Fall 2017 UEFI Plugfest

Oct. 30 - Nov. 3 | Taipei, Taiwan

Hosted by

American Megatrends

presented by

The UEFI Forum

State of UEFI

Fall 2017 UEFI Seminar and Plugfest
October 30 – November 3, 2017
Presented by Mark Doran, UEFI Forum President

Agenda

- Event Overview
- The UEFI Forum
- Specifications Update
- Summary
- Questions

Event Overview

Made Possible by…

arm

insyde®

intel®

phoenix® technologies

redhat®

Agenda

	Day 1 Oct. 30 (Mon)	Day 2 Oct. 31 (Tue)	Day 3 Nov. 1 (Wed)	Day 4 Nov. 2 (Thurs)	Day 5 Nov. 3 (Fri)
08:00-08:30		Check-in (Event) / Breakfast	Check-in (Event)	Check-in (Event)	
08:30-09:00		**State of UEFI** *Mark Doran or Dong Wei*			
09:00-09:20		UEFI Security Response Team (USRT) **UEFI Forum**	Testing Session	Testing Session	Make-up Testing and Test Suite Breakdown
09:20-09:30		Opening Ceremony			
09:30-10:00		Testing Session			
10:00-10:30					
10:30-11:00					
11:00-11:30					
11:30-12:00					
12:00-12:30		Lunch	Lunch	Lunch	Check-out (Testing Suite)
12:30-13:00		"Last Mile" Barriers to Removing Legacy BIOS **Intel**	Advances of UEFI Technologies in ARM Systems **Arm**	NFC and UEFI **AMI**	
13:00-13:30		UEFI Firmware - Security Concerns and Best Practices **Phoenix**	Introduction to the Self-Certification Test (SCT) in UEFI World **Canonical/Intel**	Edk2 Platforms Overview **Linaro**	
13:30-14:00		Testing Session	Testing Session	Testing Session	
14:00-14:30					
14:30-15:00					
15:00-15:30	Check-in (Room) / Testing Suite Setup				
15:30-16:00		Strategies for Stronger Software SMI Security in UEFI Firmware **Insyde**	Firmware Test Suite Introduction: Uses, Development, Contribution and GPL **Canonical**	UEFI Manageability and REST Services **HPE/Intel**	
16:00-16:30		Testing Session	Testing Session	Testing Session	
16:30-17:00					
17:00-17:30					
17:30-18:00					
18:00-18:30					
18:30-19:00		Social Dinner Event (18:30)			

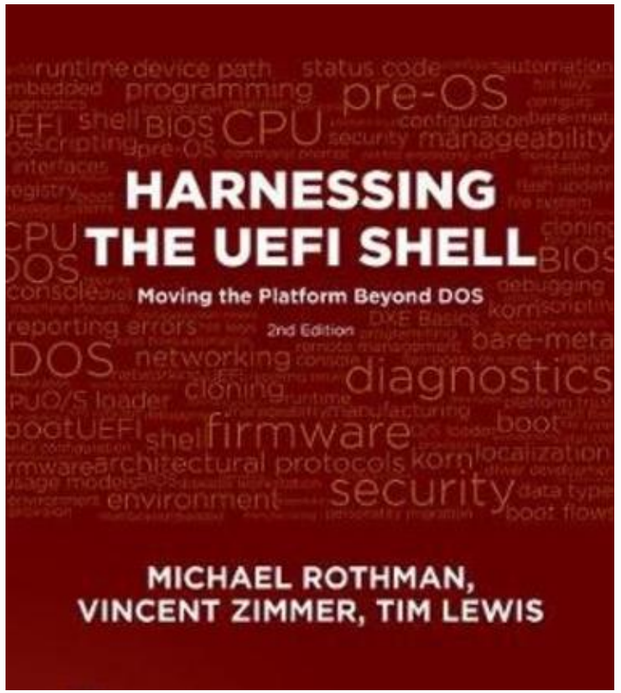
Venue Guide

	10/30 Testing Suite Check in / Check out	10/31 Event Check in	11/1&11/2 Event Check in	10/31-11/2 Lunch/Presentation
15F				
7F Room 701				
1F Front Desk				

Event Survey – Feedback Please!

