ARM TrustZone

SoC and IP

- SoC (System-on-Chip)
  - Tackles the provisioning of complex and application-specific, multifunctional processors
  - The major functional components of a complete end-product are integrated into a single chip
- Intellectual property (IP) modules
  - Pre-designed, reusable electronic components for hardware chips

SoC structure

- An SoC usually contains
  - Processors
  - IPs
    - Namely security IPs
  - Memory elements (RAM, ROM, etc.)
  - Buses

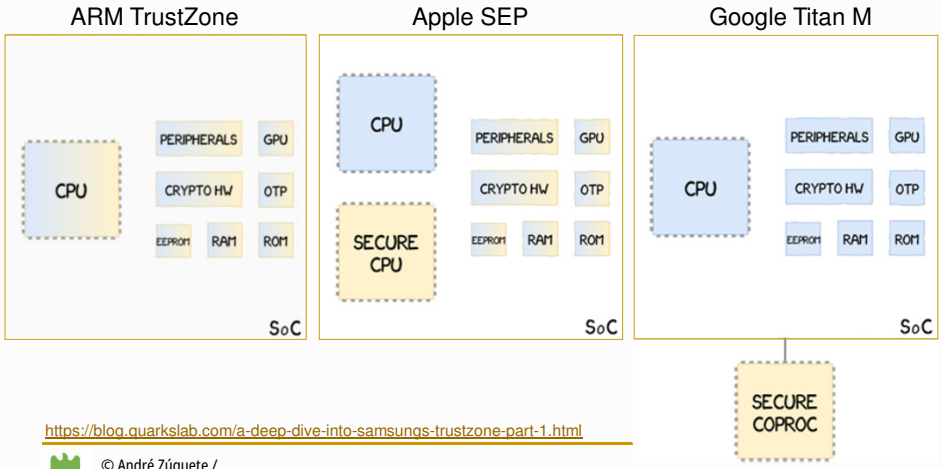
ARM TrustZone

- Set of technologies for packing special security features into a SoC
  - Extra security-related features on processor cores
    - Instructions
    - Bus lines
    - Execution levels
    - Extra logic for dealing with interruptions
  - Security-related IPs

ARM TrustZone: goal

- TEE for ARM-powered embedded systems
  - Providing hardware-based isolation
- It allows to run a trusted system in parallel with the main operation system
  - Rich OS
    - Where most applications will run
  - Secure (or Trusted) OS
    - Where secure (or trusted) applications will run
    - It can be a simple library, and not a full-fledged OS

ARM TrustZone: Comparison with other similar TEEs



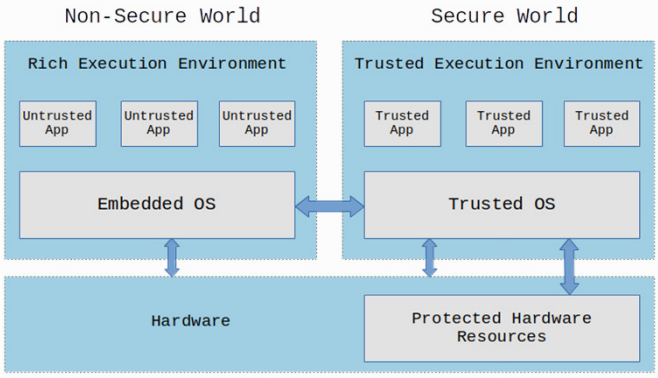
https://blog.quarkslab.com/a-deep-dive-into-samsungs-trustzone-part-1.html

Worlds

- Isolation is achieved by exploring the same CPU in two different worlds (or states)
  - Normal world → for running the Rich OS
  - Secure world → for running the Secure OS
- A CPU flag bit defines the current world
  - NS bit of the SCR (Secure Configuration Register)
  - 0 – Secure state
  - 1 – Non-secure state

Protected hardware resources

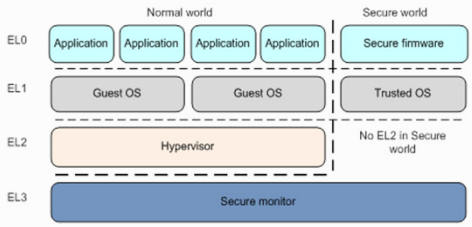
- Resources accessible only to the Secure OS



https://embeddedbits.org/introduction-to-trusted-execution-environment-tee-arm-trustzone

ARM (v8) exception levels

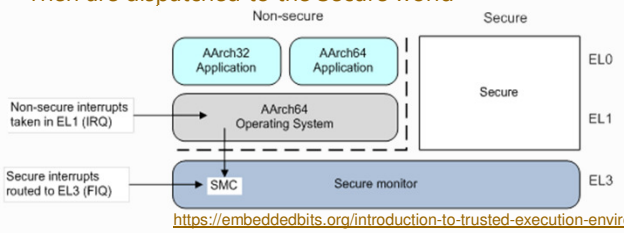
- Similar to run levels
- TrustZone introduces one EL more
  - Secure monitor (EL3)
- Combination of exception levels and states



https://embeddedbits.org/introduction-to-trusted-execution-environment-tee-arm-trustzone

