Modeling and Characterizing Fault Attacks exploiting the Memory Architecture

2023-2024

VERIMAG Laboratory (Grenoble – France)
Team PACS (Proofs and Code Analysis for Security)
Advisors: Bruno Ferres & Pierre Corbineau
bruno.ferres@univ-grenoble-alpes.fr
pierre.corbineau@univ-grenoble-alpes.fr
Keywords: Hardware security; micro-architecture; simulation; fault models

Context

Fault injections (using laser beams, EM injection, or even purely software attacks) are a real threat against all embedded systems [1, 2]. To protect the code, or evaluate the robustness of components, fault simulators are crucials tools when exploring possible effects of an attack, or to exhaustively check that no attack path has been left aside [3].

A few fault simulators at software level do exist, including CELTIC, developped in CEA-LETI [4]. However, they are often limited to very simple use cases, and do not allow using them in realistic contexts, for security evaluation. For example, peripherals, interrupts or trusted zones in embedded components — *i.e.*, the micro architectural details of the systems — are usually not taken into considerations.

Fault models currently under considerations are usually applied to a functional specification of the program execution — *i.e.*, ISA level (*Instruction-Set Architecture*). Yet a growing number of attacks are actually based on lower level characteristics of the processors architectures (memory hierarchy, buffers, pipelines).

Goals of the Internship

Several reserach directions are hence left open:

- Model: how can we efficiently simulate how the faults impact the micro-architecture?
- Characterization: how can we experimentally distinguish those faults from other, more common faults?
- Protection: which counter-measures (notably at software level) may we consider? How can we harden the program?

The internship will rely on preliminary works from the team, and may take various directions, depending on the interests of the applicant.
Depending on the direction taken, as well as the progress of the internship, physical experimentations in collaboration with CEA-LETI might be considered, to evaluate the relevance of the studied fault models.
This internship may lead to a pursuit for a Ph.D. thesis in the context of the national projects SecurEval and Arsene, which aim at developping tools to build and evaluate the robustness of embedded systems with respect to state-of-the-art attacks.

Ideal Applicant

This internship proposal is for Computer Science students, ideally at M2 level[1] (or last year of engineering school).
The applicant must be proficient in the following knowledge/skills:

- good programing skills in C/C++
- strong knowledge in processor architectures

Moreover, any interest in topics linked to computer security (hardware security, program hardening, *etc.*) is a real plus. However, the applicant may acquire those skills during the internship.

Applications

To apply, send an email to pierre.corbineau@univ-grenoble-alpes.fr and bruno.ferres@univ-grenoble-alpes.fr, with your resume, a short covering letter, as well as any document that may support your application.

Location

The internship will take place in VERIMAG laboratory, located in the campus of Grenoble:

Laboratoire VERIMAG, Bâtiment IMAG,
150 place du Torrent,
38401 Saint-Martin-d'Hères

Bibliographie

[1] B. Colombier, A. Menu, J.-M. Dutertre, P.-A. Moëllic, J.-B. Rigaud, and J.-L. Danger, "Laser-induced single-bit faults in flash memory: Instructions corruption on a 32-bit microcontroller," in *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 1–10, IEEE, 2019.

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

[3] V. Werner, *Optimiser l'identification et l'exploitation de vulnérabilités à l'injection de faute sur microcontrôleurs*. PhD thesis, Université Grenoble Alpes, 2022.

[4] L. Dureuil, *Analyse de code et processus d'évaluation des composants sécurisés contre l'injection de faute*. PhD thesis, Université Grenoble Alpes, 2016.

[1] Motivated applications at M1 level will also be considered.