# Assessing the Vulnerabilities of RISC-V using the gem5 Simulator (Access-Retired)

Mahreen Khan, Maria Mushtaq, Renaud Pacalet, Ludovic Apvrille

# Assessing the Vulnerabilities of RISC-V using the gem5 Simulator

Mahreen Khan*,[1], Maria Mushtaq*,[1],
Renaud Pacalet*,[1], Ludovic Apvrille*,[1]

*Telecom Paris, Institut Polytechnique de Paris, France

**ABSTRACT**

**Emerging RISC-V processors require rigorous security evaluation to address microarchitectural vulnerabilities inherent in their rapidly evolving ecosystem. A recent paper [Gea23] implemented both known and novel side-channel attacks targeting commercial RISC-V CPUs (U74 and C906). While this hardware-based research confirmed vulnerabilities, it could not provide detailed insights into attack dynamics. We bridge this gap using the gem5 simulation framework to systematically analyze side-channel attacks on RISC-V architectures. Our paper focuses on the access-retired attack, which exploits the unprivileged `rdinstret` instruction to infer protected filesystem data. By tracking retired instruction counts, attackers detect microarchitectural state differences caused by directory access checks. We utilize the gem5 simulator in full-system (FS) mode to capture kernel-level behaviors, allowing us to analyze critical performance metrics including instruction retirement, cache performance, and branch prediction statistics. This detailed simulation-based analysis is essential for understanding the behavior of the attack and for developing effective countermeasures. Advancing RISC-V security research with simulation tools like gem5 is thus a promising direction for mitigating future side-channel vulnerabilities.**

KEYWORDS: RISC-V Architecture ; gem5 Simulator ; Hardware Performance Counters (HPCs) ; Embedded Systems ; Side-Channel Attacks ; Attack Assessment ; Microarchitectural Security

## 1 Introduction

The open-source RISC-V instruction set architecture (ISA) has offered unprecedented flexibility for custom hardware design. However, its rapid adoption in safety-critical domains, from embedded systems to data centers, demands rigorous scrutiny of microarchitectural security. While RISC-V's modularity enables performance and power optimizations, it also introduces attack surfaces absent in traditional ISAs. Recent work by [Gea23] demonstrated this risk empirically, implementing novel side-channel attacks on commercial RISC-V cores (U74, C906) that exploit microarchitectural resource contention. Their hardware-based validation confirmed vulnerabilities but left critical gaps in understanding attack mechanics, particularly how ISA-specific features interact with microarchitectural states.

To address this limitation, we propose simulation-driven analysis using the gem5 framework [LP24], which provides cycle-accurate modeling of RISC-V processors in full-system (FS) mode. We focus on the `rdinstret`-based access-retired attack, where adversaries in-

[1]E-mail: {firstname.secondname@telecom-paris.fr

fer filesystem metadata through retired instruction count variations. Unlike hardware experiments, gem5 enables granular tracing of kernel-level events, cache states, and pipeline behaviors during attack execution. This methodology reveals how directory access checks, ostensibly protected by privilege boundaries, create measurable timing differences through cache line contention and branch mispredictions.

## 2 gem5 Methodology

To analyze the access-retired attack on RISC-V, we configure gem5 with the following setup:

1. **Simulation Mode**: We use **Full-System (FS) mode**, which models the complete hardware-software stack, including the operating system. This is essential for capturing kernel-level interactions during filesystem access checks.

2. **Disk Image and Kernel**: We configure gem5 for RISC-V, our target architecture, and modify the RISC-V disk image to include the attack binary. The system boots using the `riscv-bootloader-vmlinux-5.10` kernel.

3. **CPU Model**: Use the `O3CPU` out-of-order processor model to simulate speculative execution and branch prediction behaviors. This enables tracking of pipeline stalls and branch mispredictions.

4. **Memory System**: Configure cache hierarchies (L1/L2) and memory system [LP24].

Figure 1 summarizes the workflow for simulating gem5 in full-system mode.

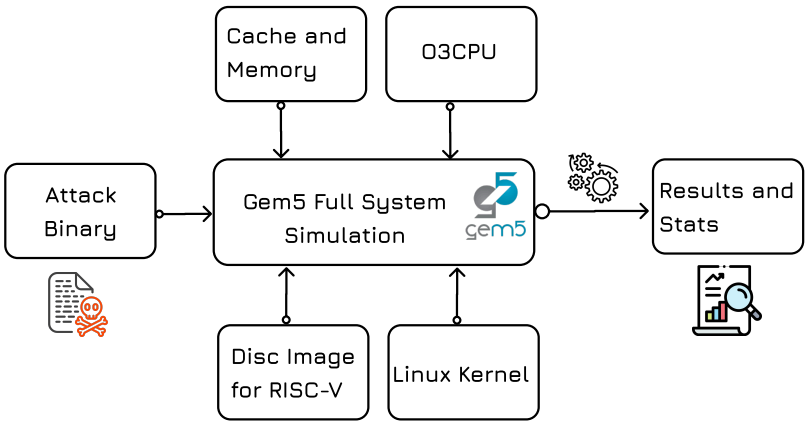


Figure 1: Gem5 full-system simulation workflow for analyzing the access-retired attack on RISC-V.

