DEPARTMENT OF
COMPUTER SCIENCE

TEXAS TECH
Whitacre College of Engineering

Cloud System Security: From Cloud Orchestration to Hardware Attacks

Chongzhou Fang
University of California, Davis
Friday, February 28, 2025
10:00 a.m.
EC 205

Abstract: In recent decades, cloud computing has profoundly changed our lives, providing the foundational infrastructure that supports countless applications. However, these shared environments are vulnerable to various hardware-based attacks, including microarchitectural side-channel attacks initiated by malicious users. Such exploitable vulnerabilities can be found across the entire cloud hierarchy, from resource orchestration software to the underlying heterogeneous hardware.

In this presentation, I will discuss my recent discoveries of vulnerabilities in modern cloud systems, examining how these security issues can be identified, evaluated, and mitigated. I will also outline my vision for building secure computing environments in an era of increasingly diverse AI applications and flexible computing resources.

Bio: Chongzhou Fang is a final-year Ph.D. candidate at the University of California, Davis. He received his B.Eng. degree in information science from Southeast University, China, and joined UC Davis in 2020. His research interests lie in the broad field of system security, including cloud scheduler security, side-channel attack and defense in heterogeneous computing environments, and the application of emerging AI technologies in system security. He has published peer-reviewed papers at security and hardware venues such as Usenix Security, ACM CCS, NDSS, and DAC, and he received an award at the CSAW Applied Research Competition for his work in cloud FPGA security.