Department of Electrical Engineering
香港城市大學
City University of Hong Kong

CityU Architecture Lab for Arithmetic and Security (CALAS) Seminar Series

Enhancing Processor Fuzzing via Hardware and Software Collaboration

Jinyan Xu, Ph.D. candidate
Zhejiang University, China

Abstract:

Modern processors are increasingly complex, making effective bug detection a persistent challenge. My work explores how hardware and software collaboration can enhance processor fuzzing to uncover both architectural and microarchitectural vulnerabilities. In this talk, I will present two efforts that together discovered over 20 previously unknown bugs, including multiple CVEs. MorFuzz improves architectural fuzzing by using runtime-guided mutation and state synchronization across designs, while DejaVuzz targets transient execution vulnerabilities with novel primitives for address space isolation and dynamic taint tracking. These techniques significantly improve coverage and reveal deep bugs in widely used RISC-V processors.

Biography:

Jinyan Xu is a Ph.D. candidate in Computer Science at Zhejiang University, advised by Prof. Yajin Zhou. His research focuses on developing novel verification techniques to ensure hardware correctness and security, with publications in computer architecture and security venues, including USENIX Security, DAC, and AsiaSys.

12 May 2025 (Mon); 9am - 11am HKT; LT-4; https://cityu.zoom.us/j/96742093029