

6.595

Secure Hardware Design

Mengjia Yan

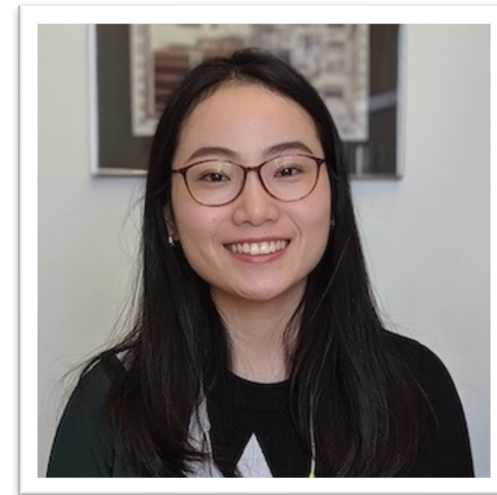
Spring 2024



Course Staff

Instructor: Mengjia Yan

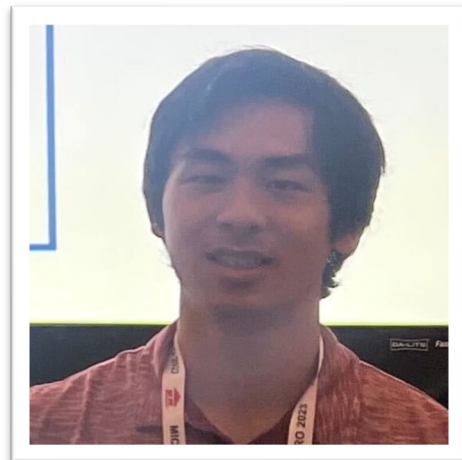
- mengjia@csail.mit.edu
- Office: 32-G840
- Office Hours: Friday 2:30-3:30pm



TAs



Yuheng Yang



Willian Liu



Peter Deutsch



Joseph Ravichandran

Email: shd-staff@mit.edu

Office: 32-G786

Office Hours (32-G7 Lobby)

- Monday: 4pm-6pm
- Wednesday: 10am-noon
- Lab Due Dates: 10am-noon & 6pm-8pm

Three Websites

- Course website: <https://shd.mit.edu/2024/>
 - All the course policy, grading details, lecture slides, lab handouts, etc.
- Piazza: Announcements and Q&A
- Canvas: Submit your lab assignments and homework

Average Response Time:

36 min

Today's Agenda

1. Course Overview: What you can get from this course?
2. Course Logistics: assignments, labs, grading, etc.
3. Review basic architecture materials (from 6.1910 [6.004])

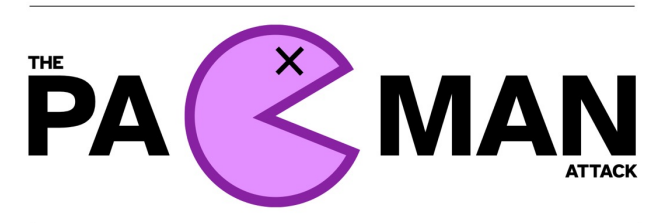
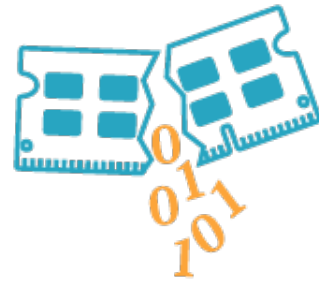
Course Overview



