UEFI Forum Update

Presented by Dong Wei, Chief Executive
Agenda

Latest Specifications
Strengthening Boot Phase Security
UEFI SCT
ACPI SCT
Summary
Latest Specifications

UEFI Specification v2.4B (4/2014)
UEFI Shell Specification v2.1 (7/2014)
UEFI PI Specification v1.3 (7/2013)
PI Package Specification v1.0B (8/2014)
ACPI Specification v5.1 (7/2014)

Q1’15: UEFI v2.next and ACPI v5.next
Strengthening Boot Phase Security

Established the Security Response Team (USRT)
Provides a communication conduit
Determine the scope of vulnerability
Assist member companies in responses

http://uefi.org/security
Chair: Dick Wilkins
More details – stay tunes for his presentation
UEFI SCT

Latest official release v2.3.1C (7/2013)
Next release v2.4B (Q1’15)
• UTWG Development in GitHub
• Removal of Shell dependency (supports 1.0 or 2.0)
• Removal of ECP dependency
• Release Candidate available for use at this event
Please test and report issues
ACPI SCT

Current thinking

- WHQL tests for Windows
- FWTS tests for Linux

FWTS now runs on luvOS (distro-neutral)

Q: luvOS on ARM?
Summary

Clear leader on x86/x64 Client and Server Systems
Required for SBSA/SBBR-compliant ARM Servers
Opportunities in the IoT and embedded market
• E.g., TinyQuark
More ISA bindings
For more information on the Unified EFI Forum and UEFI Specifications, visit http://www.uefi.org