Security Highlights of Windows 10

On November 20, 2015 the Department of Defense (DoD) Chief Information Officer (CIO) published a memo on the subject of "Migration to Microsoft Windows 10 Secure Host Baseline"[1]. This memo serves as notification that the DoD CIO will direct Combatant Commands, Services, Agencies, and Field Activities to rapidly deploy Windows 10 in their organizations, beginning in January 2016. The DoD CIO has requested that senior technology leaders across the DoD examine the costs and benefits of moving to Windows 10, and target completing the deployment by January 2017.

Formal product evaluations and operational guidance efforts also support this move. In February 2016, Windows 10 completed a Common Criteria (CC) evaluation against the NIAP General Purpose Operating System Protection Profile[2]. This evaluation provides assurance that Windows 10 includes security features that address the most serious network threats, and that these features are properly implemented. NIST FIPS 140-2 validation of the cryptographic modules in Windows 10 is currently expected to complete in March 2016. Deployment resources such as the Secure Host Baseline (SHB)[3] provide a hardened operational configuration for Windows 10 and common application software. This allows for deployments that are already compliant with common security baselines.

This document provides a high-level description of new security features in Windows 10 for senior technology leaders. It describes how these features disrupt attacker tools, techniques, and procedures used against National Security Systems today.

To take full advantage of the security enhancements provided by Windows 10, there are certain software, hardware, and firmware requirements that must be met.

- The operating system must be the 64-bit Enterprise Edition of Windows 10.
- The hardware must support memory virtualization (Intel VT-x/AMD-V) and Second Level Address Translation (Intel EPT/AMD-RVI) or SLAT.
- Device virtualization (IOMMU/Intel Vt-d/ AMD-Vi) should be supported by the hardware.
- The firmware must be based on the Unified Extensible Firmware Interface (UEFI), rather than legacy Basic Input Output System (BIOS). UEFI must also be running in native UEFI mode instead of legacy compatibility mode
- The firmware must support Secure Boot and be enabled.
- A version 1.2 or later Trusted Platform Module (TPM) should be enabled.

Security Highlights of Windows 10:

Virtualization-Based Security (VBS): Through the use of Hyper-V and hardware protections, Windows 10 protects critical operating system security components from attacks by compromised processes. VBS requires the features outlined in the figure at the top right of this factsheet.

- **Credential Guard** employs VBS to protect memory access of the Local Security Authority Subsystem Service (LSASS), where certain types of credentials used by Windows authentication mechanisms are stored. This feature addresses credential theft from memory, which is a common technique used in attacks such as Pass-the-Hash or Pass-the-Ticket.

- **Device Guard** expands the use of cryptographic code integrity, first introduced in Windows Vista, through the enforcement of policies where all executed code is cryptographically verified and integrity checked to determine what is and is not allowed to run. Device Guard is an ideal solution for enforcing policy of a hardened administrator workstation.

Control Flow Guard (CFG): CFG mitigates exploits that use certain types of Return-Oriented-Programming (ROP) code from abusing indirect function calls at runtime by verifying the target address is indeed a valid function. Windows 10 and the latest versions of Windows applications from Microsoft have been compiled to take advantage of CFG. Third party application developers should enable CFG protections to take advantage of this new anti-exploitation protection.

Security Highlights of Windows 10

Microsoft Edge: As a replacement for Internet Explorer (IE), Windows 10 ships with a new default web browser, Microsoft Edge. Edge contains most functionality of IE, but with a significantly reduced attack surface. Edge runs in a more restricted sandbox, greatly limiting what an attacker can do in the event of a compromise. Microsoft Edge also supports HTTP Strict Transport Security (HSTS), which protects against TLS downgrade attacks and cookie hijacking.

Enhanced Windows Defender: Windows Defender now runs as a protected process, providing protection from other potentially compromised system components and will consult a Microsoft cloud reputation service for unknown files. Additionally, Defender analyzes network traffic for malicious behavior.

Improved Event Logging: Windows 10 introduces a number of new events and improves existing events to include more information, providing better documentation of actions taken on the system. This increases an administrator's ability to identify malicious activity.

Untrusted Font Blocking: Windows 10 added a new Group Policy option that allows administrators to control loading of untrusted fonts. When enabled, this policy ensures that only fonts from a protected location can be loaded by the operating system and its applications. Additionally, Windows 10 includes the Usermode Font Driver Host, which moves a significant amount of font parsing code to a lower privileged sandboxed context reducing the usefulness of malicious fonts for privilege escalation attacks.

Improved Health Attestation Service: Windows 8.1 introduced the Health Attestation Service, but Windows 10 has greatly improved it. This service allows the operating system to do a system health check (including status of features such as Secure Boot, DEP, BitLocker, AV status, and patches) with the cloud before gaining access to internal resources.

Microsoft Passport: Microsoft Passport (also called Next Generation Credentials), is a new authentication scheme meant to replace the standard user name and password combination. In Windows Passport, a user enrolls their device with a TPM to store a cryptographic credential, and uses a PIN or biometric for authentication. DoD configuration guidance allows for the use of Windows Passport with a 6 digit PIN. This is a first step toward replacing traditional passwords within the DoD.

Antimalware Scan Interface (AMSI): The AMSI is a vendor agnostic interface that allows the operating system to interact with installed antimalware products through a universal mechanism. For example, Powershell, VBSript, and JScript engines now automatically submit script content to AMSI prior to execution, which provides antimalware products the ability to scan unobfuscated versions of code. Microsoft Office also leverages AMSI to scan documents for embedded malware and malicious macros. By default, Windows Defender is the AMSI provider on Windows 10.

Windows as a Service: With Windows 10, Microsoft introduced a new update strategy, focusing on significantly reducing the amount of time before new security features are released. In previous versions of Windows security features were often only released with new releases or service packs, a process that could span multiple years. Now, when features are ready for release, they may be included in patches, ensuring the operating system is always using the latest advancements in exploit mitigation and adversarial detection.

[1] "DoD CIO Memo – Migration to Microsoft Windows 10 Secure Host Baseline" [Online]. Available: http://www.esi.mil/contentview.aspx?id=658
[2] "NIAP General Purpose Operating System Protection Profile" [Online]. Available: https://www.niap-ccevs.org/pp/PP_OS_v4.0
[3] "Secure Host Baseline (SHB)" [Online]. Available: https://disa.deps.mil/ext/cop/iase/dod-images/Pages/index.aspx