Hardware Attacks on The Spotlight



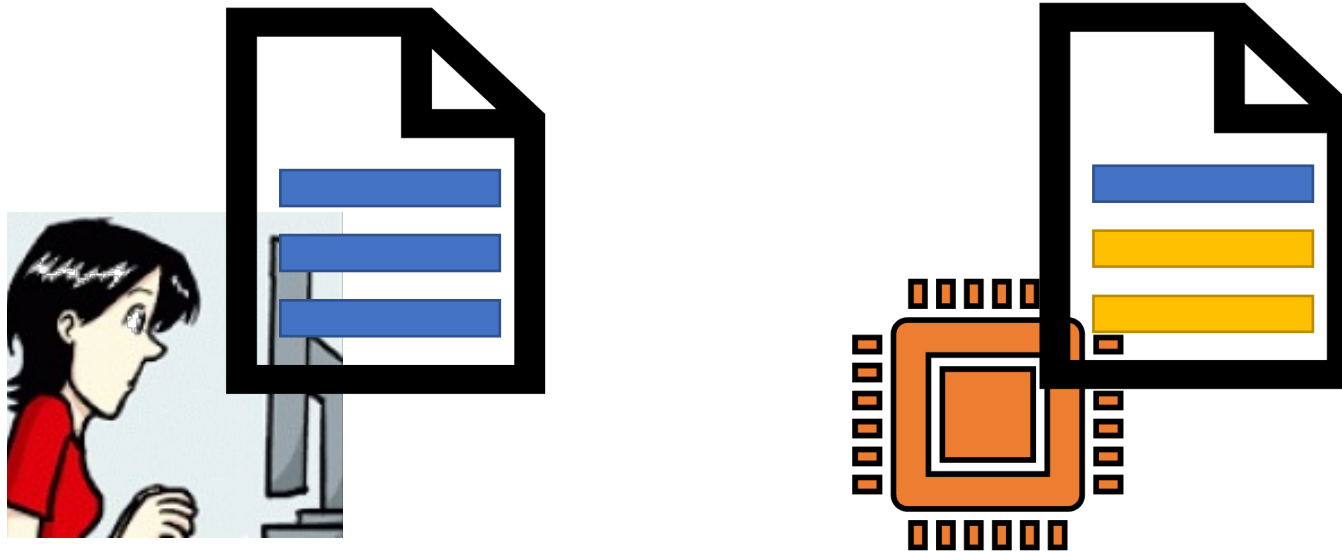
FORESHADOW





It is not a bug!

The attacks target the **key micro-architecture mechanism** of processors: speculative execution.



Mitigation Choices

- A) A comprehensive mitigation that can block all the attacks in a specific category
- B) An ad-hoc mitigation that can block some but not all the attacks in the category

Which one do you choose?

But what if?

A) is 15% slower than B) and also consumes 1.5x more energy than B)

What mitigation has been deployed?

Software Security Guidance





This information is designed for developers and systems experts looking to understand potential vulnerabilities and assess risk, with resources and recommendations for building more secure solutions.



[Overview](#) [Advisory Guidance](#) [Best Practices](#) [Disclosure Documentation](#) [Feature Documentation](#) [More Information](#)

Advisory Guidance

Overviews and one-page descriptions of security advisories along with recommended mitigations for affected environments.

Find industry-wide severity ratings in the [National Vulnerability Database](#).

 Critical  High  Medium  Low

CVSS	Title	CVE	SA	Severity	Disclosure Date
 6.0	Stale Data Read from Legacy xAPIC	CVE-2022-21233	INTEL-SA-00657	Medium	2022-08-09
 5.5	Post-Barrier Return Stack Buffer Predictions	CVE-2022-26373	INTEL-SA-00706	Medium	2022-08-09

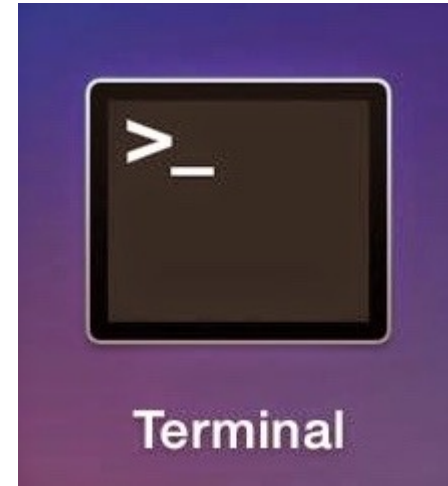
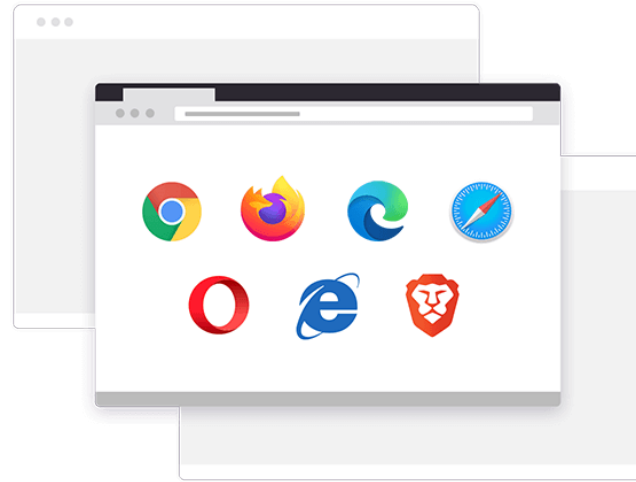
<https://www.intel.com/content/www/us/en/developer/topic-technology/software-security-guidance/advisory-guidance.html>

