Fall 2018 UEFI Plugfest – Session Details and Schedule – Subject to Change

Company	Session Title & Abstract	Presenter	Suggested Date/Time
UEFI Forum	**Welcome: State of UEFI Forum**	-Mark Doran, UEFI Forum President	Tue 10/16 9:00 – 10:00
Phoenix Session 1	**Title**: Increasing 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.	-Glenn Plant	Tue 10/16 9:30 – 10:00
ARM Session 2	**Title**: UEFI updates and Secure Software Isolation on Arm **Abstract**: The session will discuss the latest updates on UEFI Requirements into the new versions of SBBR & EBBR (for the Embedded world) Arm specifications. It will also present the challenges faced in the increasingly complex Secure world software ecosystem and the enhancements proposed to introduce isolation and virtualization to the existing Secure world Software architecture from both a specification and open source Firmware perspective.	-Matteo Carlini -Dong Wei	Tue 10/16 10:00 – 10:30
Insyde Software Session 3	**Title**: UEFI and the SDL – Security Development Lifecycle **Abstract**: In this session, we examine how the Security Development Lifecycle can be applied to the unique requirements of UEFI firmware to identify and minimize security and privacy risks.	-Trevor Western	Tue 10/16 11:00 – 11:30
AMI Session 4	**Title**: Advanced TPM Usage	-HPBird Chen	Tue 10/16 11:30 – 12:00

As of: August 31, 2018

	Abstract: Trusted Platform Modules (TPMs) have been an integral part of platform security for more than ten years. TPMs have evolved through the years and gone through several technology updates. However, many security-based capabilities of a TPM may have been overlooked from a firmware perspective. This presentation covers TPM usage from a generic standpoint for firmware and new applications of TPMs today including TPM usage on different architectures (x86 and ARM), innovative solutions based on TPM usage, and updates on industry requirements.		
Canonical Session 5	**Title**: Building Customized Tests with Firmware Test Suite **Abstract:** Firmware Test Suite (FWTS) is an open-source test suite licensed by GPL which ensures everyone is free to use, modify and redistribute FWTS. This command line tool is not only easy to use but also simple to customize for different requirements. FWTS comprises a large set of tests that can be selected to develop test scripts for various projects. FWTS's extensible framework enables developers to add new tests or to reuse existing code straightforwardly. Additionally, customized FWTS can be distributed and updated easily when it is built on Launchpad Personal Package Archives (PPA).	-Alex Hung	Wed 10/17 12:30 – 13:00
Intel Session 6	**Title:** System and Device Firmware Updates using Unified Extensible Firmware Interface (UEFI) Capsules **Abstract**: Firmware is responsible for low-level platform initialization, establishing root-of-trust, and loading the operating system. Signed UEFI Capsules define an OS-agnostic process for verified firmware updates, utilizing the root-of-trust created by firmware. The open source FmpDevicePkg in TianoCore provides a simple method to update system firmware images and device firmware images using UEFI Capsules and the Firmware Management Protocol (FMP). This session describes the TianoCore capsule implementation, implementing FMP using FmpDevicePkg, creating Signed UEFI	-TBD	Wed 10/17 13:00 – 13:30

	Capsules using open source tools, and an update workflow based on the Linux* Vendor Firmware Service (fwupd.org).		
NXP Session 7	**Title**: Capsule update with MM mode **Abstract:** UEFI defines the capsule update feature in a very descriptive way, but the implementation of the actual upgrade part is left on the developer. To update the firmware, some architectures follow the two-reset procedure. The first step is to start the upgrade process and, the second is to use the newly flashed image. With the help of MM mode, this update can be done in the same cycle. This will save time to upgrade firmware. In addition, using MM mode, which runs on the secure side of the machine, will take care of security vulnerability. In this talk, we will speak, how to do a firmware upgrade in one reset cycle using MM mode.	-Udit Kumar -Varun Sethi -Meenakshi Aggarwal	Wed 10/17 13:30 – 14:00
Linaro Session 8	**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 last year, we emulated X64 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 prevent them, and other things that would make my life easier.	-Leif Lindholm	Wed 10/17 14:30 – 15:00
Intel Session 7	**Title**: TianoCore Updates: Tags, Testing & Platforms **Abstract:** TianoCore is an open source firmware community supported by several members of the Unified Extensible Firmware Interface (UEFI) Forum. This presentation provides an update on	-TBD	Wed 10/17 15:00 – 15:30

	three significant projects related to EFI Development Kit II (EDK II), an open source implementation of UEFI. • Stable Tags: The first "stable tag" release was added to EDK II in August 2018. These tags are on a three-month cadence, with the goal of integrating major features at the beginning of each release cycle. This presentation discusses the stable tag workflow, and how the community can participate in the process. • Sample Platforms: TianoCore has migrated hardware platform support to the edk2-platforms tree, providing a repository for stable projects and firmware under development. This session provides an overview of available platforms and steps for adding new platform projects. • MicroPython* Test Framework for UEFI: In August 2018, a MicroPython engine for UEFI and related test framework were released for community evaluation. Memory and size optimizations make MicroPython ideal for pre-OS applications. This session provides an overview of the project's status and long-term goals.		