COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

DISSERTATION DEFENSE

Youssef Tobah

Exploring the Effects of Memory Vulnerabilities Across the Computer Architecture Stack

Monday, January 13, 2025
2:30pm – 4:30pm
3725 Beyster
Hybrid – Zoom Passcode: 598937

ABSTRACT: In the pursuit of more performant, power- and area-efficient systems, computers have been exposed to a plethora of security risks and vulnerabilities at various levels of the computer architecture stack. Oftentimes, the effects of a vulnerability at one level propagates into other levels, making it challenging to build defenses that encompass all the effects of a particular exploit. One such vulnerability, known as Rowhammer, allows attackers to flip bits in memory without ever accessing them by rapidly accessing adjacent addresses. Since its discovery, researchers have shown how bit-flips in memory can propagate through a victim's machine to form the basis for numerous exploits, including leaking cryptographic keys, denial of service, and privilege escalation.

This thesis explores Rowhammer at various levels of the computer architecture stack. Rowhammer attacks typically require an understanding of multiple components of the stack, including memory, architecture, and operating systems, in addition to other potential systems depending on the target. This thesis contributes to knowledge in the space at multiple levels, further demonstrating the threat Rowhammer poses beyond prior work.

More specifically, this thesis presents techniques for reverse engineering a memory controller's address mapping, how Rowhammer can be combined with microarchitectural exploits, the threat Rowhammer poses to particular software patterns, and lastly, an exploration of the efficiency of end-to-end Rowhammer attacks.

By studying Rowhammer as a systems problem involving multiple layers of the computer architecture stack, my goal is to demonstrate the need for defenses that solve the Rowhammer issue at its root.

CHAIR: Prof. Kang G. Shin