COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

DISSERTATION DEFENSE

Kevin Loughlin

Mitigating Microarchitectural Vulnerabilities to Improve Cloud Security and Reliability

Thursday, August 3, 2023
10:00am – 12:00pm
3725 Beyster
Hybrid – Zoom Passcode:257089

ABSTRACT: Cloud providers must isolate each execution context—e.g., a virtual machine (VM)—atop shared hardware. Unfortunately, commodity hardware only strongly enforces context isolation at the architectural level, failing to enforce isolation in the microarchitectural implementation of hardware. The lack of microarchitectural isolation yields a wide range of threats to system security and reliability, including denial-of-service, data loss, data leakage, and even system subversion.

Accordingly, this dissertation presents mitigations for two of the most prominent classes of modern microarchitectural vulnerabilities: transient execution attacks on CPUs---which allow arbitrary data to be leaked from processors via mis-speculation and timing side channels---and Rowhammer---which corrupts and potentially leaks data in DRAM via memory access patterns that produce silicon-level disturbance effects.
In particular, *DOLMA* provides the first hardware mitigation against all demonstrated transient execution attacks at the time of publication. *Stop! Hammer Time* presents hardware primitives upon which scalable and flexible software defenses can be built across the taxonomy of Rowhammer migrations. *MOESI-prime* introduces coherence-induced hammering, the first form of hammering shown to occur in non-malicious code, and provides a corresponding coherence protocol-based mitigation. Finally, *Siloz* isolates different VMs to private DRAM subarray groups (across which Rowhammer attacks are ineffective), thereby preventing inter-VM Rowhammer bit flips.

CHAIR: Prof. Baris Kasikci