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

Company	Session Title & Abstract	Presenter	Suggested Date/Time
Intel Session 1	**Title**: An Introduction to Platform Security **Abstract**: Researchers from Intel's Platform Armoring and Resiliency team will speak about the hardware and firmware interfaces available on Intel platforms, including UEFI firmware. This session will describe the capabilities of modern systems at a firmware and hardware level as well as various security features.	-Brent Holtsclaw -John Loucaides	Tue 3/27 12:00 – 12:30pm
Phoenix Session 2	**Title**: Firmware Security: Hot Topics to Watch **Abstract**: This presentation will cover major topics in firmware security. Highlights include UEFI and Internet of Things (IoT), security and UEFI Development Kit (UDK) 2018 and happenings in NIST Guidelines.	-Dick Wilkins	Tue 3/27 12:30 – 1:00pm
Arm Session 3	**Title**: UEFI Updates, Secure Firmware and Secure Services on Arm **Abstract**: The session will cover the latest updates on UEFI Requirements (for Secure Boot and Secure Firmware Update) into the Arm Server Based Boot Requirements (SBBR) specification. The session will also present the enhancements done to open source Firmware projects (Trusted Firmware and EDK2) to enable UEFI Secure Boot and Secure Services on Arm platforms, together with future evolutions.	-Matteo Carlini -Dong Wei	Tue 3/27 1:00 – 1:30pm
Intel Session 4	**Title**: The State of ACPI Source Language (ASL) Programming **Abstract**: Advanced Configuration and Power Interface (ACPI) is a firmware interface for operating system power management subsystems. ACPI firmware is written in a language called ACPI Source Language (ASL for short). This session provides an overview of challenges that ASL programmers face and how these difficulties impact those working in platform enabling as well as end users. Towards the end of the session, a few proposed	-Erik Schmauss	Tue 3/27 1:30-2:00pm

	solutions to improve the current state of ASL programming are discussed.		
Intel Session 5	**Title**: Implementing MicroPython as a UEFI Test Framework **Abstract:** Python is a popular high-level interpreted language, common in automated testing environments. EDK II includes a CPython implementation for UEFI, but has limited functionality and is not compliant with current Python standards. This session describes porting MicroPython to UEFI. MicroPython is a Python 3 variant designed for microcontrollers. Memory and size optimizations make MicroPython ideal for pre-OS applications. This presentation describes implementation details, performance metrics, and plans for a test framework based on the MicroPython engine for UEFI.	-Chris McFarland	Wed 3/28 12:00-12:30pm
Insyde Software Session 6	**Title:** UEFI and the Security Development Lifecycle **Abstract**: This session will examine how the Security Development Lifecycle can be applied to the unique requirements of UEFI firmware to identify and minimize security and privacy risks.	-Tim Lewis	Wed 3/28 12:30 – 1:00pm
Intel Session 7	**Title**: Attacking and Defending the Platform **Abstract:** Researchers from Intel's Platform Armoring and Resiliency team describe various firmware threat models and classes of attack. Using proof-of-concept demonstrations, this session provides real-world examples of attack classes and effective mitigation techniques. Topics include using the open source CHIPSEC framework for platform security assessment, as well as applying firmware and/or hardware features to strengthen platform resiliency.	-Erik Bjorge -Maggie Jauregui	Wed 3/28 1:00 – 1:30pm

Microsoft Session 8	**Title**: Microsoft Security Features and Firmware Configurations **Abstract**: This session will highlight Microsoft security features depending on and relating to firmware including Baby Duck, UEFI CA, Windows 10S relating to firmware updates, Virtualization-based Security (VBS) and Hypervisor-Enforced Code Integrity (HVCI) and the specific impact on firmware implementations on consumer platforms. The Hardware Security Test Interface (HSTI) 1.1.a (current), the future version, HSTI 2.0 and its ability to provide best effort assurance that the machine customers have purchased is secure by default.	-Scott Anderson -Anthony Chuang -Jeremiah Cox -Michael Anderson	Wed 3/28 1:30 – 2:00pm
Arm Session 9	**Title**: Dynamic Tables Framework: A Step Towards Automatic Generation of Advanced Configuration and Power Interface (ACPI) & System Management BIOS (SMBIOS) Tables **Abstract:** The dynamic tables framework provides a technique for generating firmware tables based on the hardware description. The hardware description can, potentially be derived from system on a chip (SoC) integration tools. The framework table generators also ensure compliance with specifications (e.g. Server Base Boot Requirements). This presentation will discuss how the dynamic tables framework can be used to generate firmware tables at run-time to describe configurable hardware and other use cases like consolidating firmware builds to a single firmware binary for a base platform. Additionally, this session will cover some of the ongoing work at Arm to implement this feature.	-Sami Mujawar	Thu 12:00-12:30pm
Microsoft Session 10	**Title**: Microsoft Sample Code on GitHub and Walkthrough on Firmware Updates to Windows Update (WU) **Abstract**: Highlight of materials that Microsoft has shared on GitHub for UEFI Firmware Updates (UpdateCapsule) to include information on uploading updates to WU.	-Sean Brogan -Bret Barkelew	Thu 3/29 12:30 – 1:00pm

Linaro Session 11	**Title**: Embedded Development Kit 2 (Edk2): Platforms Overview **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.	-Leif Lindolm	Thu 3/29 1:00 – 1:30pm
AMI Session 12	**Title**: Enabling Advanced NVMe Features Through UEFI **Abstract:** NVMe has become a widely adopted technology in the computer industry. While the UEFI specification has enabled generic support for NVMe based drives, there are still many features of NVMe that are not covered in the specification. The UEFI specification provides the building blocks for providing additional NVMe related features including controller firmware update, block SID, multiple namespaces, pyrite and SAT3 password. By providing support for these additional features, end users are given a solution that allows them to use their systems more effectively.	-Zach Bobroff	Thu 3/29 1:30 – 2:00pm