrity* verifies binaries loaded into a *protected process* and system installed dynamic libraries that implement core cryptographic functions.

Other features and changes

A number of specific security and reliability changes have been made:

- Software Restriction Policies introduced in Windows XP have been improved in Windows Vista. [16] A new *Basic user* level has been added to the *Security level*. The default hash rule algorithm has been upgraded from MD5 to the stronger SHA256. Certificate rules can now be enabled through the Enforcement Property dialog box from within the Software Restriction Policies snap-in extension.
- Additional EFS settings allow configuring when encryption policies are updated, whether files moved to encrypted folders are encrypted, Offline Files cache files encryption and whether encrypted items can be indexed by Windows Search.
- The *Stored User Names and Passwords* (Credentials Manager) feature includes a new wizard to backup user names and passwords to a file and restore them on systems running Windows Vista or later operating systems.
- A new policy setting in Group Policy enables the display of the date and time of the last successful interactive logon, and the number of failed logon attempts since the last successful logon with the same user name. This will enable a user to determine if the account was used without his or her knowledge. The policy can be enabled for local users as well as computers joined to a functional-level domain.
- Windows Resource Protection prevents potentially damaging system configuration changes,[17] by preventing changes to system files and settings by any process other than Windows Installer. Also, changes to the registry by unauthorized software are blocked.
- Protected-Mode Internet Explorer: Internet Explorer 7 and later introduce several security changes such as phishing filter, ActiveX opt-in, URL handling protection, protection against cross-domain scripting attacks and status-bar spoofing. They run as a low integrity process on Windows Vista,

can write only to the *Temporary Internet Files* folder, and cannot gain write access to files and registry keys in a user's profile, protecting the user from malicious content and security vulnerabilities, even in ActiveX controls. Also, Internet Explorer 7 and later use the more secure *Data Protection API* (DPAPI) to store their credentials such as passwords instead of the less secure *Protected Storage (PStore)*.

- *Network Location Awareness* integration with the Windows Firewall. All newly connected networks get defaulted to "Public Location" which locks down listening ports and services. If a network is marked as trusted, Windows remembers that setting for the future connections to that network.
- User-Mode Driver Framework prevents drivers from directly accessing the kernel but instead access it through a dedicated API. This new feature is important because a majority of system crashes can be traced to improperly installed third-party device drivers.[18]
- Windows Security Center has been upgraded to detect and report the presence of anti-malware software as well as monitor and restore several Internet Explorer security settings and User Account Control. For anti-virus software that integrates with the *Security Center*, it presents the solution to fix any problems in its own user interface. Also, some Windows API calls have been added to let applications retrieve the aggregate health status from the Windows Security Center, and to receive notifications when the health status changes.
- Protected Storage (PStore) has been deprecated and therefore made read-only in Windows Vista. Microsoft recommends using DPAPI to add new PStore data items or manage existing ones. [19] Internet Explorer 7 and later also use DPAPI instead of PStore to store their credentials.
- The built-in administrator account is disabled by default on a clean installation of Windows Vista. It cannot be accessed from safe mode too as long as there is at least one additional local administrator account.

See also

- Computer security

References

1. ^ Steve Lipner, Michael Howard (March 2005). "The Trustworthy Computing Security Development Lifecycle (http://msdn.microsoft.com/security/default.aspx?pull=/library/en-us/dnsecure/html/sdl.asp) ". Microsoft Developer Network. Retrieved on 2006-02-15.
2. ^ Charles (2007-03-05). "UAC - What. How. Why. (http://channel9.msdn.com/ShowPost.aspx?PostID=288259) " (video). Retrieved on 2007-03-23.
3. ^ "Windows Vista Beta 2 BitLocker Drive Encryption Step-by-Step Guide (http://www.microsoft.com/technet/windowsvista/library/c61f2a12-8ae6-4957-b031-97[illegible].mspx) ". Microsoft TechNet (2005). Retrieved on 2006-04-13.
4. ^ The January 2006 issue of The Cable Guy (http://www.microsoft.com/technet/community/columns/cableguy/cg0106.mspx) covers the new features and interfaces in Windows Firewall in greater detail.
5. ^ Michael Howard (May 26, 2006). "Address Space Layout Randomization in Windows Vista (http://blogs.msdn.com/michael_howard/archive/2006/05/26/608315.aspx) ". Microsoft. Retrieved on 2006-05-26.
6. ^ Security advancements in Windows Vista (http://download.microsoft.com/download/c/2/9/c2935f83-1a10-4e4a-a137-c1db8[illegible]/WindowsVistaSecurityWP.doc)
7. ^ *a b* "Output Content Protection and Windows Vista (http://www.microsoft.com/whdc/device/stream/output_protect.mspx) ". *WHDC*. Microsoft (April 27, 2005). Retrieved on 2006-04-30.
8. ^ Protected Processes in Windows Vista (http://www.microsoft.com/whdc/system/vista/process_Vista.mspx)
9. ^ "Windows Vista Security and Data Protection Improvements – Windows Service Hardening (http://www.microsoft.com/technet/windowsvista/evaluate/feat/secfeat.mspx#EEF ". *TechNet*. Microsoft (June 1, 2005). Retrieved on 2006-05-21.
10. ^ Impact of Session 0 Isolation on Services and Drivers in Windows Vista (http://www.microsoft.com/whdc/system/vista/services.mspx) covers Windows Vista's session isolation changes.
11. ^ AuthIP in Windows Vista (http://www.microsoft.com/technet/community/columns/cableguy/cg0806.mspx)
12. ^ The Cable Guy: Wireless Single Sign-On (http://www.microsoft.com/technet/technetmag/issues/2007/11/CableGuy/?loc=e
13. ^ EAPHost in Windows (http://www.microsoft.com/technet/technetmag/issues/2007/05/cableguy/default
14. ^ Field, Scott (2006-08-11). "An Introduction to Kernel Patch Protection (http://blogs.msdn.com/windowsvistasecurity/archive/2006/08/11/695993.asp ". *Windows Vista Security blog*. MSDN Blogs. Retrieved on 2006-08-12.
15. ^ "Digital Signatures for Kernel Modules on x64-based Systems Running Windows Vista (http://www.microsoft.com/whdc/system/platform/64bit/kmsigning.mspx) ". *WHDC*. Microsoft (May 19, 2006). Retrieved on 2006-05-19.
16. ^ Using Software Restriction Policies to Protect Against Unauthorized Software (http://technet.microsoft.com/en-us/windowsvista/aa940985.aspx)
17. ^ Windows Vista Management features (http://www.microsoft.com/technet/windowsvista/evaluate/feat/mngfeat.mspx)
18. ^ CNET.com (2007). "Windows Vista Ultimate Review (http://reviews.cnet.com/Windows_Vista_Ultimate/4505-3672_7-32013603.htn ". Retrieved on 2007-01-31.
19. ^ SPAP Deprecation (PStore) (http://msdn2.microsoft.com/en-us/library/aa480152.aspx#appcomp_topic25)

External links

- Vulnerability Report: Microsoft Windows Vista (http://secunia.com/product/13223/?task=advisories) including known unpatched vulnerabilities from Secunia
- Vista vulnerabilities (http://www.securityfocus.com/cgi-bin/index.cgi?c=12&op=display_list&vendor=Microsoft&title=Windows%20Vista) from SecurityFocus

Retrieved from "http://en.wikipedia.org/wiki/Security_and_safety_features_new_to_Windows_Vista"
Categories: Windows Vista | Software features | Microsoft Windows security technology

- This page was last modified on 11 November 2008, at 07:32.