Enhancing Trusted OS porting to RISC-V architecture using hypervisor

SAMSUNG

The GOAL

Port existing TrustedOS from ARM to RiscV quickly and efficiently

arm → RISC-V

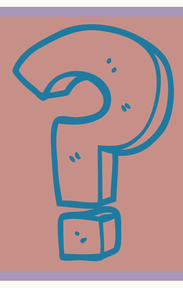
Risc-V challenges

- RISC-V has no built-in support for Secure World transition
- Memory separation between Normal and Secure World needs custom solution
- RISC-V architecture favors full virtualization

Hypervisor options

KVM

Xvisor eXtensible Versatile hypervISOR



KVM

- Type-2 hypervisor
- Poorly suited for small embedded systems
- Requires one additional kernel to operate

REJECTED

Xvisor

- Type-1 hypervisor
- 1st attempt - VTNet and ethernet stack between OSes
  - significant overhead(copy of the data for operation)
- 2nd attempt - RPMSG and shared memory , mailboxes between OSes
  - shared memory space exposed and vulnerable
- Potential solution
  - create shared memory space per application basis

REJECTED

SAMSUNG

The Solution

- Semi-hypervisor with cpu and memory isolation
- Memory isolation using PMP reconfigured during switch
- ECALL extension as a replacement for arm's SMC
- Cooperative model for switching worlds
- Shared memory created per application basis

Authors: Piotr Lipiak (p.lipiak@partner.samsung.com) Paweł Kulig (p.kulig@partner.samsung.com)