presented by

Microsoft

Windows

Microsoft Tools & Tests for Secure Boot

UEFI Winter Plugfest – February 21-23, 2012

Presented by Jeremiah Cox (Microsoft)

Agenda

- Inbox Powershell Cmdlets
- Windows Hardware Compatibility Kit
  - Tests
  - Examples
  - Demo

Inbox Cmdlets

- Admin Powershell: "`PS c:\> help secureboot`"
- **`Confirm-SecureBootUEFI`**
  - Is UEFI Secure Boot "ON", True or False?
    - **`SetupMode == 0 && SecureBoot == 1`**
- **`Set-SecureBootUEFI`**
  - Set or Append authenticated SecureBoot UEFI variables
- **`Get-SecureBootUEFI`**
  - Get authenticated SecureBoot UEFI variable values
- **`Format-SecureBootUEFI`**
  - Creates **`EFI_SIGNATURE_LISTS`** & **`EFI_VARIABLE_AUTHENTICATION_2`** serializations

WHCK: Secure Boot Logo Test

- Proper out-of-box Secure Boot configuration (enabled, proper certs, …)
- 1 “dbx” append signed by an untrusted key
- 1 “dbx” append signed by the Microsoft KEK
- Many 1kB variables are created/deleted
- A 32kB variable is created/deleted

WHCK: Secure Boot Manual Test

- "\tests"
  - Manufacturing Test
    - Programmatically Enable Secure Boot
  - Servicing Tests
    - Append a cert to "db", verify function
    - Append a hash to "dbx", verify function
    - Append a cert to "dbx", verify function
    - Append 600+ hashes to "dbx", verify size

WHCK: Secure Boot Manual Test

- "\Generate" Examples Demonstrate
  - How test certificates were created
    - The test certificates and private keys are included
  - How all of the tests were created
    - Turning certificates & hashes into signed packages
    - You can run this yourself, substitute your own certs

WHCK: Secure Boot Manual Test

- "\Examples"
  - show how to configure Secure Boot to pass the Out-of-Box tests
  - NOTE: The cert chain that signs the Windows Boot Manager will change at RC
- "\certs"
  - All of the certs you need to boot Windows

Interactive Demonstrations

- Switch to live demo…

Thanks for attending the UEFI Winter Plugfest 2012

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

presented by

Microsoft

Windows