CS 598CLF – Secure Processor Design

Fall 2019
Instructor: Chris Fletcher
Location: Siebel, Room 1302
Time: Wednesday and Friday, 11:00am to 12:15pm
Course website: http://cwfletcher.net/598fa19.html

Helpful, not necessary:
CS 433 (Computer Architecture)
CS 461 (Computer Security)
ECE 385 (Digital Systems Laboratory)
CS 423 (Operating Systems Design)

Catalog description:
Processors, more generally Microarchitectures, have recently become the front lines in the battle to construct (and destruct) secure systems. Researchers today face a choice. One can choose the Light Side and participate in an ongoing renaissance to build secure hardware, through new abstractions such as Enclave-based computing. One can also choose the "Dark" Side and participate in the largest ongoing effort to "break" (= vet) hardware the world has ever seen. This course will study both perspectives. More broadly, we will study the cutting-edge in secure processor architecture by examining the interplay between hardware, software and applied cryptography in these systems. The first several classes will feature lectures from the instructor: to give background on secure hardware systems from the standpoints of Computer Architecture and Applied Cryptography. The body of the course will be readings and discussion of late breaking (primarily last several years) papers in the field and guest lectures from industry. Course assignments will give students hands-on experience with microarchitectural covert channels. The end of semester will culminate in an original research project.

Intended audience:
This class is primarily intended for students who would like to conduct secure systems research where hardware plays a first-class role. It will also appeal to students with a casual interest in this hot topic, or who want to do research in computer security generally.

Grading:

- Paper reading (2 papers / week) - 35%
    - Discussion lead for 1-2 papers – 10%
    - 500 word summary + a discussion question / paper – 20%
    - Participation – 5%
- MPs - 15% (not counting extra credit)
- Final project - 40%
    - Proposal – 10%
    - Checkpoint – 10%
    - Final writeup (+ artifact if applicable) – 15%
    - Final presentation – 15%

Major Topics: (for finer-grain detail see here)

- Introduction
    - History of hardware and physical security
    - Crash course on relevant Computer Architecture
    - Crash course on relevant Applied Cryptography
- Microarchitectural Side/Covert Channel Attacks and Defenses
    - Traditional side/covert channel attacks and defenses
    - Speculative execution attacks and defenses
- Data Oblivious Computing
    - Compilers for data oblivious computing
    - ISAs for data oblivious computing
    - Data oblivious algorithms
    - “Constant time” programming
- Enclave-based Computing
    - New hardware support for enclave-based programming and open source initiatives
    - Automatic application partitioning for enclave-based programming
    - Attacks on enclave-based environments
- Memory Safety
    - Overview and advanced attacks
    - Hardware mechanisms for defense
- Physical Attacks
    - Modern power analysis attacks
    - Modern Rowhammer attacks