Validating Hardware Security Through Firmware Interfaces

UEFI Summerfest – July 15-19, 2013
Presented by Jeremiah Cox (Microsoft Corp.)
Agenda

• Motivation
• Challenges
• Improvements
• Call to Action
• Questions
Motivation

Why am I not at lunch right now?
Security Is Important

• Exposure
  – “Everything” is online

• Customer Expectations
  – Home
  – Enterprise
    • Intellectual Property
    • BYOD: Bring Your Own Device
      – Consumer devices need Enterprise security
      – Pervasive Device Encryption

• Cost of security failure?
Windows Hardware Certification Requirements (WHCR)

• **8.0**
  - System.Fundamentals.Firmware.UEFISecureBoot

• **8.1 Preview**
  - System.Fundamentals.Firmware.CS.UEFISecureBoot.Provisioning
    • More security improvements
    • Improve testability of security features
    • Required on Connected Standby systems
    • Recommend for all
Security is NOT Easy

Challenges
Security Is NOT Easy

• Defenders’ Dilemma
  – Attackers
    • 1 weakness == Game Over
    • PR: Declared “insecure”
  – Defenders
    • No gaps end-to-end
    • 0 security bugs
Security Is NOT Easy

• Key Management
• Digital Signing
• Access Control
• Privacy
• Secure Systems
  – Debugging
  – Recovery
  – Remanufacturing
• ...

UEFI Summerfest – July 2013  www.uefi.org
Security Is NOT Easy: One Possible Mitigation

• Security Development Lifecycle
  – Training
  – Requirements
  – Design
  – Implementation
  – Verification
  – Release
  – Response
Make life easier

**Improve Testability**
Windows Hardware Security Test Interface

• Verify security feature enablement
  – Hardware protections enabled?
    • “Platform” Secure Boot
  – Firmware protections enabled?
    • Secure Firmware Update
    • Rollback policy
  – Misconfigurations mistakes
    • Option ROM verification
Windows Hardware Security Test Interface

- Authored by domain experts
  - Chipset & BIOS vendors

- Built upon Adapter Interface Protocol (M992)
  - Defined by Microsoft, not a UEFI Specification

- **Required** on Windows 8.1 Connected Standby by 2015
  - Requirement:
    - System.Fundamentals.Firmware.CS.UEFISecureBoot.Provisioning
  - Provides testing for:
    - System.Fundamentals.Firmware.UEFISecureBoot
Windows Hardware Security Test Interface

• Cannot test everything
  – Best effort, test what is testable
  – PASS does NOT guarantee success, but...
  – FAIL prevents high risk blunders

• Deviations from reference designs may FAIL
  – Could cause delays
What do I do?

Call to Action
Call to Action

• Ask your Chipset & BIOS vendors for their HSTI implementation

• Does it pass on your system?
  – No? Find and fix the problem.
  – CS systems must PASS beginning 1/1/2015

• Request more security tools & tests

• Adopt the Security Development Lifecycle
Links

• Windows 8.1 Hardware Certification Requirements

• Hardware Security Test Interface
  – Not all have access
  – https://connect.microsoft.com/
  – Windows Pre-Release Program > Downloads

• Security Development Lifecycle
  – http://aka.ms/SDL

• Pervasive Device Encryption
  – Bing: “What's New in Windows 8.1 technet”
Thanks for attending the UEFI Summerfest 2013

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

presented by Microsoft