TEEP BOF
ARM TrustZone

Hannes Tschofenig

28th March 2017 -- IETF 98th, Chicago

ARM Architecture Profiles

Application Profile ARMv8-A

- 32-bit and 64-bit
- A32, T32 and A64 instruction sets
- Virtual memory system
- Supporting rich operating systems

Real-time Profile

ARMv8-R

- 32-bit
- A32 and T32 instruction sets
- Protected memory system

  (optional virtual memory)
- Optimized for real-time systems

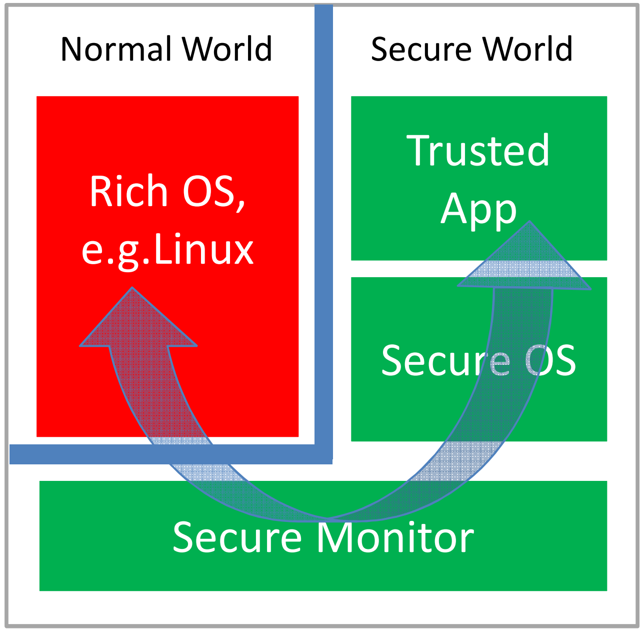
Microcontroller Profile

ARMv8-M

- 32-bit
- T32 / Thumb® instruction set only
- Protected memory system
- Optimized for microcontroller applications

TrustZone

- The TrustZone architecture was introduced as an extension to ARMv6.
- Included in ARMv7-A.
- Latest architecture is ARMv8-A.
- Isolates memory maps and extends to bus and peripherals.



Open source code available: ARM Trusted Firmware - https://github.com/ARM-software/arm-trusted-firmware/ and Opt-TEE - https://www.op-tee.org

References

- Useful background information but not needed for IETF work or implementation.
- ARM TrustZone Whitepaper:
  - http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf
- GlobalPlatform:
  - https://www.globalplatform.org/specificationsdevice.asp