Windows 10 Device Security

Peter Waxman
Principal Lead Program Manager
Session Introduction

Security is hard and new threats emerge every day. Customers are depending on security at the hardware, firmware, and software layers to keep their data and identities safe. Learn what it takes to build a Windows 10 secure device.

Session Agenda

Why Hardware Rooted Security Matters
What Does a Secure Windows Device Look Like?
How do we get there?
  - Level 1: Minimum Security Requirements for Win10
  - Level 2: Standard Security in 2019
  - Level 3: Hardware rooted protection from advanced attacks

Hardware security futures and tough problems for the industry to solve
Half a billion dollars in market cap evaporated over night!
LoJack: a Russian double agent

Fancy Bear (aka APT 28, Pawn Storm, STRONTIUM)

LoJack is a commercial pre-OS component embedded by most OEMs in their PCs

Provides persistent ability to locate, lock, wipe the device through value added subscription

Researchers discovered hijacked LoJack agents in the wild configured to connect to command and control (C2) domains owned by Fancy Bear
http://timeglider.com/timeline/5ca2daa6078caaf4
Law #1: If a bad guy can persuade you to run his program on your computer, it’s not solely your computer anymore.

Law #2: If a bad guy can alter the operating system on your computer, it’s not your computer anymore.

Law #3: If a bad guy has unrestricted physical access to your computer, it’s not your computer anymore.

Law #4: If you allow a bad guy to run active content in your website, it’s not your website any more.

Law #5: Weak passwords trump strong security.

Law #6: A computer is only as secure as the administrator is trustworthy.

Law #7: Encrypted data is only as secure as its decryption key.

Law #8: An out-of-date antimalware scanner is only marginally better than no scanner at all.

Law #9: Absolute anonymity isn’t practically achievable, online or offline.

Law #10: Technology is not a panacea.
Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.
Segmentation

Performance

Smaller attack surface
Modern Device Security Levels

Virtualization Based Security

- Kernel DMA Protection (DMAr)
- Windows Hello (SecureBIO)
- Drivers / Apps are HVCI-Ready
- Virtualization (VBS) & HVCI Enabled

System Guard

- SMM Protection
- Secure Launch aka DRTM
- Modern Standby (required for LVL3)
- Specific Platform Requirements for LVL3

LEVEL 1

- BitLocker
- UEFI Secure Boot
- Trusted Platform Module 2.0
- Device Servicing Program – Drivers/FW on WU

LEVEL 2

- BitLocker
- UEFI Secure Boot
- Trusted Platform Module 2.0
- Device Servicing Program – Drivers/FW on WU

LEVEL 3

- BitLocker
- UEFI Secure Boot
- Trusted Platform Module 2.0
- Device Servicing Program – Drivers/FW on WU
Security Promise

Prevent “evil cleaner” drive by physical attacks from malicious DMA attacks on Thunderbolt™ via malware

<10 min
<$1000 in hardware
no open chassis
PCI Leech

PLX USB3380 Dev Board + Firmware + Software

PCIe ➔ USB 3.0

$78
No Drivers Required
>150MB/s DMA
Kernel DMA Protection

The Windows 10 security for Thunderbolt™ 3 relies on the system IOMMU to prevent drive-by DMA attacks:

• Block all newly attached Thunderbolt™ 3 devices from starting and performing DMA, until an authorized user is logged in and the screen is unlocked

• Sandbox memory allocated to DMA remapping (DMAr) compatible device drivers, thus allowing the OS to start DMAr compatible devices regardless of the lock screen state (that is, plug and use immediately), which significantly improves user experience

Scope: Thunderbolt 3.0 docking stations (USB XHCI, PCIe ethernet) and external storage (CFL/CNL consumer SKU, WHL consumer/commercial SKUs)
DMA Protection Demo
Virtualization Based Security
Security Promise

Even with malware running in the Windows kernel, secrets and code running in VBS cannot be leaked or tampered
Virtualization Based Security (VBS)

Virtualization Based Security Environment

- Trustlet #1
- Trustlet #2
- Trustlet #3

Secure Kernel

Windows Platform Services

Kernel

Apps

Hypervisor

Hardware
Security Capabilities Enabled by VBS

✓ Hypervisor Code Integrity (HVCI)
✓ Credential Guard
✓ Secure Bio
✓ Hyper Guard
✓ System Guard Runtime Attestation
✓ VSM Enclaves

... This list grows over time ...
To enable VBS and HCVI by default, you need to use the commands listed below during your manufacturing process to add the necessary registry keys:

```
reg add "HKLM\System\CurrentControlSet\Control\DeviceGuard\Scenarios\HypervisorEnforcedCodeIntegrity" /v "Enabled" /t REG_DWORD /d 1 /f
shutdown /r /t 0
```

By enabling HVCI, your device will ship in enhanced security mode which is called out in Windows Security app.

