TIMA
TECHNIQUES OF INFORMATICS AND MICROELECTRONICS
FOR INTEGRATED SYSTEMS ARCHITECTURE

Internship: Mitigation of Microarchitectural Vulnerabilities

Context

Data protection is fundamentally important in an increasing number of domains. These properties are usually guaranteed through cryptographic protocols and secure primitives that are implemented, either in hardware or software, on systems of various complexity. The economical and societal challenges push for strong, fast, and robust implementations of these functions, which are implemented with the main goal to optimize overall performance. On the other hand, designers must take care that the implementations may be vulnerable to the implementation attacks. Recent research has shown how side channel attacks can be a major concern even in complex systems: attacks such as Spectre [1] or Meltdown [2], or those based on cache access latency [3], have proved that microarchitectural features aiming at improving the overall performance can actually open a side channel where confidential information can be extracted.

[1] P. Kocher et al., "Spectre Attacks: Exploiting Speculative Execution," 2019 IEEE Symposium on Security and Privacy (SP), 2019, pp. 1-19, doi: 10.1109/SP.2019.00002.
[2] M. Lipp et al., “Meltdown: reading kernel memory from user space,” Commun. ACM 63, 6 (June 2020), 46–56, doi: 10.1145/3357033
[3] A. Andreou, A. Bogdanov and E. Tischhauser, "Cache timing attacks on recent microarchitectures," 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2017, pp. 155-155, doi: 10.1109/HST.2017.7951819.

Description

Microarchitectural attacks rely on low-level information about the processor’s performance, that is usually available through internal performance indicators known as counters. These features allow advanced analysis of the processor’s behavior, performance monitoring, and tuning. The goal of this internship is to protect these elements in order to reduce the feasibility of the existing attacks. For transparency and documentation reason, the work will be carried out on an open implementation such as a processor implementing the RISC-V instruction set.

More in detail, the intern’s activities will consist of:

- Implement a working prototype of simple system based on a RISC-V CPU
- Carry out one or more microarchitectural attacks from the literature
- Identify the critical elements in the microarchitecture that make the attack feasible
- Propose and implement dedicated countermeasure(s) to protect those features
- Validate the countermeasure(s)

Prerequisites

Digital design, RISC-V, FPGA design flow (Xilinx), VHDL/Verilog.
Knowledge of hardware security is a plus, but not strictly required

Contacts	Michele PORTOLAN (michele.portolan@univ-grenoble-alpes.fr) Giorgio DI NATALE (giorgio.di-natale@univ-grenoble-alpes.fr) Paolo MAISTRI (paolo.maistri@univ-grenoble-alpes.fr)
Applications	Please send your resume, application and recommendation letter(s), first year master’s degree grades (mandatory) and second year grades (if possible)
Location	TIMA Laboratory, 46 avenue Félix Viallet, 38000 Grenoble
Starting date	Feb-2024
Duration	5 to 6 months
Allowance	In accordance with existing regulations (approx. 600€/month).

Our team welcomes applicants with diverse backgrounds and experiences. We regard gender equality and diversity as strength and an asset.