presented by

Microsoft

Microsoft UEFI Security Updates

UEFI US Fall Plugfest – September 20 - 22, 2016
Presented by Microsoft

Scott Anderson, Suhas Manangi, Nate Nunez, Jeremiah Cox, Michael Anderson

Agenda

- Introduction
- Secure Boot Debug Policy
- Device Guard-WHCR and UEFI CA
- Secure Boot Updates– Customized Secure boot Roadmap for UEFI
- TrEE –> TCG2.0
- HSTI
- Call to Action
- Conclusion
- Final group Q/A

Scott Anderson Presenting

Debug Policy

Debug Policy

- A.K.A Golden Key
- Current situation:

  What it isn't

  – This is not an issue with UEFI Secure boot
  – Private Key was not leaked
  – This issue has no impact on Encryption or Bitlocker

  And what it is

  – For RT we had a debug policy to unlock individual devices for development
  – The mechanism for debug policies was changed to simplify debug policies
  – A design issue allowed the new policies to unlock old devices/OS versions
  – A debug policy that was shipped with the HoloLens SDK was used in attack
  – RS1 and later is Secure, only down level operating systems are vulnerable
  – Must be an admin and have physical access to exploit the bug

Debug Policy (cont.)

- What's next
  - OEMs/IBVs should continue to build and ship Windows 10 devices as before – no changes
  - DBX is updated in RS1 RTM image (and later)
    - If it is not baked in to the firmware in manufacturing then OS will fix it on first boot
  - HLK test will fail if not on the default RS1 DBX
    - Latest updates to DBX may also fail, see readme in DL
    - Exception till end of October 2016 (Errata id: 5608)
  - http://uefi.org/revocationlistfile has the updated DBX list
  - Find us to discuss if you have concerns or questions

Suhas Manangi Presenting

WHCR, Device Guard and UEFI CA updates

Windows Hardware Compatibility Requirements for RS2

System.Fundamentals.Firmware.UEFISecureBoot

- **Modify bullet "30.":** Reserved Memory for Windows Secure Boot UEFI Variables. A total of at least 120 KB of non-volatile NVRAM storage memory must be available for NV UEFI variables (authenticated and unauthenticated, BS and RT) used by UEFI Secure Boot and Windows. The maximum supported variable size must be at least 64kB and there is no maximum NVRAM storage limit.

- **New bullet "41.":** Confidential & replay-protected storage[Optional until 2018]: External memory for non-volatile storage of all UEFI variables and security-sensitive BIOS settings MUST include protections of that data to insure confidentiality and integrity of the data and to mitigate against rollback attacks. This is generally accomplished by encrypting the data, applying a Message Authentication Code, and storing the resulting record in replay-protected storage such as Replay Protected Memory Block or Replay Protected Monotonic Counter.

Windows Hardware Compatibility Requirements for RS2 (cont.)

WHQL Signing requirements for kernel drivers

- **Started in RS1; this is now baseline for current and future versions of windows**
  - **All kernel drivers to be WHQL signed**
  - **All kernel drivers are required to be compatible with HVCI**
  - **File info to be added to drivers**
    - Defines a version-information resource. The resource contains such information about the file as its version number, its intended operating system, and its original filename. The resource is intended to be used with the Version Information functions.

Device Guard updates

- DG Readiness Tool v2
- DG OEM Requirements – TH1/TH2 is published
- New to RS1/RS2:
  - Secure MOR, NX Protections, SMM Protections
  - Firmware Updates to ship through Windows Updates (alternative auto updates?)

UEFI CA with Device Guard

- **DG Requirement includes removing Microsoft UEFI CA**
- **Alternatives/Options:**
  1. **System Firmware**
  2. **OEM UEFI CA - signing policy recommendations:**
     - OEM's signing policy can align with Microsoft UEFI CA signing policy, such that, OEM(s) shall sign only those UEFI drivers/apps that are already signed by Microsoft UEFI CA
     - OEM could decide to either replace Microsoft UEFI CA signature on the submitted UEFI driver/app or dual sign it on top of Microsoft UEFI CA
     - This way OEM can piggy back on Microsoft's security reviews, and reduce the attack surface by signing only those UEFI drivers/apps that they need for their platform but not everything that Microsoft UEFI CA signs/signed
     - Current Microsoft UEFI CA signing policy
     - Test that we ask submitters to perform before submitting the "Pre-submission testing for UEFI submissions"
  3. **IHV UEFI CA**
  4. **Direct Hash**

