Spring 2019 UEFI Plugfest

April 8-12, 2019
Bellevue, Washington
State of UEFI

Presented by Dong Wei
Spring 2019 UEFI Plugfest
Introduction

- Dong Wei
  - Vice President, UEFI Forum
  - Arm Fellow
Agenda

• Event Overview
• The UEFI Forum
• Specification Update
• UEFI Security & Open Source
• Fall 2019 UEFI Plugfest
• Questions
Event Overview
Made Possible by...
## Spring 2019 Session Highlights

<table>
<thead>
<tr>
<th>Time</th>
<th>Session Title</th>
<th>Presenters</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:30 – 10:00 am</td>
<td>UEFI Self Certification Tests (UEFI-SCT) and Firmware Test Suite (FWTS)</td>
<td>Supreeth Venkatesh, Arm Harry Hsiung, Intel Alex Hung, Canonical</td>
</tr>
<tr>
<td>10:00 – 10:30 am</td>
<td>UEFI Updates and Open Source Firmware evolutions on Arm</td>
<td>Matteo Carlini and Dong Wei, Arm</td>
</tr>
<tr>
<td>10:30 – 11:00 am</td>
<td>Risks to UEFI firmware due to growing attack surfaces</td>
<td>Dick Wilkins, Phoenix</td>
</tr>
<tr>
<td>11:00 – 11:30 am</td>
<td>From Runtime to Compile Time: Improving ASL Through Enhanced Namespace Resolution</td>
<td>Erik Schmauss, Intel</td>
</tr>
<tr>
<td>11:30 am – 12:00 pm</td>
<td>Microsoft UEFI Update</td>
<td>Jeremiah Cox, Microsoft</td>
</tr>
<tr>
<td>12:30 – 1:00 pm</td>
<td>Hardening Firmware Components with Host-based Analysis</td>
<td>Brian Richardson, Intel</td>
</tr>
</tbody>
</table>

Testing from 1:00 – 6:00 pm
Welcome Reception

- Tuesday, April 8 from 6:00-7:30pm
- Embassy Suites by Hilton Seattle Atrium

- Popcorn, Fresh Vegetable Platter, Cheese & Fruit Board and Spring Rolls

- Three drink tickets per person (deluxe brands, domestic beers, house wines, soft drinks)
### Spring 2019 Session Highlights

<table>
<thead>
<tr>
<th>Time</th>
<th>Session Title</th>
<th>Presenters</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:00 – 11:30 am</td>
<td>Half Duplex controller support and Multi IO support in SPI framework</td>
<td>Pankaj Bansal, NXP</td>
</tr>
<tr>
<td>11:30 am – 12:00 pm</td>
<td>Improving UEFI Network Stack Performance</td>
<td>Maciej Rabeda, Intel</td>
</tr>
<tr>
<td>12:30 - 1:00 pm</td>
<td>Case Study: Removing SMM from Intel Platforms / second half of the lunch hour</td>
<td>Sarathy Jayakumar, Intel</td>
</tr>
<tr>
<td>1:00 – 1:30 pm</td>
<td>Support Secure UEFI and OPTEE OS together on Arm</td>
<td>Meenakshi Aggarwal, Udit Kumar, NXP</td>
</tr>
<tr>
<td>1:30 – 2:00 pm</td>
<td>Role Modeling Open Source Best Practices in Firmware</td>
<td>Mark Doran, Stephano Cetola, Intel</td>
</tr>
<tr>
<td>2:00 – 2:30 pm</td>
<td>Using Capsules for Firmware Configuration Update</td>
<td>Zachary Bobroff, American Megatrends Inc</td>
</tr>
</tbody>
</table>

Testing from 9:00 – 11:00 am

Testing from 2:30 – 5:30 pm
The Evening Event: The Parlor Bellevue

**Wednesday, April 11 from 6:00 - 9:00 pm**

The Parlor Bellevue  
Lincoln Square (third floor)  
700 Bellevue Way NE Suite 300  
Bellevue, WA 98004