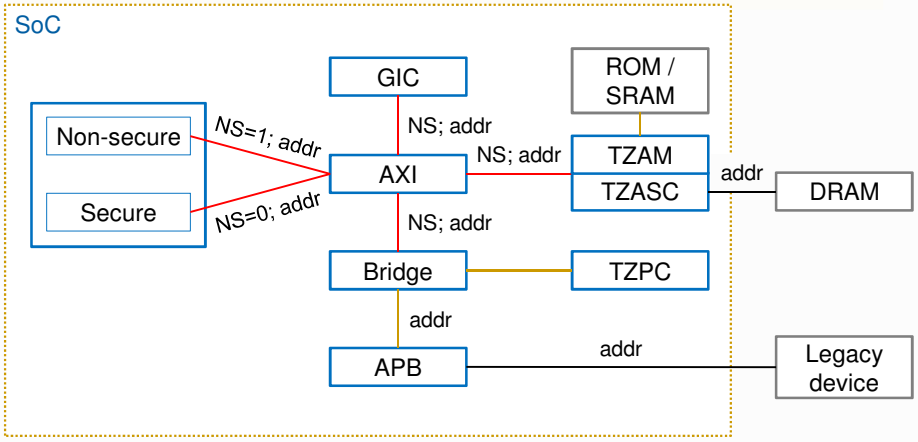
Access to the Secure world

- Calls from the Rich OS
  - SMC (Secure Monitor Call)
  - Typically implemented by Rich OS drivers
- Interrupts from the Secure hardware
  - Must be handled by the Secure OS
- Both enter first in EL3
  - Then are dispatched to the Secure world

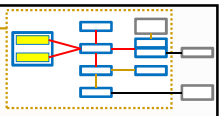


https://embeddedbits.org/introduction-to-trusted-execution-environment-tee-arm-trustzone

Architecture overview

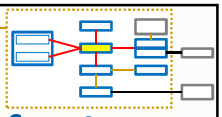


Architectural details: MMU / TLB / Cache Controllers

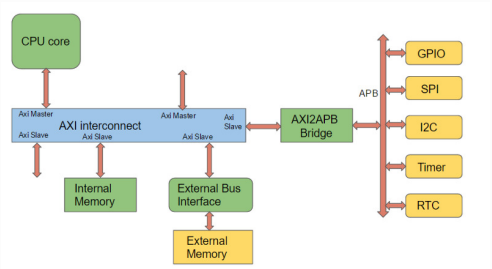


- 2 separate, virtual MMUs
  - Indexed by NS
- Single TLB
  - But entries keep the value of NS that created them
  - No need to invalidate them when switching between worlds
- The Secure world can still access non-secure memory
  - Extra bit on each entry in the secure translation table
- Single cache
  - Cache lines keep the NS address bit

Architectural details: AXI (Advanced eXtensible Interface)



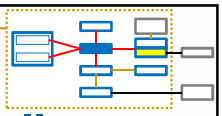
- SoC internal bus



- Extra NS line for secure read/write operations
  - Non-secure master cannot access a resource marked as secure

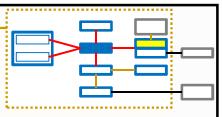
https://anysilicon.com/understanding-amba-bus-architecture-protocols

Architectural details: TZASC (TZ Address Space Controller)



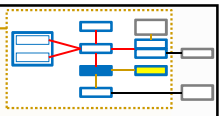
- Allows a dynamic classification of AXI slave memory-mapped devices as secure or non-secure
  - Partitioning of single memory units
- Controlled by the Secure world

Architectural details: TZMA (TZ memory Adapter)



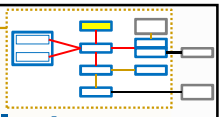
- Keeps a classification of in-SoC memory areas as secure and non-secure
  - ROM or SRAM
- Non-secure accesses cannot access secured memory areas
- Controlled by the Secure world

Architectural details: TZPC (TZ Protection Controller)



- Allows to dynamically set the security of a peripheral connected to the APB (Advanced Peripheral Bus)
  - Protects non-secure access requests to reach peripherals marked as secure
- Controlled by the Secure world

Architectural details: GIC (Generic Interrupt Controller)



- Classifies interrupts as secure or non-secure
  - Once set, cannot be changed
- Interrupts can be normal or fast (high-priority)
  - Secure interrupts usually have higher priority
- Interrupts with a security classification different from the current world force the switching to Monitor (EL3)
- Controlled by the Secure world

TrustZone bootstrap

- A TZ-enable ARM SoC boots on the secure world
  - It allows a the Secure world to configure the TZ-related components to enforce a given security policy
- The configuration data can be
  - Embedded in the SoC ROM
  - Provided by external peripherals and validated with information in SoC ROM
    - e.g. must contain a signature validated with a in-SoC public key