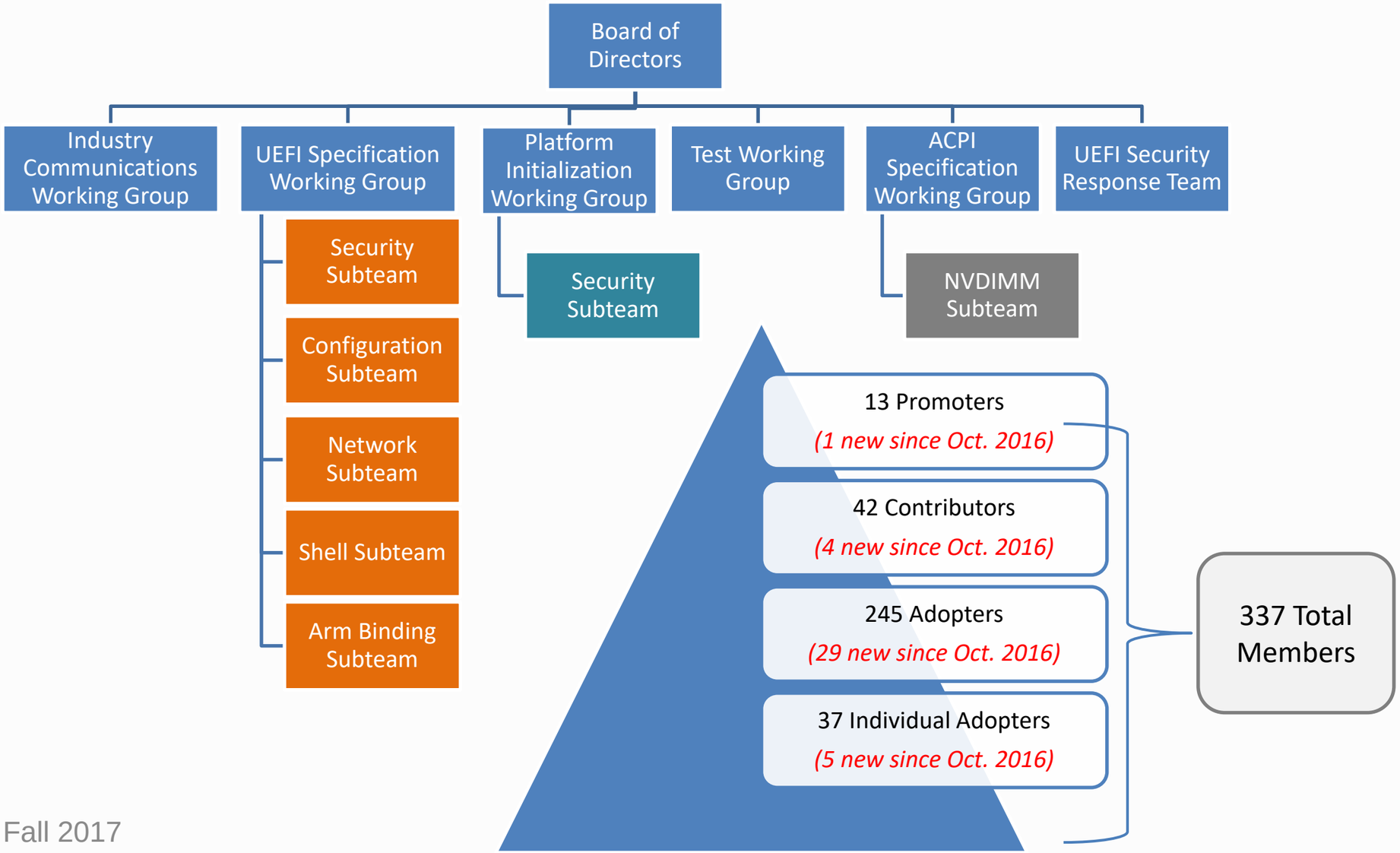
www.surveymonkey.com/r/Fall2017Plugfest

To be included in the drawing for a chance to win the latest "Harnessing the UEFI Shell" book complete your survey by 10am on Thursday, November 2.



The UEFI Forum

UEFI Forum Overview



Historical Milestones

2005	The UEFI Forum founded
2008	Apple adopts UEFI firmware; HP notebook and desktop platforms include UEFI
2009	UEFI Specification includes Arm architecture
2010	Secure Boot included in UEFI specification
2011	Linux Foundation joins the Forum
2012	Microsoft Windows 8 requires UEFI for its certification logo
2013	The UEFI Forum begins management of ACPI Specification
2015	PC hardware predominantly ships with UEFI

UEFI Today and Beyond

2017

- Industry-wide cooperation and support
- 337 members companies and individuals
- Common framework allowing developers to scale as needed

Future

- Continuous evolution across a range of platforms and enables secure cross-functionality
- Firmware security campaign and resources to educate developers on the importance of 1) implementing UEFI firmware as outlined in the specifications and 2) taking a proactive approach to security, starting at the lowest levels with regular updates.

Resources

- New Industry Resources Library
  - Features presentations, articles and other collateral from thought leaders in firmware and platform security
- Reporting Security Issues
  - If you have information on a security issue or vulnerability with a product that may be due to its UEFI-based firmware, visit http://www.uefi.org/security

Specification Update

Latest Specifications

v2.7A v2.2 v1.6 v2.5A v1.1 v6.2A < Current Versions

- First time the UEFI, Platform Interface (PI) and ACPI specifications were updated together (received a lot of input from the community and members)
- Updates represent support for upcoming hardware, such as non-volatile memory, as well as deployment learnings over the last several years, such as the UEFI variable enhancement and completeness (i.e. the SPI driver)

What's New in UEFI 2.7?

