Spring 2019 UEFI Forum Plugfest
Session Abstracts and Schedule

Company	Session Title & Abstract	Presenter	Date/Time
UEFI Forum	Welcome: State of UEFI	-Dong Wei, UEFI Forum Vice President	Tue 4/9 9:00 – 9:30 a.m.
Arm, Intel Corporation, Canonical Group Ltd.	**Title:** UEFI Self Certification Tests (UEFI-SCT) and Firmware Test Suite (FWTS) **Abstract:** In the past, UEFI-SCT existed in a private GitHub repository and source code access was restricted. UEFI-SCT binaries/tools could only be obtained by adopting the UEFI Adopter Membership Agreement. This session discusses behind the scenes initiatives that took place in the last year to make UEFI-SCT open source and encourages contributions from open source enthusiasts, supporters, UEFI forum partners etc. It also presents new contribution guidelines on how to contribute to UEFI-SCT and requests contributions with a humble thank you. Firmware Test Suite (FWTS) is the recommended ACPI SCT. It is licensed by GPL which ensures it is free to use, modify and redistribute. Contributing to FWTS is easy, and it is always welcomed and appreciated. FWTS-LIVE also receives a major update - it is now based on latest Ubuntu 18.04. Finally, FWTS-LIVE's build scripts are open source for everybody who wants customization.	-Supreeth Venkatesh, Arm -Harry Hsiung, Intel Corporation -Alex Hung, Canonical Group Ltd.	Tue 4/9 9:30 – 10:00 a.m.
Arm	**Title**: UEFI Updates and Open Source Firmware evolutions on Arm **Abstract**: The session will present the latest updates on UEFI Requirements for Arm and the latest news on Arm specifications. It will then discuss the latest evolutions in Open Source Firmware to handle the increasingly complex challenges arose in the Secure world software space by many different UEFI-based ecosystems, including the new Edge and Networking market segments.	- Matteo Carlini - Dong Wei	Tue 4/9 10:00 – 10:30 a.m.
Phoenix	**Title**: Risks to UEFI firmware due to growing attack surfaces **Abstract**: The addition of networking stacks and services, the necessity for "automatic" firmware updates and other feature enhancements are presenting new attack surfaces in UEFI based firmware for bad actors to probe and for defenders to protect. We will provide some examples of dangerous and poorly implemented features and make proposals for actions the UEFI community should consider.	- Dick Wilkins	Tue 4/9 10:30—11:00 a.m.

Spring 2019 UEFI Plugfest – Session Details and Schedule – Subject to Change

Intel Corporation Session	**Title:** From Runtime to Compile Time: Improving ASL Through Enhanced Namespace Resolution **Abstract**: The ACPI Source Language (ASL) was designed for firmware to describe platform-specific details to operating systems. This language is compiled to ACPI Machine Language (AML) bytecode which is interpreted in the OS kernel-space. Like other languages executed on a bytecode interpreter, AML has the possibility of incurring runtime errors due to programming mistakes. This session describes a class of runtime errors that are commonly found on deployed products, and a new Intel ASL compiler feature designed to eliminate these issues.	- Erik Schmauss	Tue 4/9 11:00—11:30 a.m.
Microsoft	**Title**: Microsoft UEFI Updates for 2019 **Abstract:**	- Jeremiah Cox	Tue 4/9 11:30 a.m.— 12:00 p.m.
Intel Corporation	**Title**: Hardening Firmware Components with Host-based Analysis **Abstract**: Platform firmware is a critical element for root-of-trust. Attackers are increasingly targeting firmware to deploy persistent attacks, often based on issues not detected through traditional platform validation and integration testing. Software validation methods like fuzz testing, static analysis, and fault injection are typically difficult to apply to firmware. Integration testing, the most common method of firmware validation, makes it difficult to isolate errors and identify faulty modules. This session describes host-based analysis, a new method developed by Intel to isolate firmware components and check for common software issues prior to integration with platform firmware. Host-based Firmware Analyzer (HBFA) is an open source project designed to harden firmware modules using best-in-class software validation tools. HBFA will be contributed to TianoCore, the open source community for UEFI development. This is a tool for firmware component analysis with a focus on fuzzing and symbolic testing of firmware components. Host-based methods isolate firmware components in the developer's OS environment and leverages existing open source analysis tools (ex: AFL, Peach, KLEE). This session provides an overview of tool and how it is used to improve efficiency of firmware security unit test cases.	-Brian Richardson	Tue 4/9 12:30—1:00 p.m.

