Master 2 Internship proposal

Fault attack analysis and countermeasure design for RISC-V core on FPGA

Keywords: RISC-V, Hardware security, fault injection, FPGA prototyping, ChipWhisperer, countermeasures and digital design

Contact: Valentin Egloff (valentin.egloff@lcis.grenoble-inp.fr), LCIS laboratory, Valence, France

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].

To secure microprocessors and microcontrollers against such attacks, we developed a comprehensive model of faults and fault effects. This includes characterization and analysis of faults that could lead to exploitable code vulnerabilities [3].

In the ARSENE project [4], we aim at **designing secure microprocessor** for IoT nodes using 32 bits **RISC-V core**. Based on already developed cores from the OpenHW Group, such as the CV32E40P core, we want to propose new **efficient and fair cost countermeasures** against such physical attacks. Several attack campaigns have been already carried out on a RISC-V ASIC (SiFive FE310-G002), and we understand most of the faults which explain faulty behaviors both at the RTL or ISA levels. Using this knowledge, we want to **design and assess new low cost countermeasures against clock, voltage or EM glitch fault injection.**

The intern will implement a RISC-V CV32E40P microarchitecture on FPGA ChipWhisperer board (CW305), test it and perform fault injection campaigns (clock or voltage glitches or EM pulse) using ChipWhisperer capabilities. Faulty behavior will be compared with previous observed faulty behaviors on RISC-V ASIC. Then, the intern will propose and design countermeasures suited to the determined fault model and assess their effectiveness using the FPGA ChipWhisperer board.

In this internship, the main tasks will be:

- Prototyping RISC-V core (CV32E40P) in FPGA
- Conducting fault injection campaigns using ChipWhisperer environment
- Analyzing and determining fault effect and compare with existing fault models
- Design and implementation of countermeasures
- Performing fault injection attacks to rate effectiveness of the countermeasures

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

Required skills:

- Microprocessor architectures
- Hardware design language (SystemVerilog, Verilog or VHDL)
- Hardware design and simulation tools (Vivado, Modelsim)
- 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, in CTSYS team (https://lcis.fr/ctsys)

Laboratoire LCIS, 50 Rue Barthélémy de Laffemas, 26902 Valence cedex 9, France

Financing: About 650€ per month.

For more information 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. https://hal.science/hal-03272932/file/Alshaer_DTIS_2021.pdf

[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. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=29050fd746a23979437c9f358ba143377a3d5e39

[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), pp. 464-71, Maspalomas, Spain: IEEE, 2022. https://hal.science/hal-03775870/file/2022118900-cr.pdf

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