presented by

ARM

ARM Trusted Firmware
ARM UEFI SCT update

Presented by Charles García-Tobin (ARM)
Agenda

• ARM Trusted Firmware
  – What and why

• UEFI SCT update
  – progress
ARM Trusted Firmware (ARM TF)
a little history

• 4 years ago ... (ish)
Wild west before ARM TF

- Power management development model
Wild west before ARM TF

- Power management development model
Wild west before ARM TF

- Power management development model
Wild west before ARM TF

- Power management development model

Proprietary HW

Proprietary SW+FW
Wild west before ARM TF

• Power management development model
Wild west before ARM TF

• Development model caused a few problems

Varied quality

Expense

Fragmentation

Number of PM drivers = Number HW vendors × Number of vendor SoCs
So we created specs

Power State Coordination Interface
• Powering cores up or down for idle, secondary boot, hotplug
• System reset/shutdown

SMC calling convention
• Helps in supporting multiple vendors in secure firmware

- Spec available today in ARM infocenter:
But specs are nothing without code

- So we created the ARM Trusted Firmware project
- Implements PSCI and SMC calling convention
- Provides reference early boot
- Applicable to all segments
- Open Source at GitHub
  - BSD License
  - Contributions welcome

https://github.com/ARM-software/arm-trusted-firmware
Things better as a result

• PSCI is supported by every major OS vendor

• PSCI is supported by every major Hypervisor vendor

• ARM TF has been taken as reference by most silicon vendors

• It is the standard for ARMv8-A
What is ARM Trusted Firmware?

Normal World

- EL0
  - Guest A App 1
  - Guest A App 2
  - Guest B App 1
  - Guest B App 2

- EL1
  - Guest OS Kernel A
  - Guest OS Kernel B

- EL2
  - UEFI
  - Hypervisor

- EL3
  - EL3 Runtime Firmware (Secure Monitor)
  - PSCI

Secure World

- Secure EL0
  - Trusted App 1
  - Trusted App 2

- Secure EL1
  - Trusted OS
  - Boot Firmware

Secure EL0

- Secure EL1

- Secure EL0

- Secure EL1

Key

- EL3 Execution
- Secure EL1 / EL0 Execution
- EL2 Execution
- EL1 / EL0 Execution

SMC

UEFI Plugfest – September 2016

www.uefi.org
What is ARM Trusted Firmware?

UEFI Plugfest – September 2016

www.uefi.org

14
What is ARM Trusted Firmware?

**Diagram Explanation:**

- **EL0**
  - Guest A App 1
  - Guest A App 2
  - Guest B App 1
  - Guest B App 2

- **EL1**
  - Guest Linux Kernel A
  - Trusted App 1
  - Trusted App 2

- **EL2**
  - UEFI
  - Hypervisor

- **EL3**
  - EL3 Runtime Firmware (Secure Monitor)
  - PSCI

- **Secure World**
  - Secure EL0
  - Secure EL1
  - Key
    - EL3 Execution
    - Secure EL1 / EL0 Execution
    - EL2 Execution
    - EL1 / EL0 Execution

- **Normal World**
  - Boot Firmware
  - SMC

Optional components include UEFI Plugfest – September 2016

www.uefi.org
How does it relate to UEFI specs?

- ACPI core power is intimately tied to PSCI
  - LPI states introduced in 6.0 map directly to PSCI
- Provides a generic implementation for UEFI reset run time services
- Trusted boot flow provides SEC on our reference platforms
SCT update
SCT update

• UEFI 2.5 AArch64 beta version
  – Number of updates and fixes
    • Various fixes in test for network statistics, ExitBootService, simple file system and watchdog
    • Submitted six patches
    • 10,000 warning fixed (Guid definitions, incompatible pointers) in the UEFI-SCT

• UEFI 2.6 AArch64 alpha version
  – Add support for
    • Ramdisk/NVMe part test have been submitted
SCT discussions

• SCT availability and development model
• Proposed protocols to help with testing partial implementations
• We have run into issues with robustness of shell over Seriallo
  – It crashes when the SCT framework tries to open the Seriallo protocol in exclusive mode.
Thanks for attending the UEFI US Fall Plugfest 2016

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

presented by

ARM