Windows Security

Chris Riggs
Senior Program Manager
Organizations with enormous security budgets and elite security analysts are struggling to address these modern threats.
THE EVOLUTION OF ATTACKS

Volume and Impact

Sophistication

2003-2004

Script Kiddies
BLASTER, SLAMMER
Motive: Mischief

Targeting
THE EVOLUTION OF ATTACKS

2005-PRESENT
Organized Crime
RANSOMWARE, CLICK-FRAUD, IDENTITY THEFT
Motive: Profit

2003-2004
Script Kiddies
BLASTER, SLAMMER
Motive: Mischief
THE EVOLUTION OF ATTACKS

2005 - PRESENT
Organized Crime
RANSOMWARE, CLICK-FRAUD, IDENTITY THEFT
Motive: Profit

2012 - Beyond
Nation States, Activists, Terror Groups
BRAZEN, COMPLEX, PERSISTENT
Motives: IP Theft, Damage, Disruption

2003-2004
Script Kiddies
BLASTER, SLAMMER
Motive: Mischief
EVOLUTION OF SECURITY THREATS

ADVANCED PERSISTENT ATTACKS (APT)
- Adversaries: nation states, mercenaries
- Goals: stealing IP, espionage, cyber weapons, hacktivism
- Targeting: enterprise, financial, infrastructure, government
- How: tailored-made attacks, low degree of automation, leverage system tools
- Attributes: attacks last weeks-months, movement across many machines in an org.

MALWARE
- Adversaries: crime groups
- Goals: monetary revenues through various schemes
- Targeting: consumer and enterprise
- How: typically machine generated, polymorphic, large scale volumes
- Attributes: Attack life can be hrs./days, focus on machine level, across many orgs

UNWANTED SOFTWARE
- Adversaries: commercial companies
- Goals: monetize user traffic
- Targeting: consumers
- How: lure users to change browser defaults/install software to generate traffic
- Attributes: targeting unsophisticated users, almost impossible to uninstall
“CYBER SECURITY IS A CXO ISSUE.”

Cyber threats are a material risk to your business

- **$3 Trillion**: Impact of lost productivity and growth
- **$3.5 Million**: Average cost of a data breach (15% YoY increase)
- **200+ Days**: Median number of days attackers are present on a victim's network before detection

Attacks are fast, efficient, and easier than you think

- **46%**: of compromised systems had no malware on them
- **23%**: of recipients opened phishing messages
- **50%**: of those who open, click attachments within the first hour

Source: McKinsey, Ponemon Institute, Verizon
Protection against modern security threats

Secured hardware  Secured identities  Secured data  Secured from threats
New challenges require a new platform

<table>
<thead>
<tr>
<th>Windows 7</th>
<th>Windows 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware starts before Windows, takes control, and evades detection</td>
<td>Helps prevent malware from compromising system before OS and defenses can start</td>
</tr>
<tr>
<td>Passwords are easily stolen Multi Factor authentication too hard</td>
<td>Passwords can be replaced with biometrics and easy to use multi-factor authentication</td>
</tr>
<tr>
<td>User credentials are easily stolen on companies networks</td>
<td>User credentials are protected using hardware based virtualization/isolation</td>
</tr>
<tr>
<td>Malware can bypass anti-virus and app control solutions</td>
<td>Next Gen app control and OS hardening gives IT better control of what runs in their environment</td>
</tr>
<tr>
<td>Users and apps can leak business data without restriction</td>
<td>Data separation and containment capabilities help prevent accidental data leaks</td>
</tr>
<tr>
<td>3rd party solutions required to detect targeted attacks on devices</td>
<td>Helps detect and respond to breaches with built in behavioral sensors and cloud based analytics</td>
</tr>
</tbody>
</table>

- Windows Trusted Boot
- Windows Hello
- Credential Guard
- Device Guard
- Enterprise Data Protection
- Windows Defender ATP
## Securing your hardware

