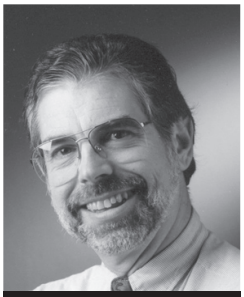
An early look at Windows Vista security


Edward Ray


E. Eugene Schultz

Edward Ray, CISSP, GCIA, GCIH, MCSE-Security, PE
NetSec Design and Consulting

E. Eugene Schultz, Ph.D., CISSP, CISM
High Tower Software

Edward Ray and E Eugene Schultz scrutinise whether Microsoft's upcoming new OS will fulfill its security promises.

Windows Vista, the new Microsoft workstation operating system, will be released on 30 January 2007. Windows Vista includes many new features, a few of which include a new graphics engine, a much-changed user interface, an enhanced desktop search function, a new version of media player, the Windows Presentation Foundation (WPF) (which provides new visual effects and perspectives as well as application development support), the Network Center (which provides a large number of networking enhancements and capabilities), and an improved version of Windows Explorer. Also included are "under the hood" improvements in areas such as security and manageability as well as power management. Six versions of Windows Vista will be available, ranging from Windows Vista Starter, a low-end version not available in Europe, Canada, and the US that provides little more than an inexpensive alternative to pirated versions of this operating system, to Windows Vista Ultimate, which offers all of the features of the other versions of this operating system in addition to support for podcast creation, game performance enhancements, and advanced online services for downloadable media, and other sophisticated features.

Like any new operating system or application product, the release of Windows Vista will have many security implications. If the trend continues, Windows Vista should be intrinsically more secure than previous versions of Windows operating systems.[1] Microsoft's claims concerning security in Vista have not been modest. For example, Jim Allchin, co-president of Microsoft's platforms and services division, has said: "Windows Vista will not need antivirus." While many view Allchin's statement with skepticism or even outright sarcasm, they will, however, have difficulty denying that Windows Vista will at least offer many security features that are either new or improved compared to Windows XP and Windows Server 2003. These features, however, come at a potentially steep price, both for home users, and for volume business licensing. This article analyzes eight of these new and/or improved security features, discusses alternatives in Windows XP and Windows Server 2003, and explores whether or not these features are worth the hassles and costs associated with upgrading to Windows Vista.

New security features

Windows Vista offers many new security-related features.[2] Some of the most important of these features include:

User Account Control (UAC)

To install and run programs on Windows systems, one must have Administrator privileges. Running with Administrator privileges, however, makes compromising systems much easier, as in the following examples:

- A user may unknowingly download and install malware from a malicious or infected website.
- A user can be tricked into opening an email attachment that contains malware and potentially installs and runs on the computer without the user's knowledge or consent.
- A removable drive (i.e. USB memory stick) can be inserted into a computer and Autoplay will attempt to run software (malicious or non-malicious) without user intervention.
- A user can install unsupported applications that can adversely affect a Windows system's performance or reliability.

With UAC, Windows Vista provides a method of separating standard user privileges and tasks from those requiring Administrative access. In standard user mode, users will be able to perform more tasks and run applications without needing to be logged on as Administrator. In addition, while users are logged on as Administrator, the Administrator Approval Mode feature in the UAC technology also helps to prevent malware from infecting users' computers. Even though users are logged on as Administrator, most programs and tasks will be run under standard user privileges. When users need to

perform administrative tasks such as installing new software or modifying certain system settings, they will first be prompted for their consent before they can complete such tasks. Note, however, that from a security perspective this feature does not quite provide the same level of security as when a user simply logs on to an unprivileged account. Still, it provides a layer of protection that is missing in Windows XP or Windows Server 2003.

