presented by

The UEFI Forum

Fall 2023 UEFI Developers Conference and Plugfest

October 9 – 12, 2023

Hillsboro, Oregon

presented by

The UEFI Forum

State of the UEFI

Presented by Mark Doran

UEFI Forum President

Fall 2023 UEFI Developers Conference and Plugfest

Introduction

Mark Doran, UEFI Forum President

Mark Doran is President of the UEFI Forum and an Intel Fellow. Mark graduated from University College London, University of London. He joined the UEFI Forum in 2009.

Agenda

- Event Overview
- The UEFI Forum
- Specification Update
- UEFI Security & Open Source
- Fall 2019 UEFI Plugfest
- Questions

Event Overview

Made Possible by our Sponsors…

Why the Shift to DevCon?

- UEFI Forum has shifted to focus on a Developers Conference format with testing as an option for interested companies
- Given the interest from the membership on education, we believe that this shift will best serve the UEFI Forum membership

Tuesday, October 10

Fall 2023 DevCon Session Highlights

Time	Session Title	Presenters
1:00 – 1:30 pm	UEFI Ecosystem Investments and Open-Source Contributions	Michael Kubacki (Microsoft)
1:30 – 2:30 pm	Using SPDM in UEFI for Device Attestation	Vincent Zimmer (Intel) and Michael Kubacki (Microsoft)
2:30 – 3:30 pm	Evolving the Secure Boot Ecosystem	Jeffrey Sutherland and Doug Flick (Microsoft)
3:30 – 4:00 pm	Hardening the Core: Enhanced Memory Protection	Taylor Beebe (Microsoft)

Testing from 2:30 – 6:00 pm

Wednesday, October 11

Fall 2023 DevCon Session Highlights

Time	Session Title	Presenters
10:00 – 10:30 am	Conversation on Bolstering UEFI Cybersecurity	Dr. Jonathan Spring (CISA)
10:30 – 11:30 am	UEFI Goes to Washington	Tim Lewis (Insyde)
11:30 am – 12:00 pm	Call for Collaborative Action: CVSS V4.0 and Firmware Vulnerability Scoring	Dick Wilkins (Phoenix)
12:00 – 1:00 pm	Lunch	
1:00 – 2:00 pm	Vulnerability Management in the UEFI Firmware Supply Chain	Brian Mullen (AMI)
2:00 – 2:30 pm	UEFI and ACPI in Arm System Architecture	Dong Wei (Arm)
2:30 – 3:30 pm	FdtBusDxe or How to Embrace Modularity and Boot-Time Platform Device Configuration to Solve a Common Tiano Complaint	Andrei Warkentin (Intel)
3:30 – 4:00 pm	UEFI and ACPI in Arm System Architecture	Felix Polyudov and Frederick Otumfuor (AMI)

Testing from 9:30 am – 3:30 pm

The Evening Event: KingPins

Wednesday, October 11 from 6:00 - 9:00 pm

KingPins Beaverton
Lincoln Square (third floor)
2725 SW Cedar Hills Blvd.
Beaverton, OR

Food: Mexican Grill Buffet

Beverages: Sodas, coffee, tea. Attendees will receive two drink tickets for alcoholic beverages.

Activities: Bowling, arcade and laser tag.

