SW Architecture for Rich IOT
Corstone-700

Arm Central Engineering - Open Source Software

Tushar Khandelwal
April 2019
Agenda

• Corstone-700 : A Rich IOT platform
• System Architecture
• Example system
• Hardware Security
• Inter Processor Communication
• Software stack – an Example
• Example Boot flow
• Reference Implementation
• Future Stories
• Demo
• Questions ?
Corstone-700 : A Rich IOT platform

• Corstone-700 is a new Arm subsystem
  • Targeting SoC designs for more demanding IoT applications
  • Incorporates a mixture of flexible Cortex-A, Cortex-M compute and security features
  • Has a wide range of generic applications
    – A specific collaboration between Arm and Microsoft supports Azure Sphere compliant solutions

• The subsystem will be supported by a reference Open Source Software stack
  • Providing the foundations for generic product solutions
System Architecture

System example

Corstone-700 subsystem

A-Class subsystem

Firewall

MHU

ROM

Debug

System control

Power control

Security enclave M-Class

Expansion

Expansion

RAM

FW
Example System

Host System

RichOS

TEE

Secure Enclave

External system
Hardware Security

Firewall

• Firewall is to authenticate and filter accesses to different regions of the system address space in an SoC

Interrupt Router

• The Interrupt Router, is a programmable router for interrupts, located before two or more Interrupt Controllers in an SoC
Inter Processor Communication

**Host**
- Cortex A32
- Secure MHU
- Non Secure MHU
- GIC-400

**Secure Enclave**
- Cortex M0+
- MHU
- NVIC

**External System**
- Cortex M3
- MHU
- NVIC

Connections:
- Secure services from Host to Secure Enclave
- Non Secure services from Host to Secure Enclave
- Sensor Data from External System to Secure Enclave
- Non Secure services from Secure Enclave to External System
Software stack – an Example

- Cortex-M0+ (Secure Enclave)
- CMSIS
- RTX/TF-M
- OpenAMP using RPMsg
- Host - Cortex-A32
- IOT client + OpenAMP using RPMsg
- OpenEmbedded Filesystem
  Little FS
- Tiny Linux
- ARM Trusted Firmware
- TEE Services (optee)
- External system- Cortex-M3/33
- RTX/Zephyr
- CMSIS
- OpenAMP using RPMsg
Example Boot flow – Host and Secure Enclave

1. Flash Image
2. Release AP out of reset by writing jump address in Boot Reg
3. Boot
4. File System + IOT Client
5. Linux

Secure Services
- TEE Secure services
- Secure Monitor
- Linux
- File System + IOT Client

Non-Secure Services
- Non-Secure Services

SE BootROM
- SE initialization

Non Secure Service
- Secure Services
- Secure Mailbox
- Non Secure Mailbox

Secure Services
- TEE Secure Services
- Secure Services
- Secure Mailbox

Non Secure Service
- Secure Services
- Non Secure Mailbox
Reference Implementation

• Reference Implementation will be opensource.

• It will provide driver reference implementation and IP configuration.

• Stack will have software for all the three systems demonstrating boot and communication

• Yocto used for build and packaging of Images

• Public instructions will help interested partners to build and run on FPGA/FVP
Future Stories

• Secure Enclave – Root Of Trust (ROT)
• Secure Boot
• Firmware Update
• Trusted Firmware M
• PSA Compliance
• Secure Services
Demo
Questions ?