COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

DISSERTATION DEFENSE

Mert Pesé

Bringing Practical Security to Vehicles

Friday, August 5, 2022
12:00 – 2:00pm
Virtual Event
Zoom

ABSTRACT: Modern vehicles are getting increasingly connected. Together with more automotive electronics and wireless interfaces, the number of possible attack surfaces goes up, raising security concerns. Although attacks vary, all of them have one component in common, namely *CAN bus injection*. The CAN bus is used inside the in-vehicle network to interconnect automotive controllers. An attacker who compromises the CAN bus can inject arbitrary CAN messages to it, making the vehicle *misbehave*. Unfortunately, automotive manufacturers (OEMs) have been reluctant to adopt any proposed countermeasure to secure CAN, mainly because (i) CAN injection requires the knowledge of OEM-proprietary semantics which differs from vehicle to vehicle, as well as due to (ii) industry-specific functional and cost constraints which have not been reflected in existing solutions.

In this thesis, I address these two points by first showing that proprietary semantics can be automatically reverse-engineered, effectively removing the barrier for CAN injection attacks. I demonstrated this by developing **LibreCAN** which can quickly and accurately reverse engineer both powertrain- and body-related information. Second, to meet the industry-specific constraints, I propose **S2-CAN** and **MichiCAN**. The former adds *confidentiality*, *authenticity* and *integrity* to the CAN bus without the overhead of cryptography, but by leveraging protocol-specific properties. The latter protects the CAN bus against attacks on its *availability* by leveraging novel hardware features of automotive controllers. The main difference to existing work is the solutions' practicality. Instead of adapting well-known cryptographic techniques from the realm of computer networks which do not satisfy aforementioned cost and functional constraints, I propose out-of-the-box solutions that leverage protocol- and hardware-based peculiarities of automotive networks and controllers. Furthermore, both solutions are fully backward-compatible with existing hardware and specifications, as well as add minimal overhead to computational resources and network metrics. Finally, I extend my contributions of practical security solutions to the area of vehicle-to-vehicle (V2V) communication. I propose **CARdea**, a two-phase anomaly detection system that sanitizes incoming data from surrounding vehicles. CARdea combines an in-vehicle light-weight anomaly detection phase with a more resource-heavy machine-learning phase that can be executed on the vehicle, edge or cloud based on available computational resources and manufacturer constraints.

CHAIR: Prof. Kang Shin