Sponsored by

arm

Thursday, October 12

Fall 2023 DevCon Session Highlights

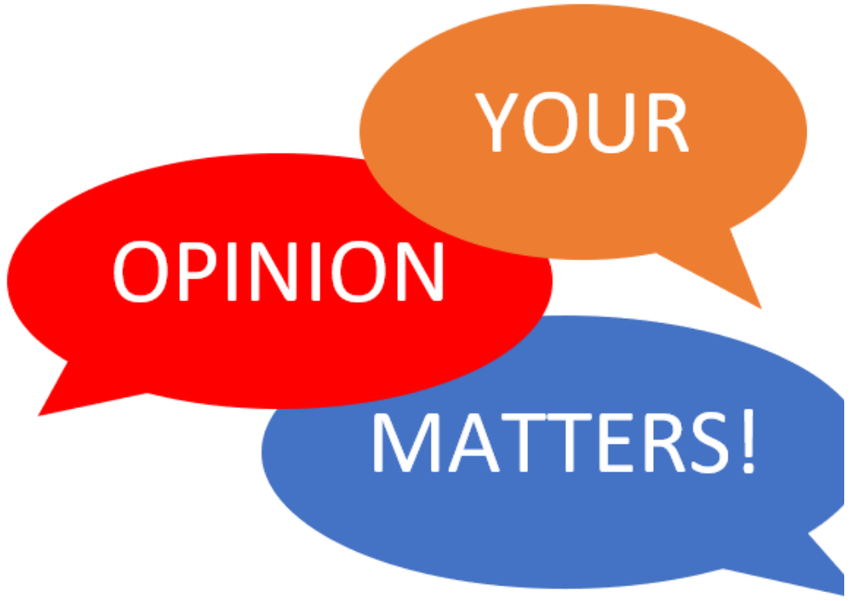
Time	Session Title	Presenters
10:00 – 11:00 am	Multi-ISA Firmware Driver Compatibility – what's the future?	Andrei Warkentin (Intel)
11:00 – 11:30 am	Extending EDK2 Functionalities to GNU-EFI	Mikolaj Lisik (Google)
11:30 am – 12:00 pm	Creating an EDK2 with a ROM Embedded EDK2 Application	Mikolaj Lisik (Google)
12:00 – 1:00 pm	Lunch	
1:00 – 1:30 pm	Firmware Configuration – Past, Present and Future	Vincent Zimmer (Intel)

Testing from 9:00 am – 4:00 pm

Speaker's Office Hours

Meet and network with the presenters after their sessions and ask your **questions**

- **Where:** The Ballroom
- **When:**
  - 4:00 – 5:00 pm on Tuesday, Oct. 10
  - 4:00 – 5:00 pm on Wednesday, Oct. 11
  - 1:30 – 2:30 on Thursday, Oct. 12

