BUD17-313: BoF - Device Tree and Secure Firmware

Joakim Bech and Jens Wiklander
Device Tree recap

- It’s used to describe hardware capabilities
- It’s a tree where the capabilities are described in nodes and properties
- It’s a separate binary (DTB), which is passed to Linux during boot
- Until now(?), it has mainly been used by Linux kernel
Device Tree in Firmware?

- Firmware is more flexible today compared to the past
- Just as kernel, desirable to have standalone binary images
- Several firmware components in use on a normal setup
  - TEE (OP-TEE etc)
  - Secure Monitor (ARM-TF etc)
  - UEFI
  - U-Boot
  - Grub
- There are uses cases when firmware wants to use and eventually modify things before handing over to kernel
  - Reserve (secure) memory
  - Secure peripherals
  - Update available memory based on SoC specific probing
  - Supply boot arguments for the kernel
Are DTB’s used in firmware today?

- **U-Boot / UEFI**
  - Updates available memory based on SoC specific probing
  - Updates the /chosen node

- **OP-TEE**
  - Adds /firmware/optee node in the DTB
  - Adds /reserved-memory/optee@0x12345678 node if needed
  - Updates passed DTB in place

- **ARM-TF**
  - Used by “plat-QEMU-virt”
  - Creates “/psci” nodes and assigns the “enable-method”
  - Passes the DTB to OP-TEE and UEFI
What’s next? Ideas, questions, issues?

- The proposals we have are
  - Apply the “QEMU” pattern on true hardware
- Where to modify DT?
  - DTS in kernel only? DTS copied to firmware and modified? In memory modifications only?
  - /proc/device-tree might look different compared to the dts-file. Tagging only a better idea? (see Peter Maydell’s devicetree/bindings/arm/secure.txt in kernel).
- What else do we need to think of?
  - Overkill to use libfdt in firmware? (ARM-TF#454)
  - Where are the bindings docs maintained?
  - FOTA updates, how to handle the DTB in firmware?
  - Read from flash once? Who? ARM-TF?
  - Splitting a DTB into several DTB’s?
Thank You

#BUD17

For further information: www.linaro.org
BUD17 keynotes and videos on: connect.linaro.org
joakim.bech@linaro.org - jens.wiklander@linaro.org