

*presented by*

**ARM**



# UEFI – What is it?

Spring 2017 UEFI Seminar and Plugfest

March 27 - 31, 2017

Presented by Dong Wei (ARM)

# Agenda



- Introduction
- Background Information
- Specification
- Summary
- Monday Schedule



# Background Information

# UEFI Forum Overview



- Non-profit industry forum
- Founded in 2005
- Formed to standardize EFI and extend to x64
- Forum maintains all specification development
- Currently at over 330 member companies and individual adopters

# Why Become a UEFI Member?



## Membership Profiles

- System Manufacturers (server, client, mobile, IoT)
- Silicon Providers
- Firmware Vendors
- Computer Peripheral/Hardware Vendors
- Software Vendors
- Operating System Developers
- Industry Advisors
- Best Practices Stewards
- Academics

## Membership Levels

- Adopter (complimentary)
  - Access to the Members-only web area
  - Invitations to member events
  - Access to UEFI technical tools and design guides
- Contributor (\$2500 annual fee)
  - Adopter benefits, plus:
    - Participation in UEFI Work Groups, by invitation
    - Participation in email reflectors
    - Access to draft specifications

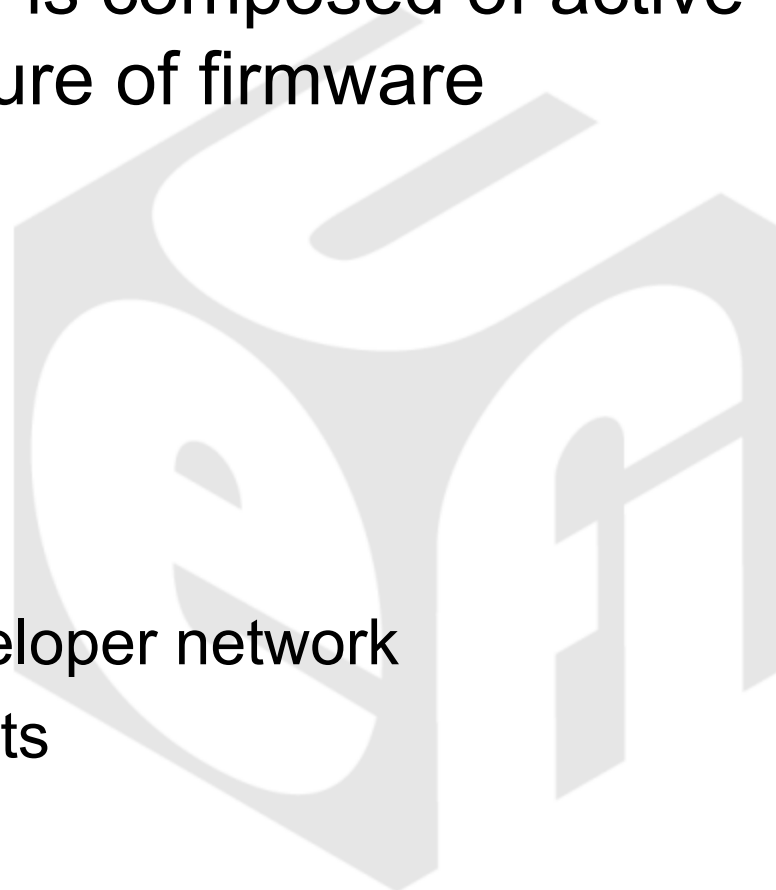
# Get Involved



UEFI Forum's community is composed of active members shaping the future of firmware technologies.
























Join to:

- Contribute feedback
- Develop technical content
- Engage with the UEFI developer network
- Participate in UEFI Plugfests



# Membership Benefits



	 Contributor	 Adopter		 Contributor	 Adopter
Voting Rights			Published spec access		
Chairperson candidacy			Tech expert access		
Unlimited participants			Marketing program access		
Plugfest attendance			Members-only area access		
Work group participation			Email list subscription		
Work-in-progress spec and private Github access			Listed as member on UEFI.org		

