State of UEFI

Spring 2017 UEFI Seminar and Plugfest
Presented by

Mark Doran, President of the UEFI Forum
Agenda

- Event Overview
- The UEFI Forum
- Specifications Update
- Summary
- Questions
Attendees

• 205 attendees
  – 186 members
  – 13 non-members, press and VIPs
  – 46 companies represented
Welcome New Members

Adopters

- AAEON Technology Inc.
- AlterScience
- Centerm Information Co., Ltd.
- Chunghsin Industry Group
- Dawning Information Industry (Beijing) Corp., Ltd.
- HXT Semitech
- LCFC
- MediCapture, Inc.
- Montage-Tech
- New H3C Technologies Co., Ltd.

- Ruijie Networks
- Shanghai Advanced Research Institute
- Shanghai IP3 Technology Co., Ltd.
- Shubo Tian
- TYA Company
- VIA Alliance Semiconductor Co., Ltd.
- Wuhan University
- Xie Tainming
- Zhejiang Dahua Technology Co., Ltd.
The UEFI Forum
The UEFI Forum founded

Apple adopts UEFI firmware;
HP notebook and desktop platforms include UEFI

UEFI Specification includes ARM architecture

Secure Boot included in UEFI specification

Linux Foundation joins the Forum

Microsoft Windows 8 requires UEFI for its certification logo

The UEFI Forum begins management of Advanced Configuration and Power Interface (ACPI) Specification

PC hardware predominantly ships with UEFI
UEFI Today and Beyond

2017

• Industry-wide cooperation and support
• 332 members companies and individual
• Common framework allowing developers to scale as needed

Future

• Continuous evolution across a range of platforms and enables secure cross-functionality
• Critical enabling factor helping drive research and innovation
Specification Update
Latest Specifications

- UEFI Specification v2.6 (January 2016)
- ACPI Specification v6.1 (January 2016)
- UEFI Shell Specification v2.2 (January 2016)
- PI Packaging Specification v1.1 (January 2016)
- UEFI PI Specification v1.5 (July 2016)
Upcoming 2017

Non-volatile memory across specifications

Broad architecture support continues

Self Certified Testing (SCT) update
Summary
Summary

• The UEFI Specification provides interfaces and mechanisms to allow for support of new technologies and improved development.

• The UEFI Specification supports a more secure system, a faster boot time, improved performance, and platform feature innovation.

• The UEFI Specification increases efficiency by allowing developers to reuse code and allows for extensibility, modularity and easy prototyping during development.
The UEFI Forum Fall 2017 Plugfest

• Taipei, Taiwan – October 2017
• More details coming soon on UEFI.org.
Questions?
Event Schedule
## Event Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00am</td>
<td>Welcome &amp; State of UEFI</td>
<td>UEFI and IoT: Best Practices in Developing IoT Solutions</td>
<td>TESTING</td>
</tr>
<tr>
<td>10:00am</td>
<td>Keynote: China Information Technology Ecosystem</td>
<td>TESTING</td>
<td></td>
</tr>
<tr>
<td>11:00am</td>
<td>ARM Updates</td>
<td>Establishing and Protecting a Chain of Trust with UEFI</td>
<td>Lessons Learned from Implementing a Wi-Fi and BT Stack</td>
</tr>
<tr>
<td>12:00pm</td>
<td>LUNCH</td>
<td>LUNCH</td>
<td>LUNCH</td>
</tr>
<tr>
<td>1:00pm</td>
<td>ARM Server’s FW Security</td>
<td>Implementation of Type 1 Hypervisor in UEFI Firmware</td>
<td>TESTING</td>
</tr>
<tr>
<td>2:00pm</td>
<td>SMM Protection in EDKII</td>
<td>Tea Break</td>
<td>Tea Break</td>
</tr>
<tr>
<td>2:15pm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:00pm</td>
<td>Tea Break</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:15pm</td>
<td>Server RAS and UEFI CPER</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:00pm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:15pm</td>
<td>A More Secure and Better User Experience for OS-based Firmware Update</td>
<td>TESTING</td>
<td>TESTING</td>
</tr>
<tr>
<td>5:00pm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5:15pm</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Thanks for attending the Spring 2017 UEFI Seminar and Plugfest

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

presented by

Mark Doran, President of the UEFI Forum