- **New private authenticated NVRAM variables with X.509 certs**
  - Previously most AVs were in UEFI Secure Boot, which is a very specific environment. This change allows for more generalized interfaces and enhances the Set and Get variables services in UEFI runtime table.
- **EFI HII Pop up protocol**
  - Added protocol to provide services for pop windows (i.e. in setup)
- **External management capability for UEFI Secure Boot**
  - Allows for out-of-band management of UEFI Secure Boot keys, including service processors and hypervisors for guest firmware
- **EFI HTTP Boot Callback Protocol (added)**
  - Can be used for HTTP boot debugging and packet inspection.
    - This allows for printing status updates to the console during a long download during handoff to network boot file over HTTP
- **Added ABI calling convention for RISC-V UEFI images**
- **New Reset Notification Protocol**
  - Registers a function to be called before gRT->ResetSystem() is executed
  - Allows for a common wae a reset (i.e. TPM, NVME storage device etc.)

What's New with ACPI 6.2?

- **Secure Devices (SDEV) ACPI Table**
  - New SDEV ACPI table, a list of devices that are allowed/denied to be hand-off by secure OS to a normal one.
- **Heterogeneous Memory Attribute Table (HMAT)**
  - New HMAT ACPI table, memory attributes for systems with heterogeneous memory architecture
- **Platform Debug Trigger Table (PDTT)**
  - New PDTT ACPI table, a standard way to notify all debuggers connected to the system of a fatal crash.
- **Processor Properties Topology Table (PPTT)**
  - New PPTT ACPI table, a description of CPU topology, available cache types and sizes.
- **Windows SMM Security Mitigations Table**
  - Reserved WSMT ACPI table, Microsoft's invention for system firmware to report its SMM security measures
  - Linux does not have a WSMT ACPI table equivalent so it does not have this SMM protection

What's New with PI 1.6?

- **Added the VOLUME_EXT_ENTRY_USED_SIZE structure**
  - No need to store it in ZeroVector anymore
- **A new bit reserved in FFS file header**
  - This allows for new file alignments and supports hardware designs where the firmware storage must be at specific alignment
- **MM Handler State Notification Protocol**
  - New protocol that is used to register a callback for each call of MmiHandler(Un)Register() and supports use of the MM infrastructure on Arm TrustZone
- **RISC-V Processor Family**
  - Adds support for RISC-V architecture for PEI and grows the list of supported CPU bindings in the UEFI specification
- **SPI Bus Overview**
  - Allows for a standardized way to access SPI NOR attached flash for accessing SPI sensors and devices

SCT Updates

- UEFI SCT v2.6A Final and UEFI SCT v2.7 Alpha
  - https://github.com/UEFI/UEFI-SCT/tree/master/Binaries/2017TaipeiPlugfest
  - Direct link for the UEFISCT.zip is here: https://github.com/UEFI/UEFI-SCT/raw/master/Binaries/2017TaipeiPlugfest/UEFISCT.zip
  - Direct link for the IHVSCT.zip is here: https://github.com/UEFI/UEFI-SCT/raw/master/Binaries/2017TaipeiPlugfest/IHVSCT.zip
- UEFI Board is considering UEFI SCT development model change
- FWTS 17.09.00 latest release for ACPI testing available at:
  - Tar: http://fwts.ubuntu.com/release/fwts-V17.09.00.tar.gz
  - PPA: https://launchpad.net/~firmware-testing-team/+archive/ubuntu/ppa-fwts-stable
  - Release notes: https://wiki.ubuntu.com/FirmwareTestSuite/ReleaseNotes/17.09.00

Upcoming 2017/2018

- Non-volatile memory across specifications
- Broad architecture support continues
- Roadmap – incorporate updates as needed by the industry. Short term holding pattern for implementations to reach full potential.

Summary

Summary

- The UEFI Specification provides interfaces and mechanisms to allow for support of new technologies and improved development
- The UEFI Specification supports a more secure system, a faster boot time, improved performance, and platform feature innovation
- The UEFI Specification increases efficiency by allowing developers to reuse code and allows for extensibility, modularity and easy prototyping during development


Save the Date!
Spring 2018 UEFI Plugfest
Embassy Suites by Hilton Seattle Bellevue
3225 158th Ave SE, Bellevue, WA 98008
March 26-30, 2018
Additional details will be made available on the UEFI Forum website at:
www.uefi.org/events/upcoming

Questions?

Thanks for attending the Fall 2017 UEFI Plugfest

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

presented by

The UEFI Forum