Internship Position

Fault Simulation and Injection on Microprocessor Architectures

Keywords: Hardware security, fault injection, simulation, microarchitectures.

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 a program execution by injecting one or more faults, then observing the erroneous behavior [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's 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 possibly propose new ones. Such methodology will also help in designing countermeasures at an appropriate cost. A preliminary analysis has already been started by performing fault injection using clock glitch on different ARM Cortex-M processors, studying the related RTL to perform simulation using QuestaSim tool, and analyzing the fault effects at both levels.

In this internship, the main tasks will be:

- conducting RTL fault simulation campaigns for different targets (Cortex-M and RISC-V),
- performing fault injection campaigns using other techniques, such as: EM pulses and Voltage glitching, and
- to automate the injection campaigns, the analysis and the results' comparisons to make the study more exhaustive.

Such exhaustiveness will help in taking the decisions related to the fault models and proposing new ones if possible. The intern is going to work with our team on a part of these tasks.

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

Required Skills

- Microprocessor architectures,
- Low level programming (C and Assembly),
- Script languages (Python and basic TCL).
- Database management is a plus,
- Knowledge of hardware design, simulation and debugging is a plus.

Internship duration: 6 months (starting February 2022)

Internship location: LCIS laboratory, Valence, FRANCE.

Financing: About 530€ per month.

For more info or in case you are Interested:

please contact or send your CV to:

ihab.alshaer@lcis.grenoble-inp.fr

christophe.deleuze@lcis.grenoble-inp.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.