UEFI CA updates

- **Microsoft UEFI CA Signing policy updates**
  - Microsoft will not sign EFI submissions that use EFI_IMAGE_SUBSYSTEM_EFI_RUNTIME_DRIVER. Instead, we recommend transitioning to EFI_IMAGE_SUBSYSTEM_EFI_BOOT_SERVICE_DRIVER. This prevents unnecessary use of runtime EFI drivers.
  - Use of EBC code: Microsoft will not sign EFI submissions that are EBC-based submissions.
  - If your submission is a DISK encryption or a File/Volume based encryption, then you MUST make sure that you either *don't* encrypt the EFI system partition or if you *do* encrypt, be sure to decrypt it and make it available by the time Windows is ready to boot.

Enforcement Date: 01/01/2017

Windows and UEFI versions

- UEFI 2.3.1c minimum requirement
  - Same is for Windows desktop and server
- What about UEFI 2.5?
  - Customized Deployment of Secure Boot is still in flux hence not recommended
  - Similarly for HTTPS boot and Platform recovery (unless fully supported by OEM)

Nate Nunez Presenting

Customized Deployment of Secure Boot

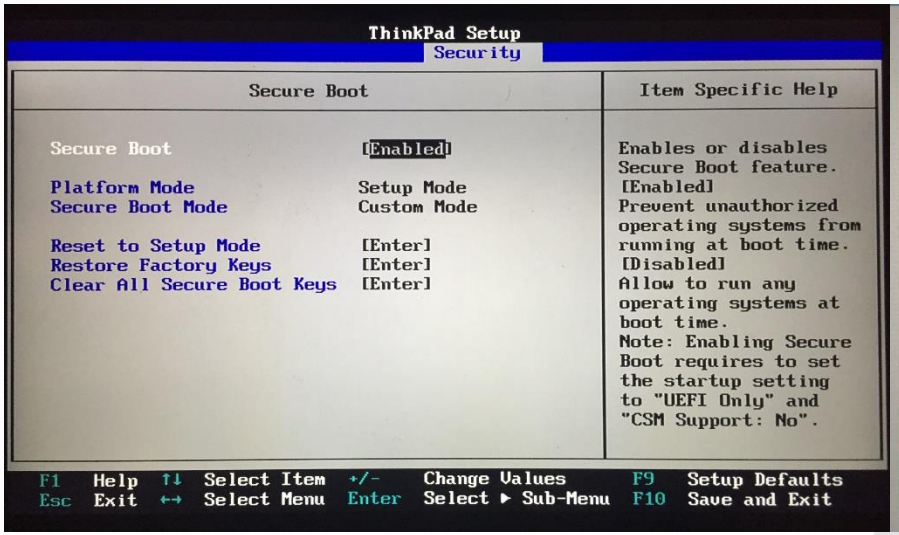
Customized Deployment of Secure Boot

- Configure Secure Boot options programmatically
  - Enterprise admins can set and deploy PK/KEK/db/dbx/[future Secure Boot variables]
  - Uses new Secure Boot modes from UEFI 2.5 Section 30.3
    - Setup, User, Deployed, Audit
- Relies on PCR[7] in TPM 2.0

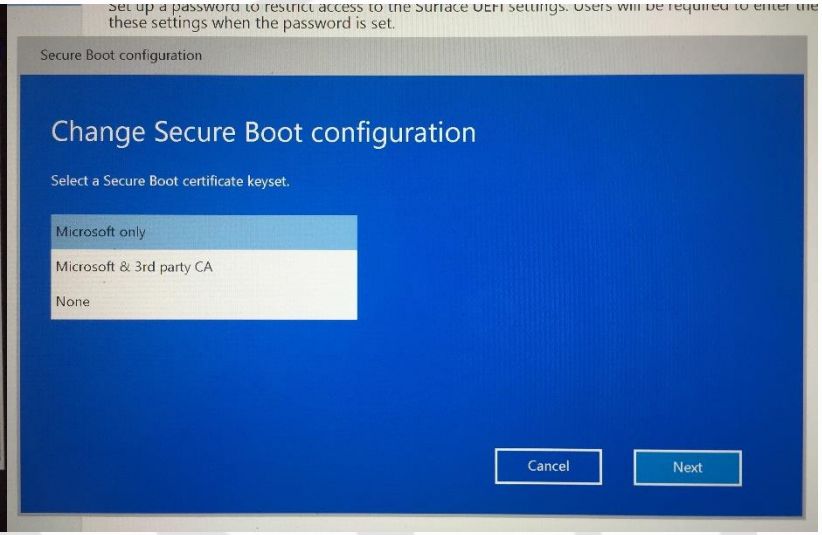
Customized Deployment of Secure Boot tentative timeline

