

Overview of Windows Vista Security: Part One

By Edward Ray and E. Eugene Schultz

Windows Vista was released to the public on the evening of January 29, 2007 – its most touted features are related to security.

Windows Vista was released to the public on the evening of January 29, 2007 with an extravaganza on Times Square in New York City. Vista replaces Windows XP, which was released in October, 2001. Windows Vista includes many new features: a new graphics engine, a substantially different “look and feel” user interface, an improved desktop search function, extended media capabilities, the Windows Presentation Foundation that delivers new visual effects and perspectives in addition to application development support, the Network Center that provides a large number of networking enhancements and capabilities, a much improved version of Windows Explorer, and added security and parental controls.¹ Six versions of Windows Vista are available, ranging from Windows Vista Starter, a low-end version not available in Europe, Canada, or the US, that provides little more than an inexpensive alternative to illegal versions of this product, to Windows Vista Ultimate, which incorporates all features in the other versions of this operating system in addition to game performance improvements, advanced on-line services for downloadable media, support for podcast creation, and other advanced functionality. Windows Vista’s most touted features are, however, related to security, the focus of this article.

Vista represents a new Microsoft effort to protect its users from malware and other forms of compromise. If the trend continues, Windows Vista should be intrinsically more secure than previous versions of Windows operating systems.² Microsoft has already made numerous statements concerning the improved level of security in Windows Vista. For instance, Jim Allchin, co-president of Microsoft’s Platforms and Services Division, has stated “Windows Vista will not need anti-virus.”³ Although this statement appears to be an overly optimistic embellishment of the truth, to say that Windows Vista offers numerous new or enhanced security features compared to Windows XP and 2003 is no overstatement whatsoever. Many of

these features present cost-benefit dilemmas, however, for home users because of usability hurdles in Windows Vista; and volume business licensing is likely to be beset with complications. This first of three articles analyzes three of these new and/or improved security features, discusses alternatives under Windows XP and 2003 and explores whether or not these features are worth the hassles and costs associated with upgrading to Windows Vista.

User Account Control (UAC)

Administrator privileges, privileges intended to be assigned to system administrators, are required to install and run programs on Windows systems. Windows users thus tend to run their systems with Administrator privileges. Running with Administrator privileges, however, makes compromising systems much easier; for example, users may naively download and install malware from a malicious or infected Web site or may be tricked into opening e-mail attachments containing malware that installs and runs itself on a computer without the users’ knowledge or consent. A USB memory stick can also be inserted into a computer running XP and Autoplay will attempt to run software (malicious or non-malicious) without user intervention. Finally, users can install unsupported applications that can affect Windows system’s performance and 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 the need to be logged on as Administrator. Additionally, while users are logged on as Administrator, the Administrator Approval Mode feature in the UAC technology helps keep malware from infecting the computer. Even though users are logged on as Administrator, most programs and tasks will 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 that from a security perspective this feature is not quite as good as simply logging on as a normal user, but it nevertheless provides a layer of protection not currently found in Windows XP or Windows Server 2003.

1 Edward W. Ray and E. E. Schultz, “Windows Vista security: Is it worth it?” *Computer Fraud and Security*, January, 2007.

2 E. E. Schultz, “Windows security: Is it getting any better?” *Proceedings of International Security Summit-Prague*, May, 2005.

3 http://www.betanews.com/article/Allchin_Suggests_Vista_Wont_Need_Antivirus/1163104965

These new security features have some drawbacks, however. The UAC feature requires Windows Vista users to specifically approve every interaction involving the installation or execution of external code. However, UAC makes no distinction between installations that are explicitly initiated by the user from the keyboard and those that might be initiated by a malicious web site.⁴ A seemingly endless set of dialog boxes thus appear; users must click “Continue” or reject the proposed software installation. All other work on the system freezes and the screen is darkened until the user makes each decision in the dialog box. The potential of more harm than good resulting thus exists: imagine the potential nightmare scenario of users flooding a corporate help desk continually asking whether to click “Continue” or “Cancel.”

