



Adversary Virtual Platform in Embedded System Environment for RED TEAM

Thesis Presentation

Master's Degree in Computer Engineering

Supervisors:

Prof. Alessandro Savino

Prof. Stefano Di Carlo

Dr. Franco Oberti

Candidate:

Ismail Sanan



**Politecnico
di Torino**



Table of Contents

- ▶ Introduction
- ▶ Background on Embedded Systems Security
- ▶ Virtual Platform: gem5
- ▶ Spectre Attack SimulationReturn-to-Non-Secure (ret2ns) Attack
- ▶ Experimental Results
- ▶ Conclusions & Future Work



Problem Statement

Embedded systems are critical infrastructure across industries but face significant security challenges:

Widespread adoption in IoT,
automotive, healthcare, aerospace

Complex supply chain and legacy
system

Vulnerable to sophisticated attacks

Limited security testing capabilities



Problem Statement



Key Challenge:

→ Is it practical for red team operators to use a virtual platform to simulate hardware-based attacks?



Objectives

This thesis aims to develop and evaluate Adversary Virtual Platforms (AVPs) for security testing of ARM based embedded systems.

Main Goals:

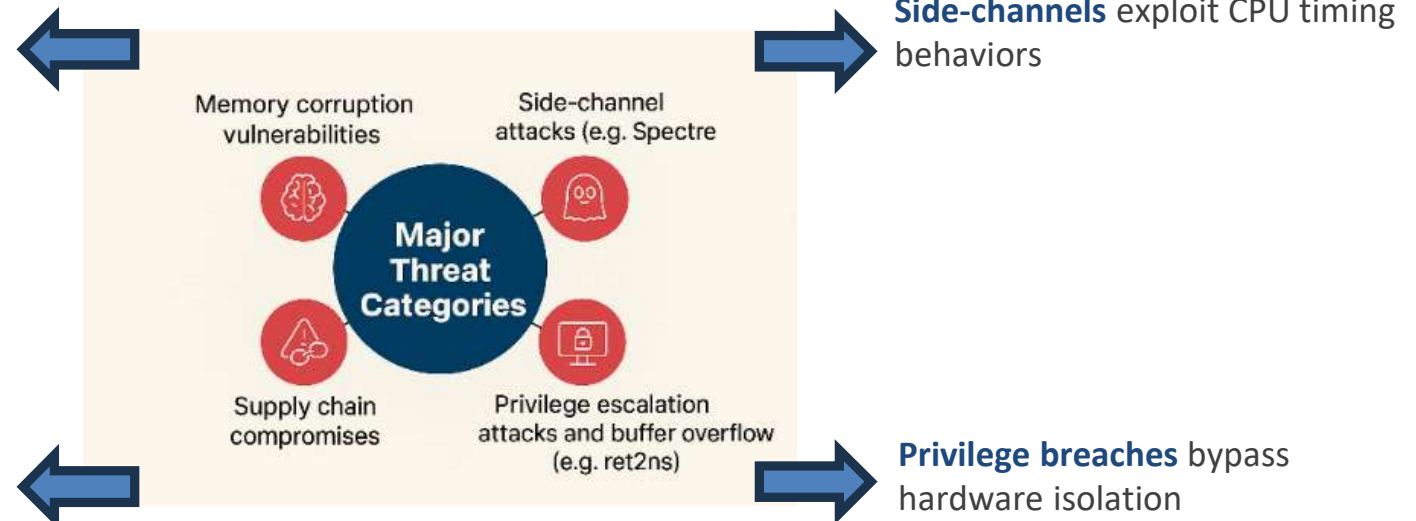
- Simulate realistic attack scenarios in controlled environments
- Demonstrate Spectre vulnerability exploitation
- Explore ret2ns attack in TrustZone-M systems
- Provide cost-effective alternative to physical hardware testing



Background - Embedded Systems Security Why Security Matters

Memory attacks corrupt execution flow

Supply chain
understanding attacks at the microarchitectural level which gem5 enables through detailed simulation and analysis