Estimate	Checkpoint
09-2016	UEFI spec fix ECR drafted
11-2016	TCG spec stabilized
12-2016	UEFI spec fix published
02-2017	Tianocore production branch stabilized and verified
03-2017	IBVs receive Tianocore
05-2017	IBVs ready to support Customized Deployment of Secure Boot
08-2017	OEMs start shipping devices with the Customized Deployment of Secure Boot feature

Windows Consistent Secure Boot Workflows



Lenovo ThinkPad, Phoenix



Microsoft Surface Book

Gabe Stocco Presenting

Brief talk on TrEE -> TCG2.0

Trusted Execution Environment TrEE (1.0)

- EFI protocol to allow OS (bootloader) to:
  - Check TPM related firmware capabilities
  - Obtain TCG measured boot log
  - Add measurements to log and extend into TPM PCRs
  - Pass TPM commands to TPM device

TrEE 1.0 -> TCG2.0

- Added support for crypto-agile functionality
  - Switch active TPM PCR banks
  - Obtain crypto-agile TCG measured boot log
- Same GUID as TrEE 1.0 protocol
- Get capability API reports new version number
  - Allowing firmware to implement one protocol
  - Caller can use different subset of functionality based on reported version

Why the change to TCG2?

- TCG adopted "TrEE" protocol as TCG2.0
- TCG as an Industry Standards Organization is influenced by community effort
- With the upcoming Windows hardware requirement for TPM 2.0 and support for SHA256 as active TPM PCR bank, Microsoft recommends to implement TCG2 protocol to be able to meet this Windows requirement

Gabe Stocco Presenting

Hardware Security Test Interface (HSTI)

HSTI

- HSTI; testing system security is more important than ever before
- HSTI provides convenient interface for self-tests
  - Helps ensure correct configuration
  - Follow up with silicon/UEFI vendor with questions
- HSTI provides excellent security value to Windows Customers

HSTI (Cont.)

- HSTI will be used to ensure correct configuration to enable value added security features
  - Microsoft is expecting you to enabling HSTI on all platforms on which it is available
- Microsoft is looking for ways to improve
  - We would love to hear suggestions, recommendations for improvements.
  - Hardware Security Testability Specification Link

Section Heading

Conclusion, call to action

Call to action

- HSTI
- TPM2.0 – TCG2.0
- Secure Boot document update coming in October

Questions?

- Some responses may require NDA with Microsoft.
- If you have questions that we do not address, please attempt to connect with us around Plugfest
- Or follow up in email using the following alias (for Security and UEFI related Questions) SAUEFI@Microsoft.com

Links

- UEFI Revocation List File
  http://uefi.org/revocationlistfile
- File info to be added to drivers
  https://msdn.microsoft.com/en-us/library/windows/desktop/aa381058(v=vs.85).aspx
- Version Information
  https://msdn.microsoft.com/en-us/library/windows/desktop/ms646981(v=vs.85).aspx
- DG Readiness Tool v2
  https://www.microsoft.com/en-us/download/details.aspx?id=53337
- DG OEM Requirements – RS1
  https://msdn.microsoft.com/en-us/library/windows/hardware/mt767514(v=vs.85).aspx
- Microsoft UEFI CA signing policy
  https://blogs.msdn.microsoft.com/windows_hardware_certification/2013/12/03/microsoft-uefi-ca-signing-policy-updates/
- UEFI CA test we ask submitters to perform before submitting -Pre-submission testing for UEFI submissions
  https://blogs.msdn.microsoft.com/windows_hardware_certification/2013/12/03/pre-submission-testing-for-uefi-submissions/
- Microsoft UEFI CA Signing policy updates
  https://blogs.msdn.microsoft.com/windows_hardware_certification/2013/12/03/microsoft-uefi-ca-signing-policy-updates/
- Hardware Security Testability Specification
  https://msdn.microsoft.com/en-us/library/windows/hardware/mt712332(v=vs.85).aspx

Thanks for attending the UEFI US Fall Plugfest 2016

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

presented by

Microsoft