UEFI Fall 2023 Developers Conference & Plugfest Presentations Overview

October 9 – 12
Embassy Suites by Hilton Portland in Hillsboro, Oregon

The full agenda is available on the UEFI Forum website. Presentations are subject to update/change.

- **Vulnerability Management in the UEFI Firmware Supply Chain**
  - Presenter: Brian Mullen, AMI
  - The UEFI firmware supply chain plays a pivotal role in modern computing, yet vulnerabilities within it can have far-reaching consequences. This presentation examines the impact of vulnerabilities at different supply chain stages on a widening network of vendors. It also analyzes recent trends in UEFI vulnerability research and identifies persistent threat categories. The session provides a detailed overview of UEFI attack surfaces and explores challenges in remediating open-source component vulnerabilities. Drawing from experiences with the Tianocore EDK2 project, it discusses real-world obstacles and complexities. Central to the presentation is a discussion of strategies for UEFI supply chain vendors to proactively eliminate vulnerabilities. Special focus is placed on employing tools and automation in pre and post-release phases.
- **Key Management with TPM in UEFI Environment**
  - Presenters: Felix Polyudov and Frederick Otumfuor, AMI
  - The UEFI environment is a critical component of the modern computing platform. Key management is essential for securing the UEFI environment, as it allows for the secure storage and use of cryptographic keys. This session covers key management in the UEFI environment and provides an overview of different use cases and abstractions provided by the UEFI spec. We'll also explore implementation options and their strengths and weaknesses and present an in-depth view of the TPM-based Key Management Service. This session is for technical audiences interested in learning more.
- **UEFI and ACPI in Arm System Architecture**
  - Presenter: Dong Wei, Arm
  - This session provides a comprehensive update on how UEFI and ACPI technologies are used in the Arm System Architecture from servers to edge and IoT devices. Arm standardizes on three major recipes for system firmware: 1) Standard Base Boot Requirements using UEFI, ACPI and SMBIOS interfaces to support the generic off-the-shelf operating systems with backward/forward portability when combined with Arm Base System Architecture hardware requirements; 2) Embedded Based Boot requirements using a reduced set of UEFI and Devicetree interfaces to support embedded Linux operating systems with standard UEFI interfaces for secure boot and OTA; 3) LinuxBoot Base Boot Requirements using ACPI, SMBIOS and a minimum set of UEFI runtime services to support some cloud provider's Linux distros. Sample implementations, such as EDK2, UBoot, Coreboot, to these recipes will be discussed.
- **A Conversation on Bolstering UEFI Cybersecurity**

    - Presenter: Dr. Jonathan Spring, Cybersecurity and Infrastructure Security Agency (CISA)
    - CISA has a broad Secure By Design and Default initiative https://www.cisa.gov/securebydesign. CISA recently published a blog post relating Secure By Design to UEFI and some opportunities for improvement (https://www.cisa.gov/news-events/news/call-action-bolster-uefi-cybersecurity-now). This session would introduce these discussions and foster a conversation with the UEFI community about sustaining and amplifying current efforts towards making UEFI and all its implementations Secure By Design and Default.
- **UEFI Goes to Washington**
    - Presenter: Presenter TBD, Insyde
    - This session will provide an overview of how UEFI is built to meet and exceed United States Executive Orders and NISA, CISA and NSA security standards. The session will explore how secure software development practices, SBOM compliance, and novel implementations of UEFI technology can be leveraged to provide secure and compliant firmware that exceeds the modern software requirements from the US government.
- **EDK2Code, VSCODE Extension for EDK2**
    - Presenter: Guillermo Antonio Palomino Sosa, Intel
    - EDK2Code extension is a Visual Studio Code extension for EDK2 developers missing IDE like features that are present for other popular development frameworks. The extension reads the compiled information or DSC files to provide full context of what has been integrated into the build process. With this information the extension provides the user new set of VSCODE commands to navigate through the source code. Some examples of commands are: Goto Library definition, Goto INF file, Goto Library implementation, etc. The Extension also provides context and syntax support for EDK2 files and ACPI files. This extension will be released as open source and will be available through VSCODE marketplace in the following weeks.
- **Multi-ISA Firmware Driver Compatibility – What's the Future?**
    - Presenter: Andrei Warkentin, Intel
    - Did you know Tiano today supports 4 64-bit architectures, yet plug-in device OpRoms are still mostly limited to x64 and CSM? While binary-translation approaches are a useful stop-gap solution for both AArch64 and RV64 ecosystems, we need a common approach that is not a technical debt nightmare and that will be adopted by IHVs and endorsed by OSVs. This talk goes over some of the possible approaches as a lead-in for an open discussion, UEFI Forum member feedback and suggestions.
- **FdtBusDxe or How to Embrace Modularity and Boot-Time Platform Device Configuration to Solve a Common Tiano Complaint**
    - Presenter: Andrei Warkentin, Intel
    - Have you ever wondered how to simplify support for minor SoC/Chipset variations or have a common firmware image for multiple boards? Have you ever wished Tiano had better interfaces for supporting complex/composite platform devices, from onboards NICs to video output devices? Do you balk at moving your platform from U-Boot to Tiano? Then this talk is for you.
- **Firmware Configuration – Past, Present and Future**

