linaro™

Arm Solutions at Lightspeed

Core Collective

Confidential Computing

Update - July 20th

Mathieu Poirier - Linaro

Progress Updates

- QEMU - System Emulation
  - 2 patchsets have been submitted to the spdm-emu project **have been merged**
    - Goal: Properly support TDISP in QEMU
    - Patchset 1: Adding the mechanic needed to expose TDISP state to QEMU device
    - Patchset 2: Adding support to convey device PCIe configuration to spdm-emu
  - Work continues to integrate the TDISP state machine with QEMU devices
    - What TDISP state is a device in?
    - Properly set the ‘T’ bit on PCIe DMA transaction when a device is in locked state

- Shrinkwrap support for QEMU
  - Work is ongoing → limited funding, limited progress

Progress Update

- QEMU - VMM
  - Foundational solution to start a Realm using the QEMU-VMM **was released publicly**
  - [RFC v1] is here
  - Specifics: RMI 2.0, RSI 1.1, upstream kernel release: ~~V13~~ **V14**
  - No support for Device Assignment

- Currently working on
  - Addressing comments from [RFC v1]
  - Providing QEMU support for V15 released on July 15th
    - System emulation
    - VMM (with new guest_memfd interface)
  - Release of [RFC v2] as soon as we are done with the above
  - Public release of instructions to build the solution using Shrinkwrap

Backlog (NO CHANGES)

- Device Assignment work
  - TF-A and RMM support for SBSA architecture with SMMU on Arm's latest DA branch
  - QEMU VMM device assignment support with Realms
  - Depends on a stable baseline (kvmtool, TF-A, RMM, kernel) from Arm
- QEMU support for Boot Sync
- Enhance QEMU Live Migration support to Realms
- Planes → coconut-svsm on Arm64
- Integration of the kernel's device security module with Veraison (3rd party authentication)
- Confidential Containers


linaro
linaro
linaro