Implementation of a TEE on a RISC-V embedded processor

TEEs (*Trusted Execution Environments*) allow developer to create enclaves in which the code execution is controlled. Such mechanisms are resistant to some 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 this kind of 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 Keystone capabilities with a collection of code samples demonstrating its security features.

Main goals for this internship are:

- Studying the Keystone TEE and tutorial for the Qemu emulator.
- Analyzing the processors supporting Keystone. We should focus on OpenHwGroup CV32E40S (including security mechanisms) and/or CVA6 (capable of running Linux).
- Implementing a System-on-Chip with the RISC-V processor and the Keystone TEE. First, targeting a Verilator model. Then, targeting a FPGA implementation.

Depending of the internship progress, extensions can be studied:

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

The internship may be extended with a PhD within the lab.

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 2024.
- **European nationality is mandatory**.
- Applications opened until filled. Please submit a curriculum, motivation letter and master grades.

References

1. Demystifying arm trustzone: A comprehensive survey. https://sandro2pinto.github.io/files/acmcsur2019-tz.pdf.
2. Keystone Enclave : https://keystone-enclave.org/
3. CVA6 : https://github.com/openhwgroup/cva6
4. CV32E40S : https://github.com/openhwgroup/cv32e40s

Contacts

- Pascal Cotret, ENSTA Bretagne / Lab-STICC.
- Vianney Lapôtre, Université de Bretagne-Sud / Lab-STICC.