Windows Defender

This program helps protect Windows Vista against pop-up ads, slow performance, and security threats due to spyware, adware, keyloggers and other unwanted software. Windows Defender monitors in real-time protected areas within the Windows Vista operating system that unwanted software targets, such as the Startup folder and Autorun entries in the registry. When a program tries to modify a protected area or function in Windows Vista, Windows Defender prompts the user to either allow or reject the change in an effort to guard against unwanted installation of software or operating system modifications. Windows Defender is enabled by default and uses signature updates to keep up with the latest attacks. It is thus not as robust as antivirus software that uses behavioral modeling as well as signatures to detect malicious software, however. Windows Defender is thus intended to serve as a complement to already installed third-party antivirus software. Note that Windows Defender is also available as a download for Windows XP or Windows Server 2003, and it performs the same functions as in Windows Vista.

Windows Firewall

A personal firewall is a critical line of defense against attempted intrusions, malware infections, denial-of-service attacks, and other types of attacks. Like the firewall functionality in Windows XP Service Pack 2 (SP2), the firewall in Windows Vista is enabled by default to help protect the user's computer as soon as the operating system is started. The Windows XP firewall restricts only inbound traffic, whereas the Windows Vista firewall supports both inbound and outbound filtering to help protect users by restricting certain outbound connections that infected or compromised PCs often attempt to establish. The firewall is also integrated with Windows Vista network awareness so that specialized rules can be applied, depending on the location of the client computer. For example, firewall rules can be defined separately for users when they are logged on to the corporate domain as opposed to when they are logged on to a public network (i.e. a wireless hotspot). Firewall management in Windows Vista is also integrated with Internet Protocol Security (IPSec) in a single console known as the "Windows Firewall with Advanced Security Console." This allows for centralization of inbound/outbound filtering and IPsec server/domain isolation settings in the user interface to simplify configuration and reduce policy conflicts. As with Windows Defender, the Windows Firewall complements (but not necessarily altogether replaces) current third-party security solutions.

Internet Explorer 7 (IE7)

No single application epitomises Microsoft's past security failures than Internet Explorer (IE). With IE 7, Microsoft is attempting to improve IE's image. IE 7 is available for Windows XP as well as Windows Vista, but certain IE 7 security features are available only with Windows Vista. New security technologies in IE 7 include:

- **Internet Explorer Protected Mode**
  Available only in Windows Vista, this feature helps reduce previous software vulnerabilities in browser extensions by eliminating the possibility of using them to install malicious software without a user's knowledge or consent. Protected Mode uses mechanisms with higher integrity levels that restrict access to processes, files and registry keys to accomplish this goal. In protected mode, system files and settings cannot be changed without a user's explicit permission.

- **ActiveX Opt-in**
  ActiveX controls have been a major weakness in IE. Some enterprises ban them outright or allow only certain ActiveX controls (such as Microsoft Update). Although many security experts advocate disabling ActiveX on Windows systems, the functionality of many websites (including online bank websites) depends on the availability of ActiveX controls on browsers. With IE 7, Microsoft introduces the concept of "ActiveX opt-in," a feature that automatically disables all controls that are not explicitly allowed by the user. In Windows Vista, the Information Bar prompts users before they can access a previously installed ActiveX control that has not yet been used on the Internet. By providing a mechanism for the user to permit or deny access for each ActiveX control before it is used, ActiveX opt-in further reduces the probability of a successful attack. Websites with functionality that depends on ActiveX controls may conceivably in time no longer be viable because of ActiveX opt-in.

- **Cross-site scripting attack protection**
  Cross-site (also known as cross-domain) scripting has plagued virtually all browsers, IE very much included. In a cross-site scripting attack, a user might visit a page on a malicious website that opens a new browser window containing a legitimate page (i.e. one at a bank website) that prompts the user to enter account information. This information could then be extracted by a malicious script and made available to the attacker. In IE 7, new cross-site script barriers help limit

the ability of malicious websites to manipulate vulnerabilities in other websites.