# Promoter Members

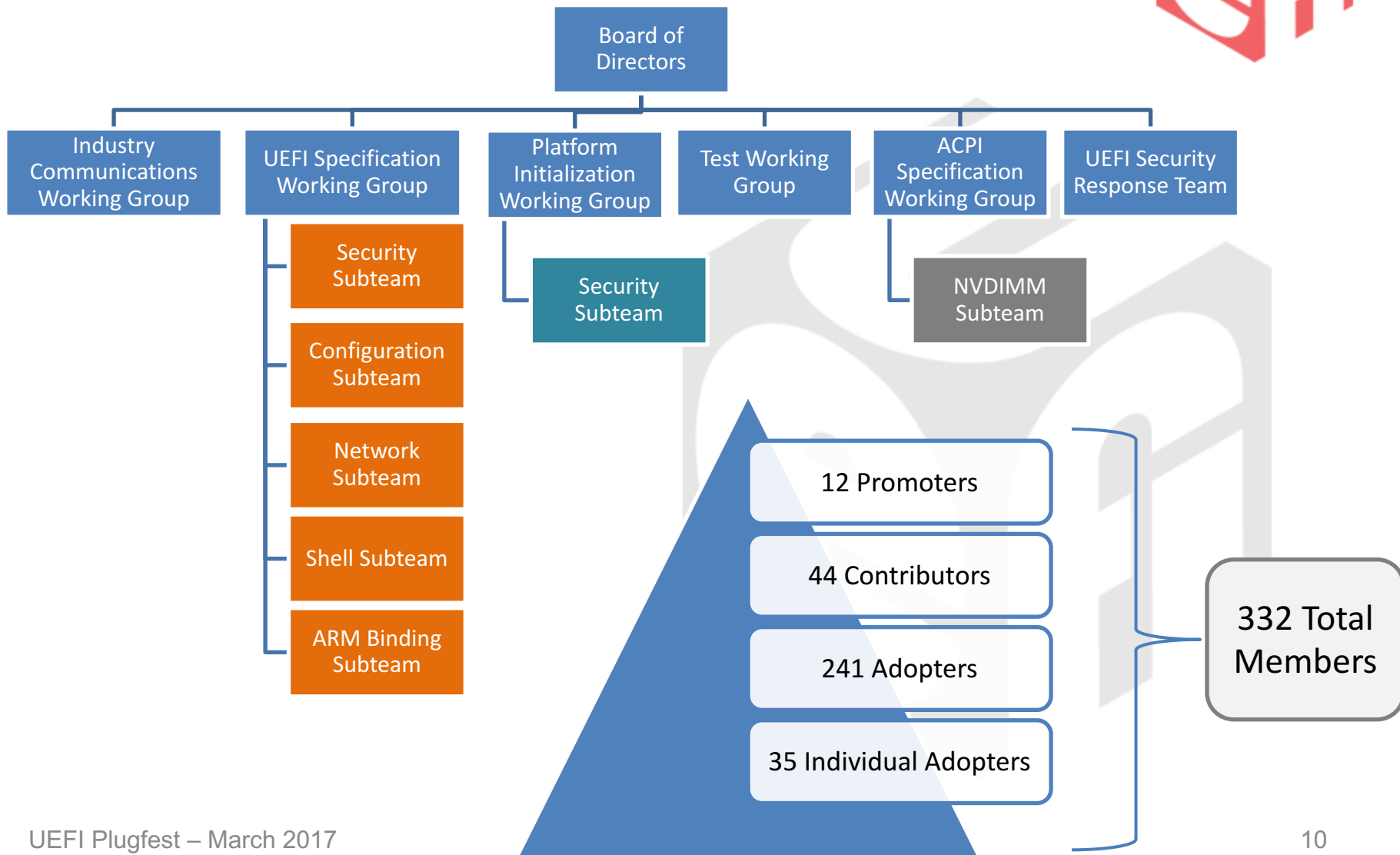




# Contributor Members



# UEFI Forum Overview



# Benefits of UEFI in the Technology Ecosystem in China



- Indigenous technology implementations
  - The technology ecosystem has the ability to develop what they want
- A common framework that isn't market or architecture dependent
- Creates new opportunities for business, developers, and the open source community



