Detecting Microarchitectural Side Channel Attacks in CPUs via Machine Learning Techniques

Alessandro Palumbo
alessandro.palumbo@inria.fr

Introduction

The continuous quest for performance has driven Systems on Chip (SoC) to incorporate advanced elements such as multiple cores, caches, and acceleration units. However, these additions often expose unexpected vulnerabilities. It has been demonstrated that by observing certain features, which are apparently unrelated to program execution—such as power consumption traces, thermal footprint, or electromagnetic emanation—an attacker may gain sufficient information to leak sensitive data [1, 2]. For example, differences in timing introduced by caches or speculative execution can be exploited to leak private information, as demonstrated by attacks like Spectre [3], Meltdown [4], and many others [1, 2].

The Internship

This project focuses on the detection of Microarchitectural Side Channel Attacks (MSCAs) on RISC-V processors through the application of Machine Learning techniques. Using the gem5 simulator [5], the behavior of a RISC-V CPU under attack is simulated and various features such as execution timing, power consumption, and cache performance are analyzed. Machine learning models are employed to recognize the signatures of side-channel attacks, with the objective of improving detection accuracy and minimizing false positives.

Project Goals

1. Get familiar with the gem5 simulator and implement a RISC-V-based processor.
2. Emulate MSCAs, such as Prime+Probe and Spectre, on the simulated platform.
3. Collect data on performance counters, execution, memory access times during the execution of benchmarks.
4. Develop Machine Learning models to detect the attacks, using algorithms like Random Forest or Support Vector Machine.

5. Evaluate the models' accuracy in terms of attack detection and minimizing false positives.

Required skills or interests

- Get familiar with the gem5 tool for CPU design and simulations:
    - Implement both the attack-free RISC-V-based CPU and the one under attack (e.g., including Microarchitectural Side Channel Attacks).
    - Run simulations to observe and collect microarchitectural feature values (such as performance counters, timing information, and cache behavior) provided by the tool.
- Get familiar with Machine Learning algorithms and computations:
    - Develop Python scripts using machine learning models that analyze the collected features to detect attacks and distinguish safe runs.
    - Evaluate and choose the best model for accurate detection (e.g., Random Forest, Support Vector Machine, Isolation Forest, etc.).

Institute

The internship will take place at CentraleSupélec in Rennes, France, in the SUSHI Inria team[1]. This team is part of the IRISA laboratory[2].

Practical aspects

The intern will receive a "gratification" of about 600€ per month. Housing options may be available on campus or close to it. This 5/6 months internship is research-oriented and lays the groundwork for potential doctoral studies. This opportunity is ideally suited for students interested in pursuing a PhD, given the advanced nature of the work and its potential applications in academic and research settings.

References

[1] Yuan, Jie, et al. "A Survey of Side-Channel Attacks and Mitigation for Processor Interconnects." Applied Sciences 14.15 (2024): 6699.

[2] Lou, Xiaoxuan, et al. "A survey of microarchitectural side-channel vulnerabilities, attacks, and defenses in cryptography." ACM Computing Surveys (CSUR) 54.6 (2021): 1-37.

[1] https://team.inria.fr/sushi/
[2] https://www.irisa.fr/en

[3] P. Kocher, et al., “Spectre attacks: Exploiting speculative execution,” Dec. 2018.

[4] Lipp, Moritz, et al. "Meltdown: Reading kernel memory from user space." Communications of the ACM 63.6 (2020): 46-56

[5] Binkert, N., Beckmann, B., Black, G., Reinhardt, S. K., Saidi, A., Basu, A., Hestness, J., Hower, D., Krishna, T., Sardashti, S., Schuette, B., Sen, R., Sewell, K., Shoaib, M., Sinkar, S., Turner, A., Wenisch, T. F., & Hill, M. D. (2011). The gem5 simulator. ACM SIGARCH Computer Architecture News, 39(2), 1-7