- **Phishing Filter**
  Phishing is a technique that many attackers use to trick computer users into revealing personal or financial information through specially worded email messages or websites. "Phishers" masquerade as legitimate persons or businesses to deceive people into revealing personal information (e.g., passwords, credit card numbers, and social security numbers). The phishing Filter in IE 7 helps protect users from succumbing to phishing scams by:
  - Comparing the addresses of websites that a user attempts to visit with a list of reported legitimate sites stored on the user's computer.
  - Analyzing websites that users visit by checking them for characteristics common to phishing sites.
  - Sending the address of a website that a user visits to a Microsoft online service that checks the site against a constantly updated list of known phishing sites.

Even if the site is unknown to the Phishing Filter service, IE 7 examines the behaviour of the site and informs the user if the site is doing anything suspicious. By doing this, the Phishing Filter helps to prevent a site from collecting user information before it has been officially reported.

Encrypting File System (EFS)

The EFS feature, which encrypts files and folders to help protect data from unauthorized access, is similar to EFS in prior Windows operating systems. Users who have authorized keys are able to access and work with encrypted files just as they would with any other file. Unauthorized users are denied access. Windows Vista adds new security, performance and manageability features including storage of user and recovery keys on smartcards, encrypting Windows page file, and encrypting the offline files cache. In addition, a number of group policy options have been added to Windows Vista to help system and security administrators define and implement organizational policies for EFS.

Device control

The threat of unauthorized use of USB key drives or other removable storage device installation on client computers creates significant security risks for many organizations. A malicious user can potentially use a removable storage device to steal a company's intellectual property. An attacker could also use a removable storage device with malicious software configured on it that includes an "Autorun" script to install malicious software on an unattended client computer. Windows Vista enables IT administrators to use Group Policy to help manage installation of unsupported or unauthorized devices. For example, you can allow users to install entire classes of devices (such as printers), but disallow any kind of removable storage device. An administrator is allowed to override these policies to install authorized hardware. Windows Vista now also supports user-level access controls for read and write access to installed devices. For example, you can allow full read and write access to an installed device such as a USB flash drive to one user account, but only allow read access to another user account on the same computer. Additional information about device control and how you can configure it is included in Microsoft's Step-By-Step Guide to Controlling Device Installation and Usage with Group Policy.[3]

BitLocker Drive Encryption

BitLocker drive encryption, which is only available in Windows Vista Enterprise and Ultimate editions, helps protect data on a client computer. When an attacker gains physical access to a computer, the potential consequences include:

- The attacker can log on to Windows Vista and copy files.
- The attacker can restart the client computer by booting another operating system to view file names, copy files, and read the contents of the hibernation or page file to discover plaintext copies of sensitive information.

Even if the files are encrypted using Encrypting File System (EFS), a careless user might move or copy a file from an encrypted location to an unencrypted location, which could leave the file in plaintext. Attackers could also tamper with the system and boot files, which may prevent normal system operation. BitLocker mitigates this risk by encrypting the entire Windows volume to help prevent unauthorized users from breaking Windows file and system protections or viewing information offline on the secured drive. Early in the startup process, BitLocker checks the client computer's system and hardware integrity. If BitLocker determines an attempt has been made to tamper with any system files or data, the client computer will not complete the startup process. This protection is obtained if the computer has a Trusted Platform Module (TPM 1.2) to protect user data and to help ensure that a client computer running Windows Vista cannot be tampered with while the system is offline. If no TPM is available, BitLocker can still help protect the data, but no system integrity validation is performed. BitLocker does not encrypt data stored outside the Windows partition, but does provide an extra added security layer for EFS by encrypting the EFS keys within the Windows partition.

Rights Management Services (RMS)

The purpose of RMS is to provide security for sensitive company documents. RMS persistently encrypts information, so that as a file or email message is transmitted enterprise-wide, only individuals who are authenticated and explicitly authorized to access it can do so. RMS requires a server (Windows 2003 or later) with Windows Rights Management installed, a Window Vista RMS client, and a RMS application that is designed to encrypt and control usage of the information it manages.

