COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

DISSERTATION DEFENSE

Shengtuo Hu

Securing Connected and Automated Vehicle through Proactive Vulnerability Analysis and Security Enhancement

Thursday, September 1, 2022
9:00 – 11:00am
Virtual – Zoom
Passcode: 786498

ABSTRACT: The rapidly evolving Connected and Autonomous Vehicle (CAV) technology brings new security challenges to vehicular systems, because newly introduced communication and system components inevitably increase the attack surface of vehicles if being abused, leading to potential safety hazards on the road. For example, the emerging Connected Vehicle (CV) technology, which enables vehicles to exchange safety and mobility information wirelessly (e.g., location and speed) with traffic infrastructure and other vehicles, opens a door for spoofing attacks. On the other hand, the development of Autonomous Vehicle (AV) results in the increasing data transfer needs of various sensors (e.g., cameras, LiDAR), which stimulates the adoption of Automotive Ethernet, the next-generation in-vehicle network. However, no common standard has been established for the security protocol of the in-vehicle Ethernet network. Therefore, it is highly desirable to systematically understand vulnerabilities in the current CAV systems and the corresponding security/safety consequences so that these flaws can be proactively discovered and addressed before large-scale deployment.

To achieve this goal, in this dissertation, we demonstrate that rigorous techniques, such as formal methods, program analysis, and trusted execution environment (TEE), can be used for proactive vulnerability discovery and security enhancement in the safety-critical CAV system. At the design level, we leverage formal methods to uncover design flaws and ensure the security guarantee of the proposed defense. To study the emerging CV network interface, we propose a model-checking-based approach, CVAnalyzer, that harnesses the attack discovery capability of the general model checker and the quantitative threat assessment of the probabilistic model checker to automate the analysis. For the in-vehicle Ethernet security, we present Gatekeeper, a gateway-based source authentication protocol. Except for the source authentication property, we then verify that Gatekeeper can defend against the spoofing attack and alleviate the impact of the DoS attack. At the implementation level, we employ both static and dynamic program analysis. To defend against the spoofing attack, we build a TEE-based defense system, CVShield, to protect the integrity of the sensor data reading and processing pipeline. To uncover semantic vulnerabilities in the CAV system, we prototype CAVFuzzer that incorporates a novel object-level mutator and utilizes the data-flow feedback to guide the fuzzing process.

CHAIR: Prof. Z. Morley Mao