Design and Formal Verification of Hardware/Software Security Mechanisms

Guillaume Hiet
guillaume.hiet@irisa.fr
SUSHI team

Damien Couroussé
damien.courousse@cea.fr
CEA List, Grenoble

Mathieu Jan
mathieu.jan@cea.fr
CEA List, Saclay

Context. Embedded systems are increasingly targeted by attackers, facing not only traditional software attacks—such as those exploiting memory safety vulnerabilities like buffer overflows—but also hardware attacks. Among the last ones, fault-injection attacks exploit hardware perturbations to move a processor into unexpected states or execution paths, potentially exposing secrets or escalating privileges. Such attacks represent an effective threat to embedded systems and leverage faults inside the processor microarchitecture, resulting in various effects at the software level [5]. However, state-of-the-art countermeasures have only recently begun addressing the fault sensitivity of microarchitectural components. Furthermore, the formal verification of the security of a processor design in a threat model that includes fault injection remains an open challenge [9]. Security mechanisms, targeting not only fault injections pure also pure software attacks, must indeed be designed so that their implementations can be formally proven. This would enable systems to be evaluated, for instance, following Common Criteria (ISO 15408) at a high level of assurance (EAL 6 and above require formal proof).

The national TwinSec research project, which frames this PhD proposal, brings together several French laboratories specializing in hardware and software security to model and analyze fault-injections' effects at physical, hardware (HW), Instruction Set Architecture (ISA) and software (SW) levels. It focuses on physical attacks and mainly on fault injection using lasers. Existing modeling tools are not yet capable of efficiently predicting a embedded systems' resistance to such attacks due to generic fault models. TwinSec proposes a more realistic attacker model through multi-level analysis to identify and cancel, at the design stage, microarchitecture-specific vulnerabilities. A key approach in this research involves HW/SW contracts [4, 6], which serve as formal abstractions at the ISA level. These contracts enables system designers to reason about security properties of HW implementations independently from SW implementations and vice versa. This PhD project seeks to leverage HW/SW contracts to design and formally verify hybrid security mechanisms that integrate both hardware and software components.

Background. In previous work, the SUSHI team relied on the Kôika language developed at MIT [2] and proposed a framework to formally specify and prove hardware security mechanism [1]. We have explored implementing a formally proven Control Flow Integrity mechanism in a RISC-V CPU developed in Kôika [2], although in a limited setting [1]. In particular, we only ensure backward-edge security with a simple shadow stack, which is of fixed size and cannot be changed between processes. However, this forms a basis for proving more complex security mechanisms. Our current approach consists in automatically compiling Kôika designs to a more explicit representation, and then manually proving the properties of interest on this representation. The manual proof effort for this second step is still very high, and specific to each property and security mechanism. In order to automate this last step, we have started to leverage SMT (Satisfiability Modulo Theory) solvers. This approach looks promising: we have succeeded in automatically proving the security properties of the shadow stack described in [1].

Several academic and industrial actors have now adopted the Chisel HDL [3] to design their RISC-V core, e.g., SiFive, Berkeley, or Google. We are now designing a new formal HDL in Coq (COQQTL[4]) that directly maps FIRRTL [5], the intermediate language used in the compilation of circuits described in Chisel. This formal HDL could help the adoption of our verification framework to evaluate HW/SW security extensions.

Concerning fault injection attacks, we propose to consider a recent countermeasure developed at the CEA, MAFIA [3], that protects the control signals of a processor microarchitecture against fault injection attacks, as a use case driving the research work in this thesis. MAFIA was originally implemented in RTL (System Verilog) and integrated into a RISC-V RV32IM 4-stage, in-order core, the CV32E40P processor. The implementation was formally verified in part [3], using µArchiFI, an open-source tool dedicated to the formal modeling and verification of microarchitecture-level fault injections and their effects on complex hardware/software systems [8].

