Microsoft Update for Windows Security
UEFI Spring Plugfest – March 29-31, 2016
Presented by Jackie Chang, Tony Lin
(Microsoft Corporation)
Agenda

• Security for Everyone
• Windows 10 Security Features
• Additional Firmware Considerations
• Summary and Call to Action
Setting the pace for change

• Driving the security experience for our customers, investing in securing their data
• Partner together to deliver a great security experience with Windows 10
• Executing on Windows as a Service (WaaS) requires agility and flexibility across our ecosystem
Security for Everyone
The attackers are **changing** their playbook...

**How do breaches occur?**

- **46%** of compromised systems had no malware on them.
- **99%** Of the exploited vulnerabilities were compromised more than a year after the CVE was published.

- **100%** of victims have **up-to-date anti-virus signatures**.
- **67%** of victims were **notified** by an **external** entity.
- **33%** of victims **discovered the breach internally**.
- **23%** Of recipients **open phishing messages** (11% click on attachments).
- **50%** Nearly 50% open e-mails and **click on phishing links within the first hour**.

*Source: Mandiant 2014 Threat Report*
Protecting our mutual customers requires ecosystem-wide effort

Window 10 security features rooted in hardware & firmware
BitLocker, Secure Boot, Health Attestation, Device Guard, Passport

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

Not letting up on software vulnerabilities though
Antivirus, System Utilities, Certificates
Windows as a Service (WaaS)

• More frequent Windows updates
• Reduces Windows ecosystem fragmentation
• Focus on new AND existing (update) devices
• Cumulative security updates
Updates and requirements for

Windows 10 Security Features
Windows 10 Security Features

- Device Guard (DG)/Credential Guard (CG)
- Secure Boot
- TPM 2.0
### OS and Hardware Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Description</th>
<th>DG or CG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 10 Enterprise</td>
<td>The PC must be running Windows 10 Enterprise. (Note: This is also available on Server, Education and IOT)</td>
<td>DG / CG</td>
</tr>
<tr>
<td>A VT-d or AMD-VI IOMMU¹</td>
<td>IOMMU enhances system resiliency against memory attacks.</td>
<td>DG / CG</td>
</tr>
<tr>
<td>x64 architecture</td>
<td>The features that virtualization-based security uses in the Windows hypervisor only supports 64-bit PC.</td>
<td>DG / CG</td>
</tr>
<tr>
<td>Virtualization extensions</td>
<td>The following virtualization extensions are required to support virtualization-based security:   - Intel VT-x or AMD-V   - Second Level Address Translation</td>
<td>DG / CG</td>
</tr>
</tbody>
</table>

¹ Input/output memory management unit
## UEFI Firmware Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Description</th>
<th>DG or CG</th>
</tr>
</thead>
</table>
| UEFI firmware version 2.3.1 or higher with UEFI Secure Boot and Platform Secure Boot | UEFI Secure Boot helps ensure that the device boots authorized code. Additionally, Boot Integrity (aka Platform Secure Boot) must be supported following the requirement in Hardware Compatibility Specification for Systems for Windows 10:  
1. [System.Fundamentals.Firmware.UEFISecureBoot](#)  
### Device Guard and Credential Guard

**Firmware BIOS Configuration Security**

<table>
<thead>
<tr>
<th>BIOS capabilities that are required:</th>
<th>DG / CG</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. BIOS password or stronger authentication supported to ensure that only authenticated Platform BIOS administrator can change BIOS settings</td>
<td></td>
</tr>
<tr>
<td>2. OEM supports capability to add OEM or Enterprise Certificate in Secure Boot DB at manufacturing time.</td>
<td></td>
</tr>
<tr>
<td>3. Protected BIOS option to configure list of permitted boot devices and boot device order (Eg: Boot only from internal hard drive) which overrides BOOTORDER modification made by OS</td>
<td></td>
</tr>
</tbody>
</table>

**Required Configurations:**

1. Microsoft UEFI CA must be removed from Secure Boot DB. Support for 3rd-party UEFI modules is permitted but should leverage ISV-provided certificates for the specific UEFI software (e.g. Software package “foo” certificate).

