# Detecting Microarchitectural Side-Channel Attacks via Hardware Security Checkers

Alessandro Palumbo
*CentraleSupélec, Inria, CNRS, IRISA*
alessandro.palumbo@inria.fr

***Abstract*—Two Hardware Security Checkers ISA-independent for real-time anomaly detection in microprocessor-based systems are presented: (1) a hash-based approach that identifies known attack patterns and (2) a Machine Learning-based model trained on system-level simulations to detect emerging threats.**
**The methodology relies on monitoring the microprocessor's behavior, specifically instruction fetching activity and performance counters, including cache activity and branch mispredictions, to identify malicious activity with minimal overhead. Experimental results demonstrate 100% detection accuracy for known attacks and strong adaptability to novel threats.**

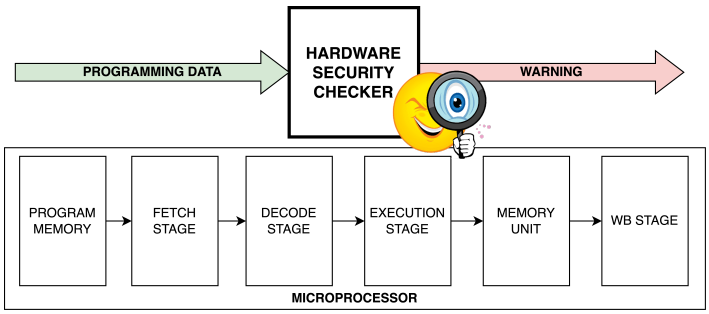


Fig. 1. The Hardware Security Checker implementation idea

## I. The Hash-based Hardware Security Checker

Monitoring microprocessor's fetching activity using hash functions. Estimating programmed malicious instruction patterns within user-defined time windows.

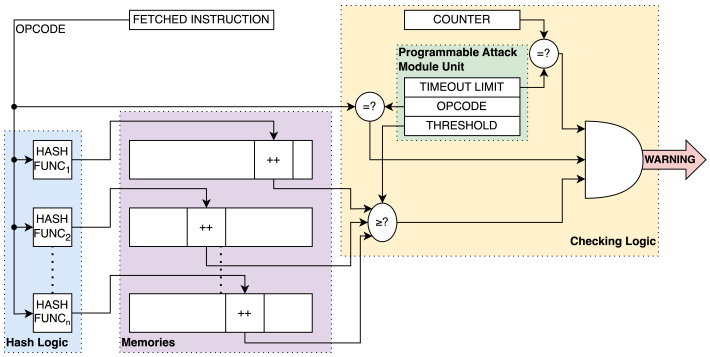


Fig. 2. The Hash-based Hardware Security Checker structure [1]

TABLE I
Best rates and the resource usage of proposed solutions

| Ref. | Acc. | FP | FN | #LUT | #FF | #BRAM | #LUTRAM |
|---|---|---|---|---|---|---|---|
| [1], Fig 2, 3 | 100% | 0% | 0% | 19,063 (3.98%) | 11,552 (6.13%) | 17 | 4,536 (0.53%) |
| [2], Fig 4 | 99.79% | 0.21% | 0% | 45,200 (6.75%) | 6,100 (NA) | 0 | 0 |

TABLE II
Best anomalies detection rates and overheads

| Ref. | Considered vulnerabilities | | | | | Targeted ISA | |
|---|---|---|---|---|---|---|---|
| | Spectre | Meltdown | Orchestration | RowHammer | Flush+Reload | x86 | RISC-V |
| [1], Fig 2, 3 | ✓ | | ✓ | ✓ | ✓ | | ✓ |
| [2], Fig 4 | ✓ | ✓ | | | | ✓ | |

## References

[1] K. A. et al., "Processor security: Detecting microarchitectural attacks via count-min sketches," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 7, pp. 938–951, 2022.
[2] M. Iamundo, "A machine learning-based security architecture to detect microarchitectural side-channel attacks in microprocessors," 2021.

## II. The Hash-based Workflow

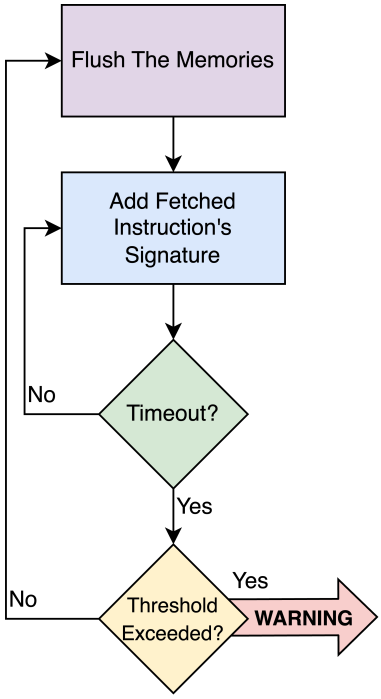


Fig. 3. The workflow of the Hash-based Hardware Security Checker [1]

## III. The ML-based Workflow

ML attack detection on system-level simulations, feature selection for generating hardware-ready code.

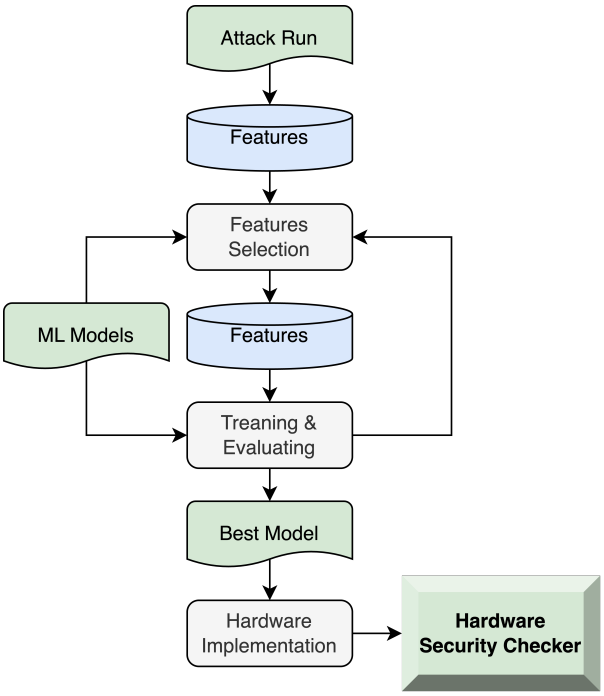


Fig. 4. The workflow of the ML-based Hardware Security Checker [2]