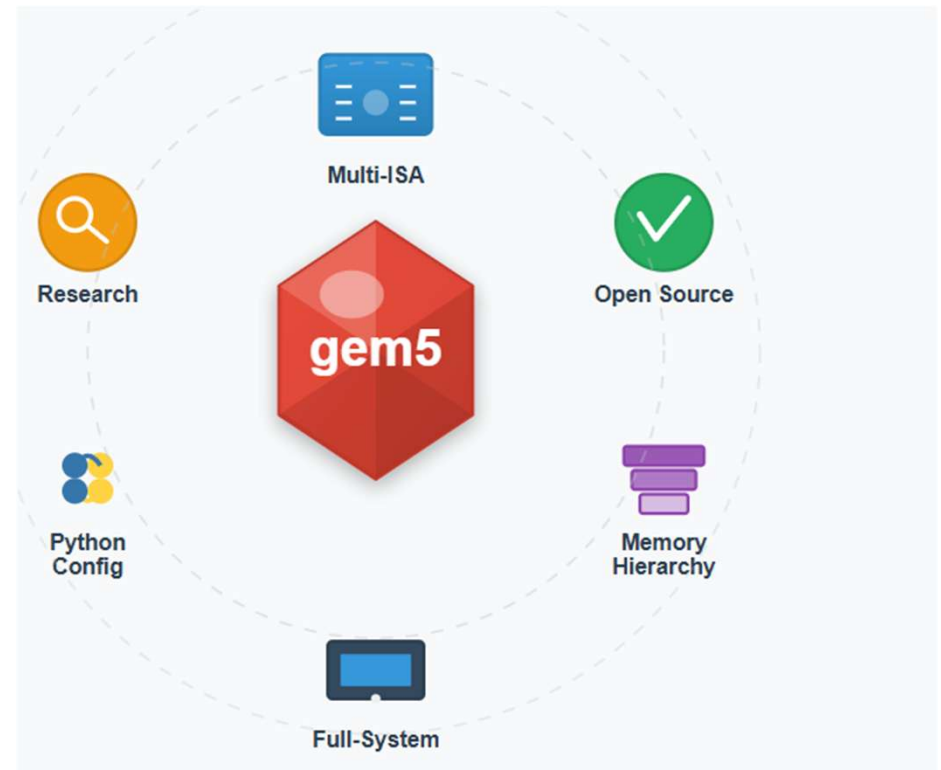




Virtual Platform - why gem5 Simulator

gem5: A Powerful Research Tool

- Open-source computer architecture simulator
- Supports multiple ISAs including ARM
- Full-system simulation mode
- System Emulation simulation mode
- Detailed microarchitectural modelling

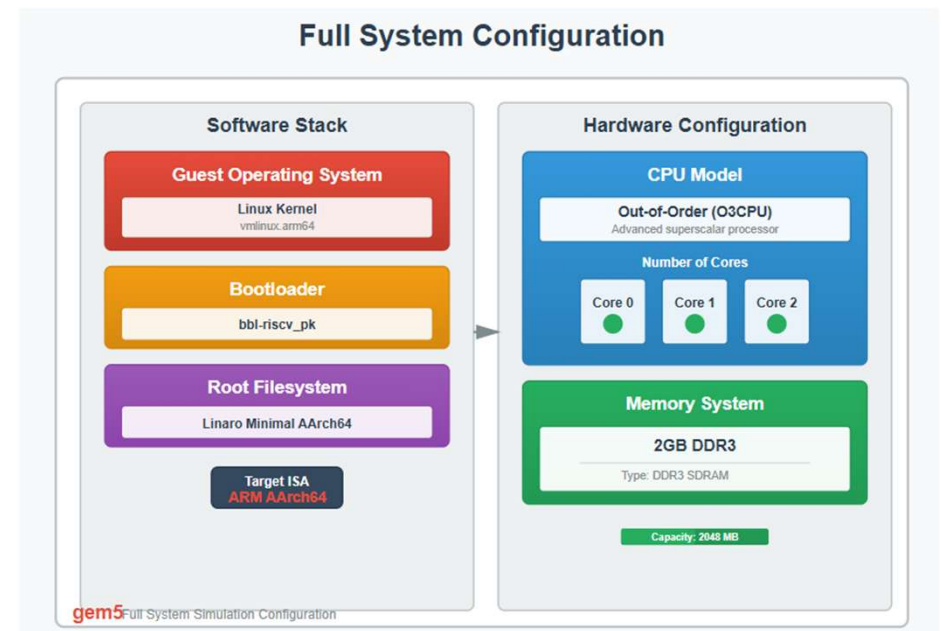




Virtual Platform - Simulation Setup

Full System Configuration:

- ❖ Guest OS: Linux (vmlinux.arm64)
- ❖ Bootloader: bbl-riscv_pkRoot
- ❖ Filesystem: Linaro Minimal
- ❖ AArch64CPU Model: Out-of-Order (O3)Cores: 3
- ❖ Memory: 2GB DDR3





Spectre Attack - Overview

What is Spectre?

A microarchitectural attack exploiting speculative execution to leak sensitive information.





Spectre Attack - Overview

What is Spectre?

A microarchitectural attack exploiting speculative execution to leak sensitive information.



