Fall 2017 UEFI Plugfest 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**	UEFI Boot Flow to OS Selection on ARM-Based SoCs **NXP**	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		Introduction to the Self-Certification Test (SCT) in UEFI World **Canonical/Intel**	Testing Session	Testing Session	
16:30-17:00		Testing Session			
17:00-17:30					
17:30-18:00					
18:00-18:30					
18:30-19:00		Social Dinner Event (18:30)			

Session Abstracts

“Last Mile” Barriers to Removing Legacy BIOS (Intel)

Date/Time: 12:30-13:00 on Tuesday, October 31

Abstract: While UEFI has become a dominant standard since its introduction in 2005, many use cases still rely on compatibility with PC/AT Legacy BIOS. These legacy corner cases are a barrier to completing the transition to modern firmware standards. Intel has identified maintaining compatibility as an issue for platform security and validation costs, and plans to eliminate legacy BIOS elements in our 2020 data center platforms. This session discusses “last mile” gaps for 16-bit compatibility and identifies UEFI capabilities that the industry can promote as alternatives, including HTTPS Boot, OS Recovery, and Signed Capsule Update.

Speaker Bio: Brian Richardson is an Intel technical evangelist who has spent most of his career as a "BIOS guy" working on the firmware that quietly boots billions of computers. Brian has focused on the industry transition to the Unified Extensible Firmware Interface (UEFI) and demystifying firmware development. Brian has presented at conferences including LinuxCon, Linaro Connect, Bsides and Intel Developer Forum. When he's not blogging for the Intel Software Evangelists project, Brian works on video production, photography, and music.

UEFI Firmware - Security Concerns and Best Practices (Phoenix)

Date/Time: 13:00-13:30 on Tuesday, October 31

Abstract: Analysis of UEFI firmware security threats, including attack vectors, mitigation strategies, validation guidelines, and proposed Next Steps for developing and maintaining more secure UEFI firmware solutions.

Speaker Bio: Richard ‘Dick’ Wilkins is Principal Technology Liaison for Phoenix Technologies, a US based firmware development company, and is Associate Professor of Computer Science at Thomas College in central Maine. He is active in several international firmware and security related standards bodies (TCG, PCI-SIG, DMTF, ACPI, and others) and sits on the board of the Unified Firmware Interface Forum (UEFI). He chairs the UEFI Security Response Team. He is a leader with the IEEE at the Section level and with the Computer Society and is active in the ACM and PMI. He has over 35 years’ industry experience in roles from software engineer and technical program manager to director of engineering at companies such as Microsoft, Hewlett-Packard, Digital Equipment Corp., Amazon.com, Convex Computer, Bsquare and Overland Storage. Dr. Wilkins holds a Ph.D. in Computer Science from Nova Southeastern University, a Master of Science in Computer Science from the National Technological University and a Bachelor of Arts in Public Administration from Saint Thomas University.

Strategies for Stronger Software SMI Security in UEFI Firmware (Insyde)

Date/Time: 15:30-16:00 on Tuesday, October 31

Abstract: Avoid design errors and software coding pitfalls when implementing SMI handlers. Device manufacturers customize UEFI firmware using new runtime interfaces that are implemented using software SMIs. Heavy customization, tight deadlines and poor code implementation can accidentally allow malware to abuse the power of SMM. This session focuses on four common software SMI vulnerabilities and how to change your UEFI firmware and applications to avoid them.

Introduction to the Self-Certification Test (SCT) in UEFI World (Canonical and Intel)

Date/Time: 16:00-16:30 on Tuesday, October 31
Abstract: The UEFI Test Working Group (UTWG) endorses two test suites: Firmware Test Suite (FWTS) and the UEFI Self-Certification Test (SCT). FWTS is focused on validating Linux compatibility, and is endorsed by UTWG for ACPI validation. The UEFI SCT is designed to validate firmware and driver behavior per the UEFI Specification. This session demonstrates the operation of both tools, and discusses how they use open source models to improve test quality.
Speaker Bios:

- Alex Hung is a Lead Software Engineer at Canonical, Ltd, specializing in firmware architecture, ACPI, and platform subsystems in the Linux kernel. He is the maintainer of the Linux Firmware Test Suite (FWTS), and is an active member in UEFI Testing Working Group (UTWG). Alex participates in both the UEFI and Linux kernel communities, and has shared his firmware expertise at multiple industry workshops and conferences.
- Eric Jin is a staff engineer at Intel Software, specializing in firmware architecture and validation. He is an active member in UEFI Test Working Group (UTWG) and member of the UTWG developer sub-team. Eric is the maintainer of the UEFI Self-Certification Test (SCT) and has supported the UEFI community for many years.

Advances of UEFI Technologies in ARM Systems (ARM)

Date/Time: 12:30-13:00 on Wednesday, November 1
Abstract: This session will discuss the ARM-related interfaces defined in the latest UEFI and ACPI specifications, the requirements of the UEFI and ACPI interfaces for the SBBR Specification, and the use of UEFI SCT and FWTS in the SBBR compliance test. Also, discussed will be the required UEFI interfaces for the embedded space when the separation of the device and OS development is desired.
Speaker Bio: Dong Wei is currently with ARM Limited as a Senior Director-Lead Architect, Platforms. Widely recognized as a thought leader in system software, Wei has led the adoption of UEFI technologies both as an individual contributor and as Chief Executive of the UEFI Forum. His efforts have helped extend UEFI technologies from servers to PCs, storage and networking devices, printers and scanners. Thousands of firmware engineers now use UEFI as the lingua franca of modern firmware development.