[1] https://gitlab.inria.fr/SUSHI-public/FMH/koika
[2] https://gitlab.inria.fr/SUSHI-public/FMH/herve
[3] https://www.chisel-lang.org/
[4] https://gitlab.inria.fr/SUSHI-public/FMH/coqqtl
[5] https://github.com/chipsalliance/firrtl

PhD Topic. The goal of the PhD is to propose approaches to formally design and verify hardware security mechanisms targeting fault injection attacks. As a starting point and a case study, we propose to consider the MAFIA countermeasure. The starting objective will be to implement MAFIA in a formal HDL such as Kôika or COQQTL. In this work, a major challenge is to express formal security properties in an attacker model that includes fault injection. As a follow-up, the security design can be extended with (i) landing pads [7] as a means to enforce forward-edge integrity; (ii) integrity of the data path, which is currently not supported by MAFIA.

Required skills or interests. The candidate should have familiarity with at least one of the following:

- Hardware design languages (e.g. Verilog/VHDL) and computer architecture;
- Or formal methods (e.g. Coq, SMT solvers).
- Knowledge of hardware security, esp. fault injection, is not required for this position but appreciated.

Institute. The PhD will take place at CentraleSupélec in Rennes, France, in the SUSHI Inria team[6]. This team is part of the IRISA laboratory.[7] The PhD will be co-advised by Guillaume Hiet (CentraleSupélec), Damien Couroussé (CEA) and Mathieu Jan (CEA).

Practical aspects. This PhD will last 3 years, starting before the end of 2025. Additional teaching activities are not mandatory but possible, notably at CentraleSupélec. Such complementary activities give rise to an additional salary.

The PhD can be preceded by a Master's internship on the same topic.

Housing options may be available on campus, or close to the campus.

References

[1] Matthieu Baty et al. "A Generic Framework to Develop and Verify Security Mechanisms at the Microarchitectural Level: Application to Control-Flow Integrity". In: *36th IEEE Computer Security Foundations Symposium, CSF 2023, Dubrovnik, Croatia, July 10-14, 2023*. IEEE, 2023, pp. 372–387. DOI: 10.1109/CSF57540.2023.00029.

[2] Thomas Bourgeat et al. "The essence of Bluespec: a core language for rule-based hardware design". In: *Proceedings of the 41st ACM SIGPLAN International Conference on Programming Language Design and Implementation, PLDI 2020, London, UK, June 15-20, 2020*. Ed. by Alastair F. Donaldson and Emina Torlak. ACM, 2020, pp. 243–257. DOI: 10.1145/3385412.3385965.

[3] Thomas Chamelot, Damien Couroussé, and Karine Heydemann. "MAFIA: Protecting the Microarchitecture of Embedded Systems Against Fault Injection Attacks". In: *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)* (2023). ISSN: 1937-4151. DOI: 10.1109/TCAD.2023.3276507.

[4] Marco Guarnieri et al. "Hardware-Software Contracts for Secure Speculation". In: *2021 IEEE Symposium on Security and Privacy (SP)*. 2021, pp. 1868–1883. DOI: 10.1109/SP40001.2021.00036.

[5] Johan Laurent et al. "Cross-Layer Analysis of Software Fault Models and Countermeasures Against Hardware Fault Attacks in a RISC-V Processor". In: *Microprocessors and Microsystems* (2019). DOI: 10.1016/j.micpro.2019.102862.

[6] Gideon Mohr, Marco Guarnieri, and Jan Reineke. "Synthesizing Hardware-Software Leakage Contracts for RISC-V Open-Source Processors". In: *Design, Automation & Test in Europe Conference & Exhibition, DATE 2024, Valencia, Spain, March 25-27, 2024*. IEEE, 2024, pp. 1–6. DOI: 10.23919/DATE58400.2024.10546681.

[7] RISC-V Shadow-stack and Landing-pads Task Group. *RISC-V Shadow Stacks and Landing Pads*. Tech. rep. Version v0.4.0. RISC-V International, 2023. URL: https://github.com/riscv/riscv-cfi.

[8] Simon Tollec et al. "µARCHIFI: Formal Modeling and Verification Strategies for Microarchitectural Fault Injections". In: *FMCAD*. 2023. DOI: 10.34727/2023/isbn.978-3-85448-060-0_18.

[9] Simon Tollec et al. "Fault-Resistant Partitioning of Secure CPUs for System Co-Verification against Faults". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)* (2024). DOI: 10.46586/tches.v2024.i4.179-204.

[6] https://team.inria.fr/sushi/

[7] https://www.irisa.fr/en