Keystone Annual Review 2023

Confidential Computing Consortium

Lily Sturmann lsturman@redhat.com

Dayeol Lee dayeolee@gmail.com

Keystone

CONFIDENTIAL COMPUTING CONSORTIUM

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

Remarks

- ❑ Code Maintenance
  - Switched to monorepo: for a better developer experience
  - Bump OpenSBI v1.1
- ❑ The project have been very slow in 2022
  - Five people from UCB graduated at the same time, and four of them left the project
  - Less momentum from the industry
- ❑ Keystone is still a popular option in academia
  - Gained 133 yearly citations (+28% YoY)
  - 100+ forks mostly from researchers

Subproject Status

2022 Projects

Trusted Loader and Dynamic Library
Cathy Lu, Anay Wadhera → Evgeny Pobachienko

Improving Measured Boot and Attestation
Rohit Mittal → Jakob Sorensen

~~Scalable Memory Isolation with RISC-V H-extension~~
~~Aniruddha Alawani~~

~~Preventing Side-Channel Attacks on Dynamic Libraries~~
~~Cathy Lu~~

Churn

New Project

Add Keystone Support to VMWare Certifier Framework (Pending)
Jakob Sorensen, Evgeny Pobachienko

Why is the Project Stuck?

- ❑ Tight Coupling with RISC-V
  - ○ Lack of Development Board
  - ○ Many focused on low-end devices which is not Keystone is aiming for
  - ○ RISC-V specification is still changing; no software standard yet
- ❑ Lack of Industry Contribution
  - ○ Code quality geared toward research (not maintainability)
  - ○ People leave the team after 1-2 years (usually at the same time)
- ❑ Lack of Application Demand
  - ○ RISC-V software ecosystem is still growing, and the application demand is weak

Key Milestones for 2023

- 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

Thank You!