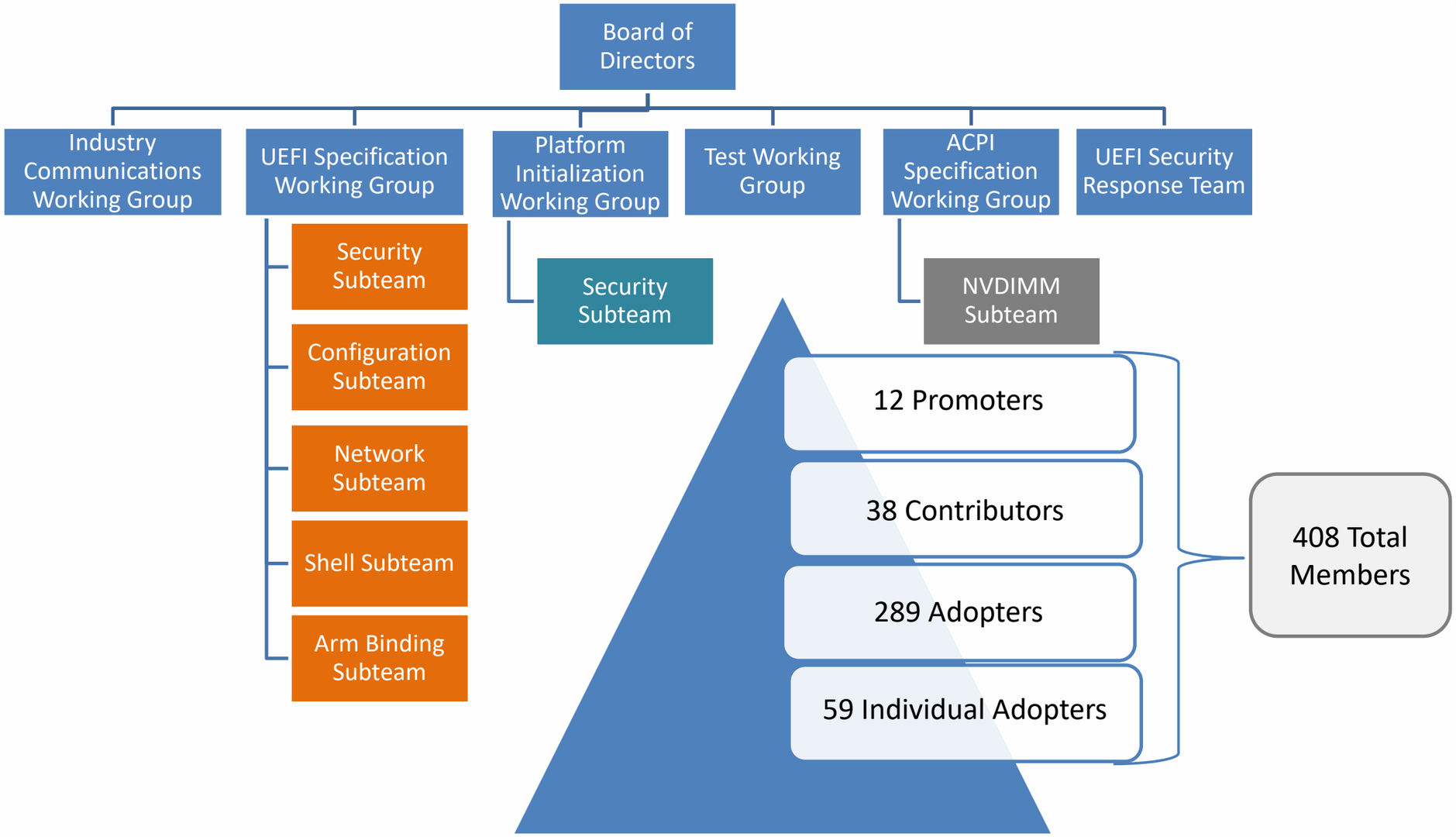


Event Survey: Your Feedback Please!

http://bit.ly/3PObDco

The UEFI Forum

UEFI Forum Overview



Specification Update

Latest Specifications

v2.10 v2.2 v1.8 v2.7 v1.1 v6.5 < Current Versions

- **Recent Updates**:
  - UEFI PI Specification v. 1.8
    - Memory security support and updated MP services
  - UEFI Specification v. 2.10
    - Introducing UEFI Conformance Profiles, allowing support for more types of platforms and implementation codebases
    - Crypto agility including SHA-384/SHA-512 signing scheme for Authenticated Variables support
    - Emerging LoongArch and RISC-V processor architecture support
    - Add confidential computing extension
  - ACPI Specification v. 6.5
    - CXL Memory support
    - LoongArch processor architecture support
    - Confidential Computing event log support
    - USB-C USB4 support

UEFI Security and Open Source Focus

UEFI Security

- As broad architecture support continues, security will continue to be a concentrated effort for the Forum and the community
- We will continue to maintain with errata and new content updates that reflect implementation experience with existing specification content
- The UEFI Forum is continuing to debunk confusion in the industry (i.e. the idea that “Platform Firmware” and its flaws and vulnerabilities refer to the firmware as “UEFI”)
- The UEFI Forum, its security response team (USRT), security sub-team (USST), SBOM Sub-team (USBT), specification working groups, and Industry Communications Working Group (ICWG) are dedicated to making UEFI compliant firmware as secure as possible. They are also dedicated to aiding members of the supply chain to respond to vulnerabilities in a timely manner and communicating with stakeholders to improve to state of the art in firmware

For more information, please read our latest white paper entitles “Decoding UEFI Firmware Unraveling the Intricacies of System Firmware, its Ecosystem and Supply Chain” at https://uefi.org/learning_center/papers.

Open Source

- Enable “Code-First” approach
- Encourage open source contributions
  - Increase in open source contributions in reference implementations, SCT and FWTS
  - Improve open source process

Questions?

Thanks for attending the Fall 2023 UEFI Developers Conference and Plugfest

For more information on the UEFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by