INSTITUT D'ÉLECTRONIQUE ET DES TECHNOLOGIES DU NUMÉRIQUE

Master thesis internship (6 months, starting Feb./March 2022):

Cache-based Side-Channel Attacks on RISC-V processors

Key words: Hardware security, cache-based side-channel attacks, RISC-V, Open Hardware

1 Scientific context

For decades, processor designers have focused on improving the performance and energy consumption of systems. However, in recent years, it has been proved that attacks directly on the hardware, allow to steal secret information by exploiting vulnerabilities, introduced as side effects, by performance optimization mechanisms. Among these, attacks have highlighted security flaws due to the use and sharing of cache memories, and other microarchitectural components in high performance processors. They typically exploit caches, performance counters or speculation units and jeopardize the safety and the of processors in industrial systems. We can cite Spectre and Meltdown as well-known examples.

The OpenHW approaches and specifically the RISC-V[1] initiative are now both an economic reality and an innovation opportunity for European actors in the field of processors architecture. This opportunity opens the way to design innovative secure processor cores.

This internship is in the frame of the ANR SecV project starting in March 2022. The project will offer an innovative open-source, secure and high-performance processor core based on the ISA RISC-V. The originality of the approach lies in the integration of a dynamic code transformation unit. **Through this project, a PhD position to pursue this internship work is secured.** Therefore, candidates interested in pursuing with a PhD are particularly welcome.

This internship position will focus on cache-based side-channel attacks, able to gain information on data that would otherwise remain secret, and will investigate the design of innovative secured-by-design open-source processing core against these attacks.

2 Scientific issues and objectives

In the OpenHW approach, the processor is proposed in the form of a block described in a hardware description language (SystemVerilog in this project) which can be modified according to the requirements of the system.

The main objective of this internship work is to study cache-based attacks vulnerabilities and to investigate new defenses to increase the security of the CVA6[2] processing core based on the RISC-V ISA. This study will serve as a preliminary work for the PhD work in the SecV project that will follow.

The main tasks for this internship work will be:

1. To gain knowledge on the literature basics of cache memories (architecture, management policies, ...) as well as on cache-based side-channel attacks.

2. To gain theoretical and practical experience with ARIANE (CVA6) RISC-V platform. This platform is provided by Thales (partner of the project).

[1] https://riscv.org

[2] https://github.com/openhwgroup/cva6

3. To gain practical experience on physical side-channel attacks on the CVA6 platform.
4. To investigate practical defenses, for instance based on different cache management policies or cache design.

3 Internship context

- **Research Laboratory:** IETR (UMR CNRS 6164)
- **University:** Polytech, Université de Nantes
- **Location:** IETR/Polytech, Nantes, FRANCE
- **Intended starting date:** February, or March 2022 (around 6 months)
- **Stipend:** between 550-600 €/month

4 Candidate profile

Master 2 student/5th year Engineering in Computer or Electrical Engineering, Embedded Systems, Electronics or Computer Science.

Candidate must be able to demonstrate theoretical/practical knowledge in the areas of
- computer,
- architecture,
- microarchitecture and
- embedded systems design.

As well as a solid background on

- Hardware description language.

Additionally, the candidate will have some knowledge or at least interest on hardware security and openHW would be a good asset.
Depending on the candidate native language, French or English will be the working language. Knowledge in French is not required.

5 How to apply

Applying candidates will prove and/or justify the requested knowledge and skills by providing:
- A CV,
- Academic records and transcripts of Master 2, or of the last year of Engineer school,
- All documents attesting the requested skills and knowledge.

Applications must be sent to:

- maria.mendez@univ-nantes.fr
- sebastien.pillement@univ-nantes.fr

Deadline for application : Applications will be considered as they arrive and until there is a successful candidate, and in all cases before December 17.