# Fault injection attacks on RISC-V microcontrollers

**Keywords**: Hardware security, fault injection, RISC-V.

**Context and motivation**:

In the context of hardware security, fault injection can be defined as a powerful physical attack, possibly non-invasive, where the attacker will try to change the normal behavior of the device during program execution by introducing one or more faults, then observing the erroneous behavior, this behavior can be further exploited as a vulnerability. The injection process can be done in different ways: exposing the device to radiations, laser beams, intense light, or an electromagnetic (EM) pulse, inducing variations in the power supply or in the clock signal, changing the environmental conditions such as the temperature, etc. [1].

Securing microprocessors and microcontrollers against such attacks requires a comprehensive understanding of the faults and their effects; this means characterizing, studying, and analyzing the faults that could lead to exploitable code vulnerabilities. On the other hand, it also requires designing countermeasures at different system levels; hardware and software, with reasonable costs [2].

In the project ARSENE[1] (Architectures Sécurisées pour le Numérique Embarqué) lot1, we aim at providing a cross-layer analysis of code and microarchitectural vulnerabilities while performing fault injection and simulation at distinct levels of RISC-V architectures, following the proposed methodology in [2]. This will help in validating the use of the fault models proposed in [3,4] when targeting different architectures from Arm Cortex-M processors, and, if necessary, proposing new models that match more the RISC-V architectures. The use of such fault models will facilitate performing vulnerability analysis of software codes and hardware designs. Thus, helping in designing countermeasures at an appropriate cost.

In this internship, the main tasks will be:

- Understanding the RISC-V architectures and its ISA in general, in addition to make a review on the existing physical fault injection attacks on RISC-V processors
- Conducting fault injection campaigns on RISC-V microcontrollers, using different injection means (e.g., clock glitch, voltage glitch, and EM pulses).
- Analyze the obtained results in order to confirm the use of existing fault models and/or proposing new ones.

**Who can apply**: Applicants must be enrolled in a Master's degree in cyber security, computer engineering, or embedded systems and have interests in hardware security.

**Required Skills**

- Processors architectures
- Embedded programming and microcontrollers
- C and Assembly programming
- Script languages (Python)
- Knowledge of hardware attacks is a plus.

**Internship duration:** 5 to 6 months (starting February 2024)

[1] https://www.pepr-cyber-arsene.fr/

**Internship location:** LCIS laboratory, Valence, France.

**Financing:** About 600€ per month.

**For more info or in case you are Interested:**

please contact or send your CV to:

ihab.alshaer@univ-grenoble-alpes.fr

**Bibliography:**

[1] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, “Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures,” Proceedings of the IEEE, vol. 100, no. 11, pp. 3056–3076, 2012.

[2] I. Alshaer, B. Colombier, C. Deleuze, P. Maistri, and V. Beroulle, “Cross-layer inference methodology for microarchitecture-aware fault models”, Microelectronics Reliability, Volume 139, 2022, 114841.

[3] I. Alshaer, B. Colombier, C. Deleuze, V. Beroulle, and P. Maistri, “Variable-length instruction set: Feature or bug?” in 25th Euromicro Conference on Digital System Design (DSD), IEEE, Maspalomas, Spain, 2022, pp. 464-471.

[4] I. Alshaer, B. Colombier, C. Deleuze, V. Beroulle, and P. Maistri, “Microarchitectural Insights into Unexplained Behaviors under Clock Glitch Fault Injection”. Smart Card Research and Advanced Applications - 22th International Conference, CARDIS 2023, Amsterdam, Netherlands, Springer, Ed, 2023.