2. BIOS options related to security and boot options must be secured to deliver the Device Guard security guarantees.

3. BIOS authentication (e.g. password) must be enabled

*NOTE: You could use [tool provided by Insyde](https://www.insyde.com) to query what certificates are present in Secure Boot.*
## Device Guard and Credential Guard

### Firmware Updates/Patches and TPM

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Description</th>
<th>DG or CG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure firmware update process</td>
<td>UEFI firmware must support secure firmware update following section <code>System.Fundamentals.Firmware.UEFISecureBoot</code> in Windows Hardware Compatibility Program requirement.</td>
<td>DG / CG</td>
</tr>
<tr>
<td>Signed Processor Microcode updates</td>
<td>Processors if supports updates then must require signed microcode updates.</td>
<td>DG / CG</td>
</tr>
</tbody>
</table>
| Firmware support for SMM protection      | SMM communication buffer protection prevents certain memory attacks thus necessary for Device Guard. This will further enhance security of VSM (Virtual Secure Mode).  

1. System MUST implement “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.                                                                                     | DG / CG  |
| 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. | DG/CG    |
| 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.                                                                 | CG       |
| 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.                                                                  | CG       |
| Intel TXT / SGX                           | Intel TXT is not supported with Device Guard, as such, TXT must be disabled in the firmware. Intel SGX neither the hypervisor, VBS, or guest VMs can use SGX, however, SGX applications may run in parallel with Device Guard at the OS level. | DG       |
Secure Boot

Deploy mode / User mode changed in UEFI2.5 from UEFI 2.3.1c

How to tell if system is shipped with secure boot?

Documentation is still in the works
TPM 2.0

TPM 2.0 is the standard we are moving to for Windows 10

• TPM 2.0 has important security enhancements over TPM 1.2
• It is our minimum hardware requirement for Windows 10 going forward

Country constraints compared with TPM 1.2 have been solved

• Voted and approved across TCG and certified by ISO

Discrete TPM certified parts are ready or in progress for all suppliers
TPM 2.0 Requirement

Windows Desktop
• For this Summer, 2016, all new devices and computers 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 from this effective date.

Windows Mobile
• All Windows Phone devices require TPM 2.0

Windows IoT
• TPM remains optional

Windows Server
• TPM remains optional unless the additional qualification (AQ) criteria for the Host Guardian Services scenario is desired, in which case TPM 2.0 is required.
## TPM Spec Versions

### Desktop firmware TPM Platforms

<table>
<thead>
<tr>
<th>IHV</th>
<th>Model</th>
<th>TCG TPM 2.0 Spec Version</th>
<th>Windows Requirements Min Spec Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>TH1</td>
</tr>
<tr>
<td>Intel</td>
<td>Atom™ Processor-based Clover Trail</td>
<td>0.88</td>
<td>.96</td>
</tr>
<tr>
<td></td>
<td>Bay Trail z3600-z3700</td>
<td>0.93</td>
<td>.96</td>
</tr>
<tr>
<td></td>
<td>4th generation Core™ (Haswell)</td>
<td>0.93</td>
<td>.96</td>
</tr>
<tr>
<td></td>
<td>Atom Z8000 – Cherry Trail</td>
<td>1.03</td>
<td>.96</td>
</tr>
<tr>
<td></td>
<td>5th generation Core™ (Broadwell)</td>
<td>1.03</td>
<td>.96</td>
</tr>
<tr>
<td></td>
<td>Braswell Platform</td>
<td>1.03</td>
<td>.96</td>
</tr>
<tr>
<td></td>
<td>6th Generation Core™ (Skylake)</td>
<td>1.16</td>
<td>.96</td>
</tr>
<tr>
<td>AMD</td>
<td>Beema</td>
<td>1.22</td>
<td>.96</td>
</tr>
<tr>
<td></td>
<td>CZ-L</td>
<td>1.22</td>
<td>.96</td>
</tr>
<tr>
<td></td>
<td>Carrizo</td>
<td>1.22</td>
<td>.96</td>
</tr>
</tbody>
</table>

Spec Versions Listed with Latest Available Firmware
Additional Firmware Considerations & Validation Options
Additional FW Considerations

• Validation Best Practices

• Reliable field-update of firmware is a critical security feature
  – EFI UpdateCapsule()
  – EFI System Resource Table (ESRT)

• SMBIOS guidance
Validation Best Practices

- Hardware Lab “a.k.a. Logo” Kit (HLK)
- HSTI – verify security configuration
- INTEL’s ChipSec – double-verify security config
ChipSec Security Analysis Tool

• Detects known FW vulnerabilities & configuration errors
• Build a relationship with ChipSec authors
  – chipsec@intel.com
• Request best available & preview versions
  – Stay up-to-date!
• Run on all systems prior to shipping!
• When updated, re-run on all supported systems!
• Understand errors, fix real bugs & report test bugs
SMBIOS General Principles

