Course Staff

• Instructor: Mengjia Yan
  • mengjia@csail.mit.edu
  • Office: 32-G840
  • Office Hours: By Appointment

• TA: Peter Deutsch
  • pwd@mit.edu
  • Office: 32-G786
  • Office Hours (32-G7 Lobby):
    • 10AM-12PM Wednesdays
    • 6PM-8PM on Lab Due Dates
    • And by appointment
Course Contributors

Joseph Ravichandran

Peter Deutsch

Jack Cook

Weon Taek Na

Miguel Gomez-Garcia

Yuheng Yang

Mengyuan Li
Today’s Agenda

1. Course Overview

2. Course Logistics: assignments, labs, grading, etc.
Course Overview
Hardware Attacks on The Spotlight
It is not a bug!

The attacks target the key micro-architecture mechanism of processors: speculative execution.
Hardware Security Defenses

Hardware Security Features

- What do hardware security features offer?
- Better performance?
- More secure due to physical shields?
- Easy to use?
Why take this course?

• The topic: Study security attacks and defenses primarily focusing on the hardware

1. Real-world hardware attacks
   • Not bugs. a) affect broadly; b) difficult to fix.

2. Defenses
   • What is good? Tradeoff between security and performance/cost

3. Hardware security features
   • Move SW features to HW. a) better performance, b) physical shield

4. Cross system abstractions
System Abstractions

Programs

Analog Circuits; Devices (transistors)
The Digital Abstraction

Voltage Transfer Characteristics

-> Build combinational and sequential circuits
-> Build general-purpose processors
The ISA Abstraction

Software’s View of the Processor

A 5-stage Pipelined Processor
The Virtual Machine Abstraction

Motivation:
- Cumbersome to use hardware resources
- Security issues when running multiple programs
- Need coordination between programs
The Virtual Machine Abstraction

Application’s View

Memory Space from 0x00...00 to 0xFF...FF (48bits)

Virtual memory (Address translation)

Physical memory sized from 2GB to 32GB

>100 processes run together

Process scheduling (Interrupts)

4-8 physical cores

Use hardware devices via APIs, such as print, read, write

System calls

Talk to the devices following protocols, tediously read/write device registers

Physical HW
System Abstractions

Programs

System Software (virtual memory, process, I/O) <- 6.1810[6.828]

Computer Architecture (caches, core, pipelining) <- 6.5900[6.823]

Digital Circuits (combinational and sequential circuits)

Analog Circuits; Devices (transistors) <- 6.6010 [6.374]
Abstractions

• A well-understood interface that hides the details within a subsystem

• Why use abstractions?
  • Good abstraction let us reason about the behaviors of a system while shielding us from the details of implementations
  • Implementation technologies can evolve while preserving the engineering investment at other levels

• Hardware security attacks usually break abstractions
Hardware Attack Examples

• Example #1: Rowhammer breaks the digital abstraction

• Examples #2: Side Channel breaks the ISA abstraction

• Note covered: hardware trojan, supply chain attacks, cryptographic accelerators, etc.
Course Assignments: Lectures, Paper Discussion, Grading

Navigate through the course website
Hardware Security: The Evil and The Good

- Attack modern processors
- Know how to design defenses better
Preview on Lab Assignments

1. Website Fingerprinting Attack
2. Cache Attack
3. Speculative Execution Attack
4. Rowhammer
5. ASLR Bypassing
6. Hardware Fuzzing and Verification
Final Project

• Original research project to substitute Labs 4-6

• Deliverables
  • Proposal (schedule pre-proposal meetings with me)
  • Weekly report (short and informal)
  • Final report + Final presentation

• Open-ended topics
  • Must have some hardware security angle
Preview of In-class CTF

1. Learn C/C++

2. Physical attacks on embedded systems/microprocessors

3. Tool chain for fuzzing and formal verification
Next: Side Chanel Overview