Implementation of a TEE on a RISC-V embedded processor

TEEs (*Trusted Execution Environments*) allow developers to create *enclaves* where the code execution is controlled. Such mechanisms can be resistant to software attacks and are already available in commercial processors such as the ARM TrustZone. We would like to get a better understanding of hardware and software requirements of using such a protection in a softcore processor based on the RISC-V standard.

Within the RISC-V ecosystem, several processor implementations are proposed by the community. Regarding TEEs, Keystone is an open-source initiative aiming to get enclaves similar to those available in ARM TrustZone. We would like to get a proof-of-concept of a RISC-V compatible TEE such as Keystone with a collection of code samples demonstrating its security features and, if possible, some weaknesses.

Main goals for this internship are:

- Studying TEEs that could be used with a RISC-V system-on-chip.
- Analyzing processors supporting these TEEs. We should focus on OpenHwGroup CVA6 (capable of running Linux).
- Implementing a System-on-Chip with the RISC-V processor and the TEE. First, targeting a Verilator model. Then, targeting a FPGA implementation on a real board.

Depending of the internship progress, extensions can be studied:

- Adding a new enclave to the TEE with different permissions.
- Adding a multi-domain protection. This part is an extension of the work done by a former PhD student in the lab.

The internship will be done in the context of the ANR SCAMA project where a PhD student is also working in our facilities.

Internship information

- Requirements: C, scripting language and a HDL language at least (ideally SystemVerilog).
- 5 to 6 months internship at ENSTA Bretagne (Brest, France). Begins in Spring 2025.
- Applications opened until filled. **Please submit a curriculum, motivation letter and master grades**.

References

1. Pinto et al. Demystifying ARM TrustZone: A comprehensive survey. 2020.
2. Keystone Enclave : https://keystone-enclave.org/
3. CVA6 : https://github.com/openhwgroup/cva6
4. Suzaki et al. TS-Perf: General Performance Measurement of Trusted Execution Environment and Rich Execution Environment on Intel SGX, Arm TrustZone, and RISC-V Keystone. 2021.

Contacts

- Pascal Cotret: pascal.cotret@ensta-bretagne.fr, ENSTA Bretagne / Lab-STICC.
- Vianney Lapôtre: vianney.lapotre@univ-ubs.fr, Université de Bretagne-Sud / Lab-STICC.