COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

DISSERTATION DEFENSE

Andrew Kwong

Applying Software-Based Side-Channels to Hardware Vulnerabilities

Wednesday, July 12, 2023
1:00pm – 3:00pm
Virtual – Zoom

ABSTRACT: The discrepancy between the abstract model used to reason about the security of computer systems and their actual hardware implementation has led to a myriad of security issues. Security researchers have demonstrated how to use shared microarchitectural components, speculative execution attacks, and even hardware based memory integrity attacks to extract sensitive information across nearly all hardware backed security domains. These ``side-channel'' attacks have violated boundaries necessary for the isolation and security of virtual machines, browser tabs, kernel memory, and even Trusted Execution Environments, making it clear that side-channels present a formidable challenge to safely multiplexing hardware.

This thesis explores these side-channel attacks at the intersection of software, hardware, and applied cryptography. By leveraging shared microarchitectural components, memory integrity vulnerabilities, and even physical effects, this thesis demonstrates new classes of attacks that extract information through these indirect channels. In doing so, it expands our understanding of the scope of side-channel vulnerabilities by demonstrating novel channels by which software-level attackers can abuse vulnerabilities present in hardware.

More specifically, this thesis investigates the threat of side-channels to secure execution environments (e.g. Intel's SGX), cryptographic schemes (both standardized by NIST and candidates for future post quantum crypto schemes), web browsers, micro architectural systems, and hardware, such as memory modules and storage devices.

By surveying the landscape of potential side-channel threats and discovering new classes of attacks, this thesis contributes novel insights into adversarial capabilities and how to develop effective mitigations. Thus, the works contained in this thesis serve as necessary stepping stones towards securing the next generation of computers against these side-channel attacks in a principled manner.

CHAIR: Prof. Daniel Genkin and Prof. Alex Halderman