Spring 2018 UEFI Plugfest

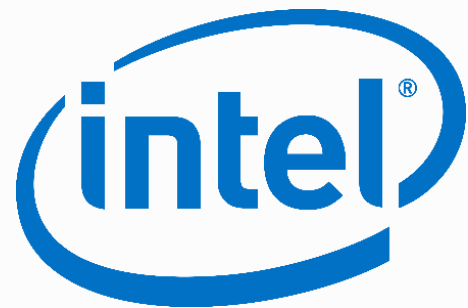March 26 – 30, 2018

Bellevue, Washington

Agenda

- Event Overview
- The UEFI Forum
- Specification Update
- UEFI Security
- Upcoming Focus
- Questions

Event Overview

Made Possible by…

Welcome Reception

Tuesday, March 27 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)

The Evening Event: The Parlor Bellevue

Wednesday, March 28 at

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

Food: Margherita Pizza, pepperoni pizza, spinach asiago and artichoke dip, beef sliders, and portabella stuffed mushrooms.

Beverages: Bottomless sodas, coffee, tea. Alcohol available for purchase.

Activities: Reserved billiard and ping-pong tables.

Sponsored by (intel)

Speaker's Office Hours
Spring 2018 UEFI Plugfest
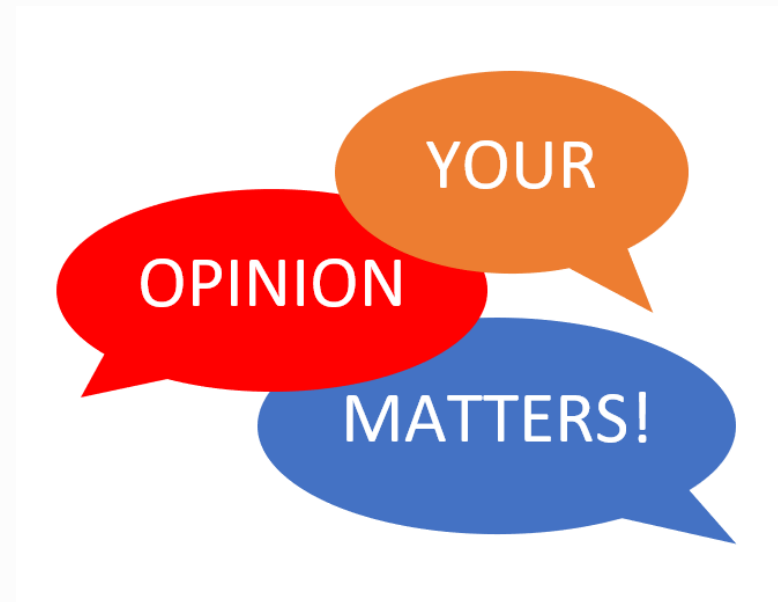
- What: Meet with the presenters after their sessions
- Where: Embassy Suites Ballroom
- When: 3:00 – 4:00 pm
- Why: Ask questions and discuss more

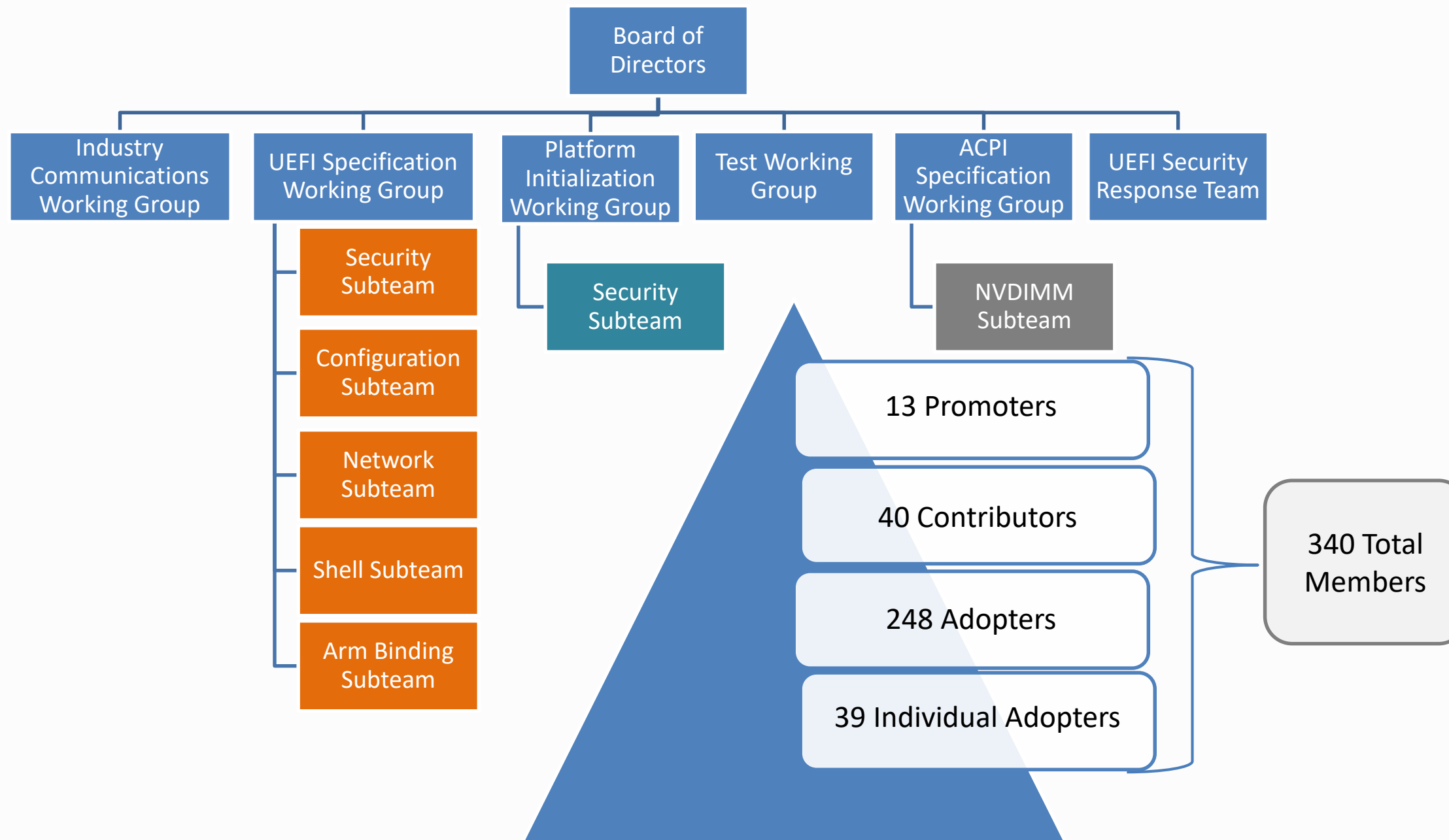# Event Survey: Your Feedback Please!

