Hardware Security

Bulletin Description

This is a graduate course in hardware security. We will learn about how hardware can support the design of secure software systems and how to keep the hardware itself secure from malicious actors. The course will be discussion based, with classes organized around reading and discussing papers. In addition, students will work on a semester long research project of their choosing.

General Course Info

Term:	Spring 2016
Department:	COMP
Course Number:	790
Section Number:	132
Time:	TTh 2:00 – 3:15
Location:	SN 011
Website:	https://sites.google.com/a/cs.unc.edu/hardware-security-sp2016

Instructor Info

Name:	Cynthia Sturton
Office:	FB354
Email:	csturton@cs.unc.edu
Phone:	919-590-6020
Website:	http://www.cs.unc.edu/~csturton
Office Hours:	By appointment

Textbook and Resources

There are no required textbooks. Required readings will be posted online in the course schedule.

Course Description

Hardware sits at the base of any system stack and as such forms the foundation upon which the security of the system rests. Hardware can enhance the system's security by providing the tools and building blocks

that will support the design of secure software. Examples of such building blocks include Intel's Secure Enclave, Trusted Platform Modules, and even hardware-supported page tables. But, hardware can also be the weakest link – if the security of the hardware is compromised, the security of the entire system is compromised.

In this class we will learn about different ways in which hardware can support software, known threats to the security of hardware, and the latest research on mitigating those threats. Some of the topics we will cover in this class include: Hardware Trojans, Side Channel Analysis, IP Piracy, Hardware Roots of Trust, and Tamper Resistance.

Target Audience

The class is designed for students who are interested in hardware and systems security. The course will be research focused: classes will be centered around discussion of published research in the security and hardware communities, students will work on an original research project, and students will write a conference-style paper describing their work.

Prerequisites

This class is open to all CS graduate students. Undergraduate CS students and graduate students outside the CS department who wish to take the class should attend the first week of class and speak to the instructor at the end of class.

Course Requirements

Students will read 1 to 2 papers per class. Classes will be organized around a combination of lecture and paper discussions; reading the paper is necessary in order to contribute to the discussion. For each paper, students will write a short synopsis and review.

Students will be responsible for presenting some yet-to-be-determined number of papers during the semester (three is the current plan).

Students will work in groups of 2 on an original research project. At the end of the semester, each group will submit a conference-style paper and give a short (10–15 min) presentation in class describing their work.

Key Dates

Project proposal presentations: 2/9/16
Project proposals due (11:59 PM): 2/11/16
Project status report presentations: 3/10/16
Final in-class presentations: 4/26/16
Final project report due (11:59 PM): 4/28/16

Grading Criteria

Final project: 38%
Class discussion & written reviews: 35%
Leading paper discussions: 27%

Course Policies

Classes are centered around discussions of papers; attendance is necessary in order to participate in the discussion.

Honor Code

Any outside source used as part of a paper review (other papers, textbooks, websites) must be properly cited.

The final project must be original research. Students will work in groups of 2 or 3 for the final project, and submit one written report per group.

In the course of this class we may discuss known vulnerabilities and attacks on computer systems. This is not an invitation to exploit these vulnerabilities in real systems. You may not attempt to break into any system that is not your own; you may not attempt to thwart or circumvent the security of any system that is not your own. Doing so is, at a minimum, a violation of the honor code, and possibly a violation of the law.

Course Schedule

The course schedule will be posted on the course website.

Disclaimer

The professor reserves to right to make changes to the syllabus, including project due dates. These changes will be announced as early as possible.