**Food:** Mexican Grill Buffet

**Beverages:** Bottomless sodas, coffee, tea. Beer and wind (alcohol available for purchase)

**Activities:** Reserved lounge with Billiards, Foosball, Giant Jenga, Shuffleboard ad Ping-Pong.

Sponsored by

[ intel logo ]
<table>
<thead>
<tr>
<th>Time</th>
<th>Session Title</th>
<th>Presenters</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:30 – 1:00 pm</td>
<td>UEFI topics for the manufacturing efficiency/second half hour of lunch</td>
<td>Rafael Machado, Flex Institute of Technology</td>
</tr>
<tr>
<td>1:00 – 1:30 pm</td>
<td>How Writing Portable UEFI Drivers Improves Reliability (and Helps Me)</td>
<td>Ard Biesheuvel and Leif Lindholm, Linaro</td>
</tr>
<tr>
<td>1:30 – 2:00 pm</td>
<td>Redfish Implementation for UEFI</td>
<td>Jason Spottswood, HPE</td>
</tr>
<tr>
<td>2:00 – 2:30 pm</td>
<td>Redfish Host Interface: UEFI and OS implications</td>
<td>Samer El Haj Mahmoud, Lenovo</td>
</tr>
<tr>
<td></td>
<td></td>
<td>John Leung, Intel</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mike Rothman, Intel</td>
</tr>
</tbody>
</table>
Afternoon Break
Speaker’s Office Hours

• Afternoon Break Time
• Meet with the presenters after their sessions
  • Where: The Ballroom
  • When: 3:00 – 4:00 pm

• Soft drinks, coffee and sweets sponsored by

American Megatrends  insyde  phoenix technologies
Event Survey:
Your Feedback Please!

https://www.surveymonkey.com/r/2019SpringUEFIPlugfest
The UEFI Forum
UEFI Forum Overview

Board of Directors

Industry Communications Working Group
UEFI Specification Working Group
Platform Initialization Working Group
Test Working Group
ACPI Specification Working Group
UEFI Security Response Team

Security Subteam
Configuration Subteam
Network Subteam
Shell Subteam
Arm Binding Subteam

Security Subteam
NVDIMM Subteam

13 Promoters
43 Contributors
254 Adopters
44 Individual Adopters

354 Total Members
Specification Update
Latest Specifications

- **Updates Represent:**
  - ACPI 6.3 – PCC Operation Region, I3C Host Controller, Generic Initiator, Peripheral-attached Memory, HMAT Enhancement, NVDIMM Health Error Injection and ARS Update, ARS Error Injection, GTDT Extension, Load Extension and Unload Deprecation, Arm SPE Support, etc.
  - PI 1.7 – PEI Core PEIM Migration Support Change, SecCore/PeiCore BFV Requirement Change, MM MP Protocol issues, EFI_SW_DXE_BS_EC_BOOT_OPTION_LOAD_ERROR Extended Data, New Status Codes, PEI Delayed Dispatch, New Architectural PPI for PI PEI Core FV Location, etc.
  - UEFI 2.8 – Redfish Support (Discover Protocol, REST EX Protocol, JSON Structure Protocol, JSON Capsule Support, REST Style Formset, etc.), Peripheral-attached Memory, EBC Requirement Removal, CCIX PER Log Error Structure, Runtime Calls May Return Unsupported, etc.
UEFI SCT Status

• Latest stable binary version - UEFI SCT 2.6 A is published at [https://uefi.org/testtools](https://uefi.org/testtools)
  – Source code was only available to Contributors
• UEFI SCT 2.7 A coming soon
  – Now open source development at [https://github.com/tianocore/edk2-test](https://github.com/tianocore/edk2-test)
  – Tag edk2-test-stable201904 is intended as 2.7A beta quality for plugfest
  – UEFI Forum to recommend afterwards
FWTS Updates

• FWTS 19.02.00 updates tests for ACPI 6.3
  – FWTS 19.03.00 intended as beta quality for plugfest
  – UEFI Forum to recommend afterwards
UEFI Security and Open Source Focus
UEFI Security

- 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.
- Broad architecture support continues.
- New UEFI webinar: Secure Coding: https://www.youtube.com/watch?v=fkZPVEhQUmc&feature=youtu.be
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
Fall 2019 UEFI Plugfest

- Details of the Fall Plugfest will be out soon
  - Location: Asia
  - Timeframe: Late October or early November

- Additional details will be available on the UEFI Forum website at [www.uefi.org/events/upcoming](http://www.uefi.org/events/upcoming)
Questions?
Thanks for attending the Spring 2019 UEFI Plugfest

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