Why It Matters:

Affects multiple CPU vendors, Advanced Attack to bypass traditional security boundaries



Spectre Attack - Simulation Process

Implementation Steps:

1. **Compilation:** Cross-compile Spectre exploit for ARM
2. **gem5 Setup:** Configure O3 CPU model with branch prediction
3. **Execution:** Run exploit in full-system mode
4. **Data Collection:** Extract data and cache timing
5. **Visualization:** Use Kotana for pipeline analysis



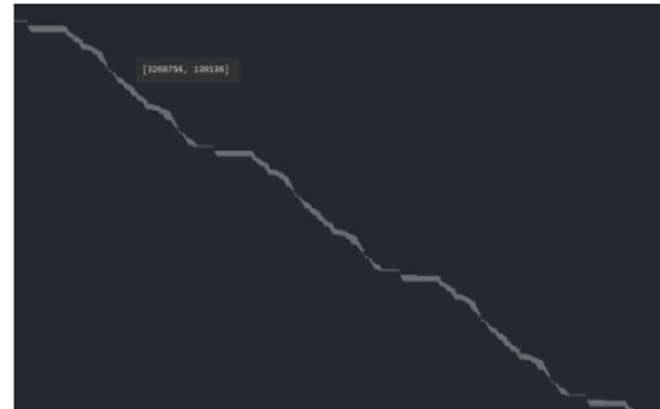
Spectre Attack - Results

Successful Information Leakage Demonstrating

Key Findings:

- ✓ Spectre attack successfully simulated in gem5
- ✓ High score (999/999) indicates successful data extraction
- ✓ Pipeline visualization using Kotana for deeper analysis
- ✓ QEMU user-mode also validated attack feasibility

```
1  
2  
3 Reading 40 bytes:  
4 Reading at malicious_x = 0xffffffffffffeb6... 999 999  
5 Reading at malicious_x = 0xffffffffffffeb7... 999 999  
6 Reading at malicious_x = 0xffffffffffffeb8... 999 999  
7 Reading at malicious_x = 0xffffffffffffeb9... 999 999  
8 Reading at malicious_x = 0xffffffffffffeba... 999 999  
9 Reading at malicious_x = 0xffffffffffffebb... 999 999
```





ret2ns Attack - Overview

Return-to-Non-Secure Attack:

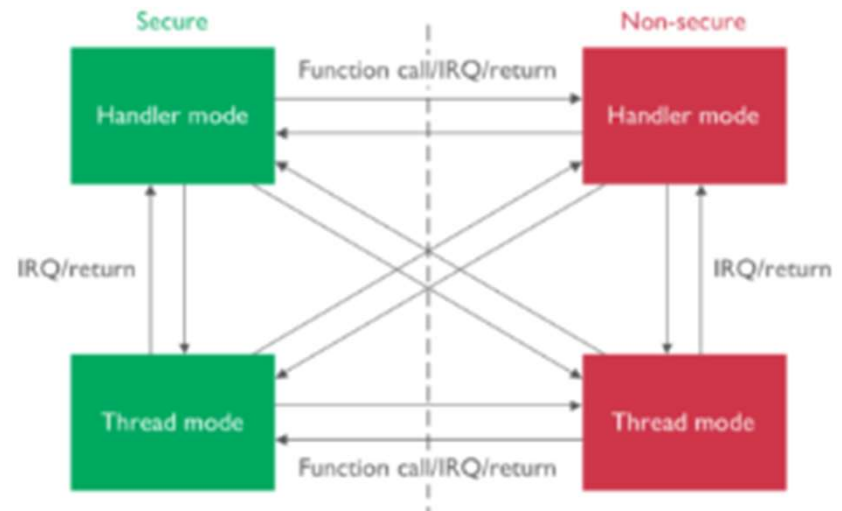
Exploits TrustZone-M's fast state-switching mechanism to redirect execution from secure to non-secure state with elevated privileges.

Attack Prerequisites:

- Memory corruption in secure state
- Vulnerable control-flow pointers (BXNS/BLXNS)
- Lack of control-flow integrity checks

Attack Flow:

Secure State → Corruption → Redirect → Non-Secure Code Execution (with privileged access)





ret2ns Attack - Simulation Challenges

gem5 Architectural Limitations:

- No standard TrustZone-M extension available
- Security-critical branch instructions incompletely modeled
- MPU functionality gaps in simulation framework

System-Level Challenges:

- Complex integration of Buildroot with TF-M security framework
- Intricate memory domain partitioning requirements
- Custom bootloader development necessitated by platform constraints



Comparison

Spectre Simulation:

Platform	Success	Accuracy	Limitations
gem5 FS Mode	✓	High	Timing approximations
gem5 SE Mode	✗	N/A	Crashes before completion
QEMU User-Mode	✓	High	Limited microarchitecture detail



Comparison

Ret2ns Simulation:

Aspect	Status	Notes
TrustZone-M Setup	Partial	Requires custom extensions
State Transitions	Limited	Missing BXNS/BLXNS support
MPU Simulation	Incomplete	Manual workarounds needed



Conclusion

Key Achievements:

- ✓ Successful Adversary Virtual Platform development for ARM Cortex-M3
- ✓ Validated Spectre attack in gem5 full-system simulation
- ✓ Identified critical gaps in TrustZone-M simulation capabilities
- ✓ Demonstrated cost-effective security evaluation methodology

Future Directions:

- Extend gem5 TrustZone-M support
- Expand gem5 security extensions



Thank you for listening!

Any questions?