- Minimize the number of SMBIOS fields necessary to uniquely track device models
- Keep the dependency on current version of SMBIOS (3.0.0.0)
- Don’t disrupt CHID definition / driver publishing process
- Provide clarity on how each SMBIOS field provides a hierarchical structure
- Focus on user-facing string formats where relevant
- Emphasize data consistency (below are examples of data inconsistencies)

<table>
<thead>
<tr>
<th>Product Version</th>
<th>SKU Number</th>
<th>Base Board Product</th>
<th>Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Specified</td>
<td>To be filled by O.E.M.</td>
<td>INVALID</td>
<td>Type1Family</td>
</tr>
<tr>
<td>Null</td>
<td>Invalid</td>
<td>Type2 – Board Product Name 1</td>
<td>(all 0xf’s)</td>
</tr>
<tr>
<td>Not Applicable</td>
<td>Type1Family</td>
<td>To be filled by O.E.M.</td>
<td></td>
</tr>
</tbody>
</table>
SMBIOS fields

- Hierarchical structure to denote a device model:

<table>
<thead>
<tr>
<th>Depth</th>
<th>SMBIOS Field</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Type 1 Manufacturer</td>
<td>Product brand (logo/name on device)</td>
</tr>
<tr>
<td>Level 2</td>
<td>Type 1 Family</td>
<td>Product line as marketed to customers</td>
</tr>
<tr>
<td>Level 3</td>
<td>Type 1 Product Name</td>
<td>Friendly name for product model (what a customer can purchase); <em>excludes</em> configuration variance</td>
</tr>
<tr>
<td>Level 4</td>
<td>Type 2 Product</td>
<td>Identifier for baseboard (model variant)</td>
</tr>
<tr>
<td>Level 5</td>
<td>Type 1 SKU Number</td>
<td>Value to identify specific configuration variance (such as storage, region, software preload)</td>
</tr>
</tbody>
</table>

- Clarity on Enclosure Type usage
  - Desktop, Notebook, All in One, Tablet, Convertible, Detachable
  - Other value, if none of the above match
Summary and Call to Action
Getting to “Yes” together

1. My device’s software & firmware are developed according the Security Development Lifecycle.
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.

Resources
- [www.microsoft.com/SDL](http://www.microsoft.com/SDL)
- [Microsoft Security Response Center](https://msrc.microsoft.com)

Platform & Tools
- ChipSec and [HSTI](https://www.hstii.com)
- SigCheck
- [Tool provided by Insyde](https://www.insyde.com) to query certificates present in Secure Boot.

Your strengths or challenges? Where can we partner?
Call to Action

Implement UpdateCapsule and ESRT on all Windows devices

Follow the SMBIOS guidance (forthcoming)

Attend the upcoming WinHEC events
Taipei/Shenzhen in April (planning update)
Taipei/Shenzhen in TBD (hands-on lab)

UpdateCapsule and ESRT If there’s any additional help we can provide, e-mail us at sauefi@microsoft.com
Links - Appendix

- Secure the Windows 8.1 boot process
- Device.DevFund.DeviceGuard.DriverCompatibility
- Device.DevFund.DeviceGuard.DriverCompatibility
  https://msdn.microsoft.com/en-us/library/windows/hardware/mt589732(v=vs.85).aspx#filter_driver__deviceguard_drivercompatibility
- Driver compatibility with Device Guard in Windows 10
  http://go.microsoft.com/fwlink/p/?LinkId=627463
- DF - HyperVisor Code Integrity Readiness Test
- System.Fundamentals.Firmware.UEFISecureBoot
- Insyde’s “Secure Boot Checkup Utility”
  http://apps.insyde.com/sbutil.html
- UEFI 2.5 Spec on UEFI.org
  http://www.uefi.org/sites/default/files/resources/UEFI%202_5.pdf
- Secure Boot Overview
- Windows 8.1 Secure Boot Key Creation and Management Guidance
- UEFI Validation Option ROM Validation Guidance
- UEFI Validation Option ROM Validation Guidance, How to test for it:
- fTPM: A Firmware-based TPM 2.0 Implementation
- Populating the EFI System Resource Table (ESRT)
- HSTI – Hardware Security Test Interface
- ChipSec.exe tool
  https://github.com/chipsec/chipsec
- DMTF.org SMBIOS specification
  http://www.dmtf.org/standards/smbios
Thanks for attending the UEFI Spring Plugfest 2016

For more information on the Unified EFI Forum and UEFI Specifications, visit http://www.uefi.org