OEMs can also use the unattend process to enable HVCI:
https://docs.microsoft.com/en-us/windows-hardware/customize/desktop/unattend/microsoft-windows-deviceguard-unattend
Secure Biometrics
Security Promise

1. Customers can be confident that the latest security enhancements are in place to ensure the identity of the user.

2. Windows guarantees user presence at the time of authentication.

Goal is to achieve more secure end to end assurance of authentication to a relying party (cloud entity).
Value of Secure Bio

**Secure Input**
Hardening of biometric data path using virtualization.

- Benefit
  Prevent software based replay or injection. Ensure freshness of samples.

**Secure Match and Credential Release using VBS**
Benefit
Prevent tampering of match result. Prevent unauthorized usage of Hello keys.

- Enterprise grade biometric security.

**Attestation**
Integration into device health reports.

- Benefit
  FIDO 2.0 L2 Certification.

- Cryptographic proof that secure bio was used to relying party.

- Conditional access signal.

**WebAuthN, FIDO 2.0 Integration**
Benefit
Re-Authorization to major websites.
Secure Bio Face & Fingerprint Requirements

Platform:
• Meet level 2 requirements for VBS from System.Fundamentals.Security.VirtualizationSupport
• Secure biometric trustlet configuration registry keys set
• Ship specific supported IR Camera and/or fingerprint hardware.

Camera & Fingerprint Sensor Requirements:
• Described in latest Windows 10 compatibility spec: https://go.microsoft.com/fwlink/?linkid=2027110
System Guard: Secure Launch & SMM Protection
Security Promise

Ensures the Hypervisor and VBS and by extension the rest of the OS are protected from malicious / vulnerable firmware on the device
Secure Launch
aka Dynamic Root of Trust for Measurement

UNIFIED EXTENSIBLE
FIRMWARE INTERFACE

Windows
Boot Manager
& OS Loader

Windows 10

Virtualization Based
Security Environment

Trustlet #1

Trustlet #2

Trustlet #3

Secure Kernel

Hypervisor

Kernel

Apps

Windows Platform Services

© 2018 Microsoft
Secure Launch
aka Dynamic Root of Trust for Measurement

Secure Launch

UNIFIED EXTENSIBLE FIRMWARE INTERFACE

Secure Launch

Windows 10

虚化安全环境

虚拟化安全环境

安全内核

内核

平台服务

应用程序
System Guard Details

How:

• System Guard relies on Dynamic Root of Trust for Measurement (DRTM) to securely launch Hypervisor and VBS after device firmware is finished booting

• Additionally SMM firmware code is prevented from accessing OS & VBS memory

Details:

• Windows 10 1809 release depends on Intel TXT and Runtime BIOS Resilience features; future support planned for AMD and Qualcomm variants

• Ships in Pro and Enterprise SKUs of Windows 10
SMM Attacks

System Management Mode

• Code runs at ring -2: highest privilege level on CPU
• Completely invisible to OS & anti-malware
• Intended for power mgmt, HW emulation, mitigate HW bugs, proprietary OEM code,..

Ideal environment for malware - super rootkits!!
Securing SMM

Intel Runtime BIOS resilience provides the following security properties:

• SMM entry point locked down
• All code within SMM locked down
• Memory map and page properties locked down
• OS memory not directly accessible from SMM at all
• Firmware vendors can also provide the capability to attest to its presence
Enabling System Guard

Customers can enable System Guard on capable systems via usual set of management knobs:

- Group Policy object
- MDM controls via CSP
- Direct end user enablement possible via Windows Security app UI
- Direct setting of System Guard registry key
  - Add a new key: HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\SystemGuard
  - Add a new DWORD value under HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\SystemGuard
  - Enabled = 1

Core isolation

Security features available on your device that use virtualization-based security.

Memory integrity
Prevents attacks from inserting malicious code into high-security processes.

Firmware protection
Windows Defender System Guard protects your device from compromised firmware.

Memory access protection
Protects your device’s memory from attacks by malicious external devices.
System Guard: Win10 1809 Requirements

**System.Fundamentals.Security.SystemGuard**

Windows 10 October 2018 Update (1809): Requires Intel vPro processor: Coffeelake, Whiskeylake or later

Implement Level 2 requirements
Implement Intel Runtime BIOS Resilience
Implement Modern Standby
Provision TPM 2.0 with platform hierarchy indices required by TXT
Include TXT ACM binary in flash image
Update system FW via Update Capsule (recommended)
Demo: Attestation of HW Security Posture
System Guard Validation

Use System Guard HLK Test included to validate requirements

Windows Indicators of Secure Launch:
• WDSC Verification of Windows Secure Launch
• MSInfo32 Verification of Windows Secure Launch
• Basic Verification of DRTM PCR Measurement

SMM Audit Tool to verify SMM configuration
• Add MS SMM Audit/Test driver to a debug UEFI build:
  https://github.com/Microsoft/MS_UEFI/tree/share/XmlAndUnitTest/UefiTestingPkg/AuditTests/SmmPagingAudit
• Run Audit Shell tool
• Run Windows Tool to generate report and check for issues
Windows Security app
End user facing status & configuration of HW security settings
Windows Security App – Device Security UI

Core isolation

Security features available on your device that use virtualization-based security.

Memory integrity
Prevents attacks from inserting malicious code into high-security processes.

