presented by

The UEFI Mini-Summit

Linux Community's Guide to UEFI

Introduction by:

Dong Wei – HP

Jeff Bobzin – Insyde Software

August 22, 2014

Agenda

- UEFI Introduction
- UEFI Mini-Summit Schedule
- Panel Discussion
- Q&A

The UEFI Forum Background

- Non-profit industry forum
- Founded in 2005 with 11 promoter members
- Currently at 250+ member companies
- Formed to standardize EFI and extend to x64
- Forum maintains all spec development

The UEFI Forum

Membership Profiles

- PC manufacturers
- Server manufacturers
- Computer peripheral
- Hardware vendors
- Software vendors
- Operating system developers
- Industry advisors
- Best practices stewards
- Academics

Membership Levels

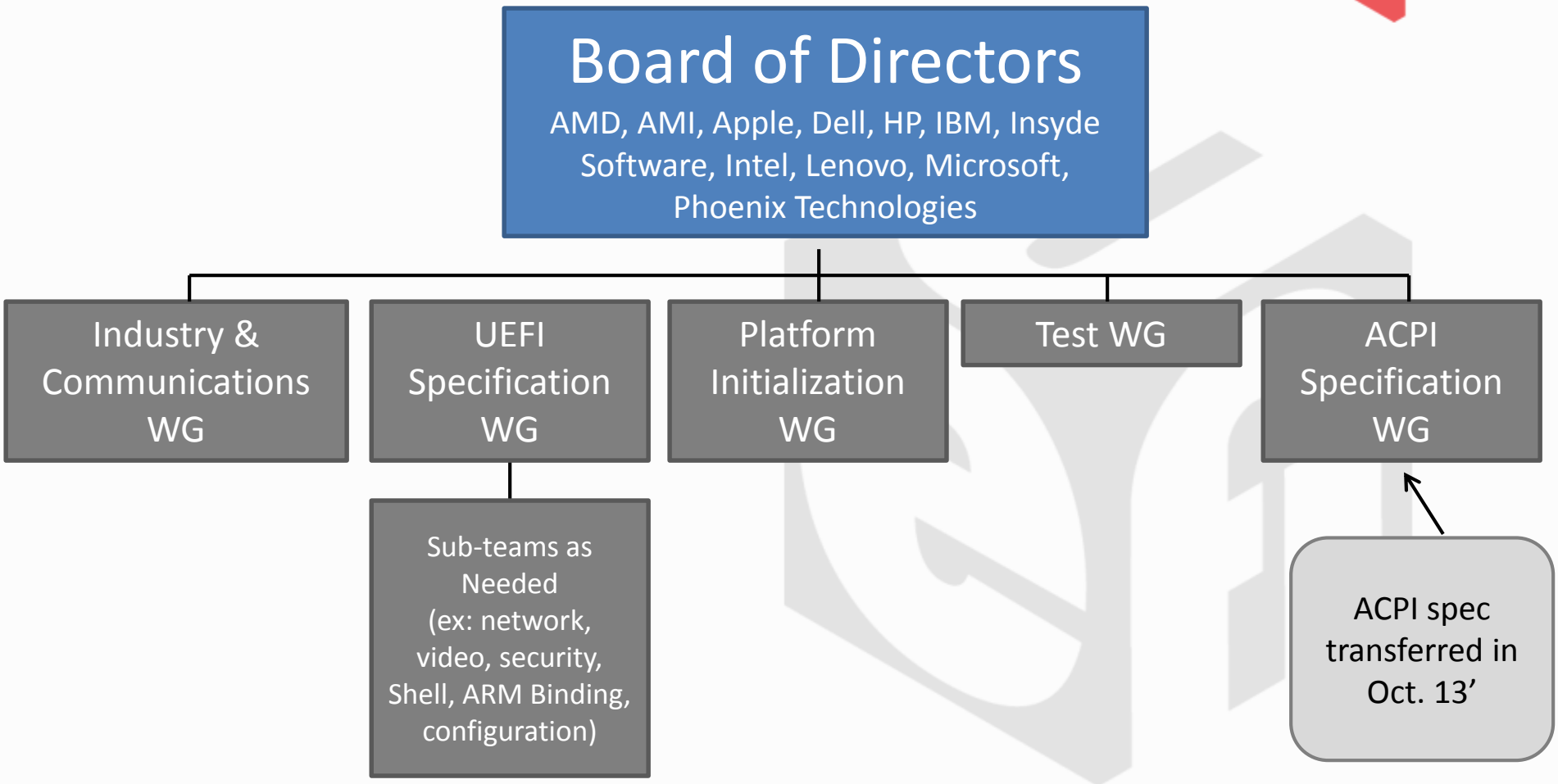
Adopter (complimentary)

- Forum's members-only site access
- Plugfest/event invitations
- Tools and design guides access

Contributor ($2500 annual fee)

- Adopter benefits, plus…
- Opportunity to participate in UEFI Working Groups via invitation
- Email reflector participation
- Preview of draft spec revisions

The UEFI Forum



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
- Supports x64, ia32, IA64, ARM AArch32 and ARM AArch64

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

Specification Milestones

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

Why Are We Here Today?

- On the rise:
  - Open source implementations
  - Usage of mobile and non-PC devices
  - Integration of mobile and non-PC devices with traditional computing devices
  - …security vulnerabilities
- Value proposition: UEFI Forum specifications support…
  - Cross-functionality between devices, software and operating systems
  - Enhanced security options and data protection
  - Faster boot-times (including dual-boot) with better configuration control
  - Faster recovery in cases of system outages
  - Flexibility regarding specifications' features used and disabled

Why Are We Here Today?

- Increased usage of UEFI Forum specifications (UEFI & ACPI) in Linux OSes (Fedora 18, OpenSUSE 12.3, Ubuntu 12.10)
- Opportunities for Linux Community & UEFI Forum
  - Continued and increased involvement of Linux-related companies and leadership groups
  - Strengthened collaboration between firmware and OS communities; ensures the right stakeholders are brainstorming, sharing and developing valuable industry advancements
    - Example of current project idea: automation of platform-based, self-managed key stores

Panelists

- Zach Bobroff, AMI
- Brian Richardson, Intel
- Matthew Garrett, Nebula
- Roy Franz, Linaro/Cavium
- Dong Wei, HP

Questions & Answers

Mini-Summit Schedule

Time	Session	Presenters
10:45 a.m.	Intro, panel and Q&A	Dong Wei, HP Jeff Bobzin, Insyde
11:45 a.m.	UEFI Secure Boot – Strengthening the Chain of Trust	Jeff Bobzin, Insyde Kevin Lane, HP
Lunch 12:35 p.m. – 2:30 p.m.		
2:30 p.m.	UEFI Test Tools for Linux Developers	Brian Richardson, Intel Alex Hung, Canonical
3:30 p.m.	Building ARM Servers with UEFI and ACPI	Dong Wei, HP Roy Franz, Linaro
4:30 p.m.	Self-signing the Linux Kernel (the hobbyist approach)	Zach Bobroff, AMI

Resources

Upcoming Events

- IEEE Conference on Security and Privacy – November 2014
- Fall UEFI Plugfest – 10/13 – 10/17 (member-only)

Helpful Links

- UEFI Primer – uefi.org/primer
- UEFI FAQ – uefi.org/faq
- Top Misconceptions White Paper – uefi.org/top10
- ACPI press release – uefi.org/ACPIv5.1

Become a member

- Visit uefi.org/join to learn more

For more information,
visit http://www.uefi.org

Thank you.