Keystone Annual Review 2024

Confidential Computing Consortium

Lily Sturmann lsturman@redhat.com

Dayeol Lee dayeolee@gmail.com

Goals of the Project

- ❑ Enable TEE on (almost) **all RISC-V processors**
  - ○ Follow RISC-V standard ISA
  - ○ Standard TEE specification for various RISC-V sub-ISA
- ❑ Make TEE **easy to customize** depending on needs
  - ○ Base implementation vs. platform-specific implementation
  - ○ Reuse the implementation across multiple platforms
- ❑ **Reduce the cost** of building TEE
  - ○ Reduce hardware integration cost
  - ○ Reduce verification cost
  - ○ Integrate with existing software tools

Annual Review

- ❑ Basic Info:
  - ○ Current Stage: **Incubation**
  - ○ Mentor: **Lily Sturmann**
- ❑ Technical Charter
- ❑ Progression Status
- ❑ Budget Allocation
- ❑ License Scans
- ❑ OpenSSF Best Practices Badge

Annual Review

- ❑ Basic Info:
  - ○ Current Stage: **Incubation**
  - ○ Mentor: **Lily Sturmann**
- ❑ Technical Charter → Unchanged
- ❑ Progression Status
- ❑ Budget Allocation
- ❑ License Scans → Unchanged
- ❑ OpenSSF Best Practices Badge

Key Milestones from the Previous Review

- Better application support
    - Dynamic library support
- Parity with industry standards
    - Standard crypto for measured boot / attestation
- Increase dev board accessibility
    - Participate in RISC-V development board program
    - Expecting a supply chain relief in mid 2023
- Work closely with RISC-V AP-TEE working group
    - Not directly relevant, but they are interested in pushing towards server-class RISC-V TEE in the future

Annual Milestone Review

- ❑ [On Track] Better Hardwasre/Application Support
  - Dynamic loading of binaries PR#326 PR#415
  - Keystone BR2 External RFC PR#323
  - [WIP] Structured measurement
- ❑ [Off Track] Parity with Industry Standard
  - Lagged because unable to make informed decision
- ❑ [Establishing] Collaborate with External Entities
  - [Establishing] RISC-V SMMTT Standard WG (+ Rivos)
  - [Off Track] RISC-V AP-TEE WG

Growth Goals towards Graduation Stage

- Technical Improvements
  - [WIP] Application/hardware support
  - [WIP] Improve memory isolation
  - [Not Started] HW integration (HW-based encryption, measured boot)
- Maintenance
  - Version planning
  - Contributor program
  - Reliable contribution pipeline (e.g., CI/CD, documentation, etc)
- Inclusion and Diversity
  - Outreachy Intern (end of year round)
  - Open communication channel
  - Community meetings

Budget Allocation

- ❑ GitHub Team
  - ○ $1672 / year

    (<$880 if we kick out non-active members)
- ❑ Test Infrastructure
  - ○ RISC-V hardware platforms for CI/CD (~$2500)
- ❑ Video conferencing support (TBD)
  - ○ Zoom account for community meetings
- ❑ Open Communication Channel
  - ○ TBD

Thank You!