Will it be worth it?

Predictably, Microsoft marketing is touting Windows Vista as the "best thing since sliced bread." At the same time, however, organizations and individuals must at some point make a decision concerning whether or not to upgrade to this new operating system. Windows Vista offers many new features, but Windows XP, Microsoft's earlier workstation operating system, has proven to have many useful features, so many that now organizations and individuals are faced with the issue of potentially diminishing returns in migrating from Windows XP to Windows Vista. In other words, Windows XP works well – is it worth the trouble and expense of upgrading to Windows Vista when Windows XP basically delivers what most people want?

The central focus of this paper, however, is on Windows Vista security, not the entire set of functions in this new operating system. Windows XP security was better than in Windows 2000 or Windows NT, yet Windows XP systems too frequently have fallen prey to malware and intruders. Windows Vista offers a number of new security features that appear to reduce the vulnerability of this new operating system to many types of security threats, but nearly every new feature comes at some cost – in particular; numerous usability liabilities. For example, the new IE7 features reduce the likelihood of malware being installed in Windows Vista systems via this browser. The price to be paid is users frequently getting prompted concerning whether or not to download something.[4] It is safe to say that most users will not really understand the meaning or purpose of these features. Additionally, they are likely to soon become irritated by the barrage of dialog boxes that will appear in connection with this function; they are, consequently, likely to disable these features.

Consider also the potential complications in connection with Windows Vista's BitLocker functionality. Any time encryption is used, key escrow considerations become paramount. If BitLocker's key escrow capabilities work as advertised, data loss due to key destruction or corruption will not occur. Similarly, mechanisms that check for and enforce legitimate software licensing have typically caused undesirable side effects. BitLocker's integrity checking function could thus misfire to the point that users of legitimate versions of Windows Vista could be denied access to their own systems.

So, do the security-related benefits of Windows Vista outweigh the costs? There is no question that Windows Vista represents a genuine improvement in security capabilities compared to its predecessors (e.g., Windows XP). In particular, any built-in features that lower the potential for malware infections in Windows operating systems are potentially extremely valuable. Additionally, the fact that Windows Vista security has to a greater extent been built for inexperienced users, users who are unlikely to get much if any support from professional system administrators, is a major advantage of this new operating system. At the same time, however, the downsides of many of the new security-related features in Windows Vista are not presently very well understood. An understanding of these downsides will come over time – as the Windows Vista user community interacts with these features in the many contexts in which this new operating system will be deployed. The answer to this question, therefore, is that time will tell. One thing is certain – most organizations and individuals who currently use Windows XP are sufficiently happy with it and have no huge impetus to make the switch to Windows Vista. Even though Windows XP systems have too frequently succumbed to attacks, organizations and individuals have developed a certain level of comfort with security in this older operating system and have learned to deploy a sufficient number of ancillary controls such as installing and updating antivirus and antispyware software and deploying personal firewalls to bring down security-related risks in connection with using this software to an acceptable level. A widespread switch to Windows Vista will thus happen in time, but it is extremely unlikely that it will happen in the near future.

References

1 Schultz, E. E., Windows security: Is it getting any better? Proceedings of International Security Summit-Prague, 2005.

2 Windows Vista Security Guide, 2006. www.microsoft.com/downloads/details.aspx?FamilyId=A3D1BBED-7F35-4E72-BFB5-B84A526C1565&displaylang=en.

3 Microsoft Corporation, Windows Vista: Step-By-Step Guide to Controlling Device Installation and Usage with Group Policy, 2006. http://www.microsoft.com/technet/windowsvista/library/9fe5bf05-a4a9-44e2-a0c3-b4b4eaaa37f3.mspx

4 Sturgeon, W., Is Vista security a selling point? Web posting, November 20, 2006. http://news.com.com/Is+Vista™+security+a+selling+point/2100-1029_3-6137223.html