Fault attack analysis and countermeasure design against clock glitch for RISC-V core

Keywords: Hardware security, fault injection, RTL fault simulation, countermeasures, digital design

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 [3].

In the ARSENE project [4], we aim at designing secure microprocessor for IoT nodes using 32b RISC-V core. Based on already developped cores from the OpenHW Group, such as the CV32E40P core, we study fault effect and their characterization to propose countermeasures against such physical attacks. An attack campaign was already carried out, but we lack details on what is happening at the RTL level. Using fault model at the RTL level, we design low cost countermeasures against clock glitch fault injection.

The goal of the internship is to to analyze and determine which registers are the most susceptible to fault injection leading to security compromise. Based on the already carried out attacks, the intern will simulate the core and inject fault to reproduce the same attack effects such as instruction skips, register corruption, etc. In a second time, the intern will propose and design countermeasures suited to the determined fault model. The intern will study the state of the art for countermeasure against clock glitch, implement one or several countermeasures and assess their effectiveness.

In this internship, the main tasks will be:

- Understanding the RTL description for the CV32E40P RISC-V core
- Conducting RTL fault simulation campaigns
- Analyze and determine fault effect at RTL level and propose a fault model
- Perform a brief summary of the state of the art for countermeasures against clock glitch fault
- Design and implement the countermeasure
- Perform fault injection attack to rate effectiveness of the countermeasure

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
- SystemVerilog, Verilog or VHDL
- Hardware design and simulation tools (e.g. Modelsim or Questasim)
- C and assembly
- Knowledge of hardware attacks or RISC-V ISA is a plus

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

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:

valentin.egloff@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.

[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

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