DEPARTMENT OF COMPUTER SCIENCE

TEXAS TECH
Whitacre College of Engineering

From Autonomous Vehicles to IoT: Cybersecurity Risks and Defense Strategies for Emerging Technologies

Wei Wang, Ph.D.
Saint Louis University
Monday, March 3, 2025
1:30 p.m.
Livermore 104

Abstract: Autonomous driving systems (ADS) and Internet-of-Things (IoT) are revolutionizing transportation, smart cities, and critical infrastructure by enabling greater automation, efficiency, and connectivity. However, their increasing reliance on complex software and intricate communication protocols introduces significant cybersecurity risks. My research addresses two critical challenges: exploiting and securing Simultaneous Localization and Mapping (SLAM) systems in autonomous vehicles and robotic platforms, and enabling secure, seamless collaboration among heterogeneous IoT devices.

In this talk, I will first present an adversarial attack on SLAM systems, demonstrating how small, carefully crafted perturbations can mislead autonomous navigation and compromise ADS reliability. I will then introduce a lightweight defense mechanism to enhance the robustness of SLAM in real-world scenarios. In the second part, I will discuss a novel key extraction protocol to allow secure and reliable asymmetric communication between heterogeneous IoT devices. I will conclude by highlighting open research challenges in securing emerging autonomous and IoT systems and outlining my future research directions to build more resilient cyber-physical infrastructure.

Bio: Dr. Wei Wang is an Assistant Professor in the Department of Computer Science at Saint Louis University. His research focuses on Cyber-Physical Systems (CPS), including Cybersecurity, Autonomous Driving, IoT, and Wireless Networking. His work spans the full lifecycle of CPS, from theoretical analysis and system modeling to hardware/software design, implementation, experimental simulation, and real-world evaluation. His group has published many papers in premier conferences and journals, including CCS, USENIX Security, NSDI, SIGCOMM, SenSys, ICNP, INFOCOM, TON and TOSN. His work is currently supported by the National Science Foundation (NSF) CRII Award. More information about his research group and publication record is available at https://www.wei-wang-research.com.