Firmware protection
Windows Defender System Guard is protecting your device from compromised firmware.

Windows Defender Credential Guard
Credential Guard is protecting your account login from attacks.

Memory access protection
Protects your device’s memory from attacks by malicious external devices.

Enhanced sign-in security
Windows Defender System Guard is providing additional security for Windows Hello.
Futures & Challenges
Speculative Execution Side Channel Attacks

“The fundamental solution to the problem, though, would be a ground-up reworking of the [computer] architectural definition” Mark Hill, professor of CompSci, U. of Wisconsin
Return address protection with hardware

**Initial attempt to implement stack protection in software failed**
Microsoft REDTEAM designed software shadow stack (RFG) did not survive internal offensive research

**Control-flow Enforcement Technology (CET)**
Indirect branch tracking via ENDBRANCH
Return address protection via a shadow stack
Hardware-assists for helping to mitigate control-flow hijacking & ROP
Robust against our threat model

```
Return EIPn-1
Param 1
Param 2
Return EIPn
```

ESP after call

```
Return EIPn-1
Return EIPn
```

SSP after call

Stack usage on near CALL

Call pushes return address on both stacks

Ret/ret_imm
pops return address from both stack
Exception if the return addresses don’t match

No parameters passing on shadow stack
RowHammer

Repeatedly accessing a DRAM row induces bit flips

Flipping bits in memory without accessing them: an experimental study of DRAM disturbance errors [Kim et al., ISCA 2014]

Attacker can modify data of other processes, code at other Priv Levels

E.g. Exploiting the DRAM rowhammer bug to gain kernel privilege [Seaborn & Dullien, Blackhat 2015]

“New Rowhammer Attack Hijacks Android Smartphones Remotely” Wired, 5/2018

Glitch: “remote Rowhammer exploit on ARM Android devices makes it possible for an attacker who controls a malicious website to get remote code execution on a smartphone without relying on any software bug” https://www.vusec.net/projects/glitch/

Aweke et al., ANVIL: Software-Based Protection Against Next-Generation Rowhammer Attacks (2016)
Call to action

• Understand the level 2 and level 3 requirements!


• Enable VBS in the factory on devices where appropriate

• Pick appropriate device line & deliver initial level 3 capability

• Thoroughly embrace delivering firmware updates via Windows Update + UEFI capsule

• Evaluate adoption of project Mu for Modern UEFI: https://microsoft.github.io/mu/
**Security Goal**

Prevent “evil cleaner” drive by physical attacks from malicious DMA attacks

**Goals for 1803 Release**

Use IOMMU to block newly attached Thunderbolt™ 3 devices from using DMA until an authorized user is logged in and the screen is unlocked.

Automatically enable DMA remapping with compatible device drivers (Memory Sandboxes) to improve overall user experience.

In future releases, we are looking to harden protection on all external PCI ports and cross-silicon platforms.

---

**Diagram Description:**

1. Connect peripheral
2. New devices are enumerated and functioning
3. Peripheral Drivers opted-in DMAr?
   - Yes: Enable DMAr for the peripherals
   - No: Wait for user to login/unlock screen
4. User logged in AND Screen unlocked?
   - Yes: Enable DMAr for the peripherals
   - No: Wait for user to login/unlock screen
Improve transparency: Device Security Features

Security at a glance
See what's happening with the security and health of your device and take any actions needed.

- Device security
  View status and manage hardware security features
- Account protection
  No action needed.
- Firewall & network protection
  No action needed.
- App & browser control
  No action needed.

- Security processor
  Your security processor, called the trusted platform module (TPM), is providing additional encryption for your device.

- Secure boot
  Secure boot is on, preventing malicious software from loading when your device starts up.

Your device meets the requirements for enhanced hardware security.
System Guard HLK Tests

SystemGuardTest::TestDmaProtection
• Verifies Kernel DMA protection is implemented

SystemGuardTest::TestTxtSinitSigner
• Verifies SINIT ACM signer pub key hash is trusted

SystemGuardTest::TestTxtCpuSrtmStat
• Verifies CPU_SCRTM_STAT contains legitimate value (0 or 1)
SystemGuardTest::TestOsSinitDataCap
• Verifies what Windows supplied for SinitDataCap was not modified

SystemGuardTest::TestLcpControl, SystemGuardTest::TestLcpAuthorities, SystemGuardTest::TestNvInfo
• Verifies TPM Platform hierarchy indices are correctly provisioned per System Guard requirements
Windows 10

Virtualization Based Security Environment

Trustlet #1
Trustlet #2
Trustlet #3

Secure Kernel

Kernel

Hypervisor

Windows Platform Services

Apps

© 2018 Microsoft
Windows 10

Virtualization Based Security Environment

Secure Kernel

Hypervisor

Apps

Windows Platform Services

Trustlet #1

Trustlet #2

Trustlet #3
Secure Boot: Static Root of Trust

Secure Boot implementation includes OEM UEFI in the root-of-trust.

UEFI code is complex and servicing is not mature.

Dozens of vulnerabilities discovered in UEFI in recent years.

Secure boot currently uses static root of trust – OEM firmware included in attack surface.