<table>
<thead>
<tr>
<th>Biometrics</th>
<th>TPM</th>
<th>Virtualization Based Security</th>
<th>UEFI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move from what you know to what you have</td>
<td>Supports Windows 10 security features</td>
<td>Architectural change to address malware threats</td>
<td>Faster and more secure devices</td>
</tr>
<tr>
<td>Microsoft Hello Facial recognition Fingerprint</td>
<td>Made better in Windows 10 with next gen SOC, TPM 2.0</td>
<td>Isolates critical Windows components and data from threats</td>
<td>Device is secured from power on to power off</td>
</tr>
</tbody>
</table>
TPM 2.0
Executive Summary

✔ Trusted Platform Mode is a critical component to Windows 10 features and delivering on our security promises to customers

✔ **TPM 2.0** firmware or discrete must be enabled by default and is the minimum hardware requirement for Windows 10 (Anniversary Update).

  Exception: This does not apply to OEM systems for special purpose commercial systems, customer orders, and customer images with a custom image

✔ Microsoft recommends working with discrete or firmware TPM suppliers to meet this requirement for Windows 10
TPM Requirements for new Anniversary Update Systems

Windows Desktop
For this Summer, 2016, all new devices and computers, all SKU’s, must implement and be in compliance with the International Standard ISO/IEC 11889:2015 or the Trusted Computing Group TPM 2.0 Library, Revision 1.16 (or later) specification and a component which implements the TPM 2.0 must be present and enabled by default.

Windows Mobile
All Windows Phone devices require TPM 2.0

Windows IOT
TPM remains optional on Windows IOT

Windows Server
TPM remains optional for unless the additional qualification (AQ) criteria for the Host Guardian Services scenario in which case TPM 2.0 is required.
# Windows 10 (Anniversary Update) Feature Dependencies on TPM

<table>
<thead>
<tr>
<th>Win 10 Feature</th>
<th>TPM 1.2</th>
<th>TPM 2.0</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>UEFI Secure Boot</td>
<td></td>
<td></td>
<td>- No TPM requirement</td>
</tr>
<tr>
<td>Conditional Access</td>
<td></td>
<td></td>
<td>- No TPM requirement</td>
</tr>
<tr>
<td>Enterprise Data Protection</td>
<td></td>
<td></td>
<td>- No TPM requirement</td>
</tr>
<tr>
<td>Windows Defender - Advanced Threat Detection</td>
<td></td>
<td></td>
<td>- No TPM requirement</td>
</tr>
<tr>
<td>Device Guard / Configurable Code Integrity</td>
<td></td>
<td></td>
<td>- No TPM requirement</td>
</tr>
<tr>
<td>Windows Hello</td>
<td></td>
<td></td>
<td>- No TPM requirement</td>
</tr>
<tr>
<td>Credential Guard</td>
<td>Yes</td>
<td>Yes</td>
<td>- More secure with TPM 2.0</td>
</tr>
<tr>
<td>Measured Boot</td>
<td>Yes</td>
<td>Yes</td>
<td>- More secure with TPM 2.0</td>
</tr>
<tr>
<td>Device Health Attestiation</td>
<td>Yes</td>
<td>Yes</td>
<td>- Requires TPM</td>
</tr>
<tr>
<td>Virtual Smart Card</td>
<td>Yes</td>
<td>Yes</td>
<td>- Requires TPM</td>
</tr>
<tr>
<td>Passport: Domain AADJ Join</td>
<td>Yes</td>
<td>Yes</td>
<td>- Supports both versions, but requires TPM with HMAC and EK certificate for key attestation support.</td>
</tr>
<tr>
<td>Passport: MSA / Local Account</td>
<td>Yes</td>
<td>Yes</td>
<td>- Requires TPM 2.0 for HMAC and EK certificate for key attestation support</td>
</tr>
<tr>
<td>BitLocker</td>
<td>Yes</td>
<td>Yes</td>
<td>- TPM 1.2 or later required or a removable USB memory device such as a flash drive</td>
</tr>
<tr>
<td>Device Encryption</td>
<td></td>
<td>Yes</td>
<td>- For Modern Standby devices, all require TPM 2.0</td>
</tr>
</tbody>
</table>
Device Guard / Credential Guard
Two paths to choose from