    - Presenters: Vincent Zimmer, Gahan Saraiya and Christine Chen, Intel
    - One of the most pervasive actions for firmware necessitates configuration for various boot flows without rebuilding the firmware. Configuration spans from venerable local setup screens through scripted out-of-band management, automated configuration, and provisioning. Since the early UEFI specification and its adoption of circa 2001 Intel HII with IFR and VFR, the industry has evolved in configuration practice. These evolutions include out-of-band standards like RedFish, FDT, USF YAML, FSP UPD, and UFFAF. This talk will review common classes of configuration workflows, survey of present practices, challenges, and open up the discussion to align these practices going forward.
- **Using SPDM in UEFI for Device Attestation**
    - Presenters: Jiewen Yao, Vincent Zimmer, Intel and Michael Kubacki, Microsoft
    - Security Protocol and Data Model (SPDM) is a DMTF defined industry standard for device authentication, provisioning, measurement collection, and secure communication. The UEFI specification 2.10 release describes how to perform device authentication in UEFI firmware. The TCG Platform Firmware Profile (PFP) Specification 1.06 release describes how to leverage SPDM to collect device measurements in the pre-boot phase. In this talk, we will introduce SPDM and how to apply it in EDKII firmware to support the mechanisms defined in UEFI 2.10 and TCG PFP 1.06. In addition, we will review a Microsoft Surface use case on making use of SPDM to interact with a Solid State Disk (SSD) device.
- **Hardening the Core: Runtime Configurable UEFI Memory Protections**
    - Presenter: Taylor Beebe, Microsoft
    - Taylor from the Microsoft Core UEFI team will talk about all things UEFI memory protections including recent design updates to make them runtime configurable and increase security posture. He'll discuss changes made to the Windows boot loader to support memory protection, tests which have been created to check the integrity of UEFI memory, and problems still yet to be solved on the road to more secure firmware.
- **UEFI Ecosystem Investments and Open-Source Contributions**
    - Presenter: Michael Kubacki, Microsoft
    - Join Michael from Microsoft's Core UEFI team for a comprehensive overview of the team's recent endeavors within the UEFI ecosystem. A wide range of topics will be covered, from firmware security best practices to open-source firmware features and test tools. Along the way, Michael will highlight contributions made to the UEFI Forum and our future plans. Finally, you'll see how all the pieces connect and can be demonstrated in an open-source virtual platform.
- **Evolving the Secure Boot Ecosystem**
    - Presenters: Jeffrey Sutherland and Doug Flick, Microsoft
    - In this talk, we delve into pivotal areas shaping the future of secure boot processes and UEFI CA signing. Our exploration begins with a comprehensive overview of Secure Boot Certificate rolling, encompassing key essentials, current progress updates, and the persistent challenges encountered. Additionally, we dissect the impending shifts in Microsoft's requirements for UEFI CA signing, unraveling the emerging prerequisites and their implications. Furthermore, we reveal Microsoft's feature plans for Secure Boot, shedding light on how these

advancements bolster system security. Join us to navigate the evolving landscape of system security and compliance.

- **Extending EDK2 Functionalities to GNU-EFI**
  - Presenter: Mikolaj Lisik, Google
  - GNU-EFI is an alternate development environment made for creating EDK2 with the gnu gcc compiler. GNU-EFI applications have access to the official EDK2 API (Boot and Runtime Services), however they can't link native EDK2 code. This creates an issue when attempting to use functions that are not a part of the API. The presentation will go through an explanation of how GNU-EFI handles edk2 API calls as well as how to extend it to port internal EDK2 functionality into it when needed, by the example of SEV-SNP page state change functions.
- **Creating an EDK2 with a ROM Embedded EDK2 Application**
  - Presenter: Mikolaj Lisik, Google
  - AMD SEV-SNP (Secure Encrypted Virtualization, Secure Nested Paging) adds a functionality of measuring the OVMF by the AMD-PSP (Platform Secure Processor), but not the further boot stages. This created the opportunity of creating a fully measured computational environment as long as it can be fully contained inside the ROM and run by UEFI upon startup. The presentation will focus on creating a specialized EDK2 build that will allow making that happen. The solution is not tied to a specific application and fully supports GNU-EFI applications as workloads as well.
- **Call for Collaborative Action: CVSS V4.0 and Firmware Vulnerability Scoring**
  - Presenter: Dick Wilkins, Phoenix
  - This talk will discuss the new, about to be released, CVSS V4.0 scoring system and how it has changed. Also, other developments in the scoring of software vulnerabilities. We will make a call to action for those involved in the platform/system firmware supply chain to coordinate our vulnerability scoring methodologies to insure consistent scores within our scope.