presented by

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?

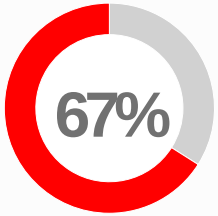
46%

of compromised systems had no malware on them

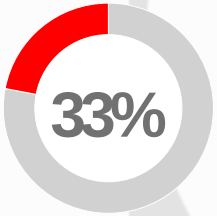
99%

Of the exploited vulnerabilities were compromised more than a year after the CVE was published.

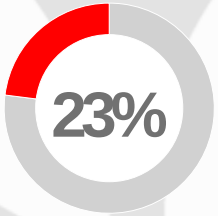
of victims have **up-to-date anti-virus signatures**



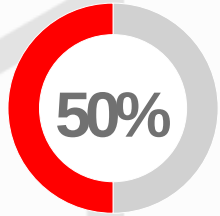
of victims were **notified** by an **external** entity



of victims **discovered** the breach **internally**



Of recipients **open phishing messages** (11% click on attachments)



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

Device Guard and Credential Guard

OS and Hardware Requirements

Requirements	Description	DG or CG
Windows 10 Enterprise	The PC must be running Windows 10 Enterprise. (Note: This is also available on Server, Education and IOT)	DG / CG
HVCI Compatible Drivers	MUST meet all HVCI Compatible Driver requirements as described in "Filter.Driver.DeviceGuard.DriverCompatibility". "Device.DevFund.DeviceGuard.DriverCompatibilibity"	
A VT-d or AMD-Vi IOMMU[1]	IOMMU enhances system resiliency against memory attacks.	DG / CG
x64 architecture	The features that virtualization-based security uses in the Windows hypervisor only supports 64-bit PC.	DG / CG
Virtualization extensions	The following virtualization extensions are required to support virtualization-based security: • Intel VT-x or AMD-V • Second Level Address Translation	DG / CG

[1] Input/output memory management unit

Device Guard and Credential Guard

UEFI Firmware Requirements

Requirements	Description	DG or CG
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 2. System.Fundamentals.Firmware.CS.UEFISecureBoot.ConnectedStandby (this includes Hardware Security Test Interface)	DG / CG

Device Guard and Credential Guard

Firmware BIOS Configuration Security	BIOS capabilities that are required: 1. BIOS password or stronger authentication supported to ensure that only authenticated Platform BIOS administrator can change BIOS settings 2. OEM supports capability to add OEM or Enterprise Certificate in Secure Boot DB at manufacturing time. 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 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 to query what certificates are present in Secure Boot.	DG / CG

Device Guard and Credential Guard

Firmware Updates/Patches and TPM

Requirements	Description	DG or CG
Secure firmware update process	UEFI firmware must support secure firmware update following section System.Fundamentals.Firmware.UEFISecureBoot in Windows Hardware Compatibility Program requirement.	DG / CG
Signed Processor Microcode updates	Processors if supports updates then must require signed microcode updates.	DG / CG
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

IHV	Model	TCG TPM 2.0 Spec Version	Windows Requirements Min Spec Version		
			TH1	TH2	RS1
Intel	Atom™ Processor-based Clover Trail	0.88	.96	.99	1.16
	Bay Trail z3600-z3700	0.93	.96	.99	1.16
	4th generation Core™ (Haswell)	0.93	.96	.99	1.16
	Atom Z8000 – Cherry Trail	1.03	.96	.99	1.16
	5th generation Core™ (Broadwell)	1.03	.96	.99	1.16
	Braswell Platform	1.03	.96	.99	1.16
	6th Generation Core™ (Skylake)	1.16	.96	.99	1.16
AMD	Beema	1.22	.96	.99	1.16
	CZ-L	1.22	.96	.99	1.16
	Carrizo	1.22	.96	.99	1.16

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)

Product Version	SKU Number	Base Board Product	Family
Not Specified	To be filled by O.E.M.	INVALID	Type1Family
Null	Invalid	Type2 – Board Product Name 1	(all 0xf’s)
Not Applicable	Type1Family	To be filled by O.E.M.	

SMBIOS fields

- **Hierarchical structure to denote a device model:**

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

- **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
- Specific OEM recommendations: https://msdn.microsoft.com/en-us/library/windows/hardware/dn756802(v=vs.85).aspx
- Microsoft Security Response Center
- Windows Platform Binary Table – Security Recommendations

Platform & Tools

- Device Guard requirements: https://technet.microsoft.com/en-us/library/dn986865(v=vs.85).aspx
- Windows UEFI Firmware Update Platform
- ChipSec and HSTI
- SigCheck
- Tool provided by Insyde 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
https://technet.microsoft.com/en-us/windows/dn168167.aspx
- Device.DevFund.DeviceGuard.DriverCompatibility
https://msdn.microsoft.com/en-us/library/windows/hardware/mt589731(v=vs.85).aspx#device_devfund_deviceguard_drivercompatibility
- Filter.Driver.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
https://msdn.microsoft.com/en-us/library/windows/hardware/dn955152(v=vs.85).aspx
- System.Fundamentals.Firmware.UEFISecureBoot
https://msdn.microsoft.com/en-us/library/windows/hardware/dn932807(v=vs.85).aspx#system_fundamentals_firmware_cs_uefisecureboot_connectedstandby
- 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
https://technet.microsoft.com/en-us/library/hh824987.aspx
- Windows 8.1 Secure Boot Key Creation and Management Guidance
https://technet.microsoft.com/en-us/library/dn747883.aspx
- UEFI Validation Option ROM Validation Guidance
https://technet.microsoft.com/en-us/library/dn747882.aspx
- UEFI Validation Option ROM Validation Guidance\How to test for it:
https://technet.microsoft.com/en-us/library/dn747882.aspx#HowToTestForIt
- fTPM: A Firmware-based TPM 2.0 Implementation
http://research.microsoft.com/en-us/um/people/ssaroiu/publications/tr/msr/msr-tr-2015-84.pdf
- Populating the EFI System Resource Table (ESRT)
https://msdn.microsoft.com/en-us/library/windows/hardware/dn917847(v=vs.85).aspx
- HSTI – Hardware Security Test Interface
https://msdn.microsoft.com/en-us/library/windows/hardware/dn879006(v=vs.85).aspx
- 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

presented by

Microsoft