presented by

Microsoft UEFI Certification Authority

UEFI PlugFest – September 19-20, 2013

Presented by Jeremiah Cox (Microsoft Corp.)

Agenda

- Digital Signing
- Secure Boot
- UEFI CA
- Improving User Choice
- Conclusions

Digital Signing

Digital Signing

- A foundation for Secure Boot
- Additional bits…
- Prevent tampering
- Provide signer-defined claims
  - Certification Authorities
    - Identity of signer
      - Think passport
  - WHQL: Microsoft Windows Hardware Compatibility Publisher
    - Passes “Logo” tests
  - …

Digital Signing: CA Claims

- Identity, identity, identity

- Trustworthiness?
  - NOT evaluated by CA's
  - No background checks, recommendations, polygraphs, mental fitness evaluations

Digital Signing: Revocation

- Lost signing keys?
  - Revocation & Re-Key
- Malicious actors?
  - Revocation
- Prevents polymorphic malware
  - New malware requires new cert

  $ + forgery + time

Digital Signing: Extended Validation

- a.k.a “EV” Code Signing
- Benefits
  - Stronger assurance of identity
  - Private keys in FIPS 140-2 L2 hardware
- Non-benefit
  - Trustworthiness of subject - not addressed
- Leveraged by Windows SmartScreen

What is Secure Boot?

Secure Boot == Rootkit Prevention

- Only “trusted” code executes
  - System vendor pre-populates trust list
  - User customizes as desired
- “Windows 8.x” Certified systems must:
  - Ship secure-by-default
  - Trust Windows 8.x
    - Not trust <8.0, *not* Secure Boot “enlightened”
  - Provide user choice
    - Options to disable & customize

Secure Boot OS “do’s”

- Continue Secure Boot into the OS
  - Kernel Mode Code Integrity
  - Solid revocation story
- Block development & test modes…
  … that weaken code integrity
  - Kernel Driver TESTSIGNING
  - Kernel Debugging

Microsoft's UEFI CA

- A signing service for UEFI modules
- Most new PCs trust Microsoft's UEFI CA
  - Not required
  - May not be present in high-security or highly-integrated devices

Secure Boot: Trust Decisions

- In-Box Trust List
  - … varies by OEM …
  - – Windows 8.x - almost always present
  - – Microsoft UEFI CA – usually
  - – Canonical Ltd. Master Certificate Authority - some
- User Choice
  - – Disable for compatibility with legacy
  - – Customize to suit your taste

Microsoft UEFI CA Myth: Microsoft Charges $99

- Paid to Symantec
  - $99 (introductory price)
- Paid to Microsoft
  - $0

- Microsoft's cost to operate the CA
  - $<big number>
  - We appreciate your commitment to submit quality, secure code

Microsoft UEFI CA Myth: Microsoft Signs Everything

- No
- Why?
  - $99 Symantec certificate does not prove
    - Secure Boot & security competency
    - Trustworthiness

0 != sizeof(dbx)

What does Microsoft UEFI CA sign?

- Secure Boot “enlightened” modules
  - Do not permit untrusted code to execute

- It does **NOT** sign:
  - GPL Version 3 (or similar) licensed code
    - GRUB 2
  - Modules that permit untrusted code to execute
    - GRUB 0.9
  - Hobby projects, code still in development, test code, platform specific tools
- Chain loaders are effectively cross signing
  - Merit deeper review
- In the future anything that gets to kernel may be an attack that is exploited and we can no longer sign

Before submitting to the MS UEFI CA

- Use the Security Development Lifecycle
  - Or similar
  - Threat models, security reviews, …
- Test
  - Function
  - Security
  - Test Secure Boot signing & enlightment
    - http://aka.ms/uefica-test

Microsoft UEFI CA: Needs

- Establish better identity and trustworthiness
- Reduce turnaround time without compromising quality in security

Microsoft UEFI CA: Future

- Require EV certs
- Require organizations, not individuals
- Improved information gathering

User Experience

- Today:
  - OEMs must allow Secure Boot to be disabled and customized
  - OEMs can implement in the way that they think makes most sense for users
- Microsoft is committed to support industry efforts to improve the consistency and usability of Secure Boot configuration

Improving User Choice

- We should consider standardizing experience:
  - Nomenclature in BIOS options
  - File format to enroll in db
  - Entry points to relevant BIOS menus
- Benefits:
  - Always works
  - Simplifies documentation
  - Reduces customer support

Secure Boot: Present User Test

- If I am physically present, I am the owner
  - Stolen or borrowed devices?
  - "Evil Maid" can install a rootkit
  - Solution: BIOS password
- I understand the consequences of "Yes"
  - Users want forward progress
  - Faced with an unknown prompt? Click "Yes"
  - Facilitates ransomware
  - UAC, SmartScreen provide learnings

What should I remember?

Conclusions

Conclusions

- Revocation happens
- EV Certificates
  - Provide additional identity assurance
  - Provide additional protection for private keys
  - Coming to the Microsoft UEFI CA
- Microsoft supports user choice in the Secure Boot ecosystem

Links

- HOWTO: test sign UEFI drivers & apps
  - http://aka.ms/uefica-test
- Microsoft Root Certificate Program
  - http://aka.ms/rootcaprogram
- Security Development Lifecycle
  - http://aka.ms/SDL
- Ransomware
  - http://en.wikipedia.org/wiki/Ransomware_(malware)

Thanks for attending the UEFI PlugFest 2013

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

presented by