Internship Position

RTL Countermeasures against fault injection attacks

Keywords: Hardware security, fault injection, RTL fault simulation, countermeasures.

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 has physical access to the device or its surrounding environment. The attacker will try to change the normal behavior of the device during program execution by injecting one or more faults, then observing the erroneous behavior, this behavior can be further exploited as a vulnerability [1]. 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. [2].

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 [1].

In the project CLAM (Cross-layer fault analysis for microprocessor architectures), we aim at providing a cross-layer analysis of code and microarchitectural vulnerabilities while performing fault injection and simulation at three distinct levels: physical, RTL and software. This will help in evaluating the realism of the already existing fault models and proposing new ones. Such fault models can be used to perform vulnerability analysis of software codes and hardware designs. Thus, helping in designing countermeasures at an appropriate cost.

Already adapted software fault models have been proposed [3]. Moreover, RTL fault models also have been proposed. The proposed fault models (software and RTL) allow obtaining identical results to the results obtained by physical fault injections.

In this internship, the main tasks will be:

- Understanding the RTL description for an ARM Cortex-M processor. (The access to the RTL description will be provided under the ARM Academic Access Agreement)
- Designing low-cost and efficient countermeasures at the RTL level based on the proposed RTL fault models.
- Conducting RTL fault simulation campaigns of the processor for the countermeasure evaluation.

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

- Microprocessor architectures.
- Verilog/VHDL.
- Script languages (TCL).
- Hardware design and simulation tools (e.g., ModelSim & Vivado).
- Knowledge of hardware attacks is a plus.

Internship duration: 5 to 6 months (starting February 2023)

Internship location: LCIS laboratory, Valence, France.

Financing: About 550€ 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] I. Alshaer, B. Colombier, C. Deleuze, V. Beroulle and P. Maistri, "Microarchitecture-aware Fault Models: Experimental Evidence and Cross-Layer Inference Methodology," *2021 16th International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS)*, 2021, pp. 1-6.

[2] 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.

[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, Ed., 2022