Securing Arm Servers

Matteo Carlini (Arm)
Agenda

- A little recap from SFO-201
- Introducing Secure Partitions
- Secure Partitions Software Architecture
- Trusted Firmware-A Updates: Secure Partition Manager
- Trusted Firmware-A Updates: SDEI & EHF
- EDK2: StandaloneMM & Arm MM Interface
- Arm System Guidance Platforms
- Arm SGI-575 Platform
- Secure Variable Access on Arm SGI-575
- Future evolutions
- References
A little recap from SFO17-201

Arm Trusted Board Boot vs UEFI Secure Boot

- TWO DISTINCT MECHANISMS:

Complete CoT – Putting all together

Secure Variable access

- EL0: Guest App1, Guest App2
- EL1: Linux Kernel A, Linux Kernel B
- EL2: UEFI Firmware – BL33
- EL3: Arm Trusted Firmware – BL31

Secure World
- TBB
- Secure Partition Manager
- Secure Partition Variable access
- Secure Storage
- KEK
- db/dbx
- TBB BL1
- S-EL0

Normal World
- S-EL0
- S-EL1
- S-EL2
- TBB BL2
- TBB SL2
- ROTPK SHA-256
- UEFI firmware
- Secure Boot
- Secure Boot
- Secure Boot

Linaro Connect Hong Kong 2018
Introducing Secure Partitions

● A Secure Partition is an unprivileged software sandbox environment running in the Secure World, under the control of privileged software, to instantiate PI Standalone Management Mode, in order to execute MM (secure) services.

● Use Cases
  ○ Secure Storage access
    ■ Secure Variables (Keys, Signatures, …)
    ■ Secure Firmware Update
  ○ Management Services
    ■ Errata handling
    ■ BMC communication
    ■ RAS Error Handling
  ○ RNG
  ○ Others?
Secure Partitions Software Architecture

- Main design goals:
  - Isolated execution context
  - Limited access to system resources
  - OS agnostic
  - Leverage Arm MM Interface Specification, Arm TrustZone & UEFI Standalone MM
  - Well defined interfaces
  - Code reuse between normal/secure world whenever possible
  - Reduced services code into privileged firmware (EL3)
Trusted Firmware-A Updates – SPM

- Secure Partition Manager (SPM) responsibilities:
  - Allocate resources requested by Secure Partitions
  - Perform architectural and system setup required by the Secure Partition to fulfil a service request
  - Implement standard interfaces (defined by current and upcoming specifications)
    - Used by the SPM for initialising a Secure Partition
    - Used by a Secure Partition to fulfil service requests
    - Used by the Non-secure world for accessing the services exported by a Secure Partition (MM Interface)

- SPM vs SPD:
  - SPM and SPD are mutually exclusive
  - SPD does NOT handle S-EL0 TAs: management left to Trusted OS at S-EL1
  - SPM instead takes directly care of all lifecycle of SPs (at EL3 today, potentially at S-EL2 in future evolutions)
  - SPM will track the evolutions of the Arm MM/Secure Partitions Specifications
Trusted Firmware-A Updates – SDEI & EHF

● Exception Handling Framework
  ○ A brand new framework for triaging RAS errors in EL3 prior to handling or delegation to lower ELs
  ○ RAS error interrupts & external aborts delegation through SDEI
  ○ v8.2 RAS extensions support (→ v8.4 RAS extensions coming next…)
  ○ It can be used by any event delegation mechanism

● Software Delegated Exception Interface dispatcher
  ○ Implements a Physical SDEI dispatcher into EL3 Runtime Firmware
  ○ Provides a mechanism to deliver high priority System events (Interrupts/Aborts) from EL3 to a registered Normal world SDEI Client (OS/Hypervisor)
  ○ Hooks into EHF as a way of delegating RAS errors to Normal world
  ○ Device RAS Driver is platform specific

● DRAM error handling prototyped on Arm SGI-575 (with DMC-620 RAS driver)

● RAS error handling in a Secure partition under development

● All upstream components (SPM, SDEI, EHF), included into Trusted Firmware-A v1.5 release (March 2018)
EDK2 – StandaloneMmPkg & MM

- **StandaloneMmPkg**
  - New package for hosting multi-arch support for Standalone MM (as per PI Specification v1.5 Volume 4: MM Core Interface)
  - Newly implemented support for AArch64 MM (based on prior work on x86 platforms [Smm*Pkgs])
  - Initially developed under edk-staging, now into edk2
    
