ECE 796/896/992 – Systems Security

Instructor: Dean Sullivan
Office: Kingsbury W214
Email: dean.sullivan@unh.edu
Office hours: TBD, or by appointment

Course Description: This course will focus on security at the intersection of hardware and software exploring a range of topics – from microarchitectural side-channels and transient execution attacks targeting commodity platforms, to fault injection and timing attacks on DRAM/CPU and caches, fuzzing of embedded systems and Trusted Execution Environments (TrustZone), cryptanalysis of hardware cryptographic engines using power analysis, and automated analysis and generation of attack workloads – to illustrate modern research challenges and applications in the area. Understanding of both theoretical underpinnings and practical demonstration will be emphasized, with a heavy bent towards the latter.

Course Purpose: This course will focus mostly on application of attacks in systems security within the context of building the skillset to construct more resilient platforms capable of meeting modern threats.

Credits: 4 credits

Pre-Requisites and Co-Requisites: CS 410/419 or equivalent (CS 415/416) and ECE 562 or equivalent (CS 520)

Text: Research and other materials will be provided by the instructor.

Programming Language: Programming experience will be helpful, including knowledge of one or more of the following - C/C++, Python, assembly (x86 & ARM), or HDL (Verilog/VHDL).

Software: Will be provided by instructor.

Course Goals:

- To introduce students to systems security and enable them to engage in related projects and research
- To introduce students to the fundamentals of security and privacy, threat models, offensive and defensive research, and relate them to areas of practical applications
- Introduction to microarchitectural side-channels and transient execution attacks
- Fundamentals of fault injection on DRAM and CPUs
- A survey of timing channel techniques targeting cache architectures
- To understand apply practical cryptanalysis as applied to hardware cryptographic accelerators using demonstration platforms

- To develop fuzzing techniques (black, grey, and white-box) for embedded systems and modern smartphones
- To instruct students on the automatic analysis and generation of attack workloads using evolutionary programming driven by microarchitectural telemetry
- To instruct students on the secure and resilient design of systems
- To survey current and emerging systems security topics

Course Topics (Tentative):

- Performance monitoring (MSRs) and timing
- Cache covert and timing channels (Flush+Reload, Prime+Probe, Eviction sets)
- Microarchitectural side channels (Meltdown & Spectre attacks)
- Transient execution attacks (RIDL, ZombieLoad, MDS, Machine Clears)
- Fault injection (Rowhammer, Plundervolt)
- Cryptanalysis (CPA and DPA) and introduction to ChipWhisperer/Sakura-G
- Embedded system vulnerability discovery via fuzzing (P2IM, DIMA)
- Introduction to ARM TrustZone and Coresight, smartphone rooting
- Smartphone vulnerability discovery via (Coresight-assisted) fuzzing
- Introduction to analysis and generation of attack workloads (MicroGP, GeST)
- Resilient systems design and architecture

Homework/Laboratory: The distinction between homework and laboratory will be blurred in this course as most assignments will blend aspects of both and require significant in-person effort.

Lab 1: Cache side-channel attacks
Lab 2: Microarchitectural and transient execution attacks
Lab 3: Fault-Injection
Lab 4: Cryptanalysis
Lab 5: Fuzzing

Readings/Presentation:
This course will source primarily from research materials. To that end, students will be required to both read, review, and present on these papers. Details will be provided for crafting an effective review and presentation.

Final Project: The final project will require coalescing the theoretical and practical skills learned throughout the course. Two forms of final will be allowed (796 only): 1) A survey paper on an agreed upon topic; 2) An agreed upon project demonstrating a novel attack/defense.

Grading:

Final Project	35%
Labs	45%
Readings	10%
Presentations	10%

Grading Scale:

A: 100 – 90
B: 89 – 80
C: 79 – 70
D: 69 – 60
F: Below 60

ECE 896: All students registered as ECE 896 will have additional design, report, and analysis requirements. In addition, these students will not be allowed to choose a survey option for final project and will be required to give an oral presentation and IEEE formatted report. Topics will be agreed upon with the professor.

Cheating and Plagiarism: Although exchanging ideas is encouraged, you must complete the course assignments by yourself (or with members of your team). It is forbidden under any circumstances to provide solutions to your classmates, share answers, or use someone else's work as your own. You may ask the instructor what is considered honest. **COPYING IS A VIOLATION OF UNH ACADEMIC INTEGRITY POLICIES AND WILL BE TREATED AS SUCH.**

Make-up Policy and Late Work: You will have a total of 5 late lab days which you can distribute amongst the assignments. In other words, you may use 1 late lab day for 5 labs or 5 late lab days for 1 lab.

Disability Statement: The University is committed to providing students with documented disabilities equal access to all university programs and facilities. If you are a student with a documented disability who will require accommodations in this course, please registers with Disability Services for Students (DSS). If you have received an accommodation letter for this class, please contact me immediately so we can discuss the necessary arrangements.

Emotional or Mental Health Distress: Your academic success in this course is very important. If, during the semester, you find emotional or mental issues are affecting that success, please contact the University's Counseling Center (PACS: 603-862-2090 or www.unh.edu/pacs).