Security Highlights of Windows 7

Windows 7, the latest operating system release from Microsoft®, contains new security features which might be of interest to many DoD and Intelligence Community customers. This guide highlights many of these security features and is for information purposes only. It should in no way be construed as an NSA endorsement of the product.

Security Development Lifecycle

In 2002, Bill Gates stated that security is a major issue and declared "Trustworthy Computing" the company's highest priority. Since then, Microsoft developed the Security Development Lifecycle (SDL) methodology, which utilizes secure design principles such as threat modeling, component isolation, least privilege, and source code testing. A fundamental goal of the SDL process is to reduce the attack surface. Since adoption of the SDL process, the number of Common Vulnerabilities and Exposures (CVE) on Microsoft products in the National Vulnerability Database has declined. Windows Vista was the first operating system that was fully developed under the SDL process. In Windows 7, the SDL process continues via retention of original or enhanced security features from Windows Vista and the introduction of several new security features.

OVERVIEW

Many DoD and Intelligence Community customers have a variety of security needs. Operating Systems are just one component that is relied upon to satisfy these security needs. This guide highlights many of the new security features in Windows 7, just one of the many commercial operating systems available.

SECURITY FEATURES

- Internet Explorer 8
- AppLocker
- DNS Security Extensions
- BitLocker To Go
- Improved User Access Control
- Biometric & Smart Card Enhancements
- Direct Access
- Advanced Firewall Polices

Windows 7 Security Features

Internet Explorer 8 (IE8): Utilizes Data Execution Protection (DEP), provided the hardware supports it, and Address Space Layout Randomization (ASLR) by default to help protect against malicious code execution and incorporates the most recent anti-phishing technology and improved restrictions on ActiveX controls.

AppLocker: Replaces Software Restriction Policy (SRP) and provides greater flexibility to govern which applications are allowed to run and from which locations.

Domain Name System (DNS) Security Extensions: Designed to prevent DNS spoofing, such as DNS cache poisoning, by providing data integrity for DNS client resolvers through digitally signed response to DNS queries.

Bitlocker To Go: Provides encryption support for mass storage devices such as USB flash devices and external hard drives. Support for password-protection and certificate-based authentication is available for IEEE 1667 compliant USB devices.

Improved User Account Control (UAC): Retains same level of security with fewer prompts. This is achieved by a reduction in the number of applications that require elevated privilege, and customization of threat levels for UAC prompts.

Biometric & Smart Card Enhancements: Automates plug-and-play driver installation without user intervention. Supports fingerprint reader and Elliptic Curve Cryptography for Windows Logon.

The Information Assurance Mission at NSA

SNAC DoD 9800 Savage Rd., Ft. Meade, MD 20755-6704 410-854-6632 DSN: 244-6632 FAX: 410-854-6604 www.nsa.gov/snac

Direct Access: Provides seamless and secure access to enterprise resources without the need for a Virtual Private Network (VPN). Leverages Internet Protocol 6 (IPv6) and Internet Protocol security (IPSec) to provide secure network infrastructure.

Advanced Firewall Policies: Allows IT administrators to more easily manage firewall policy by providing the ability to apply separate rules for remote and local client connections to the domain.

Security Features Retained From Windows Vista

Buffer Overflow Protection: Buffer overflows are a common source of vulnerabilities used to gain control of an operating system. Windows 7 retains or improves security features from Vista to help mitigate this issue, including the use of DEP (provided the hardware supports it), ASLR, stack and heap canaries, and exception handling protection.

Least Privilege: Limits the damage from exploiting a service by executing it with its own credentials, restricting access to critical resources. Also, administrator accounts are restricted to user-level permissions by default, limiting the scope of potentially dangerous operations such as web surfing or email reading.

Malware Protection: Provides defense-in-depth protection such as anti-phishing technology, and Windows Defender that offers spyware scanning.

Kernel Protection: Helps prevent rootkit installation via kernel patch protection, which checks the internal kernel data structures for changes (a feature available only on 64-bit versions), and driver signature verification, which ensures code authenticity (enabled by default for both 32-bit and 64-bit versions).

Firewall: A bi-directional firewall, filtering both incoming and outgoing network connections, for defending against malicious activity.

BitLocker: A capability to encrypt hard-drive operating system disk volumes, providing data integrity and confidentiality. When using BitLocker on a machine with a Trusted Platform Module, the boot sequence performs an additional check of the startup code to ensure system integrity.

Security Conclusion

A preliminary System and Network Analysis Center (SNAC) analysis has determined that the new Windows 7 security features, coupled with the use of the SDL process throughout the development cycle, has assisted in the delivery of a more secure product. Windows 7 security features target major avenues of traditional operating system attacks. Because no product is error-free, it is inevitable that security weaknesses will be discovered and new classes of attacks will be invented. Therefore, before deploying any product into an operational environment, information systems security engineering should be applied to address the threats, assess the risks, and minimize potential damage.

SNAC DoD 9800 Savage Rd., Ft. Meade, MD 20755-6704 410-854-6632 DSN: 244-6632 FAX: 410-854-6604 www.nsa.gov/snac