Fully-funded 3 year PhD position,
Université Grenoble Alpes & CEA, France

Fault Injection Attacks : Automated Analysis of Counter-Measures At The Binary Level

Institutions : Vérimag / Université Grenoble Alpes
LSL / CEA
Supervisors : Marie-Laure Potet marie-laure.potet@univ-grenoble-alpes.fr,
Laurent Mounier laurent.mounier@univ-grenoble-alpes.fr
Sébastien Bardin sebastien.bardin@cea.fr

Context. Physical fault injection attacks aim at modifying a runtime execution (and taking advantage of it) by disturbing the behaviour of the underlying hardware through physical means such as laser beams, magnetic pulses or power glitches. These attack vectors have been historically used against highly secured components and cryptographic applications. Yet, they are now more and more widespread, with for example recent bypass of secure bootloaders on micro-processor [7]. Moreover, progress in the field do make multi-fault attacks now feasible, and these scenario must be considered for example in certification process[1].

This doctoral work is part of the RAR TwinSec project (2025-2029), an ambitious French project whose goal is to build a digital twin for multi-fault injection analysis, from hardware to software. Robustness against fault injection can be obtained through the insertion of adequate counter-measures, be it hardware or software, inserted by the developer or by a compiler, or simply offered by a component. In this doctoral work, we focus on software counter-measures, even if the envisioned approaches may be applicable to some forms of hardware protections (e.g., hidden registers or memory).

In the case of single faults, robustness analysis comes down to simulate (in a broad sense : tests, symbolic execution, formal proof) the faults, evaluate their potential impact and deploy adequate protections. These analysis can be performed at different levels (source, binary, RTL, etc.). Going to multi-fault brings several significant challenges, not yet adequately addressed by the state of the art methods :

- the fault effects can combine together, hence the need to consider several fault models at the same time;
- the combinatorial explosion due to all the potential combinations of faults along a run may yield a huge number of attack paths, that need to be analyzed and understood in order to place the protections only where it is truly necessary;
- this combinatorial explosion also affects the underlying analysis technique, which may be completely overwhelmed, requiring more scalable ways to handle the multi-fault aspect ;
- finally, reasoning about counter-measures becomes more subtle, as the defense themselves can be attacked.

The supervisors have a long and fruitful collaboration on security-oriented program analysis. An efficient variant of binary-level symbolic execution for fault injection has been developed in the open-source BINSEC platform [1,2] from CEA (« Adversarial Reachability » [2]), while a methodology has been proposed by Vérimag [4,5] for analyzing counter-measures in a modular way at the source level. The general goal of the thesis is to propose and develop a methodology allowing to analyze counter-measures at the binary level with a high level of automation. More precisely we will have to:

[1] https://www.commoncriteriaportal.org/

- define an assertion language allowing to specify both fault models and counter-measures;

- propose binary-level equivalence checking methods allowing to verify properties of correctness and robustness of the given counter-measures, based on the notion of robust reachability offered by the BINSEC platform.

The methodology to be developed should allow to identify in a given code, its counter-measures, the underlying fault model against which they can protect as well as their intrinsic weaknesses. We envision an incremental method, where the good properties of the proven counter-measures allow to mitigate the inherent explosion of the search space. The approach will be validated at the binary level, possibly in collaborations with other partners from project TwinSec.

The large scope of this doctoral work will allow for rich exchanges within the TwinSec project, the « secure compilation » axis of Verimag and the « binary-level security » team of LSL.

PhD Student Profile (any of the following): Master in Embedded Systems, Master in Computer Science, Master in Cybersecurity

Expected skills: at least one among Formal methods and tools (symbolic execution), Compilation, Code security, Computer Architecture

Localization: Laboratoire Vérimag, Grenoble, France (potentially : CEA, Saclay, Paris area, France)

Application. Please send the following documents to the individuals listed above:
- Your CV
- A letter of motivation (in French or English)
- A copy of your Master's transcript (M1 and M2)
- Letters of recommendation

Period of application: All applications will be considered until the position is filled; PhD expected to start in Autumn 2025.

References

[1] https://binsec.github.io/

[2] Adversarial Reachability for Program-level Security Analysis.
Soline Ducousso and Sébastien Bardin and Marie-Laure Potet.
European Symposium on Programming (ESOP) april 2023

[3] Moving code analysis from safety to security : attacker model
Soline Ducousso,
thèse Université Grenoble Alpes, 2024

[4] Countermeasures Optimization in Multiple Fault injection context.
Etienne Boespflug, Cristian Ene,Laurent Mounier, Marie-Laure Potet.
Workshop on Fault Diagnosis and Tolerance in Cryptography, (FDTC 2020)

[5] A compositional methodology to harden programs against multi-fault attacks.
Etienne Boespflug, Laurent Mounier, Marie-Laure Potet, Abderrahmane Bouguern
Workshop on Fault Diagnosis and Tolerance in Cryptography, (FDTC 2023)

[6] Formally verified hardening of C programs against hardware fault injection.
Basile Pesin, Sylvain Boulmé, David Monniaux, and Marie-Laure Potet.
In **Proceedings of the 14th ACM SIGPLAN International Conference on Certified Programs and Proofs**, 2025.

[7] Fill your Boots: Enhanced Embedded Bootloader Exploits via Fault Injection and Binary Analysis
Jan Van den Herrewegen, David Oswald, Flavio D. Garcia , Qais Temeiza
IACR Trans. on Cryot. Hardw. Embed. Systems, 2021:56-81, 2021