PhD position

Dynamic memory management for RISC-V processor securization

Keywords: HW security, processor architecture, memory hierarchy

1 Introduction and context

Hardware side-channel attacks target specific features of processor architectures in order to steal sensitive information, such as the secret keys of encryption algorithms [1]. In particular, cache side-channel attacks (CSCAs) represent a major threat to modern processor architectures.

Cache side-channel attacks can target both instruction and data caches, at various cache levels depending on the implementation. Cache memories are considered preferential targets for such attacks because of their role as buffers close to the CPU, through which data from all kinds of applications, whether sensitive or not, pass. The implementation of CSCAs relies on the attacker's ability to measure or observe activity on the cache, enabling him to deduce information on memory accesses.

The subject of this PhD will focus on timing CSCAs, i.e. attacks that rely on the measurement of execution time to track data stored or not stored in the cache, and thus learn about memory access patterns. Examples include the Prime+Probe [2] and Flush+Reload [3] attacks.

The ANR-funded SEC-V research project brings together a consortium of academic and industrial research laboratories to propose solutions for dynamically securing the architecture of a RISC-V processor core [4]. The attacks considered in this project are in particular CSCAs, and part of the work therefore concerns the implementation of innovative means of securing the core's cache memories.

2 Scientific issues and objectives

Within the SEC-V project, we propose to study the security advantages of implementing a micro-decoding unit for instructions, enabling dynamic management of the microarchitecture, as a countermeasure to CSCA. The objective of this thesis is to study the advantages of using scratchpad memories [5, 6] for security purposes. Indeed, these memories can allow the temporary storage of sensitive data without inducing performance loss, as their implementation does not require complex control logic. With a view to optimizing performance, these memories are accessible via software requests and therefore offer better performance in terms of energy consumption and are less expensive in terms of silicon area. The main idea is to avoid caching sensitive data, by using the scratchpad memory instead for this purpose, while leveraging the dynamic aspect studied in the SecV project.

This PhD work will focus on the following research objectives:

- Drawing up a bibliography on the use of scratchpad memories for security purpose.
- Propose countermeasures to CSCAs based on scratchpad implementation. Different strategies will be implemented and evaluated (constant time, offuscation, scrambling, isolation, ...) One of the main difficulty is on the dinamic memory management hierarchy between the cache and the scratchpad.

- Modify the architecture of the CVA6 processor core to implement the countermeasure.
- Verify the implementation on an FPGA board and perform verification tests.

3 Candidate profile

The candidate must have a master level (or equivalent) and must be able to demonstrate theoretical/practical knowledge in the areas of:

- Knowledge of processor architecture
- Knowledge of hardware security
- Understanding of hardware description languages (VHDL, SystemVerilog)

4 PhD context

This PhD thesis is part of the research activities of the ASIC team within the IETR laboratory (Institute of Electronics and Digital Technologies), based at Nantes Université. The team conducts advanced research in the design of specialized digital circuits, particularly focusing on processor architectures optimized for complex embedded applications. The lab has recognized expertise in hardware architecture, performance optimization, and FPGA prototyping, closely aligned with industrial challenges in embedded computing and artificial intelligence.

This PhD is in the SecV project framework, and the candidate will collaborate with the other researchers and PhD/master students within the project. He/She may co-supervise internship students. He/She may have some opportunities for teaching (added to his payroll), if interested.

- **Research Laboratories:** IETR (UMR CNRS 6164)
- **University:** Nantes Université
- **Location:** IETR/Polytech, Nantes, FRANCE
- **Intended starting date:** September or October 2026 (3-year duration)

5 To apply

Applications must be submitted exclusively via the AMETHIS platform. No applications received outside of the AMETHIS process will be considered.

For further information, please email:

- **Pr. Sébastien Pillement**, sebastien.pillement@univ-nantes.fr ,
- **PhD. Bastien Deveautour**, bastien.deveautour@univ-nantes.fr .

Applications will be reviewed as they are received. Auditions will be held following the application period. Applications that do not meet the qualifications will not be considered for auditions.

As integration into the IETR laboratory requires access to a restricted secure area, we ask you to take into account the time required to review your profile if you wish to apply (the process can take up to two months).

References

[1] Valentin Martinoli. "Secure Processors with respect to Micro Architectural Attacks". PhD thesis. Université Grenoble Alpes, 2023. URL: https://theses.hal.science/tel-04145576/.

[2] D. A. Osvik et al. "Cache Attacks and Countermeasures: The Case of AES". In: *Topics in Cryptology – CT-RSA*. 2006.

[3] Yuval Yarom and Katrina Falkner. "FLUSH+RELOAD: a High Resolution, Low Noise, L3 Cache Side-Channel Attack". In: *23rd USENIX Security Symposium (USENIX Security 14)* (2014).

[4] J. Pottier et al. "RISC-V Processor Enhanced with a Dynamic micro-Decoder Unit". In: *International Conference on Electronics, Circuits and Systems*. 2024.

[5] I. Puaut and C. Pais. "Scratchpad memories vs locked caches in hard real-time systems: a quantitative comparison". In: *2007 Design, Automation & Test in Europe Conference & Exhibition*. Design, Automation & Test in Europe Conference. 2007. URL: http://ieeexplore.ieee.org/document/4212020/.

[6] A. Singh et al. "SPX64: A Scratchpad Memory for General-purpose Microprocessors". In: *ACM Transactions on Architecture and Code Optimization* (2021). URL: https://dl.acm.org/doi/10.1145/3436730.