Device Guard

A new approach for Windows desktop
Requires change in process for apps
Offers incredible protection

Traditional approach

The way things have always been
Requires additional software to manage
Carries increased risk
## Device Guard

### Hardware-rooted app control

- Windows desktop can be locked down to only run trusted apps, just like many mobile operating systems (e.g., Windows Phone)
- Untrusted apps and executables, such as malware, are unable to run
- Protects kernel mode processes and drivers from zero days and vulnerabilities using HVCI
- Requires Windows 8 or Windows 10 certified hardware

### Getting apps into the circle of trust

- Supports all apps including Universal and Desktop (Win32)
- Apps must be specially signed using the Microsoft signing service. No additional modification is required
- Signing services are available to OEMs, IHVs, ISVs, and Enterprises
Push for HVCI Compliance on New Devices and Existing Peripherals

- Tied to key enterprise features and security, we require for Windows 10 (Anniversary Update):
- All drivers to meet Hypervisor-Enforced Code Integrity requirements (HVCI) within 90 days of RTM running the HLK
- Validate UEFI firmware support Device Guard enablement
- Move peripherals drivers to HVCI compliance and perform validation

- Windows System Compatibility can be achieved with drivers tested with 1507, 1511 or Anniversary Update HLKs until Windows RS1 RTM, plus 90 days
<table>
<thead>
<tr>
<th>Requirements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows 10 Enterprise</strong></td>
<td>The PC must be running Windows 10 Enterprise. (also available on Server ’16, Education)</td>
</tr>
<tr>
<td><strong>A VT-D or AMD-Vi IOMMU¹</strong></td>
<td>IOMMU enhances system resiliency against memory attacks.</td>
</tr>
<tr>
<td><strong>x64 architecture</strong></td>
<td>The Windows hypervisor only supports 64-bit PC</td>
</tr>
<tr>
<td><strong>Virtualization extensions</strong></td>
<td>Virtualization extensions are required to support virtualization-based security:</td>
</tr>
<tr>
<td></td>
<td>• Either Intel VT-X or AMD-V</td>
</tr>
<tr>
<td></td>
<td>• CPU supports Second Level Address Translation</td>
</tr>
</tbody>
</table>
## Device Guard / Credential Guard Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure firmware update process</td>
<td>UEFI firmware must support secure firmware update following section <a href="#">System.Fundamentals.Firmware.UEFISecureBoot</a> in Windows Hardware Compatibility Program requirement.</td>
</tr>
</tbody>
</table>
| Firmware support for SMM protection                   | Firmware SMM code must be reviewed and hardened to prevent memory attacks. This will provide a strong platform security foundation for VSM (Virtual Secure Mode).  
1. System MUST implement the ACPI WSMT table, as described in the “Windows SMM Security Mitigation Table” document. All non-reserved WSMT protection flags field MUST be set indicating that the documented mitigations are implemented.  
2. SMM must not execute code from memory that is writable by the OS. |
| UEFI NX Protections                                    | [UEFI RunTime Services](#)  
1. Must implement UEFI 2.6 specification’s EFI_MEMORY_ATTRIBUTES_TABLE. The entire UEFI runtime must be described by this table.  
2. All entries must include attributes EFI_MEMORY_RO, EFI_MEMORY_XP, or both  
3. No entries must be left with neither of the above attribute, indicating memory that is both executable and writable. Memory MUST be either readable and executable OR writeable and non-executable. |
| Firmware security patch for Secure MOR Implementation | Secure MOR bit prevents certain memory attacks thus necessary for Credential Guard. This will further enhance security of Credential Guard.                                                                     |
| Trusted Platform Module (TPM) version 1.2 or 2.0      | TPM 1.2 and 2.0 provides protection for encryption keys that are stored in the firmware. TPMs, either discrete or firmware will suffice, but this is a must have requirement for Credential Guard.                                   |
| Intel TXT / SGX                                        | Intel TXT is not supported with the Microsoft hypervisor. TXT must be disabled in the firmware. Intel SGX is not utilized by the Microsoft hypervisor, VBS, or guest VMs. SGX applications may run in the Windows root when Device Guard is enabled.     |
System Management Mode (SMM) Mitigations:

- Firmware must consider attacks from kernel malware
- It must protect itself from security compromise
- It must NOT facilitate bypass of a hypervisor
Virtualized Based Security seeks to create a secure environment. Platform firmware, including SMM, must play a key role in providing a secure foundation. SMM is opaque to the OS, and the OS must assume SMM is within the same trust domain as the OS itself.