# 3 Results

The gem5 simulator successfully implemented and analyzed the access-retired attack on the RISC-V architecture. The results align closely with hardware measurements, demonstrating gem5âs ability to model detailed microarchitectural behavior and provide insights into attack mechanisms.

Our experiments show a clear side-channel signal through systematic differences in microarchitectural metrics when accessing existing versus non-existing files. As shown in Figure 2, the retired instruction count increases by 25% (from 3,300 to 4,120) when a target file exists, even though the system calls return NULL in both cases. This increase is due to extra kernel checks, such as permission validation.

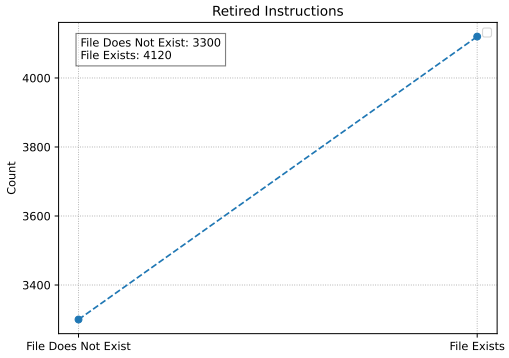


Figure 2: Retired instruction counts comparison.

The simulated execution time nearly doubles (from 65.61s to 151.30s) when the file exists, as illustrated in Figure 3. This extended duration correlates with the higher retired instruction count.

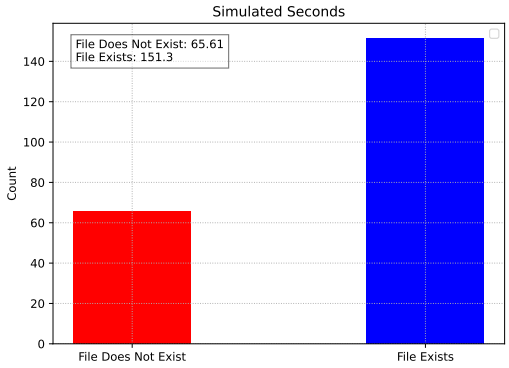


Figure 3: Simulated execution time comparison.

Additionally, the total number of simulated instructions rises by 20% (from 267M to 320M) for file existence as shown in Figure 4. Memory subsystem behavior also differentiates file existence, as evidenced by increases in branch fetching, indirect branch lookups, and reorder buffer entries. Table 1 summarizes the metrics comparing file existence and non-existence scenarios. These consistent differences confirm that failed system calls leak file existence information through multiple microarchitectural vectors.

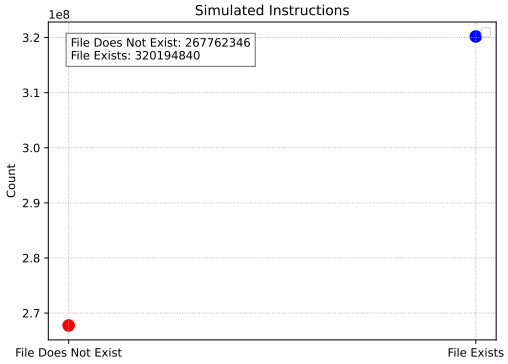


Figure 4: Total instruction counts comparison.

Table 1: Comparison of Metrics for File Existence

| Metric | File Exists | File Does Not Exist |
|---|---|---|
| Retired Instructions | 4,120 | 3,300 |
| Indirect Branch Lookups | 3,915,281 | 2,825,809 |
| Load Instructions Executed | 71,511,594 | 55,635,190 |
| Branches Fetched | 90,168,771 | 76,010,909 |
| Reorder Buffer Total | 678,320,302 | 575,317,912 |
| Simulated Seconds | 151.30 | 65.61 |
| Simulated Instructions | 320,194,840 | 267,762,346 |

# 4 Future Work

Future work could focus on developing a security research platform for RISC-V based on gem5, providing a modular framework for analyzing vulnerabilities. This platform could include customizable templates for cache and pipeline designs, and automated tools for profiling and visualizing key metrics like speculative execution and cache behaviors. Integrating standardized APIs would further enhance its versatility, enabling researchers to explore attack vectors and mitigation strategies more effectively.

# 5 Conclusion

This paper demonstrates the feasibility of using gem5 for RISC-V security research by implementing and validating access-retired attack. Simulation-based approaches provide a powerful tool for advancing RISC-V security, enabling researchers to identify and mitigate vulnerabilities in a cost-effective and scalable manner.

# References

[Gea23] Lukas Gerlach et al. A security risc: microarchitectural attacks on hardware risc-v cpus. In *IEEE Symposium on Security and Privacy (SP)*, 2023.

[LP24] Jason Lowe-Power. Gem5 documentation, Sat 29 June 2024. [Online]. Available: `https://www.gem5.org/documentation/`.