DEPARTMENT OF COMPUTER SCIENCE
TEXAS TECH
Whitacre College of Engineering

Secure and Timely Execution in Cyber-physical Systems

Jinwen Wang
Washington University in St. Louis
Friday, February 21, 2025
10:00 a.m.
IMSE 121

Abstract: Cyber-physical systems (CPSs), such as self-driving cars, are integral to modern life. Execution timing is critical to CPS, as missing a deadline can result in severe outcomes. In this talk, I will present my work on guaranteeing execution timing in CPS security. I will first introduce a real-time trusted execution environment (TEE) to defend against OS-level attackers capable of launching denial-of-service attacks on safety-critical functions. This approach bridges the gap between the existing commercial TEE deployment paradigm, which focuses solely on confidentiality and integrity, and CPSs, which require additional availability. I will then describe a mission execution integrity attestation system that verifies the real-time mission execution integrity of CPSs without compromising their timely execution requirements, bridging the gap between existing remote attestation solutions and the execution timing demands of CPSs. Finally, I will outline future directions for securing heterogeneous CPSs, involving emerging hardware and software architectures, such as accelerators and virtualization.

Bio: Jinwen Wang is a final-year Ph.D. candidate in the Department of Computer Science and Engineering at Washington University in St. Louis, advised by Prof. Ning Zhang. He received his master's degree in computer science from Tsinghua University. His research interests lie in system and software security in cyber-physical systems across diverse architectures, including CPU and GPU.