CS59300: Microarchitecture Security

Spring, 2023
Updated: Oct 27 2022

Instructor: Mohammadkazem (Kazem) Taram
E-mail: kazem@purdue.edu
Web: https://www.cs.purdue.edu/homes/mtaram/
Office Hours: tbd
Class Hours: TTH 1:30
Office: tbd
Class Room: RED 103

Course Description

This course will focus on the interaction of computer security and computer architecture. We will start with the basic architectural background: caches and memory hierarchy, out-of-order execution, speculative execution, and branch prediction. Then we will discuss fundamental system security concepts such as isolation, memory safety, side- and covert-channels, etc. This gives us the necessary background to dive deeper into understanding of how microarchitecture can be exploited to leak information. We will discuss the classic and recent attacks that leverage different architectural structures/components which include caches, branch prediction, DVFS, DRAM, and accelerators/FPGAs. We will then cover high-performance architectural solutions to mitigate those attacks. We will also talk about fundamentally secure approaches and architectures such as constant-time programming, capability-based architectures, and information flow tracking. Finally, we will discuss how architecture can provide efficient support for security and privacy, where we talk about solutions such as Trusted-Execution Enviourments (TEEs) and architecture support for memory safety and isolation.

Learning Objectives

- Understand the performance-security tradeoffs and challenges brought by architectural performance optimizations
- Learn how to design secure processor architectures
- Learn how to evaluate architecture security solutions (performance and security)

Prerequisites

Prerequisites: Undergraduate Computer Architecture (CS250 or equivalent).

Course Format

- **Lectures:** 60% of the class will be lectures by the instructor. Lectures will be in-person. Students are expected to attend most of the lectures.
- **Student Presentations:** Students (individually or in groups, depending on the size of the class) are expected to present and lead the discussion of papers from the research literature to class. The papers will be selected by the instructor. A good presentation will include the necessary background and motivation, will explain overall merit and technical details, and provide answers to questions from the audience. While presenting a paper, a critical perspective will be encouraged and students do not need to necessarily defend the paper. All students are expected to read the paper before each class and participate in the class discussion.
- **Programming Assignments:** There will be two labs to prepare students for their research projects. The first lab will be on microarchitectural attacks where we implement multiple attacks on real systems. The second lab will be on microarchitectural mitigations, where we evaluate the performance overhead of a security mitigation strategy in a architecture simulator.
- **Research Projects:** Students will work on a research project within the scope of the course. Depending on the topic/class size the projects can be done individually or in groups. Students will present the project proposal, status, and results to class during the course.
- **Reading Quizzes:** There will be online quizzes due the start of each class to further encourage students to read the papers.
- **Office Hours:** Office hours attendance are optional. Office hours will be announced during lecture and/or Piazza.

Reading Materials

This will be mostly a paper reading course, but we will do some readings from the following textbook.

"Principles of Secure Processor Architecture Design", Jakub Szefer

This is part of the oustanding Synthesis Lectures series, which can be found here: Synthesis Lectures on Computer Architecture. Those books will be free to access while you are on the Purdue domain. There are so many great references there (including another security book by Ruby Lee), any number of which would be useful for research in architectural security.

High-Level Course Outline

- Introduction

- Computer Architecture background
- Fundamental Security concepts
- Traditional Side-Channel attacks and defenses
- Transient execution attacks and defenses
- Rowhammer attacks and defenses
- Physical Side-Channel attacks and defenses
- Some more general defense approaches
- Fundamentally secure architectures/approaches

Assessments

- Research Project: 40%
- Paper Presentations: 20%
- Online Quizzes (for readings): 20%
- Midterm: 20%