Fall 2023 UEFI Developers Conference and Plugfest

October 9 – 12, 2023
Hillsboro, Oregon
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
<table>
<thead>
<tr>
<th>Time</th>
<th>Session Title</th>
<th>Presenters</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:00 – 1:30 pm</td>
<td>UEFI Ecosystem Investments and Open-Source Contributions</td>
<td>Michael Kubacki (Microsoft)</td>
</tr>
<tr>
<td>1:30 – 2:30 pm</td>
<td>Using SPDM in UEFI for Device Attestation</td>
<td>Vincent Zimmer (Intel) and Michael Kubacki (Microsoft)</td>
</tr>
<tr>
<td>2:30 – 3:30 pm</td>
<td>Evolving the Secure Boot Ecosystem</td>
<td>Jeffrey Sutherland and Doug Flick (Microsoft)</td>
</tr>
<tr>
<td>3:30 – 4:00 pm</td>
<td>Hardening the Core: Enhanced Memory Protection</td>
<td>Taylor Beebe (Microsoft)</td>
</tr>
</tbody>
</table>

Testing from 2:30 – 6:00 pm
### Fall 2023 DevCon Session Highlights

#### Wednesday, October 11

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

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

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

- Board of Directors
- Industry Communications Working Group
- UEFI Specification Working Group
  - Security Subteam
  - Configuration Subteam
  - Network Subteam
  - Shell Subteam
  - Arm Binding Subteam
- Platform Initialization Working Group
- Test Working Group
- ACPI Specification Working Group
- UEFI Security Response Team
- Security Subteam
- NVDIMM Subteam

- 12 Promoters
- 38 Contributors
- 289 Adopters
- 59 Individual Adopters

Total Members: 408
Specification Update
## Latest Specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Version</th>
<th>Recent Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>UEFI Specification</td>
<td>v2.10</td>
<td></td>
</tr>
<tr>
<td>UEFI Shell Specification</td>
<td>v2.2</td>
<td></td>
</tr>
<tr>
<td>UEFI PI Specification</td>
<td>v1.8</td>
<td></td>
</tr>
<tr>
<td>Self Certification</td>
<td>v2.7</td>
<td></td>
</tr>
<tr>
<td>PI Distro Package</td>
<td>v1.1</td>
<td></td>
</tr>
<tr>
<td>ACPI Specification</td>
<td>v6.5</td>
<td></td>
</tr>
</tbody>
</table>

**< Current Versions**

- **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 forAuthenticated 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