EEL 5937: Attacks and Defense in Secure Architectures

Instructor: Dr. Fan Yao (fan.yao@ucf.edu)
Office: Zoom (Zoom invitation is sent through webcourse)
Email: fan.yao@ucf.edu
Course Schedule: Fridays, 3:00PM – 5:30PM
Office Hours: Fridays 12:30PM – 3:00PM, Zoom (Link to be announced)

Target Audience:

This course is aimed at graduate students or senior undergraduate students who would like to conduct research in secure processor design. It would also be appealing to students who are interested in engaging in hot topics in computer architecture security in general.

Course Description and Objectives:

The landscape of security has shifted significantly from software to computer hardware, particularly commodity processors. Recent advancements in adversarial activities (such as Spectre and Meltdown) have demonstrated the severity of security issues on modern processor architectures. Investigating and defending against attacks that manifest on modern processor architectures/microarchitectures is becoming the new frontier in security system design.

The course will bring students insights on the cutting-edge research in processor security with the understanding of the interactions between software, operating systems and the underlying system hardware. Students will gain hands-on experience on real-world attacks and defense techniques via a course project throughout the semester.

Pre-requisites:

Students in this course should have taken at least one prior course in computer architecture. Acceptable courses include EEL 4768 or an equivalent course. If unsure, contact the instructor, and discuss the requirements.

Topics covered:

Note: the topics are subject to change according to enrollment and student interests.

(1) Traditional secure processors design
   a. Tamper resistance
   b. Attestation

(2) Microarchitecture attacks
   a. Side channels
   b. Covert channel

c. Speculation attacks
d. Countermeasures on microarchitecture attacks

(3) Software attacks on program memory
a. JOP and ROP attacks
b. Memory corruption attacks
c. Detection and defense for CFI, DFI and memory corruption

(4) Physical attacks on memory
a. Rowhammer attacks
b. Countermeasures

(5) Trusted Execution Environment
a. Intel SGX
b. Attacks exploiting security enclave
c. Securing enclave applications

Textbook:

There is no required textbook for this class. However, the following textbook is strongly preferred:

1. Modern Processor Design: Fundamentals of superscalar processors, John Shen and Mikko Lipasti, Waveland Press, 2013
2. Security Basics for Computer Architects, by Ruby B. Lee, Synthesis Lectures on Computer Architecture, 2013.
3. Computer Architecture: A Quantitative Approach (Hennessy and Patterson), Morgan Kaufman, 5th edition.

Online Resources:

A number of readings are expected to be in the form of research articles and papers. Most of these resources are available online through IEEE Xplore, ACM Digital library. All of the UCF students are expected to have access to one of these databases. If you don't have access, contact the instructor immediately.

Grading policy:

This course targets at emerging security topics in processor design. The first a few lectures will cover some basic background in computer architecture and processor microarchitecture. The major body of the class is in-class presentation and discussions. Students are required to explore most recent research topics in secure processor design, proposal a original project and complete the project by the end of the semester.

The grading breakdown will be as below:

- Paper reading and presentation: 40%
    - Paper presentation: 2-3 papers 20%
    - Paper summary: 2 papers/week 20% (300-words summary + 2 questions)

- Final Project: 40%
    - Attack demonstration + Proposal: 10%
    - Final Project Presentation: 10%
    - Final Project write-up: 20%

- Assignments: 10%

- Discussion/participation: 10%

<u>Class Policy and requirements</u>:

There will be a course project that will be a semester-long development experience. Strong coding skills are needed and prior experience with simulators would help get started easily.

In most of the case, students are recommended to work on the project individually. Group work of 2 is allowed though contribution of each member must be clarified in the final report, while the amount of work should typically be doubled.

Academic integrity will be strictly enforced. If caught cheating, the student shall be reported and may result in failing the course. Students should familiarize themselves with UCFs Rules of Conduct at http://osc.sdes.ucf.edu/process/roc.