Hardware Security Features



- What do hardware security features offer?
- Better performance? More secure due to physical shields?
- Pros and cons?

What programmers see?



A computer system

System Abstractions

Programs



**Virtual
Machine**

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



**Instruction Set
Architecture (ISA)**

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

Digital Circuits (combinational and sequential circuits)



**Digital
Abstraction**

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

Hardware Attack Examples

- Hardware security attacks usually **break abstractions**
- Example #1: Side Channel breaks the ISA abstraction
- Examples #2: Rowhammer breaks the digital abstraction

Course Logistics: Lectures, Paper Discussion, Grading

Navigate through the course website



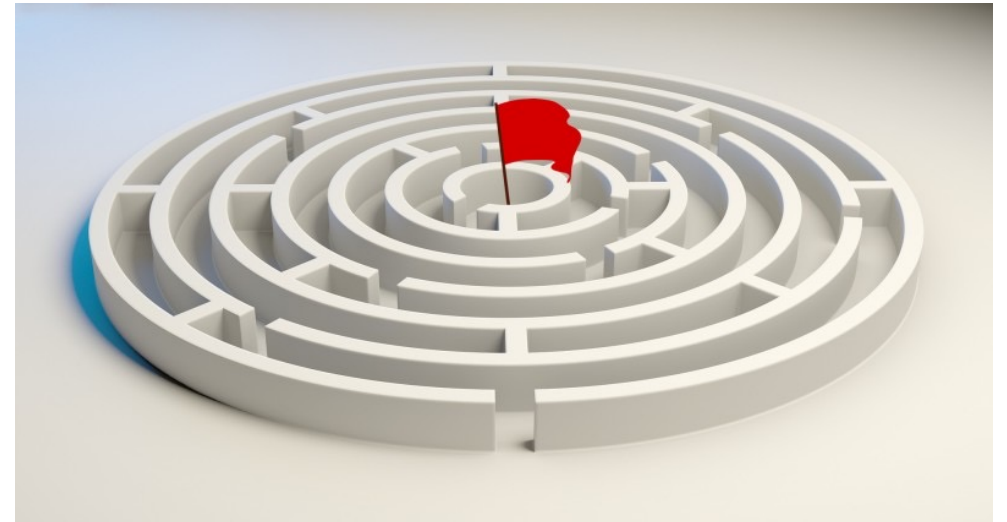
Hardware Security: The Evil and The Good

- Attack modern processors
- Know how to design defenses better



Preview of Lab Assignments

1. Website Fingerprinting Attack
2. Cache Attack
3. Speculative Execution Attack
4. Rowhammer
5. ASLR Bypassing
- 6a. Hardware Fuzzing
- 6b. Formal Verification for Hardware



Preview of Recitation Sessions

1. Learn C/C++ (CTF)
2. Attack Platform Introduction and Cache Attacks Office Hours
3. Physical attacks (CTF)
4. RISC-V System Programming
5. Tool chain for hardware formal verification

Paper Discussions

- Mimic PC meetings
 1. Two discussion leaders: One summarizes the paper, the other points out the pros and cons of the paper
 2. The audience ask questions and clarifications, discussion leaders answer questions
 3. The whole class votes: a) best paper; b) accept; c) reject
- Paper assignment and grading details will be released in Week 3

