

Qi Alfred Chen

alfchen@uci.edu

<https://www.ics.uci.edu/~alfchen/>

Title: Ghost Cars and Fake Obstacles: Autonomy Software Security in Emerging Autonomous Driving and Smart Transportation Systems

Abstract: Transportation systems today will soon be transformed profoundly due to two recent technology advances: Connected Vehicle (CV) and Autonomous Vehicle (AV). Such transformation leads to the creation of a series of next-generation transportation systems such as smart traffic lights and self-driving cars, but it may also introduce new security problems and challenges. In this talk, I will describe my current research that initiates the first effort towards systematically understanding the security of the autonomy software in CV and AV systems. I will first describe my work that performs the first security analysis of the next-generation CV-based traffic signal control, which discovers new vulnerabilities at the traffic control algorithm level that can cause massive traffic jams. Next, I will describe my work that performs the first security analysis of LiDAR-based object detection in AV systems. I will conclude by discussing defense directions, and also future research directions in securing emerging CV/AV systems.