CECS
CENTER FOR EMBEDDED & CYBER-PHYSICAL SYSTEMS
UNIVERSITY OF CALIFORNIA · IRVINE

CECS Seminar



"Security in Heterogeneous Systems"

Yicheng Zhang

Ph.D. candidate of
University of California, Riverside

Monday, April21st
11:00 a.m.-12:00 p.m.
Location: EH 2430

Abstract:

To improve the performance and efficiency of modern computing systems, architects increasingly adopt heterogeneous designs that tightly integrate specialized accelerators such as GPUs and FPGAs. These accelerators enable substantial speedups for compute-intensive workloads like machine learning and AR/VR. However, they also diverge fundamentally from traditional CPU-based systems and introduce a new class of security risks. Unlike prior work that focused on CPU vulnerabilities such as Spectre and Meltdown, heterogeneous systems expose new attack surfaces due to their architectural complexity and shared resource usage. In this talk, I will present my research efforts to uncover and mitigate security vulnerabilities in these heterogeneous platforms. First, I will introduce a set of side-channel attacks targeting AR/VR devices, leveraging rendering performance counters to recover sensitive user inputs such as virtual keystrokes and voice commands. I will then shift to large-scale cloud environments, where I demonstrate the first end-to-end side-channel attack that exploits NVLink, NVIDIA's high-speed GPU interconnect, through contention-based and performance-counter-based microarchitectural channels. To conclude, I will present a defense framework that uses GPU side-channel signatures to validate kernel execution integrity. This approach detects tampering from attacks like buffer overflows and Rowhammer, turning side channels into a practical tool for runtime verification. Together, these efforts lay the groundwork for securing future heterogeneous computing platforms across both edge and cloud environments.

Biography:

Yicheng Zhang is a fourth-year Ph.D. candidate at the University of California, Riverside, advised by Prof. Nael Abu-Ghazaleh. Prior to that, he received his M.Sc. from UC Irvine and his B.S. from Sichuan University. His research interests lie in computer architecture and system security, with a focus on AR/VR security and microarchitectural security. His work has been recognized by top-tier conferences and journals including multiple USENIX Security, IEEE S&P, IEEE DSN and IEEE TIFS. More information can be found at his website: https://yichez.site/

Hosted By: Prof. Zhou Li