



How to Protect the Pre-OS Environment with UEFI

UEFI Fall Plugfest – October 24-27, 2011 Presented by Tony Mangefeste

Agenda





- How we got here
- The problem
- A solution
- Authentication versus
 Verification
- Signing

The Long Road...

- SPA .
- BIOS provided hooks for field-patch
- Hooks were exploited
- And limitations of BIOS
 - MBR, Disk Size, INTx
 - Wild West of Option ROMs
- Difficult to Service

The Problem



- Protecting the UEFI Boot Entry versus Firmware Recovery Mode
- The Extended Service Partition (ESP) is unlocked and accessible
- PE/COFF's not authenticated
- Multiple Entry Points
- Regardless UEFI is best pathway forward

A Solution



- Secure Boot Using Authenticode to sign PE/COFF images
- Signatures stored in NVS provide an approach to authenticate images
- Signatures may be hashes, keys, certificates
- Signatures are tamper-proof

Authentication vs Validation



- Authentication does not guarantee quality of code
- Not feasible for firmware to perform malware signature validation
- Firmware is offline and resource limited
- Therefore, signing is the best way to restrict unauthorized execution in the boot path ...

Signing

- Microsoft is using Winqual to provide a UEFI Signing Service
 - -Winqual hosts 11,000+ companies
 - Minimal one-time administrative costs
 - Free signing of UEFI images
 - All images uniquely identified by company
- Creates an independent certificate authority (CA) for UEFI images

Come try it out...



- Offering signing of UEFI images this week at UEFI Plugfest
- Your company must have an IEA with Microsoft or a Winqual Account
- No formal announcement of release at this time, available only for testing this week ...

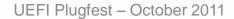
Thanks for attending the UEFI Fall Plugfest 2011



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

presented by

Microsoft®



But wait, there's more ...



Welcoming Remarks – Aven Chuang, Insyde Software
UEFI Forum Updates – Dong Wei, VP of the UEFI Forum



Best Practices for UEFI Driver Compatibility – Stefano Righi, American Megatrends, Inc.

Understanding Platform Requirements for UEFI HII — Brian Richardson, Intel Corporation



UEFI Security Enhancements – Kevin Davis, Insyde Software **How to Protect the Pre-OS Environment with UEFI** – Tony Mangefeste, Microsoft



Pre-OS Display Switching using GOP – James Huang, AMD Debug Methodology Under UEFI – Jack Wang, Phoenix Technologies

Download presentations after the plugfest at www.uefi.org