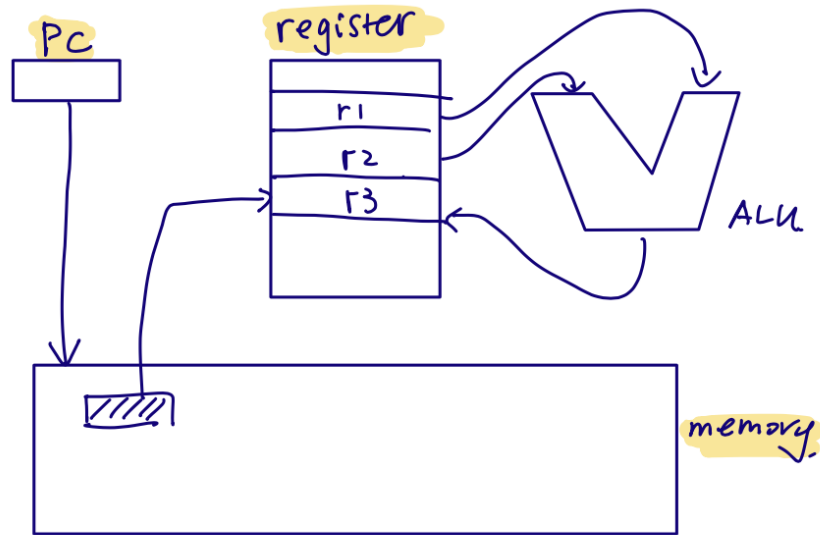
Review

Basic Architecture Concept

- ISA and Pipelined Processors
- Virtual Memory

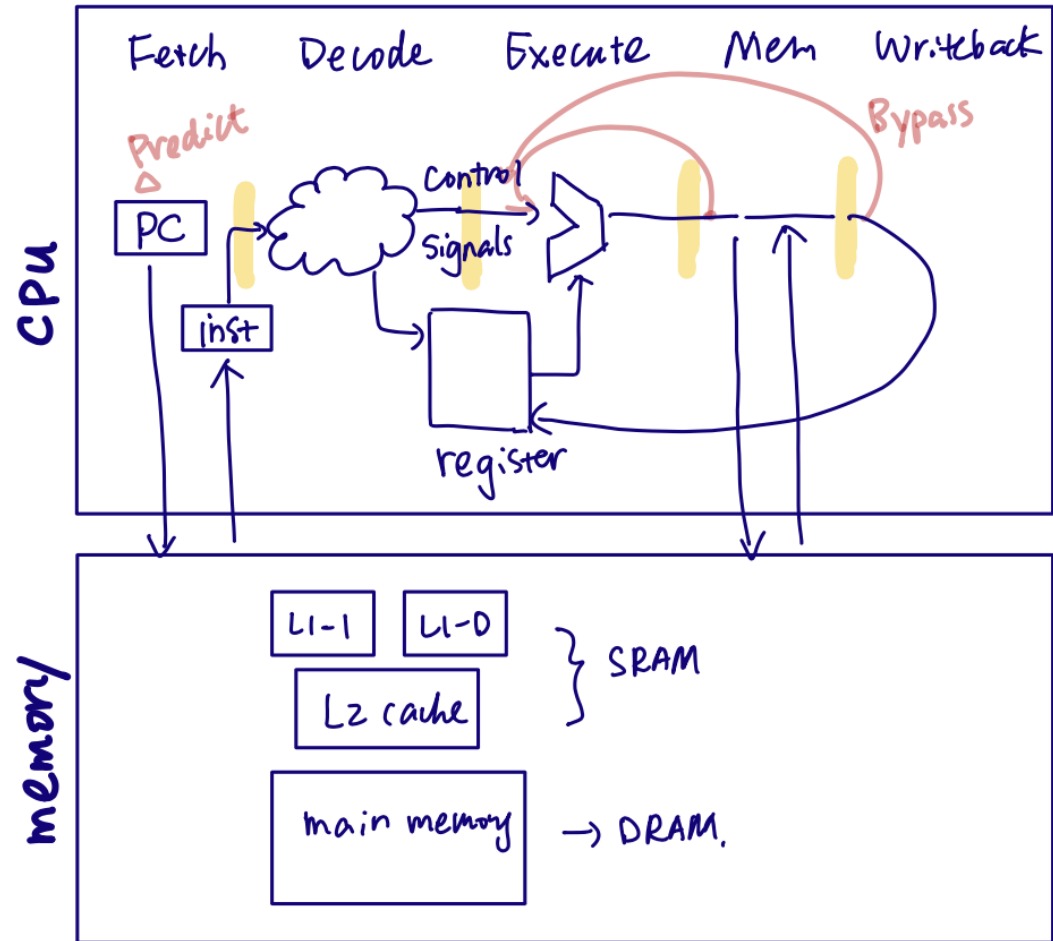


ISA and A Pipelined Processor