NXP	SESSION CANCELED DUE TO TRAVEL ISSUES		Wed 4/10 11:00—11:30 a.m.
Intel Corporation	**Title**: Improving UEFI Network Stack Performance **Abstract:** Network booting is an important pre-OS feature. Technologies like PXE and iSCSI Network Boot, defined almost two decades ago, are still being widely used on legacy BIOS and UEFI server platforms. However, pre-OS networking typically falls short of OS-based network performance, mostly due to background events. This session is a proposal for improving UEFI network stack performance, based on a proof-of-concept for performance-oriented design utilizing multiprocessing mechanisms (UEFI MP Services Protocol) and a lightweight TCP/IP stack (lwIP). The presentation includes results achieved in comparison to existing network boot implementations.	- Maciej Rabeda -Vincent Zimmer	Wed 4/10 11:30 a.m.— 12:00 p.m.
Intel Corporation	**Title**: Case Study: Removing SMM from Intel Platforms **Abstract**: The broadcast System Management Mode (SMM) model has been used for many years to manage priority system events but has a number of disadvantages. Overuse of System Management Interrupts (SMI) results in performance degradation, increases latency with higher core counts, and introduces potential race conditions. SMM is also difficult to debug and has access to system resources outside of the OS environment, which makes it target for firmware exploits. This session expands on Intel's initiative to reduce SMM footprint and provide alternatives for handling runtime platform events. Intel described SMI reduction methods based on Protected Runtime Mechanism (PRM), UEFI Capsule, and the Baseboard Management Controller (BMC) at the 2018 OCP Regional Summit. The presentation features a case study and demonstration using Intel® Xeon® Scalable Processors with EDK II firmware.	- Sarathy Jayakumar	Wed 4/10 12:30—1:00 p.m.
NXP	CANCELED DUE TO TRAVEL ISSUES - BREAK		Wed 4/10 1:00—1:30 p.m.
Intel Corporation	**Title**: Role Modeling Open Source Best Practices in Firmware **Abstract**: Since 2004, the TianoCore community has been a model for open source firmware implementations of UEFI. Today, we continue to grow our community by improving our infrastructure and aligning with current open source best practices. As our project matures, we	-Mark Doran -Stephano Cetola	Wed 4/10 1:30—2:00 p.m.

	have worked to improve our licensing to be less restrictive, allowing more contributions from more organizations. This session presents changes being made to TianoCore based on community feedback. These efforts come with a unique set of challenges, as partners demand open source further down the stack. Customer needs often do not line up directly with community expectations, so finding a common ground can require creative problem solving. We have leveraged feedback through monthly community meetings and opened our design process up to involve the community early in the development cycle. The innovation and perspective gained is well worth the effort to show how open is the new normal, even in firmware.		
American Megatrends Inc.	**Title**: Using Capsules for Firmware Configuration Update **Abstract**: Capsules have been used by UEFI for updating of device firmware for several years. UEFI 2.8 has introduced a new feature where the firmware exposes HII configuration information to the operating system. The operating system or additional tools can in turn provide a capsule back to the firmware for updating of HII configuration settings. This presentation will be an overview of this new feature in UEFI 2.8 and explores real world use cases.	- Zachary Bobroff	Wed 4/10 2:00—2:30 p.m.
Flex Institute of Technology	**Title:** UEFI topics for the manufacturing efficiency **Abstract:** After passing the design phase of a new equipment other challenges arise, when thousands of devices start to be manufactured, with the target to deliver to the users' equipment that work as expected. At this presentation, the manufacturing point of view will be presented to the UEFI community, presenting situations related to the BIOS, showing real scenarios that could be improved by the BIOS teams and ideas that would make the manufacturing process more efficient.	- Rafael Machado	Thurs 4/11 12:30—1:00 p.m.
Linaro	**Title**: How Writing Portable UEFI Drivers Improves Reliability (and Helps Me) **Abstract**: UEFI provides all the interfaces needed to write software portable between different architectures. However, many current executables have only been validated on a single platform. Through a joint effort between SuSe and Linaro, we emulatedX64 option ROMs on ARM systems which let us find some common mistakes you need to avoid when writing drivers to run on ARM... or work through more than accident elsewhere. This talk gives a summary of common mistakes, how to avoid them, and other things that would make my life easier.	- Ard Biesheuvel - Leif Lindholm	Thurs 4/11 1:00—1:30 p.m.

HPE	**Title:** Redfish Implementation for UEFI **Abstract:** The DMTF Redfish specification defines a management standard for scalable enterprise systems with one the goals being to improve interoperability. However, the BIOS attribute registry and BIOS schemas were not standardized by the DMTF. Instead, it was left for the support of BIOS settings to be implementation specific. Hence, all BIOS attributes across the various IBV implementations are unique and heterogenous. HPE would like to present implementation guidance for UEFI vendors so that the construction of the Redfish BIOS resource is interoperable across the datacenter. The guidance requires updates to the DMTF schemas and UEFI specification to promote a common translation of HII formsets to Redfish attribute registries.	-Jason Spottswood	Thurs 4/11 1:30—2:00 p.m.
Intel Corporation and Lenovo Corporation	**Title**: Redfish Host Interface: UEFI and OS implications **Abstract**: Learn about the DMTF Redfish Host Interface and its relationship to UEFI, BMC firmware, and Operating Systems. See a demo of the latest OS support for this industry standard interface for in-band access to the Redfish REST API. Discuss use-cases for system management, as well as challenges and next steps in ecosystem enablement.	- Samer El Haj Mahmoud, Lenovo Corporation -John Leung, Intel Corporation -Mike Rothman, Intel Corporation	Thurs 4/11 2:00—2:30 p.m.