PhD offer
Software Mitigations for Cache and Covert Timing SCAs

Context

This PhD takes in the context of the ANR project SCAMA (*Secure-by-Design Computing Against Microarchitectural Attacks* which involves four French laboratories including Lab-STICC.

Security failure in computing systems has become one of today's biggest concern. The primary threat is the fact that modern computing architectures –from computational optimizations to storage elements and interfaces, from end-user applications to the operating system and hypervisor, and from microarchitecture to underlying hardware– may hide unexpected vulnerabilities. This concern is gaining further momentum, with the spectacular aggressiveness of Spectre, Meltdown, and ZombieLoad vulnerabilities. They demonstrate that even hardware, which is often considered as an abstract layer that behaves correctly by executing instructions and giving a logically correct output, is leaking critical information as a side effect of software implementation and execution. Even worse, the many undocumented parts of modern architectures open doors for yet undescribed SCAs (*Side-Channel Attacks*).

This proposal tackles the problem of these vulnerabilities at the intersection of software and hardware to propose secure-by-design computing, where we strike a balance between security and hard-earned performance benefits.

PhD works

The PhD candidate will have to work on software mitigations for cache and covert timing SCAs.

The main goal is to propose software countermeasures that address vulnerabilities collected by another project partner in order to get an SCA-resistant software layer based on a Trusted Execution Environment (*TEE*) in a RISC-V platform. The PhD candidate will study and implement strategies allowing the software stack to exploit the hardware countermeasures proposed by a third project partner where another PhD student will be based. Consequently, they will closely collaborate to extend the processor instruction set and to develop low level drivers.

We plan to extend the Keystone enclave model [1] with SCA-resistant countermeasures. In order to propose a strong defense against SCA, we plan to propose contributions at different levels of the software stack.

1. We will extend the Keystone Runtime with embedded virtual machines dedicated to the execution of sensitive codes.

2. Secondly, we will propose a novel enclave model allowing the exploitation of proposed hardware and software protections against SCA.

The software stack developed in this PhD thesis will be merged with contributions of other project partners in order to propose a platform demonstrating SCAMA contributions.

Application

- PhD takes place in the Lab-STICC laboratory at ENSTA Bretagne, Brest, France. Starts from September/October 2024.
- The candidate must have previous knowledge in several topics among the following:
  - C and its compilers (GCC, Clang/LLVM).
  - Basics of assembly (prererably RISC-V or ARM).
  - Computer architecture.
  - Scripting language and at least an HDL language at least (ideally SystemVerilog).
- Applications opened until filled. Please submit a curriculum, motivation letter and master grades.

Contacts

- Pascal Cotret, Lab-STICC / ENSTA Bretagne pascal.cotret@ensta-bretagne.fr
- Vianney Lapôtre, Lab-STICC / Université de Bretagne-Sud vianney.lapotre@univ-ubs.fr
- Loïc Lagadec, Lab-STICC / ENSTA Bretagne loic.lagadec@ensta-bretagne.fr

References

[1] D. Lee, D. Kohlbrenner, S. Shinde, K. Asanović, and D. Song, "Keystone: An open framework for architecting trusted execution environments," in *Proceedings of the Fifteenth European Conference on Computer Systems*, 2020, pp. 1–16.

[2] Q. Ducasse, P. Cotret, and L. Lagadec, "JIT Compiler Security through Low-Cost RISC-V Extension," in *2023 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*, 2023, pp. 125–128.

[3] Q. Ducasse, G. Polito, P. Tesone, P. Cotret, and L. Lagadec, "Porting a JIT Compiler to RISC-V: Challenges and Opportunities," in *Proceedings of the 19th International Conference on Managed Programming Languages and Runtimes*, ser. MPLR '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 112–118. [Online]. Available: https://doi.org/10.1145/3546918.3546924

[4] N. Gaudin, J.-L. Hatchikian-Houdot, F. Besson, P. Cotret, G. Gogniat, G. Hiet, V. Lapotre, and P. Wilke, "Work in progress: Thwarting timing attacks in microcontrollers using fine-grained hardware protections," in *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2023, pp. 304–310.

[5] M. Mushtaq, M. M. Yousaf, M. K. Bhatti, V. Lapotre, and G. Guy, "The Kingsguard OS-level mitigation against cache side-channel attacks using runtime detection," *Annals of Telecommunications - annales des télécommunications*, Jan. 2022. [Online]. Available: https://hal.science/hal-03545078