(Project-Funded) Postdoc Proposal (18 months)
Fault models for RISCV security

Vincent Beroulle & Laure Gonnord – Grenoble-INP/LCIS

February 21, 2023

1 Context

The increasing complexity of the processors and the applications they run means that the software fault models (such as instruction skips, or instruction replacement) usually used to analyze the vulnerability of their code are no longer sufficient to express the diversity of faulty behaviors in modern architectures. Indeed, architecture designers have progressively added many complex hardware blocks (such as pipeline, cache memory, branch prediction, or speculative execution) to processors in order to optimize program execution.

From the software security point of view, such complex hardware is highly imprevisible, making the development of end-to-end cyberphysical systems (software, operating system and hardware) a real challenge. One common approach both all these activities is to redesign functionalities and optimisations from scratch, using security as a first class component.

At the LCIS Laboratory, and more generally in the context of the local (Grenoble-INP) security project (CLAM), a sequence of work have addressed the problematic of designing software and hardware that should be resistant to faulty behaviors and also vulnerability attacks:

- Previous and ongoing PhD thesis had the objective of designing fault models that should be at the same time accurate and usable to formalize realistic attacks on hardware [2, 1].
- Some countermeasures have been proposed, at least manually, to handle these vulnerabilies at the assembly level [3].
- Another ongoing PhD student, Sebastien Michelland currently works on the design of compiler-based software countermeasures to hardware vulnerabilities, with a particular accent on semantic expressivity.

The objective of this postdoc project is to capitalize on this existing work in order to provide securising hardware bricks for 32bits RISCV, in the context of the PEPR Project ARSENE.

Thanks to physical fault injection campains (with clock, voltage and EM glitches) and fault simulation of the RISCV architecture description the goal is :

- First, to study and understand the main RISCV architecture vulnerabilities;
- Second, to propose hardware countermeasures (e.g., fault detector or fault tolerance mechanisms) when no easy software countermeasures can be proposed.

2 Objective and Program

The context of this project is the French national effort en cybersecurity[1], and especially embedded system security, within the ARSENE project, which was accepted Fall 2022. The funding of the postdoc

[1] https://www.gouvernement.fr/recherche-programmes-et-equipements-prioritaires-de-recherche-3-milliards-d-euros-mobilises-pour-la

UGA/Grenoble INP & LCIS, Valence, France
E-mails : Vincent.Beroulle@@grenoble-inp.fr, Laure.Gonnord@grenoble-inp.fr (LCIS coordinator for ARSENE)

as well as its environment (travels, conferences, equipment) is guaranteed.

In the context of the ARSENE "lot1 project", the candidate will:

- Automate the fault injection campains and fault simulations
- Propose ISA level fault models, RTL fault models and compare these fault models with existing fault models (typical and more advanced)
- Design both software and hardware solutions (countermeasures) to protect the code and architecture against fault injection
- Evaluate the proposed solutions

The candidate will participate to the redaction of deliverables, namely, one deliverable on state-of-the-art of riscv hardware verification, and another one the evaluation of security hardware modifications on performance, and space.

3 Location and Supervision

The postdoc will take place in the LCIS lab, Valence, France in the CTSYS team[2]. The lab and the team take a strong place in the Cybersecurity european and french communities: they are involved the national PEPR project ARSENE, and many european and/or industrial projects around security.

The laboratory and the Ésisar engineer school also share a cybersecurity platform for graduate teaching, that contains hardware to physically realize hardware attacks, and also a private network for admin security teaching. The school and UGA/Grenoble INP also recently initiated an ambitious project called Cyberskills (french national "Metiers d'avenir" project; 4.3M€ for the Grenoble/Valence consortium) that will capitalize on the research outputs of ARSENE in order to provide updated course offers in embedded systems security. As an example, a new apprenticeship engineer curriculum opens in september 2023[3].

The postdoc will be supervised by **Vincent Beroulle**. Vincent Beroulle is Professor at Grenoble INP, Esisar. His received the M.S. and Ph. D. degrees in microelectronics from the University of Science of Montpellier, France, in 1999 and 2002, respectively. In 2002, he joined the Grenoble Institute of Technology (Grenoble INP) as an Assistant-Professor and became Full Professor in 2019. He is currently director of the LCIS laboratory in Valence. His main research interests deal with the security and robustness of heterogeneous integrated systems. Other persons from the LCIS lab (Laure Gonnord, Christophe Deleuze, David Hely, ...) will also participate to the postdoc research. In the context of the ARSENE project, we will also interact with people from the TIMA and Verimag research labs (Grenoble).

4 Profile of the candidate

- PhD in microelectronics, or embedded systems, or hardware/embedded system security.
- Good knowledge of embedded programming and microcontrollers.
- Good knowledge of processor architectures and digital design
- Knowledge in hardware security or fault tolerant architectures would be appreciated.

Communication and management skills are also expected: in the context of this project, the candidate would have to coordinate research between computer scientists (expert in compilation, langage design) and architects (experts in hardware design, fault models).

[2] https://lcis.grenoble-inp.fr/themes/securite-des-systemes-embarques-et-distribues-critiques
[3] https://esisar.grenoble-inp.fr/fr/formation/apprentissage

References

[1] Ihab Alshaer, Brice Colombier, Christophe Deleuze, Paolo Maistri, and Vincent Beroulle. Cross-layer inference methodology for microarchitecture-aware fault models. *Microelectronics Reliability*, 139:114841, 2022.

[2] Louis Dureuil, Guillaume Petiot, Marie-Laure Potet, Thanh-Ha Le, Aude Crohen, and Philippe de Choudens. Fissc: A fault injection and simulation secure collection. In Amund Skavhaug, Jérémie Guiochet, and Friedemann Bitsch, editors, *Computer Safety, Reliability, and Security*, pages 3–11, Cham, 2016. Springer International Publishing.

[3] Johan Laurent, Christophe Deleuze, Florian Pebay-Peyroula, and Vincent Beroulle. to be published, dec 22.