Exploits may be mounted via SMM.

To protect against these threats, changes to SMM programming practices and assumptions must be introduced.

The OS must be able to determine what SMM security mitigations have been implemented on a specific platform.

The OS must rely on SMM firmware to accurately self-report which of the Microsoft recommended security best practices it has implemented.

To accomplish this, Microsoft has defined the ACPI static table Windows SMM Security Mitigations Table (WSMT).
Windows SMM Security Mitigations Table (WSMT)

Device Security
Best Practices
Protecting our customers requires an ecosystem effort

Window 10 security features rooted in hardware
• BitLocker, Secure Boot, Health Attestation, Device Guard, Credential Guard, Windows Hello, Microsoft Passport

Researcher & attacker interest follows
• 37 unique publicly disclosed firmware issues in the last ~2 years according to Intel Security ATR
• Exploits can lead to security control bypass

Not letting up on software vulnerabilities though
• Antivirus, System Utilities, Certificates

Targeted Security Promises
1. My device’s software & firmware are developed according the Security Development Lifecycle. (or equivalent, ISO/IEC 27034)
2. Security issues are monitored, investigated and resolved by a formal security response process.
3. My device’s software & firmware can be updated in the field when future issues are discovered.
4. My device has the proper hardware to take advantage of Window security features.
5. Firmware security best practices are followed.
6. My device is not vulnerable to publically known UEFI vulnerabilities at the time of release.
7. Security Certificates added to my device are documented and justified, with a pre-defined security response plan.
Device Security for OEMs

- Firmware is software...
  - ✓ Follow industry best practices (e.g. NIST 800-147, ISO/IEC 19678:2015)
  - ✓ Conduct security reviews on your firmware
  - ✓ Plan to regularly address reported vulnerabilities going forward and in the field with updates.

- Proper implementations provide opportunity to demonstrate security benefits of modern hardware

- Follow best practice checklists in ChipSec, HSTI & HLK

<table>
<thead>
<tr>
<th>Security Checklist for OEMs</th>
<th>Tool Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. UEFI/BIOS lock down configs</td>
<td>HSTI / ChipSec</td>
</tr>
<tr>
<td>2. UEFI/BIOS vulnerability assessment</td>
<td>ChipSec (fix all warnings and errors)</td>
</tr>
<tr>
<td>3. UEFI/BIOS updated</td>
<td>Via UEFI Firmware Update Capsule</td>
</tr>
<tr>
<td>4. Secure MOR enabled</td>
<td>HSTI</td>
</tr>
<tr>
<td>5. Platform Secure Boot enabled</td>
<td>HSTI</td>
</tr>
<tr>
<td>6. Boot Guard / Hardware Verified Boot</td>
<td>HSTI</td>
</tr>
<tr>
<td>7. Confirm enabled TPM 2.0</td>
<td>HLK</td>
</tr>
<tr>
<td>8. Static DBX updated</td>
<td>HLK</td>
</tr>
<tr>
<td>9. HVCI driver compliance</td>
<td>HLK / WHQL</td>
</tr>
</tbody>
</table>

Tools:
- Run ChipSec: https://github.com/chipsec/chipsec
- Run HSTI: http://aka.ms/htdocs/hsi
Call To Action

1. Be ready to enable and support our existing and new security features in Windows 10
2. Update firmware regularly
3. Leverage our security best practices
4. Run tools, including HSTI, ChipSec, & HLK
5. Provide feedback to us: winhec@microsoft.com