Using DTB Overlays in OPTEE

Bryan O'Donoghue
bryan.odonoghue@linaro.org

Linaro connect
Bangkok 2019

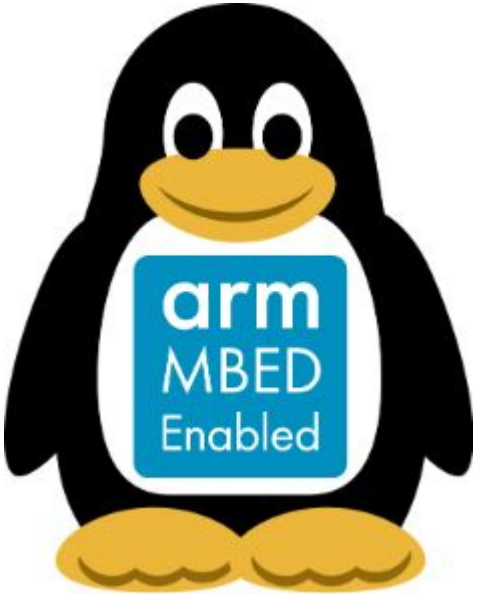
Introduction

Bryan O'Donoghue

- Based out of Dublin Ireland
- Avid Linux Geek
- Former Intel
- With Arm and Linaro for ~3 years now

Arm Mbed Linux OS (MBL)

- Arm Mbed Linux OS team based out of Cambridge UK
- A secure boot root of trust Linux system
  - Root of trust from reset vector
  - TF-A
  - OPTEE
  - U-boot FIT with signature checking
  - Linux Kernel
- Integrates with Arm Pelion for application update
- https://os.mbed.com/linux-os/



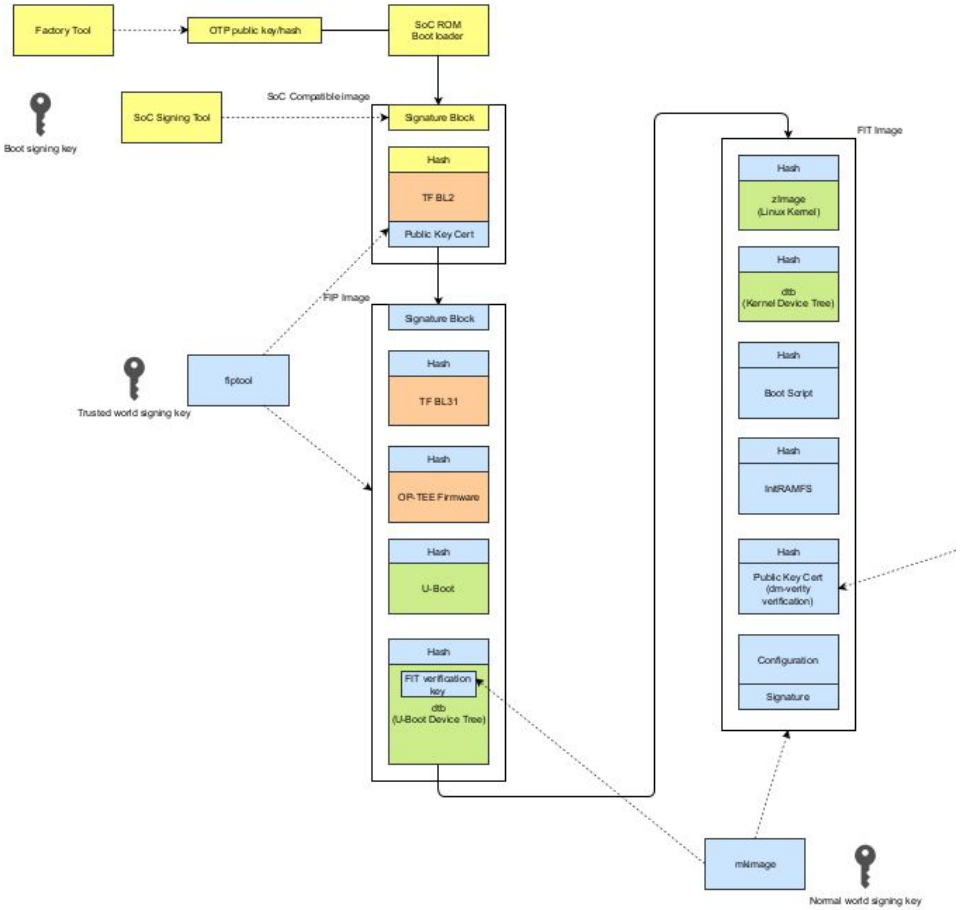
TrustedFirmware.org

OP-TEE.org

MBL Trusted Boot Flow

- A key goal is to be able to update components in as granular a way as possible
- Critically the kernel DTB should not live in the TF-A FIP
- Kernel DTB is to live in u-boot FIT

devicetree
.org



MBL Boot Flow

Arm32

- TF-A BL1
- TF-A BL2
  - FIP
    - BL32 OP-TEE
    - BL33 U-Boot
- BL32 OP-TEE
  - Switch to normal world
- BL33
  - FIT image
    - Load Kernel
    - Initramfs
    - DTB
- Linux Kernel

- OP-TEE wants to pass data to Linux via DTB
  - /memreserve/ 0x08000000 0x02000000; #SHMEM
  - /memreserve/ 0x10000000 0x01000000; #TZDRAM
  - `firmware { optee { … } }`
  - psci { `compatible = "arm,psci-0.2"; method = "smc"; };`
- Usually the DTB is passed from the TF-A to OP-TEE
- <u>Recall</u> the trusted boot requirements place the kernel DTB inside of the U-Boot FIT Image.

Solution is OP-TEE DTB Overlay

- OP-TEE provides a DTB overlay at a known location
  - optee_os/core/arch/arm/plat-imx/conf.mk
  - Config = mx7swarp7_mbl
  - CFG_DT_ADDR ?= 0x83100000
  - CFG_EXTERNAL_DTB_OVERLAY = y
- U-boot
  - Loads the Kernel DTB from the FIT image
  - imxtract ${bootscriptaddr}#conf@imx7s-warp.dtb fdt@imx7s-warp.dtb ${fdt_addr}
  - Then applies the OP-TEE provided DTB overlay
    - $fdt_addr = 0x83000000
    - $fdtovaddr = 0x83100000
  - fdt addr ${fdt_addr}
  - fdt resize 0x1000
  - fdt apply ${fdtovaddr}

Conclusions & Questions

- Using OP-TEE DTB overlay decouples the FIP and kernel DTB - awesome !
- Currently OP-TEE and u-boot agree on a fixed address
- Further work required to allow OP-TEE pass the address of the overlay as a parameter
- MBL will utilize this method as it more closely aligns with our Trusted Boot Requirements

Thank you

Join Linaro to accelerate deployment of your Arm-based solutions through collaboration

contactus@linaro.org

Linaro connect
Bangkok 2019