Arm Trustzone

Gary Jessop III

TEE

Trusted Execution Environment

INTEL – SGX
AMD - Secure Execution Environment
ARM - Trustzone

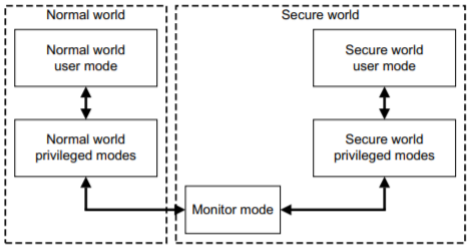


Figure 3-1 : Modes in an ARM core implementing the Security Extensions

Exeptions and Securebits

Exception Levels

The higher the number the more privileges given

When exceptions occur it branches to a vector table to run a handler for that exception

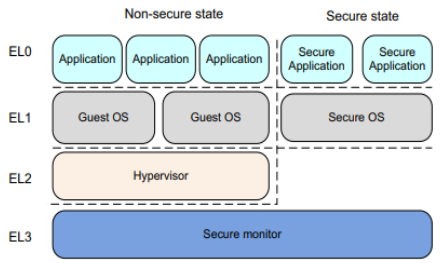
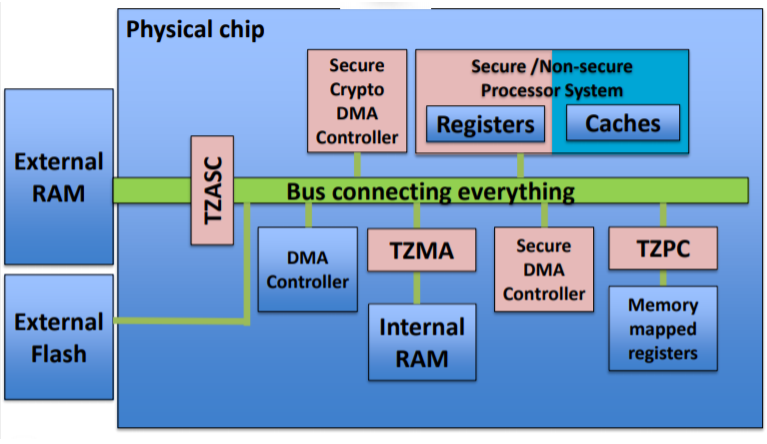


Figure 17-5 Security model when EL3 is using AArch64

Overview



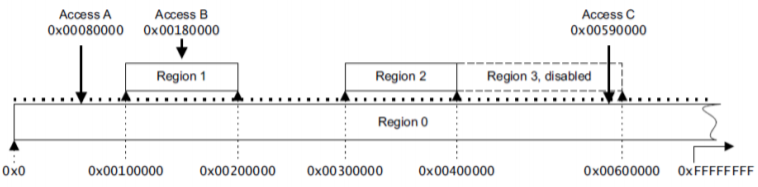
System Bus

AMBA3 AXI
- Extra control signal for the read and write channels of the bus
- NS bit
  - AWPROT[1]: Write transaction – low is Secure and high is Non-secure
  - ARPROT[1]: Read transaction – low is Secure and high is Non-secure

AMBA3 APB
- Secure peripheral bus
- NS bit
  - AWPROT[1]: Write transaction – low is Secure and high is Non-secure
  - ARPROT[1]: Read transaction – low is Secure and high is Non-secure

TZSAC

Trustzone Address Space Controller
- Split external RAM in regions Region 0 covering everything,
- Region 1-8 configurable Each region can be configured to allow:
  - Secure read
  - Secure write
  - Non-Secure read based on ID
  - Non-Secure write based on ID



TZPC & TZMA

TZPC (Trustzone Protection Controller)

- Allows control of TZMA
- Configuration of hardcoded data

TZMA (Trustzone Memory Adapter)

- Controls the regions of internal ram

Flaws – Design Implementation

Qualcomm

Had a secure loading feature retro engineered before release

Nintendo

jamais vu and déjà vu

Arbitrary TrustZone/BootROM code execution

Resources

- https://www.trustonic.com/news/technology/what-is-trustzone/
- https://genode.org/documentation/articles/trustzone
- https://www.microcontrollertips.com/embedded-security-brief-arm-trustzone-explained/
- https://www.youtube.com/watch?v=ecBByjwny3s
- https://gbatemp.net/threads/nintendo-switchs-arm-trustzone-explanation-by-yifanlu.463524/http://www.openvirtualization.org/open-source-arm-trustzone.html
- https://cs140e.sergio.bz/docs/ARMv8-A-Programmer-Guide.pdf
- http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf
- https://usermanual.wiki/Document/ARMArchitectureReferenceManual.754195650/view