PURDUE UNIVERSITY | Elmore Family School of Electrical and Computer Engineering

Faculty Candidate Seminar -- Purdue Computes: Systems-Hardware

Zirui "Neil" Zhao

Ph.D. Candidate, Computer Science Dept.
University of Illinois, Champaign-Urbana

Thursday, March 28, 2024
10:30 A.M. – 11:30 A.M.
BHEE 317

Modern Clouds: Side-Channel Attacks and Defenses

Abstract

Cloud computing, which has seen significant growth over the past decade, fundamentally relies on the sharing of hardware resources among users. This approach enhances resource utilization and reduces operational costs. However, it also enables unintended information leakage through microarchitectural side channels. Despite the threat of side-channel attacks, cloud vendors remain skeptical about the practicality of these attacks in production cloud environments, leading to inadequate side-channel mitigations.

My PhD research focuses on exploring side-channel attacks in realistic cloud settings and developing comprehensive defenses across the computing stack. In this talk, I will first introduce a series of novel attack techniques that address practical challenges in conducting side-channel attacks in public clouds. Using these techniques, I demonstrated an end-to-end, cross-tenant side-channel attack on Google Cloud. This demonstration was subsequently recognized by Google as a critical-level bug, prompting a review by their product team. In the second part of this talk, I will introduce Untangle, a novel framework for side-channel defense. Untangle is designed to quantify and reduce information leakage in defense schemes based on dynamic resource-partitioning. Untangle opens up a defense paradigm that allows a controlled amount of information leakage in exchange for improved performance. To conclude, I will outline future research directions aimed at developing secure and efficient cloud systems resistant to side-channel attacks.

Bio

Zirui Neil Zhao is a PhD candidate in Computer Science at the University of Illinois Urbana-Champaign (UIUC), advised by Prof. Josep Torrellas. His research is primarily focused on computer architecture, system security, and cloud computing, with a special interest in understanding and mitigating side-channel threats in modern computer systems like clouds. His work has been published in top-tier conferences in the fields of computer architecture and security. He received the W. J. Poppelbaum Memorial Award for creativity in computer architecture design from the CS department of UIUC in 2023. For more information about his work and achievements, please visit https://neilzhao.me.

ECE Host: T.N. Vijaykumar ~ vijay@purdue.edu