EECS 598: Topics in Hardware Security

Instructor: Daniel Genkin, genkin@umich.edu

The security of a system is only as good as its weakest link. Even if a system's software is perfectly secure, the complex interactions between the system's hardware and the physical world have not been properly understood. Side-channel attacks exploit unintentional, abstraction-defying leakage from physical devices (such as the device's power consumption, electromagnetic radiation or execution timing variations) to recover otherwise-unavailable secret information.

In this class, we shall review recent papers in the area of side channel attacks and their mitigations. Specific topics include (but not limited to):

1. Physical side channel attacks such as power and electromagnetic analysis
2. Microarchitectural attacks such as cache attacks, and Rowhammer
3. Speculative execution attacks: Spectre, Meltdown and Foreshadow
4. Side channel mitigations and countermeasures

Class requirements:

1. 45min – 1hour presentation
2. Final project
3. Active participation in paper discussion

Class prerequisites: Prior experience in low level programing (C / C++ / assembly) is required. Familiarly with basic signal processing (for physical attacks) as well as basic operating system principles (for microarchitectural attacks) will be helpful. The class might also include some basic cryptographic background which is required for understanding attacks on cryptographic systems.