# Specifications



# UEFI Technology



Firmware supports numerous systems and devices

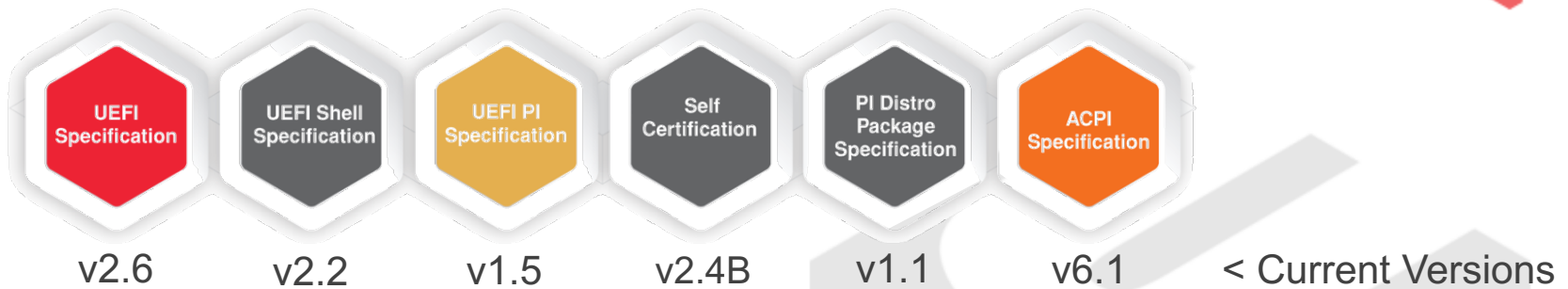


Developed by community composed of all impacted markets & technologies

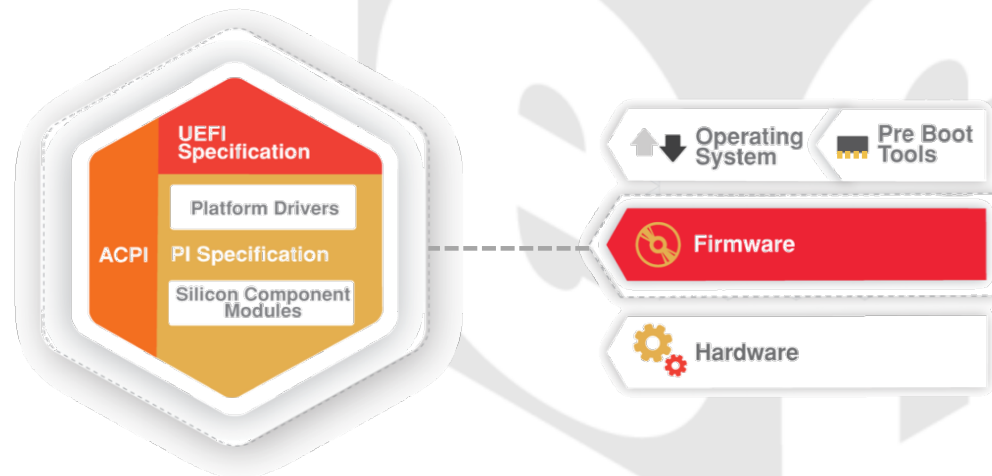
Improves:

- System performance
- System security
- Platform future-proofing
- Interoperability between devices and systems

# Specification and Tools



System Stack >



# UEFI & ACPI Specifications



- **Unified Extensible Firmware Interface (UEFI)**
  - Defines firmware interface in pre-OS space
  - Standardizes platform interfaces for interoperability
  - Extensible across all platforms
  - Architecture-agnostic
    - Currently officially supports IA64, ia32, x64, ARM AArch32 and ARM AArch64
    - RISC-V support coming
- **Advanced Configuration and Power Interface (ACPI)**
  - Key element in OS-directed configuration and Power Management (OSPM)
  - Flexible mechanisms for device discovery, thermal management and reliability, availability and supportability (RAS) features
  - Enables platform technologies to evolve independently in the operating system and hardware

# Top Misconceptions



- **UEFI vs. Legacy BIOS**

- Legacy BIOS rooted in IBM PC design
- UEFI defines a standard interface for transferring control to an OS

- **UEFI Secure Boot**

- Optional spec protocol for most general purpose systems
- Can be disabled on most systems; up to system vendors which policies are implemented
- Designed to protect system from malware and unauthenticated binaries

- **UEFI vs. TianoCore**

- TianoCore is not UEFI, it is a *reference implementation* of the UEFI specification and not required
- It is possible to have other implementations: proprietary, U-Boot, Coreboot, etc.
  - Therefore, UEFI as an abstraction layer may still be attractive to some segments such as the embedded market where TianoCore may not be as attractive as U-Boot as the underline implementation





# Summary



# Summary



- UEFI defines a standard interface for transferring control to an operating system
- UEFI Specification documents the UEFI standard interface
- UEFI Forum is a widely-participated industry standard consortium
  - It owns the definition and promotion of the UEFI Specification and its Test Suite
  - In addition, it owns the definition and promotion of the Advanced Configuration and Power Interface (ACPI) and Platform Initialization Specification (PI Specifications)



# Seminar and Plugfest Schedule



# Monday Schedule



2:00 - 3:00pm

- TianoCore, the Open Source UEFI
  - Brian Richardson, Intel

3:15 - 4:15pm

- General FW Overview Recommendations for Windows OS
  - Fei Zhou, Microsoft

4:15 - 5:15pm

- Code Coverage in Firmware Automation Testing
  - Liu Zhi, Intel

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*

Dong Wei, ARM, The UEFI  
Forum