UEFI Boot Flow to OS Selection on ARM-Based SoCs (NXP)

Date/Time: 13:00-13:30 on Wednesday, November 1
Abstract: In embedded systems, there are many development boards containing multiple OS images (where OS images are stored on removable media (USB/SD etc)), making it difficult to select appropriate OS image. This session demystifies generalized methods to selecting appropriate OS images using UEFI services. Additionally, it will highlight major data structures, function prototypes, arguments passed between different phases (PEI, DXE, BDS, etc.) and important Pcds (Platform configuration database) to be initialized with specific information on ARM-based SoCs.
Speaker Bios:

- Meenakshi Aggarwal is a Software Engineer in NXP and responsible for porting different IPs on layerscape SoCs.
- Wasim Khan is a Software Engineer and has been working with NXP since 2013. His focus is on UEFI bootloader for NXP SoCs.
- Vabhav Sharma is a Software Engineer with UEFI platform experience, leading a team at NXP and is responsible for UEFI porting on different layerscape SoCs.

Firmware Test Suite Introduction: Uses, Development, Contribution and GPL (Canonical)

Date/Time: 15:30-16:00 on Wednesday, November 1

Abstract: Firmware Test Suite (FWTS) is the recommended ACPI 6.1 Self-Certification Test (SCT). This command line tool is easy to use and provides explanatory and informative. Its open-source nature allows developers to add new tests easily, and many code examples such as ACPI, UEFI and SMBIOS are available for references. Code contribution are appreciated and technical discussion and code reviews on the mailing list are answered by an active community. As licensed by GPL, FWTS ensures it is available and suitable to everyone who wants to use it publicly and privately.

Speaker Bio: Alex Hung is a Lead Software Engineer at Canonical, Ltd, specializing in BIOS architecture and ACPI & platform subsystems in Linux kernel. Hung is also a maintainer of firmware test suite (FWTS), and is an active member in UEFI Testing Working Group (UTWG). He participates in both UEFI and Linux kernel communities and has shared his expertise in BIOS and firmware test suite at several industry workshops and conferences.

NFC and UEFI (AMI)

Date/Time: 12:30-13:00 on Thursday, November 2

Abstract: NFC is a technology that has permeated many aspects of everyday life. Using NFC, you can now pay with your phone or enter secure building areas. However, the UEFI specification lacks any implementation of NFC. AMI will cover a proposed solution for NFC implementation in UEFI, how to best fit NFC into the UEFI specification, and potential use cases.

Speaker Bio: Tony Lo is the Senior Manager of TDI Department at American Megatrends Inc. He has 20+ years of experience in UEFI/BIOS development. He is a technical lead/architect with team management experience. Tony has a passion for various firmware architectures and new technology.

Edk2 Platforms Overview (Linaro)

Date/Time: 13:00-13:30 on Thursday, November 2

Abstract: For a couple of years now, the Linaro OpenPlatformPkg repository has been used to collate a number of (at least partially) open source EDK2 platform ports. However, with a now properly defined process for the TianoCore edk2-platforms and edk2-non-osi repositories, these platforms are now moving over there and OpenPlatformPkg. This session will discuss the process, the current state of things and the practicalities of working with edk2-platforms.

Speaker Bio: Leif Lindholm is employed by Arm, but full-time assigned into Linaro where he works as the tech lead of the Enterprise Group UEFI team. He is also one of three TianoCore stewards, with a special focus on open source platform code.

UEFI Manageability and REST Services (HPE and Intel)

Date/Time: 15:30-16:00 on Thursday, November 2

Abstract: With the increase in platform firmware complexity and capabilities, there is an increased need to standard firmware manageability is increasing. The UEFI 2.7 Specification defines REST services to provide secure solutions for managing modern platforms. This session describes enterprise configuration scenarios, discusses implementation gaps in the UEFI specification, and proposes enhancements related to vendor-specific REST services.

Speaker Bios:

- Ye Ting is a UEFI Firmware Architect working in Software and Services Group at Intel. She joined Intel in 2005 and focused on UEFI firmware for 12 years. She is an active member in UEFI Specification Working Group (USWG) and responsible for hosting regular meetings in UEFI Networking Sub team under USWG. She contributed IPv6 related contents to UEFI specification v2.2 and HTTP(S) boot, DNS, WIFI etc. to later updates in UEFI specification. She has a master degree and bachelor degree both from Huazhong University of Science & Technology in Wuhan.
- Abner Chang is the master technologist at Hewlett Packard Enterprise Taipei Design Center. He joined HPE at 2013, with over 17 years of system firmware experience including 14 years at Phoenix Technologies as a software architect. Abner has experience with UEFI, EDK II, and UEFI HII related protocols. Abner has contributed multiple UEFI protocols (HII Image Decoder, HII Font Glyph Generator, HII Image Ex, HII Font EX) and contributes to the UEFI/PI RISC-V processor architecture binding.