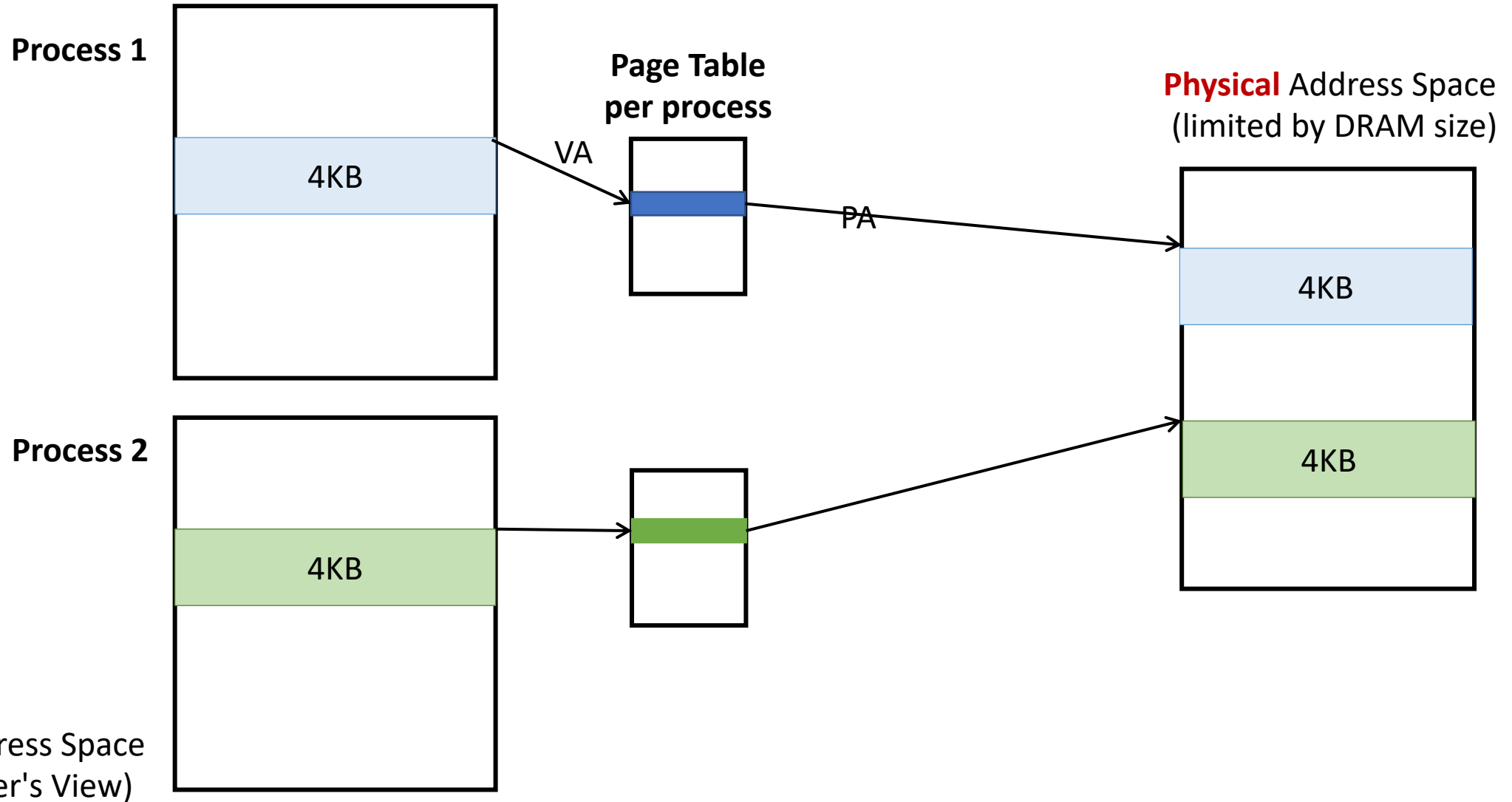
inst: Add r3, r1, r2.

Software's View of the Processor



A 5-stage Pipelined Processor

Virtual Address & Address Mapping



Next: Side Chanel Overview

