THE CENTER FOR ADVANCED COMPUTER STUDIES

at

the University of Louisiana at Lafayette

Lafayette, Louisiana

Proudly announces a presentation

Dr. Qi (Alfred) Chen

Assistant Professor
Department of Computer Science
University of California, Irvine

will give a presentation entitled

Towards Secure and Robust AI Stack in Emerging Autonomous Cyber-Physical System

****

Abstract: Autonomous CPS (Cyber-Physical System) systems consist of both cyber and physical components working jointly to achieve highly automated operations in the physical world. Notable examples of such systems include Autonomous Driving (AD) vehicles and delivery drones/robots, which are increasingly deployed and commercialized in the real world. Specifically, AD technology has always been an international pursuit due to its significant benefit in driving safety, efficiency, and mobility. Over 15 years after the first DARPA Grand Challenge, its development and deployment are becoming increasingly mature and practical, with some AD vehicles already providing commercial services on public roads (e.g., Google Waymo in Phoenix and Baidu Apollo in China). In AD technology, the AI stack is highly security-critical: it is in charge of safety-critical driving decisions such as collision avoidance and lane-keeping, and thus any security problems in it can directly impact road safety. In this talk, I will describe my recent research that initiates the first systematic effort towards understanding and addressing the security problems in industry-grade AD AI stack. I will be focusing on two critical modules: perception and localization, and talk about how we are able to discover novel and practical sensor/physical-world attacks that can cause end-to-end safety impacts such as crashing into obstacles or driving off-road. I will also briefly talk about my recent research on AI stack security in smart transportation in general, especially those enabled by Connected Vehicle (CV) technology. I will conclude with a discussion on defense and future research directions.

DATE: FRIDAY, SEPTEMBER 10, 2021

TIME: 11:00 A.M – 12:00 NOON

LOCATION: Via Zoom

Biography: Qi Alfred Chen is an Assistant Professor in the Department of Computer Science at the University of California, Irvine. His research interest spans software and AI security, systems security, and network security. Currently, his research focuses on security problems at the AI and software stacks in autonomous CPS and IoT systems (e.g., autonomous driving and intelligent transportation). His works have high impacts in both academic and industry with over 30 research papers in top-tier venues in security, mobile systems, transportation, software engineering, and machine learning; a nationwide USDHS US-CERT alert, and multiple CVEs; over 50 news articles by major news media such as Forbes, Fortune, and BBC News; and vulnerability report acknowledgments from USDOT, Apple, Microsoft, Comcast, Daimler, etc. Recently, his research triggered over 25 autonomous driving companies to start security vulnerability investigations; some confirmed to work on fixes. He serves as reviewers for various top-tier venues such as Usenix Security, ACM CCS, NDSS, TIFS, TDSC, T-ITS, etc., and co-found the AutoSec workshop (co-located with NDSS'21). He received various awards such as NSF CRII Award, NDSS'19 and NDSS'20 best poster awards, UCI Chancellor's Award for mentoring, and UMich university-wide Distinguished Dissertation Award. His group won the champion (1st place) in the world's first AutoDriving Security CTF organized by Baidu Security in 2020. Chen received his Ph.D. from the University of Michigan in 2018.

Zoom Meeting: https://ullafayette.zoom.us/j/92747376335