Hardware Security and Side-Channels

Course Description:

The goal of this course is to prepare students for a world where hardware vulnerabilities can leak secrets to software-only attackers. Students will read cutting-edge research papers and complete lab assignments that will guide them towards conducting state-of-the-art side-channel attacks against real hardware. This course will practically demonstrate the pitfalls of widely adopted modern hardware design decisions, and will prepare students to design hardware and software resilient against such attacks.

Course meetings will be split roughly 50-50 between lectures prepared by the instructor and student-led discussions on relevant research papers. The papers and lectures will cover a range of hardware security topics, including but not limited to: cache side-channels, speculative execution attacks, memory attacks, secure hardware design, how side-channels can subvert commonly deployed cryptosystems and Trusted Execution Environments, and more.

General Course Information:

Term: Spring 2025
Department: COMP
Course Number: 790
Section Number: 184

Time: TuTh, 12:30-1:45PM
Location: SN115
Website: https://andrewkwong.org/comp790-184.html

Instructor Information:

Name: Andrew Kwong
Office: FB340
Email: andrew@cs.unc.edu
Website: https://andrewkwong.org
Office Hours: TBA

Target Audience:

This class is intended for graduate students and advanced undergraduate students interested in exploring how real-world systems can fail due to design choices in the underlying hardware. A background in computer security is not required, though students may find it helpful.

Prerequisites:

There are no prerequisites for this course, though it will help to have taken upper division courses on computer architecture and operating systems. Interested undergraduates may request an override.

Goals and Key Learning Objectives:

By the end of this course, students should:

- Be capable of carrying out a variety of side-channel attacks that form the building blocks of offensive hardware security research
- Be comfortable with reading cutting edge research papers in hardware security, and be able to analyze the papers' strengths and weaknesses
- Be capable of beginning to pursue novel research on a topic within hardware security

Grading Criteria:

Class Participation (10%):

Students are expected to contribute to class discussions following paper presentations. Students should be able to ask insightful questions and demonstrate that they have read and understand the assigned readings.

Paper Presentations (15%)

Students will give conference style talks on assigned papers. They will prepare slides and a 20-30 minute presentation on the papers. They will then lead the class on discussing the papers' contributions and impact.

Paper Reviews (15%)

Students will submit mini-reviews on assigned papers that pinpoint the paper's strengths and weaknesses. These will be submitted to Canvas.

Lab Assignments (60%)

Students will complete programming-oriented lab assignments that are designed to guide them towards carrying out real-world attacks on hardware. There will be three to four in total, focused on providing students with an opportunity to put theory into practice.

Class Schedule and Important Dates:

Please see the class website for a detailed calendar of important dates and the reading schedule.

Accessibility Resources and Services:

The University of North Carolina at Chapel Hill facilitates the implementation of reasonable accommodations, including resources and services, for students with disabilities, chronic medical conditions, a temporary disability, or pregnancy complications resulting in barriers to fully accessing University courses, programs and activities.

Accommodations are determined through the Office of Accessibility Resources and Service (ARS) for individuals with documented qualifying disabilities in accordance with applicable state and federal laws. See the ARS Website for contact information: https://ars.unc.edu or email ars@unc.edu.

Counseling and Psychological Services:

CAPS is strongly committed to addressing the mental health needs of a diverse student body through timely access to consultation and connection to clinically appropriate services, whether for short or long-term needs. Go to their website: https://caps.unc.edu/ or visit their facilities on the third floor of the Campus Health Services building for a walk-in evaluation to learn more.

Title IX Resources:

Any student who is impacted by discrimination, harassment, interpersonal (relationship) violence, sexual violence, sexual exploitation, or stalking is encouraged to seek resources on campus or in the community. Reports can be made online to the EOC at https://eoc.unc.edu/report-an-incident/. Please contact the University's Title IX Coordinator (titleixcoordinator@unc.edu), Report and Response Coordinators in the Equal Opportunity and Compliance Office (reportandresponse@unc.edu), Counseling and Psychological Services (confidential), or the Gender Violence Services Coordinators (gvsc@unc.edu; confidential) to discuss your specific needs. Additional resources are available at safe.unc.edu.

Policy on Non-Discrimination:

The University is committed to providing an inclusive and welcoming environment for all members of our community and to ensuring that educational and employment decisions are based on individuals' abilities and qualifications. Consistent with this principle and applicable laws, the University's Policy Statement on Non-Discrimination offers access to its educational programs and activities as well as employment terms and conditions without respect to race, color, gender, national origin, age, religion, creed, genetic information, disability, veteran's status, sexual orientation, gender identity or gender expression. Such a policy ensures that only relevant factors are considered and that equitable and consistent standards of conduct and performance are applied.

If you are experiencing harassment or discrimination, you can seek assistance and file a report through the Report and Response Coordinators (see contact info at safe.unc.edu) or the Equal Opportunity and Compliance Office, or online to the EOC at https://eoc.unc.edu/report-an-incident/.

Diversity Statement:

I value the perspectives of individuals from all backgrounds reflecting the diversity of our students. I strive to make this classroom an inclusive space for all students. Please let me know if there is anything I can do to improve. I appreciate suggestions.

Syllabus Changes:

I reserve the right to make changes to the syllabus, including assignment due dates and test dates. These changes will be announced as early as possible.