    [https://lists.01.org/pipermail/edk2-devel/2018-February/021462.html](https://lists.01.org/pipermail/edk2-devel/2018-February/021462.html)

- **EFI_MM_COMMUNICATION_PROTOCOL**
  - AArch64 DXE runtime driver for communication between the Normal world firmware and the MM environment in the Secure world
  - Leverage the MM_COMMUNICATE SMC defined in the Arm MM Interface Specification
    
Arm System Guidance Platforms

- Integrated reference system designs for demonstrating latest Arm IP components
- Mobile, Infrastructure & IoT platforms
- Publicly released SGx FVPs (*Fixed Virtual Platforms*), that model the functionality of key components
  - “*Programmer’s View*” of processor, memory and peripherals
  - Allow early development on Arm IPs without the need for real HW
  - Provided under *End-User License Agreement*
  - Complete reference Software stack built and maintained by Arm
- SGI (SG for Infrastructure platforms) are a ready to go option to develop software on Armv8.2 Cortex-A cores
- SGx Platform support now going upstream into TF-A and UEFI EDK2
  - SGI-575 is now available!
  - Others to come out soon (SGI-572, SGM-775, …)
Arm SGI-575 Platform

- Reference platform for 2018 infrastructure solutions: Server, Networking, Storage

- Armv8.2-A based
  - 8x Cortex-A75 cores, 2x MP4 clusters
  - DynamIQ Shared Unit (DSU)
  - GIC-600, MMU-600
  - 2xDMC-620 (also for RAS errors injection)

- FVP Limitations
  1. No real hardware for secure storage
     - Must rely on a simple flash partition for variable/key storage
  2. No crypto engine integrated
     - All Software Crypto operations
  3. No CD-ROM drive mount point available
Arm SGI-575 Platform (2)

- Fully supported boot (from PCIe/SATA)
  - Fedora Enterprise 27
  - Debian 9.3
- KVM Hypervisor support
Secure Variable access on Arm SGI-575

Normal World

EL0
Applications

EL1
OS Kernel

Sign1

Set/GetVariable()

GetVariable()

MM_COMMUNICATE

Secure World

CryptoLib

NOR Flash Driver

VariableSmm

SPM shim

EL2

EDK2 Boot

EDK2 Runtime

VariableSmmRuntimeDXE

EDK2 Boot: Read Signatures

OS Runtime: (Authenticated) Read/Write Keys / SignaturesDBs

Secure Partition Manager

EL3

Arm Trusted Firmware

UEFI Variables in SGI-575 NOR Flash partition:
- Keys
- SignatureDB
Future evolutions (1) – Multiple Services

- Multiple parallel Secure Partitions enabling concurrent Secure Services to run simultaneously at S-EL0
- Each Secure Service into each SP is isolated from any other
- MM Interface will evolve into Secure Partition Client Interface (SPCI)
- SP Runtime interface (SPRT) in the Secure World
Future evolutions (2) – Multiple S-EL1

- Secure-EL2 in future Arm architectures (v8.4 onwards)
- Enable scenarios with multiple TEE/TOS running in parallel and TOS coexistence with MM services running into Secure Partitions at either multiple S-EL0 or multiple S-EL1
References

- SFO-201: Secure Boot on Arm systems
  - http://connect.linaro.org/resource/sfo17/sfo17-201/
- Arm MM Interface Specification
- Arm Trusted Firmware-A – Secure Partition Manager design document
  - https://github.com/ARM-software/arm-trusted-firmware/blob/master/docs/secure-partition-manager-design.rst
- Arm SDEI Specification
- Arm Trusted-Firmware-A – SDEI design document
  - https://github.com/ARM-software/arm-trusted-firmware/blob/master/docs/sdei.rst
- Arm Secure-EL2 extension
- Arm Fixed Virtual Platforms, including latest System Guidance for Infrastructure
- SGI-575 Platform support:
  - Arm Trusted Firmware: https://github.com/ARM-software/arm-trusted-firmware/pull/1319
  - EDK2-Platforms: Coming soon!
- SPCI-SPRT Specifications (alpha versions):
  - https://connect.arm.com/dropzone/systemarch/DEN0077A-Secure%5FPartition%5FInterface%5FSpecification-1.0alp0.pdf
  - https://connect.arm.com/dropzone/systemarch/DEN0078A-Secure%5FPartition%5FRuntime%5FSpecification-0.1alp0.pdf
Thank You
(matteo.carlini@arm.com)

#HKG18
HKG18 keynotes and videos on: connect.linaro.org
For further information: www.linaro.org