For perspective, security professionals should look at the prior history of Windows operating systems and what the operating system was originally intended to do. Windows was initially created to run on standalone computers; as a result its earlier operating systems lacked the kind of user account controls that are basic in UNIX and Linux operating systems. Microsoft is now playing catch-up. UAC can be best described as a work in progress.

Windows Defender

Windows Defender, also available as a download for Windows XP or 2003, helps protect computers 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 this unwanted intruder software targets, such as the Startup folder and the Autorun entries in the registry. When a program tries to modify a protected area or function in Windows Vista, Windows Defender prompts users 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 many versions of anti-virus software that use behavioral modeling as well as signatures to detect malicious software. This feature is intended to serve as a complement to already installed third-party anti-virus software.

Windows Defender is also available for Windows XP and 2003 and performs the same function as in Vista. However, it is a very poor substitute for third-party anti-spyware solutions. A recent two-week study of Windows Defender showed the product missed 84 percent of a sample set of 25 spyware and malicious code samples.⁵ The programs that Windows Defender missed were a mix of spyware, Trojan horse programs, and keyloggers. The study identified variants of common malware programs like DollarRevenue Trojan, PeperTrojan, and Playboydialler that made it by Windows Defender. Some of the variants were recently released, though others dated back to 2006. Of the four programs Windows Defender did stop, most were non-malicious adware. While many were not Vista compatible and simply crashed, others were able to install on Vista systems. Organizations deploying Windows Vista should thus look at defense-in-depth solutions in addition to Windows Defender.

Windows Firewall

The critical first line of defense against malware is often a personal firewall, as is the case with roaming laptops and home users. Similar to the firewall functionality in Windows XP Service Pack 2, the firewall in Windows Vista is enabled by default to help protect the user's computer as soon as Windows Vista boots.⁶ The Windows XP firewall restricts only inbound traffic, whereas the Windows Vista firewall restricts both inbound and outbound to help protect users by restricting operating system resources that behave unexpectedly. The initial configuration of the Windows Firewall in Windows Vista is inbound traffic filtering only; users will need to enable outbound filtering manually or via Group Policy. 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 the 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 does not necessarily replace) current third-party security solutions.

Conclusion

Windows Vista is based on a new, better security paradigm. The three security features discussed in this article are only a few of the many new security features in this new operating system. Because of the many exposures in Windows systems due to users running workstations with Administrator privileges, the most critical of these features is UAC, although the value of the other features should not in any way be downplayed. From a security perspective, Windows Vista thus looks extremely promising. The main downside is usability. Will users brave the myriad of dialog boxes that inquire whether they really want to do something? Or will they simply opt out of having to approve software downloads and other potentially dangerous events? That remains to be seen.

Next month's article will focus on Internet Explorer 7, Encrypting File System enhancements and device control features.

About the Authors

Edward Ray, CISSP, GCI, GCIH, MCSE, is President of NetSec Design and Consulting, Inc. which specializes in computer, data and network security and secure network design. Mr. Ray is a member of the IEEE and ISSA and can be reached at eray@netsecdesign.com.

Eugene Schultz, Ph.D., CISM, CISSP, is the Chief Technology Officer and Chief Information Security Officer at High Tower Software, a company that develops security event management software. He founded and managed the U.S. Department of Energy's Computer Incident Advisory Capability (CIAC), co-founded FIRST, the Forum of Incident Response and Security Teams, and has been elected to the ISSA Hall of Fame. He can be reached at eeschultz@sbcglobal.net

4 David DeJean, “Counterpoint: Does OS X Really Shine Brighter Than Vista?” *Information Week*, January 19, 2007.

5 <http://www.informationweek.com/story/showArticle.jhtml?articleID=196902106>

6 Microsoft, *Windows Vista Security Guide*, November, 2006. <http://www.microsoft.com/downloads/details.aspx?FamilyId=A3D1BBED-7F35-4E72-BFB5-B84A526C1565&displaylang=en>.