www.surveymonkey.com/r/Spring2018Plugfest
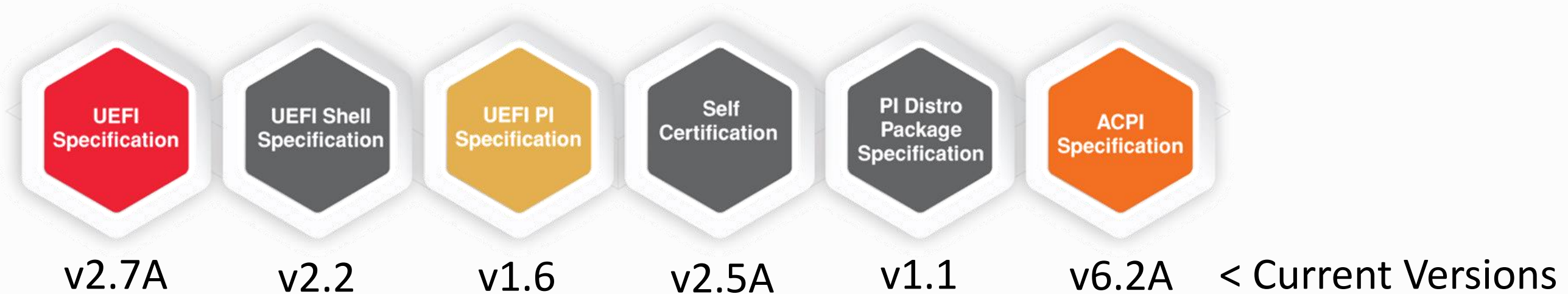
The UEFI Forum

UEFI Forum Overview

www.uefi.org

Specification Update

Latest Specifications

UEFI Specification	UEFI Shell Specification	UEFI PI Specification	Self Certification	PI Distro Package Specification	ACPI Specification	
v2.7A	v2.2	v1.6	v2.5A	v1.1	v6.2A	< Current Versions

- **Summer 2017**: First time the UEFI, Platform Interface (PI) and Advanced Configuration and Power Interface (ACPI) specifications were updated together (received a lot of input from the community and members)
- **Updates Represented**: Support for upcoming hardware, such as non-volatile memory, as well as deployment learnings over the last several years, such as the UEFI variable enhancement and completeness (i.e. the SPI driver)
- **Next Up**: A minor revision for the Platform Interface (PI) specification. This revision addresses some changes that are coming out of implementation, work catching up, and reconciliation with specification language

UEFI Security

www.uefi.org

UEFI Security

The Spring UEFI Plugfest this year has several sessions addressing UEFI security and many of the testing sessions will also include security testing.

Join and contribute to the discussion on firmware security

- We're all in this together; for security to work, it can't be looked at in terms of industry silos. Security is the collective responsibility for everyone in the industry – from OEMs to developers and extends all the way to sys-admins and even consumers.
- New security challenges will continue to appear as the industry continues to evolve. UEFI exist to help the platform security ecosystem meet the changing demands, primarily through thoughtful and consistent implementation of firmware security specifications.
- UEFI Forum's firmware security resources help everyone in the industry to put security first, as well as collaborate on firmware solutions.

UEFI Security

Mitigate the risks through placing security first and following the specifications as intended

- The need to secure systems at the firmware level continues to be a priority for the UEFI Community.
- Properly implemented, the security specifications established by UEFI Forum can help everyone in the ecosystem mitigate the security risks.
- People need to understand that placing "Security First" applies to firmware as well as the OS, in order to mitigate security risks.
- UEFI Forum is committed to helping the ecosystem (OEMS, Developers, Sys-Admins, and even Consumers) establish and follow industry specifications to mitigate security risks and do its part to minimize security threats. Security is a collective responsibility of the entire industry, and it must start with platform security.

www.uefi.org

UEFI Security

Don't dread firmware Updates. They are worth the time.

- Firmware updates are painful, but necessary.
- Incorrect implementation can increase security risks; UEFI Forum's specifications provide developers with a proactive approach to create security by design and reduce security vulnerabilities.
- UEFI Forum is committed to strengthening the platform security ecosystem by making UEFI's firmware security resources available to developers, and helping OEMs to publish regular security updates.

Upcoming Focus

- 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.

Additional details will be available on the UEFI Forum website at
www.uefi.org/events/upcoming

Questions?

www.uefi.org

Thanks for attending the Spring 2018 UEFI Plugfest

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

presented by

The UEFI Forum